frontiers | Frontiers in Marine Science

TYPE Policy and Practice Reviews
PUBLISHED 29 August 2025
DOI 10.3389/fmars.2025.1616906

OPEN ACCESS

EDITED BY
Maohan Liang,
National University of Singapore, Singapore

REVIEWED BY
Peng Cui,
Nanjing Forestry University, China
Wenwen Li,
Shanghai Maritime University, China

*CORRESPONDENCE
Shibo Li
sbli@shmtu.edu.cn

†These authors have contributed equally to this work and share first authorship

RECEIVED 23 April 2025
ACCEPTED 19 August 2025
PUBLISHED 29 August 2025

CITATION
Jin Y, Feng Y, Liu C and Li S (2025) Navigating the digital seas: Legal challenges and global governance of maritime cyber operations. *Front. Mar. Sci.* 12:1616906. doi: 10.3389/fmars.2025.1616906

Navigating the digital seas: Legal challenges and global governance of maritime cyber operations

Yongming Jin[1,2†], Yuan Feng[1,2†], Chaomin Liu[3†] and Shibo Li[3*]

[1]School of International Affairs and Public Administration, Ocean University of China, Qingdao, China, [2]Institute of Marine Development, Ocean University of China, Qingdao, China, [3]School of Law, Ocean University of China, Qingdao, China

Rapid digitization of the maritime sector has heightened its exposure to cyber threats, calling for a reexamination of international legal frameworks. This study examines how the United Nations Convention on the Law of the Sea (UNCLOS) could be adapted or supplemented to govern emerging Maritime Cyber Operations (MCOs) more effectively. Using a multi-level governance perspective that integrates legal analysis and case studies, we identify critical gaps in UNCLOS and related maritime law. UNCLOS currently struggles with unresolved jurisdictional ambiguities across territorial seas, exclusive economic zones (EEZs), and the high seas. There is also persistent uncertainty about whether cyberattacks qualify as 'uses of force' under international law, and existing enforcement mechanisms are ill-equipped to address cyber operations by state or non-state actors. Although soft-law efforts like the Tallinn Manual 2.0 provide helpful interpretative guidance, they lack binding authority and broad consensus. Additionally, ongoing technical vulnerabilities in crucial maritime infrastructure—from port automation systems to undersea communication cables—further compound these governance challenges. To confront these issues, this paper proposes an integrated multi-level governance approach. It recommends updating UNCLOS (potentially via a supplementary protocol), adopting industry-wide cybersecurity standards, and strengthening both regional and international cooperation. By bridging the legal and technical aspects of maritime cybersecurity, the study offers policymakers a structured set of practical strategies. This framework is intended to lay a foundation for future policy that addresses urgent maritime security needs while preserving the efficiency of global maritime commerce in an increasingly digital world.

KEYWORDS

maritime cyber operations, cybersecurity, maritime security, Tallinn Manual, law of the sea, UNCLOS

1 Introduction

The maritime domain has been profoundly transformed by digital technology (Liu and Feng, 2025). Currently, over 95% of transoceanic data relies on fiber-optic submarine cables, making them critical infrastructure for global communication and national security (Bueger and Liebetrau, 2021; Matis, 2012). As shipping, port logistics, and navigation systems become increasingly networked and reliant on digital systems, oceanic spaces have become vulnerable to "maritime cyber threats" — a spectrum of malicious activities targeting maritime digital systems (Newberry, 2014). This paper focuses specifically on Maritime Cyber Operations (MCOs), defined as offensive or defensive cyber activities aimed at disrupting, interfering with, or manipulating critical maritime infrastructure—such as vessels, ports, and submarine cables — or their associated data systems. A Maritime Cyberattack is an offensive MCO, typically intended to cause damage, disruption, or unauthorized access. Recent events illustrate this vulnerability: in 2017, the shipping giant Maersk suffered the NotPetya malware attack, incurring losses of up to $300 million and halting operations at dozens of ports worldwide (Warwick, 2017; Caprolu et al., 2020); in 2020, the International Maritime Organization (IMO) headquarters networks were breached, disrupting its operations (Diaz, 2020).

These maritime cyberattacks expose the structural limitations of UNCLOS in addressing digital challenges (Kim, 2024). Drafted in an era without anticipation of today's physical–digital convergence, UNCLOS now leaves maritime domains exposed to risks such as remote manipulation, data theft, and systemic disruption (Ross, 2014). UNCLOS Article 113 exemplifies this gap—it prohibits the physical destruction or injury of submarine cables but remains silent on cyber threats that compromise cable integrity or data flow without physical intervention. Likewise, UNCLOS mandates that vessels on the high seas are subject to exclusive flag-state jurisdiction (Article 92), which can leave coastal states with insufficient legal basis to act against hackers on foreign-flagged ships operating offshore, even if those activities impact the coastal state (Kraska, 2011; Roach, 2021). The result is jurisdictional ambiguity – especially in EEZs and other areas beyond territorial waters – regarding which state's laws apply and who may enforce them. These ambiguities span prescriptive jurisdiction (which state's law can regulate a given cyber activity), enforcement jurisdiction (which state can interdict or punish offenders), and adjudicative jurisdiction (which judicial forum, if any, can resolve disputes). The international response to these evolving threats remains inadequate (Morel, 2016; Todorov, 2021). As of early 2025, no UNCLOS amendment or protocol specifically addresses cyber threats at sea, and the gap between fast-evolving threats and dated legal frameworks continues to widen.

Addressing maritime cyberattacks within existing legal frameworks is now a pressing issue in international security governance. Traditional maritime security studies have focused primarily on physical threats, creating a research gap regarding cyber challenges (Lymperopoulos, 2024). While the international community has made progress through initiatives like the Tallinn Manual 2.0, significant legal and enforcement obstacles persist in maritime contexts (Petrig, 2020). This jurisdictional ambiguity is particularly problematic.

This study analyzes Maritime Cyber Operations — their threat profiles and their impact on maritime law, advocating for a robust maritime cybersecurity governance mechanism through international cooperation. Our research objective is to investigate how UNCLOS and related maritime law can be interpreted, adapted, or reformed to better govern MCOs. We approach this by examining emblematic cyber incidents at sea, analyzing applicable UNCLOS provisions (and their limitations), and surveying multi-level governance responses. By identifying where international law fails to mitigate cyber risks in the maritime domain, we aim to formulate both short-term and long-term solutions.

We adopt a typological case-study approach within a multi-level governance framework to structure our analysis. Section 2 develops a conceptual classification of MCOs and illustrates each category with real-world examples such as the NotPetya malware attack, GPS spoofing incidents, and submarine cable sabotage. In Section 3, we examine how existing international law—particularly UNCLOS—applies to these scenarios, revealing normative tensions (for example, whether a cyberattack qualifies as a "use of force" or violates "innocent passage") and practical enforcement gaps (such as the legal inability to interdict a vessel engaged in cyber piracy). Section 4 then surveys current governance efforts, from United Nations discussions to regional initiatives, and proposes a coordinated multi-level governance model (global, regional, and national) to fill those gaps. Throughout this inquiry, we draw on expert commentary (including the Tallinn Manual 2.0) and integrate legal analysis with cybersecurity insights, striving for an interdisciplinary understanding of the challenges and potential solutions.

By bringing together principles of maritime law, cyber law, and public policy, our study offers one of the first in-depth explorations of "maritime cybersecurity governance." We clarify the key terminology and legal scope of this emerging field, differentiate the various categories of maritime cyber threats, and link those threats to the corresponding provisions of UNCLOS. We also outline concrete measures to bolster resilience against cyberattacks at sea — ranging from interpretative clarifications of UNCLOS to the adoption of voluntary industry standards. Our overarching aim is to provide policymakers and negotiators with guidance to close critical governance gaps proactively, rather than waiting for a serious maritime cyber incident to compel action.

2 Understanding maritime cyber operations

The maritime domain — long bounded by physical geography — now extends into cyberspace, exposing critical infrastructure and economic stability to new digital threats. In this section, we outline the landscape of Maritime Cyber Operations, examining their

scope, typologies, and real-world manifestations as a foundation for the legal and governance analysis that follows.

2.1 Conceptual definition and uniqueness

We define Maritime Cyber Operations as any offensive or defensive cyber activities targeting maritime assets and infrastructure – such as vessels, ports, offshore platforms, and undersea communication systems – or their associated digital networks. These operations range from network intrusions and malware attacks disrupting shipping logistics, to electronic spoofing of navigation signals, to defensive cyber measures protecting ships at sea. For clarity, this paper uses "Maritime Cyberattack" to denote malicious offensive MCOs intended to cause harm or disruption (e.g., deploying malware to cripple a port's systems). The broader term "Maritime Cyber Operation" encompasses any cyber activity (including espionage or preparatory intrusions) that may not rise to the level of a destructive attack. We refer to "Maritime Cyber Threats" when discussing latent risks or capabilities that could materialize as attacks. While these terms overlap in practice, maintaining these distinctions is helpful when mapping them to legal frameworks, as, for example, only some hostile MCOs might qualify as an unlawful "attack" under international law. The unique, cross-domain nature of MCOs, involving diverse actors and producing tangible consequences from virtual attacks, is illustrated in Figure 1.

2.1.1 Cross-domain effects

Virtual cyberattacks in the maritime domain can produce tangible physical consequences with significant real-world implications. The 2017 NotPetya attack illustrates this cross-domain impact, as it compromised Maersk's logistics management system, halting operations at over 80 ports worldwide and incurring economic losses exceeding $300 million (Warwick, 2017; Caprolu et al., 2020). This incident demonstrated not only the technical vulnerabilities inherent in maritime shipping systems but also revealed how cyberattacks can generate substantial spillover effects throughout the physical economy and global supply chains.

2.1.2 Jurisdictional complexity

MCOs present unique legal challenges as their sources, targets, and impacts often span multiple national jurisdictions, potentially involving territorial waters, Exclusive Economic Zones (EEZs), or the high seas simultaneously. This multi-jurisdictional nature creates substantial conflicts in legal applicability and enforcement jurisdiction. For example, a single cyber incident might entail a Liberian-flagged vessel operating on the high seas experiencing a cyberattack originating from servers in Eastern Europe that affects an Asian-based parent company. Determining the appropriate judicial and enforcement jurisdiction for investigation and enforcement becomes exceptionally challenging under existing international legal frameworks. National legal systems and UNCLOS provisions were not designed to handle operations that transcend maritime zones and legal regimes in this way.

2.1.3 Diversity of actors

The threat landscape for MCOs extends beyond military or state actors to include terrorist organizations, transnational criminal syndicates (e.g., drug traffickers using cyber means to disable coast guard sensors), pirate networks, hacktivist groups, and private-sector entities (whether victims or inadvertent conduits). These diverse actors may target maritime assets to achieve various objectives ranging from political pressure and economic extortion to strategic deterrence. The maritime sector's increasing integration of artificial intelligence (AI), big data analytics, and Internet of Things (IoT) technologies has further elevated the technical complexity of MCOs and expanded their potential threat vectors, making attack attribution increasingly difficult and complicating response efforts. International law's distinction between state and non-state actors becomes blurred in cyberspace, making it harder to apply concepts like state responsibility or "armed attack" thresholds.

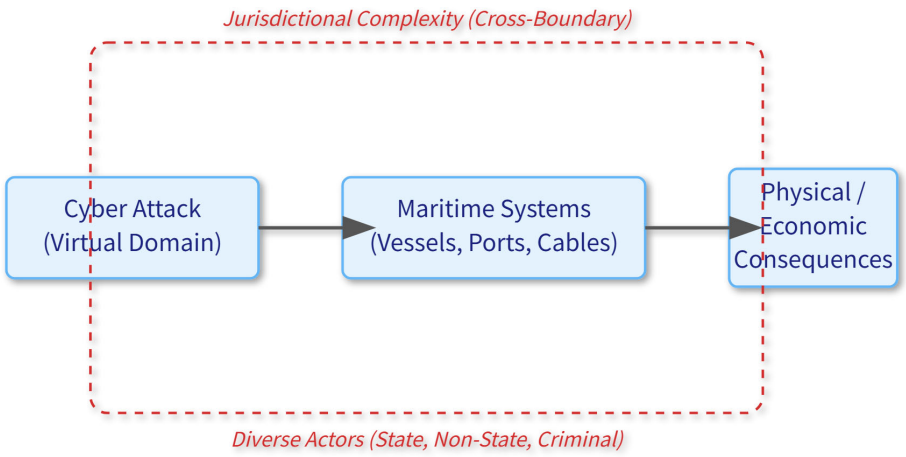

FIGURE 1
Conceptual diagram of MCO uniqueness.

2.2 Typological analysis

Having defined the concept of MCOs, we next categorize them by their technical methods and strategic purposes. Viewed by target and actor characteristics, MCOs can be classified into five broad types (Ducheine and Pijpers, 2021), as summarized in Table 1. These categories are not rigid or mutually exclusive — a state-sponsored espionage campaign, for example, may include defensive measures to protect that state's own vessels, just as a military-initiated cyber operation could provoke law enforcement action if it crosses into criminal conduct. We present each subtype alongside real-world examples to highlight its distinctive characteristics and challenges.

2.2.1 Cyber governance

Cyber governance encompasses the collaborative process through which governments, international organizations, and private sector entities develop, implement, and enforce cybersecurity rules and standards (Ducheine and Pijpers, 2021). In the maritime domain, governance objectives primarily focus on safeguarding critical elements of maritime infrastructure including shipping systems, submarine cable networks, and offshore facilities (Dimakopoulou and Rantos, 2024). This involves establishing frameworks for risk management, incident reporting, and compliance verification, often drawing on broader international cybersecurity norms while tailoring them to specific maritime operational contexts. On the defensive side, international organizations and industry groups have sought to improve governance. On the offensive side, state and non-state actors may conduct cyber operations to influence or disrupt governance, for example, by hacking the databases of regulatory bodies or exploiting the digitalization of governance processes (e-certificates, automatic identification systems, etc.) to create loopholes or advantages.

The International Maritime Organization has taken significant steps to strengthen maritime cybersecurity. A notable initiative includes the issuance of the Guidelines on Maritime Cyber Risk Management, which mandated that from January 2021 onwards, shipping companies incorporate cyber risk controls into their safety management systems under the International Safety Management (ISM) Code (Kanwal et al., 2024). These IMO guidelines – effectively a soft law instrument – represent an important advancement in formalizing cybersecurity practices across the maritime industry. Additionally, the IMO's guidelines actively encourage member states to develop national cybersecurity frameworks that align with internationally recognized standards such as NIST CSF 2.0, with appropriate adaptations for their respective shipping industries (Dimakopoulou and Rantos, 2024). One documented case of an attack on governance itself was the 2020 cyberattack on the International Maritime Organization – hackers took down the IMO's public website and internal systems for several days, delaying meetings and sowing confusion (Diaz, 2020).

However, the IMO guidelines remain advisory rather than binding, leading to inconsistent implementation across regions. Moreover, no comprehensive international convention or uniform standard addresses maritime cybersecurity, resulting in fragmented policies among states with varying technical capacities. In short, there is still no dedicated, enforceable global framework for maritime cybersecurity governance.

2.2.2 Cyber protection

Cyber protection encompasses comprehensive technical and organizational security measures designed to prevent, detect, and mitigate cyber attacks against maritime infrastructure and systems (Hutchins, 2020; Ducheine and Pijpers, 2021). This approach integrates multiple defensive layers including advanced cybersecurity firewalls, encrypted communications protocols, and real-time monitoring systems deployed across vessels, ports, and associated maritime facilities. These protective mechanisms serve to significantly reduce both the success probability and potential impact of hostile cyber operations targeting critical maritime assets. Effective cyber protection also involves proactive vulnerability assessments, regular security audits, robust incident response plans, network segmentation onboard ships, and continuous monitoring of shipboard and port IT/OT systems to ensure resilience against evolving threats.

The 2017 NotPetya attack against Maersk illustrates the transformative effect of significant cyber incidents on organizational security postures. The breach crippled Maersk's IT systems worldwide—forcing the company to halt operations across dozens of countries and reinstall software on 4,000 servers and 45,000 PCs (Cimpanu, 2018; Greenberg, 2019). In response, Maersk undertook a comprehensive upgrade of its global management system, implementing stronger defenses configured to counter advanced threats like ransomware and trojans. This incident-driven security transformation demonstrates how major cyber events often catalyze substantial improvements in maritime sector cybersecurity practices.

TABLE 1 Typology of maritime cyber operations.

Type	Objective	Example
Cyber Governance	Rule-Making and Compliance	IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3);
Cyber Protection	Defensive Technologies and Policies	Maersk's System Upgrade Post-NotPetya
Cyber Law Enforcement	Transnational Crime Prosecution	Jurisdictional Disputes in High Seas Cyberattacks; Use of Budapest Convention.
Intelligence & Counterintelligence	Data Theft and Countermeasures	Maritime GPS Spoofing Incidents
Military Cyber Operations	Strategic Deterrence and Combat Support	NATO Baltic Sea Cyber Defense Exercises

Despite these improvements, challenges persist. Many commercial ships continue to run outdated software, and crew cyber awareness training is inconsistent (Eichenhofer et al., 2020). Smaller ports and shipping companies often lack resources for state-of-the-art cybersecurity, making them attractive "weak links" for attackers (Heering, 2020; Chae et al., 2024).

2.2.3 Cyber law enforcement

Cyber law enforcement in maritime contexts involves the investigation and prosecution of cybercrimes that cross multiple international boundaries via the maritime domain. This category of operations addresses questions like: Who can legally intervene if a vessel is suspected of launching cyberattacks? How can evidence be collected from multiple jurisdictions? What laws apply to cybercrimes committed at sea? For example, a Liberian-flagged tanker navigating the high seas might suffer a cyberattack originating from servers in Europe that affects its parent company in Asia. Under current international legal frameworks, determining the appropriate jurisdiction to investigate and respond to such an incident is exceptionally challenging (Nguyen and Golman, 2021). Such operations require specialized forensic capabilities, international legal assistance treaties, and clear frameworks for attributing attacks to specific actors, all of which are currently underdeveloped for the maritime domain.

The legal framework for addressing these challenges remains inadequate. UNCLOS does not explicitly define or address "maritime cybercrime," creating a fundamental gap in international maritime law. Current enforcement practices therefore rely on alternative frameworks such as Article 32 of the Budapest Convention, which provides mechanisms for cross-border data access (Council of Europe, 2024; Shires, 2024). However, this solution has two major limitations:

First, the Budapest Convention suffers from limited global ratification, particularly across Asia and Africa, meaning many states cannot effectively utilize this framework for transnational enforcement actions (De Hert et al., 2018). Second, even where ratified, the Convention's cross-border evidence collection mechanisms remain contentious when they intersect with sovereignty principles, as many states express reluctance to permit foreign agencies direct access to data within their territories (Nguyen and Golman, 2021).

In traditional maritime enforcement, UNCLOS Article 92 establishes the principle of flag state jurisdiction, stipulating that vessels on the high seas are primarily subject to the laws of their registering state (Liao, 2021). However, this principle creates significant enforcement dilemmas in cybercrime scenarios:

When the attack's source state differs from the vessel's flag state, the flag state often lacks practical capacity to enforce effectively, while coastal states or the victim's state typically lack direct intervention authority under existing legal frameworks (Jin and Techera, 2021). Without a specific legal mechanism designed for maritime cybercrime, enforcement agencies must rely on broader instruments such as the UN Convention against Transnational Organized Crime (UNTOC) or INTERPOL mechanisms (Nguyen and Golman, 2021). These conventions, however, lack the specificity needed for maritime cybercrime, resulting in increased enforcement costs and reduced operational effectiveness.

To address these legal gaps, several scholars have proposed developing either a supplementary protocol to UNCLOS or establishing an entirely new international convention specifically designed to create clear enforcement and evidence-gathering mechanisms for maritime cybercrime (De Hert et al., 2018). Such an instrument would enable states to form a unified legal framework addressing maritime enforcement and judicial jurisdiction, cross-border evidence collection, and international cooperation. This would significantly enhance enforcement efficiency while reducing the legal uncertainties that currently hinder effective response to maritime cyber threats (Shires, 2024).

2.2.4 Cyber intelligence & counterintelligence

Intelligence gathering and counterintelligence activities are critical covert components of cyber confrontations in the maritime domain, particularly among major powers and regional actors. For intelligence gathering, some states employ unmanned underwater vehicles (UUVs) or hacking techniques to intercept submarine cables, which carry 99% of transoceanic data and are vital national security assets (Bueger and Liebetrau, 2021). These activities represent a significant threat as submarine cables are essential infrastructure for global communications. Other states use electronic interference to target Global Navigation Satellite Systems (GNSS), such as GPS and GLONASS, aiming to disrupt adversaries' vessel or air force positioning, thereby affecting military operations and international trade (Clark, 2016). These operations often aim to gain strategic advantage, monitor adversaries, or acquire sensitive commercial or military information, operating in a legal grey area due to their covert nature and the difficulty of attribution. Peacetime espionage, for instance, is not clearly prohibited under international law (including UNCLOS), leaving these covert operations in a legal gray zone. Their hidden nature makes evidence collection difficult, and exposing such activities can quickly escalate diplomatic or military tensions.

In recent years, heightened risks to subsea infrastructure have spurred international attention to underwater surveillance and protection capabilities. For example, following the 2022 Nord Stream pipeline sabotage, states intensified security monitoring of submarine cables and energy infrastructure (McCabe and Flynn, 2024). This incident demonstrated the vulnerability of critical maritime infrastructure and the need for enhanced protective measures. However, the current international legal framework lacks clear definitions and regulations for such cyber intelligence and counterintelligence activities, complicating enforcement efforts and creating ambiguity in appropriate response mechanisms.

2.2.5 Military cyber operations

Military cyber operations occur when cyberattacks are directly linked to national military strategies, encompassing offensive electronic warfare, disruption of adversary command-and-control systems, and preemptive cyber strikes against key maritime targets (Tanodomdej, 2019). These operations represent a deliberate extension of conventional naval capabilities into the digital

domain, with potential real-world consequences for maritime security (Liu and Feng, 2025). Such operations can range from disrupting an adversary's naval communications during a conflict to degrading port infrastructure to hinder mobilization or logistical support, or hacking an autonomous drone swarm. According to the Tallinn Manual 2.0, if such actions reach a certain "armed attack" threshold (Rule 69, focusing on scale and effects comparable to kinetic attacks), they may trigger claims of individual or collective self-defense under international law (Efrony and Shany, 2018). This threshold determination has significant implications for how nations may legally respond to cyber aggression in maritime contexts. However, the international community has yet to reach a consensus on these matters, with differing national interpretations of what constitutes "cyber warfare" and "use of force" in the maritime environment (Spector, 2017). These interpretational differences create strategic ambiguity that both constrains and enables various forms of cyber operations at sea.

2.2.6 Legal challenges of the Tallinn Manual 2.0

Although the Tallinn Manual 2.0 provides an academic framework for applying existing international law to cyber operations, its Western-centric drafting process has sparked controversy over its interpretations of cyber warfare (Tanodomdej, 2019). This controversy stems primarily from the composition of its expert panel and their underlying assumptions about international norms. Some states argue that its thresholds for the use of force favor Western cyber warfare interests while overlooking the cybersecurity challenges faced by developing countries (Efrony and Shany, 2018). This criticism reflects broader geopolitical tensions in the development of international cyber norms. Furthermore, specific interpretations within the Manual, such as Rule 69 on "Use of Force," which considers the scale and effects of a cyber operation, and Rule 4 on "Violation of sovereignty," which addresses violations of sovereignty through cyber means not amounting to a use of force (e.g., intrusions causing effects on another state's territory), remain highly contested. The application of these rules to MCOs, such as determining whether disrupting a nation's shipping logistics via cyber means constitutes a use of force or a sovereignty violation, lacks universal agreement and presents significant interpretative challenges for the maritime domain. Rule 6, on due diligence to prevent harmful cyber operations from a state's territory, is another key but contested point relevant to flag state responsibilities. The Tallinn Manual's lack of binding legal force and its unresolved stance on the relationship between state sovereignty and cyber operations mean that states continue to rely on national policies and military strategies when conducting cyber military actions (Schmitt et al., 2017). This reliance on domestic frameworks often leads to inconsistent approaches and potential escalation risks in maritime cyber confrontations.

In the future, the international community may need to develop a more binding convention on cyber warfare to clarify the legality of military cyber operations and regulate state use of force in cyberspace, thereby preventing unnecessary conflict escalation and international security risks (Barnsby and Reeves, 2017). Such a convention would be particularly valuable for maritime cybersecurity, where the interconnected nature of global shipping and naval operations creates unique vulnerabilities and strategic challenges.

2.3 Typical cases and real-world challenges

Building on the typological distinctions, analyzing specific cases further illustrates the potential harms of MCOs and connects them to specific legal controversies under UNCLOS and general international law. The following subsections highlight several high-profile incidents from recent years, demonstrating the real-world implications of cyber vulnerabilities in maritime contexts.

2.3.1 The NotPetya attack (2017) – global shipping disruption and use of force ambiguity

In June 2017, the NotPetya malware attack struck multiple multinational companies around the world. Among the hardest hit was Maersk, the world's largest container shipping line (Warwick, 2017). Unidentified hackers deployed the NotPetya malware to target multiple multinational corporations, breaching Maersk's global logistics platform and halting operations at over 80 ports worldwide, with effects rippling across the global supply chain (Taddeo, 2019). This sophisticated cyber assault represented one of the most significant disruptions to maritime logistics in recent history. The attack not only caused direct losses—estimated at $300 million for Maersk—but also disrupted logistics systems, impacting the normal functioning of global trade for weeks afterward (Liu et al., 2018). These financial and operational impacts demonstrated the potential scale of damage from targeted maritime cyber operations.

This incident exposed the cybersecurity vulnerabilities of port automation systems and demonstrated how cyberattacks in the transnational maritime sector can produce significant spillover effects, affecting critical industries like finance, energy, and manufacturing (Kshetri, 2022). By crippling port logistics, the attack struck the very economic engine of global trade, as modern research shows that port throughput is a direct function of regional economic activity and investment (Guo et al., 2025). The cascading nature of these disruptions revealed the deeply interconnected nature of modern global commerce. Moreover, the NotPetya attack underscored that weak links in modern supply chain cybersecurity could be exploited by hacker groups or state actors, posing systemic risks beyond a single sector. The attack's sophisticated execution raised questions about attribution and appropriate response mechanisms under international law. Consequently, global shipping and logistics firms must bolster cybersecurity investments and develop robust defense strategies to mitigate the occurrence and spread of similar incidents (Simon and Omar, 2020). These protective measures have become essential components of maritime operational resilience in an increasingly digitized industry.

Legally, NotPetya was collateral damage from a broader cyber campaign (widely attributed to a state actor aiming at Ukrainian infrastructure), yet its impact on shipping was tantamount to a major

disruptive event traditionally covered by maritime law. A key controversy is whether such a cyber operation, if attributable to a state, constituted an unlawful "use of force" or armed attack against affected states. The damage was extensive, but there was no physical destruction of ships or port facilities. Under the Tallinn Manual 2.0's effects-based approach (Rule 69), some argue NotPetya's spillover could meet the use of force threshold. Others note the temporary nature and lack of physical property damage or loss of life might place it below this threshold. This ambiguity challenges UNCLOS Article 301 (peaceful uses of the seas) and the UN Charter's prohibition on the use of force. Furthermore, the incident highlighted gaps in flag state responsibility (UNCLOS Art. 94) if a vessel unwittingly spreads malware, and the lack of clear accountability mechanisms. The NotPetya attack starkly illustrates the limitations of existing legal frameworks and underscores the urgent need for global-level cooperation to establish norms for state behavior affecting maritime trade, and regional/national level measures for critical infrastructure protection.

2.3.2 GNSS spoofing incidents – navigational hazard and state responsibility

In recent years, an increasing number of cases involving tampered vessel position and heading data have exposed the security risks of Global Navigation Satellite Systems (GNSS). These vulnerabilities represent a critical concern for maritime safety and security worldwide. GNSS spoofing attacks falsify satellite signals, causing navigation systems to receive erroneous positional data, which can lead vessels to misjudge their locations or appear as "ghost ships" with anomalous routes in maritime management systems (Androjna et al., 2021). The significance of these attacks extends beyond simple navigation errors to potentially catastrophic consequences for maritime traffic management and safety.

For instance, in strategic waters like the Persian Gulf, Black Sea, and Eastern Mediterranean, multiple incidents of GNSS signal anomalies have caused significant positional deviations in vessel data, suspected to be linked to state-sponsored or non-state cyber warfare (Bai et al., 2024; Zorri and Kessler, 2024). In June 2017, over 20 commercial vessels in the Black Sea near Novorossiysk, Russia, reported their GPS positions as being inland at a nearby airport (Zorri and Kessler, 2024). These incidents frequently occur in geopolitically contested areas, suggesting deliberate interference rather than technical malfunctions. Additionally, GNSS spoofing may be combined with illegal activities such as smuggling, illegal fishing, or evading international sanctions, as attackers can use spoofing to conceal a vessel's true route and avoid surveillance (Wu et al., 2020). This dual-use nature of spoofing technology creates complex enforcement challenges that span both cybersecurity and traditional maritime law enforcement domains.

These incidents highlight the shipping industry's heavy reliance on navigation and signal systems while reflecting the growing fusion of geopolitical rivalry and cyberattack techniques. The vulnerability of navigational infrastructure represents a systemic risk to maritime operations globally. In response to escalating GNSS spoofing threats, the IMO and national governments are working to enhance AIS and GNSS security through encrypted communications, authentication technologies, and multi-source data validation. These technical countermeasures aim to create more resilient navigation systems that can detect and mitigate spoofing attempts, often by integrating multi-source data validation, such as using advanced AI to visually confirm a vessel's presence in adverse weather, thereby providing a crucial check against compromised digital signals (Androjna et al., 2020; Chen et al., 2023; Hao et al., 2023; Spravil et al., 2023). This regulatory gap requires urgent attention from international maritime authorities to establish comprehensive frameworks for navigation system security.

Legally, GNSS spoofing directly challenges the safety of navigation, a cornerstone of UNCLOS. If spoofing occurs in territorial waters, it could be deemed prejudicial to the coastal state's peace, good order, or security, thus rendering a vessel's passage non-innocent under Article 19(2)(k) (interference with communication systems) or 19(2)(l) (any other activity not having a direct bearing on passage), even if the vessel itself is a victim. On the high seas, it impacts the freedom of navigation (Article 87) and the obligation of states to ensure safety at sea. The difficulty in attributing spoofing and its often transnational nature underscore the need for enhanced regional cooperation on technical standards and early warning and national-level interagency coordination. Furthermore, establishing international norms on non-interference with GNSS signals, potentially through a global-level initiative clarifying state responsibility for allowing or conducting such operations from their territory (due diligence principle), is crucial.

2.3.3 Vulnerability of submarine cable security – a legal blind spot for cyber threats

Approximately 95% of transoceanic communication data depends on submarine fiber-optic cables, which serve as critical infrastructure for international communications, financial transactions, government correspondence, and military intelligence (Bueger and Liebetrau, 2021). These cables, often only a few inches in diameter, lie mostly unprotected on the seabed. In recent years, governments and security experts have warned that, in the event of military conflict or political standoffs, underwater vehicles or remotely operated robots could be used to sabotage or intercept these cables, posing severe threats to global economies and national security (McGeachy, 2022). These threats represent an evolution from traditional physical risks to sophisticated hybrid threats combining physical and cyber elements.

Currently, UNCLOS provides the primary provisions for submarine cable protection. Articles 113 – 115 oblige States to criminalize the willful or negligent breaking or injury of submarine cables beneath the high seas (or EEZ for this purpose) if it causes a communication interruption, and address liability for such physical damage. However, these articles were written with physical cutting or damage in mind (e.g., a ship's anchor dragging and breaking a cable). Cyber threats to cables present a new challenge (Clark, 2016). Instead of cutting the cable, an attacker might target the landing stations or network control systems that manage data flows, or use cyber means to induce malfunctions in repeaters or other electronic components. Such attacks do not "damage" the cable in the traditional UNCLOS sense, but they compromise its functioning and the confidentiality/integrity of the data transmitted. UNCLOS

has no explicit provision about protecting data flowing under the sea or against cyber-induced interference with cable functioning that does not involve a physical break. This regulatory gap reflects the challenge of applying pre-digital legal frameworks to contemporary security threats. Should these infrastructure risks materialize, their impacts would be incalculable, potentially disrupting global communications, financial systems, and critical services simultaneously. Although international awareness of this security threat is growing, UNCLOS does not clearly define whether a state's data theft from an adversary's submarine cables constitutes "use of force" under Article 2(4) of the UN Charter (Guilfoyle et al., 2022). This ambiguity creates significant challenges for attribution, deterrence, and response frameworks.

In the future, the international community may need to revise UNCLOS or establish a new legal framework to clarify the legal applicability of submarine cables in the context of cyberattacks and develop effective response mechanisms through international cooperation (McCabe and Flynn, 2024). Such reforms would need to balance national security interests with the protection of global digital commons and establish clear thresholds for what constitutes an attack on submarine infrastructure worthy of international response.

The vulnerability of submarine cables directly implicates UNCLOS Articles 113 - 115, which, as noted, primarily address physical damage. Cyber interference or data theft challenges the interpretation of "breaking or injury" and highlights a significant normative gap. This necessitates a global-level re-evaluation or supplementation of UNCLOS to explicitly cover cyber threats to cables, potentially by broadening the definition of "damage" or creating new obligations regarding data integrity. National legislation designating cables as critical infrastructure and regional agreements for monitoring and protecting shared cable routes are also vital components of the proposed multi-level governance framework to address this specific vulnerability.

2.4 Summary

MCOs present multifaceted threats to global shipping, maritime infrastructure security, and regional stability. These threats manifest through diverse forms including disruption of logistics systems, navigation interference, and vulnerability exploitation in critical communications infrastructure. The NotPetya attack, GNSS spoofing incidents, and submarine cable security concerns illustrate the widespread potential impacts of cyber operations in the maritime domain, from economic disruption to national security implications.

Confronting this emerging non-traditional security challenge requires a critical reassessment of the applicability of existing international and maritime law frameworks. Current governance mechanisms, particularly the United Nations Convention on the Law of the Sea, were developed before the digital revolution and consequently lack provisions that adequately address cyber threats in maritime contexts. The international community faces significant hurdles in establishing consensus on key definitions, thresholds for use of force in cyberspace, and appropriate response mechanisms.

The next section will focus on the potential applicability and shortcomings of UNCLOS, further dissecting the dilemmas contemporary maritime law faces in the digital age. This analysis will examine how traditional maritime legal frameworks can be interpreted or modified to address the unique characteristics of cyber operations at sea, while identifying areas where new legal instruments may be necessary to ensure comprehensive governance of maritime cybersecurity.

3 Legal frameworks and their limitations

Building on the above understanding of MCO threats, this section examines UNCLOS and related maritime law to assess how well they address these emerging risks. We review UNCLOS's core provisions — on use of force, enforcement and jurisdiction, and dispute resolution — to evaluate the strengths and limitations of the current legal framework in handling cyberattacks at sea. We also explore how traditional maritime law intersects with evolving cybersecurity law to identify pathways for adapting the legal regime. The conceptual gap between the traditional physical scope of UNCLOS and the modern realities of MCOs is summarized in Figure 2.

3.1 Consensus and divergence on international law in cyberspace

Since 2013, the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) have consistently affirmed the applicability of international law to cyberspace. In their successive reports, these bodies have specifically acknowledged that cyberattacks may, under certain circumstances, constitute a "use of force," thereby triggering the right to self-defense under Article 51 of the UN Charter (UN OEWG, 2021; Elhaw, 2023). Despite this general consensus, the international community has failed to establish a unified standard for determining precisely what scale or nature of cyberattacks would qualify as "armed attacks" (Nguyen, 2013).

The current legal discourse reveals two predominant recognition models among states. The United States advocates an "effects-based" standard, asserting that cyberattacks causing destruction comparable to physical attacks — such as critical infrastructure paralysis or widespread social chaos — can legitimately trigger self-defense rights (Banks and Criddle, 2016). In contrast, China and Russia emphasize a "means-based" standard, arguing that Article 51 applies only to attacks directly employing military means, such as state-backed cyber warfare operations (Haataja and Akhtar-Khavari, 2018).

This fundamental divergence is further complicated by scholarly critiques of the existing international legal framework's adequacy in addressing various forms of cyberattacks. While Article 2(4) of the UN Charter prohibits states from using force to infringe upon another's sovereignty, traditional interpretations of "force" in international law

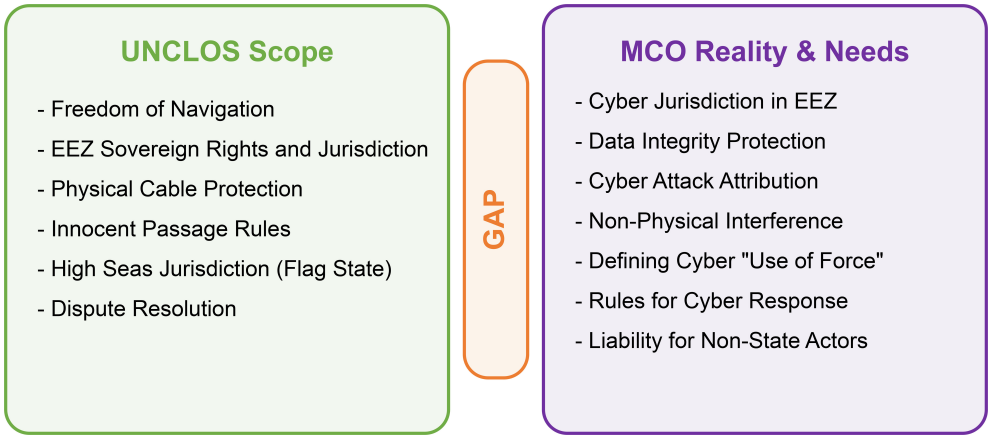

FIGURE 2
Conceptual gaps between UNCLOS provisions and the realities of maritime cyber operations.

typically focus on physical harm. This creates a significant gap, as cyberattacks primarily target information systems and economic infrastructure rather than causing immediate physical damage (Haataja, 2017). The Tallinn Manual 2.0 (Rule 4) reflects expert division on whether any cyber operation that breaches sovereignty is an internationally wrongful act. Recognizing these limitations, several states have proposed establishing a new international cybersecurity convention specifically designed to address the gaps in the existing legal system and provide clarity regarding the legal scope and characterization of cyberattacks (Alweqyan, 2024).

In the maritime domain, these legal challenges become considerably more complex due to the unique jurisdictional frameworks established by UNCLOS. We confront critical questions such as whether cyber eavesdropping on submarine cables infringes a coastal state's sovereignty or sovereign rights, and how a cyberattack on the high seas should be legally characterized under current maritime law. Although UNCLOS, as the foundational framework of maritime law, does not explicitly address cyberattacks, its fundamental principles—such as freedom of the high seas and innocent passage—provide potential avenues for legal interpretation and application.

The distinctive characteristics of maritime scenarios necessitate specialized research to determine how UNCLOS's principles and provisions can be effectively extended to encompass cybersecurity threats. The subject-matter and enforcement jurisdictional complexity of maritime environments significantly complicates legal interpretation. For instance, under the principle of high seas freedom (Article 87), a critical question arises whether cyberattacks should be considered a threat to navigational freedom, thereby justifying intervention. Similarly, regarding Exclusive Economic Zone coastal state prescriptive and enforcement jurisdiction (Article 56), ambiguity persists about whether coastal states possess the legal authority to enforce countermeasures against cyberattacks occurring within their EEZs, particularly when such attacks target vessels or installations under their subject-matter jurisdiction.

3.2 Extended interpretation of UNCLOS provisions

MCOs impacting the high seas, EEZs, or critical infrastructure such as submarine cables fall squarely within UNCLOS's core jurisdictional scope. The convention comprehensively regulates freedoms of navigation on the high seas, establishes resource utilization and enforcement rights in EEZs, and provides specific protections for the security of submarine cables and pipelines. When cyberattacks disrupt these facilities or substantially interfere with lawful maritime activities, they constitute direct challenges to the established maritime order that UNCLOS was designed to protect and maintain. Even though UNCLOS predates cyber threats, its foundational principles can — through careful interpretation — be extended to modern maritime cybersecurity challenges while respecting the convention's original intent. The subsections below examine how key UNCLOS provisions apply across different maritime zones and clarify the conditions for their application to cyber incidents.

3.2.1 Submarine cable protection (Articles 113–115) – physical damage *vs.* cyber interference

UNCLOS Article 113 explicitly prohibits the intentional or culpably negligent breaking or injury of submarine cables beneath the high seas (which includes the EEZ for this purpose) in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications. States are obliged to ensure such acts are punishable offenses. Articles 114 and 115 deal with indemnity for loss incurred by owners of cables or other cables/pipelines due to such breakage or injury, and for cable owners who sacrifice an anchor or net to avoid injuring a cable. As discussed in Section 2.3.3, these provisions were originally designed to address only physical acts of interference. The contemporary digital landscape has dramatically transformed the nature of potential threats to submarine cable infrastructure. With the exponential increase in

global data transmission via submarine cables, cyber eavesdropping and data tampering have emerged as significant security vulnerabilities that were not contemplated when UNCLOS was drafted. Recognizing this evolution, a 2019 International Seabed Authority report explicitly expanded the scope of cable protection to include data integrity (ISA, 2019), providing a foundation to modernize Article 113. Accordingly, there is a compelling need to broaden the interpretation of "breaking or injury" to include harm to data integrity or functionality. However, this idea remains largely academic and contested, with no supporting state practice or judicial affirmation so far. Furthermore, such an expanded interpretation would require clarification regarding every state's specific responsibilities and enforcement jurisdictional authority in safeguarding cable network security, particularly as these responsibilities intersect with traditional maritime security frameworks and emerging cybersecurity governance structures.

3.2.2 Innocent Passage principle (Article 19) – cyber activities in territorial seas

Under UNCLOS, foreign vessels exercising "innocent passage" through a coastal state's territorial waters must conform to specific behavioral requirements that expressly prohibit activities prejudicial to the coastal state's peace, good order, or security. Article 19(2) lists activities considered non-innocent. While cyberattacks are not explicitly mentioned, several sub-provisions could encompass MCOs: (c) "any act aimed at collecting information to the prejudice of the defense or security of the coastal State" (covering cyber espionage); (j) "the carrying out of research or survey activities" (potentially covering electronic reconnaissance); and particularly (k) "any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State." When a vessel launches a cyberattack—such as infiltrating a port management system—during its passage through territorial waters, such conduct fundamentally violates the innocent passage requirement established in Article 19 (Honniball, 2020). This interpretation applies the existing legal framework to new technological contexts without requiring amendment to the convention itself.

The application of this principle to cybersecurity contexts, however, presents significant evidentiary challenges. The inherently transnational and covert nature of cyberattacks creates substantial obstacles for coastal states attempting to gather sufficient forensic evidence linking specific vessels to cyber activities that directly threaten their security (Tabish and Chaur-Luh, 2024). This evidentiary burden is particularly problematic given the time-sensitive nature of maritime security responses and the technical complexity of attributing cyber operations. To address these implementation gaps, the international community must establish uniform enforcement standards and protocols. The development of comprehensive Maritime Cybersecurity Guidelines through authoritative bodies such as the International Maritime Organization represents a promising approach to supplement UNCLOS's existing framework with specific technical and procedural standards (Marten, 2011). Such guidelines would provide coastal states with clearer benchmarks for identifying violations while establishing consistent international practices for response and enforcement when innocent passage is compromised through cyber means.

3.2.3 Right of visit on the high seas (Article 110) – limitations for cyber offences

UNCLOS Article 110 expressly authorizes warships (and other duly authorized ships or aircraft clearly marked and identifiable as being on government service) to exercise the right of visit on the high seas against foreign ships (other than those entitled to complete immunity) suspected of engaging in specific prohibited activities, including piracy, slave trading, or unauthorized broadcasting. This right is an exception to the exclusive flag state jurisdiction on the high seas (Article 92) and is strictly limited to the enumerated offenses. It does not extend to the EEZ unless the suspected activity also falls under coastal state sovereign rights or jurisdiction in the EEZ (e.g., illegal fishing). However, the convention provides no explicit legal basis for addressing cyberattacks occurring on the high seas, creating a significant enforcement jurisdictional gap in the existing maritime legal framework (Trevisanut, 2014). This limitation reflects the technological context in which UNCLOS was originally negotiated and adopted. To address this emerging challenge, future revisions to UNCLOS provisions or the conclusion of supplementary international agreements could establish clear conditions and thresholds for exercising the right of visit in cases involving high seas cybercrime. Such developments would substantially enhance the legal foundation and operational feasibility of international enforcement cooperation in this domain (Hong and Ng, 2010).

The institutional frameworks for maritime cybersecurity governance remain in preliminary exploratory stages, yet important developments are emerging. Several states and international organizations have initiated substantive discussions regarding the feasibility of implementing a "digital extension" within the existing UNCLOS framework (Liao, 2021). This approach would adapt established maritime principles to address cyber threats without requiring comprehensive treaty renegotiation. Concurrently, a growing number of coastal states have advanced legal arguments asserting that digital infrastructure—including cyber resources, submarine cables, and offshore platforms within Exclusive Economic Zones—should receive protection under existing UNCLOS provisions. These states contend that when such infrastructure faces malicious cyberattacks, coastal states should be granted enhanced enforcement jurisdictional authority to respond effectively (Jenisch, 2012). This evolving interpretation would significantly expand coastal state enforcement capabilities while potentially redefining traditional understandings of maritime enforcement jurisdiction in the digital age.

3.3 Jurisdictional, use of force, and enforcement controversies

The intersection of maritime law and cybersecurity presents significant challenges in subject-matter jurisdiction, enforcement, and judicial authority that traditional legal frameworks struggle to address. This section examines the fundamental limitations of the

UNCLOS in regulating maritime cyber operations, highlighting conceptual gaps, enforcement jurisdictional ambiguities, and dispute resolution complexities. Our analysis of these legal deficiencies underscores the need for innovative interpretations or even formal amendments to existing maritime law in order to effectively govern maritime cyber activities.

3.3.1 Traditional provisions overlook cyber threats

UNCLOS was fundamentally designed with specific legislative priorities: ensuring freedom of navigation, facilitating responsible resource development, and establishing frameworks for environmental protection. This foundational maritime treaty, negotiated during the 1970s and early 1980s, could not anticipate the sophisticated cyber threats that now regularly target maritime facilities and operations. The absence of cyber considerations in UNCLOS creates a significant regulatory gap in addressing contemporary maritime security challenges.

The convention lacks direct provisions to address activities that disrupt maritime operations through non-physical means such as data interception, unauthorized system intrusions, or remote interference with navigational and operational systems. For example, there is no concept of "cyber piracy" or "maritime cyber terrorism" analogous to existing provisions for physical acts. UNCLOS Article 94 (flag state duties) does not explicitly mention cybersecurity obligations for vessels, and there is no clear threshold for when a cyber operation constitutes a "use of force" at sea under UNCLOS Article 301 or general international law. This absence is particularly problematic as cyber vulnerabilities in maritime infrastructure have become increasingly evident, with potential impacts on vessel navigation systems, port operations, offshore installation controls, and maritime communication networks.

Furthermore, UNCLOS's enforcement mechanisms were designed primarily for physical threats that occur within clearly defined maritime zones. These mechanisms prove inadequate when confronting cyber operations that originate from distant locations, transit through multiple jurisdictions, and cause effects across various maritime boundaries without any physical presence in the affected areas. This enforcement jurisdictional disconnect significantly undermines the convention's ability to provide an effective legal framework for addressing modern cybersecurity threats.

The growing integration of digital technologies in maritime operations—including automated navigation systems, remote monitoring capabilities, and interconnected port management systems—has created new vulnerabilities that fall outside UNCLOS's traditional security paradigm. As maritime operations become increasingly dependent on digital infrastructure, this gap between conventional maritime law and emerging cyber threats continues to widen, necessitating innovative legal interpretations or formal amendments to address this evolving security landscape.

3.3.2 Enforcement gaps and jurisdictional ambiguities

Maritime cyberattacks present unprecedented enforcement and judicial jurisdictional challenges due to their complex technical architecture. These attacks frequently utilize transnational server networks and intermediary nodes distributed across multiple legal jurisdictions, creating substantial obstacles for victim states attempting to swiftly identify the original attack source or determine the attacker's state affiliation and flag jurisdiction. This technical complexity fundamentally undermines UNCLOS's traditional enforcement framework, which presumes clear attribution and enforcement jurisdictional certainty.

The attribution problem is further exacerbated when state actors deliberately employ "third-party proxies" to conduct cyber operations against maritime targets on the high seas or within Exclusive Economic Zones. These proxy relationships are strategically designed to maintain plausible deniability and avoid leaving conclusive digital evidence that would enable definitive attribution under international law. Such operational tactics effectively render UNCLOS's enforcement and accountability mechanisms practically inapplicable, as they rely on the ability to establish clear lines of responsibility that these operations deliberately obscure.

The enforcement jurisdictional fragmentation inherent in maritime cyberattacks creates significant legal barriers to effective investigation and prosecution. When cyber incidents affect maritime infrastructure, the investigation typically requires access to digital evidence located across multiple national jurisdictions, each with different legal systems, evidentiary standards, and procedural requirements. This fragmentation often leads to delays in response times and creates substantial gaps in enforcement capacity that sophisticated threat actors can exploit. This is compounded by the limitations of flag state jurisdiction versus coastal state interests, especially on the high seas or in the EEZ, and the lack of rapid, internationally sanctioned response mechanisms for purely cyber incidents not covered by Article 110.

Addressing these fundamental challenges necessitates the development of more robust transnational judicial cooperation frameworks specifically tailored to maritime cybersecurity incidents. Enhanced information-sharing mechanisms among maritime authorities, intelligence agencies, and cybersecurity entities would significantly improve attribution capabilities and strengthen enforcement outcomes. Furthermore, standardized protocols for cross-border digital evidence collection and preservation would help overcome the enforcement jurisdictional barriers that currently impede effective responses to maritime cyber threats.

3.3.3 Dispute resolution applicability and accountability challenges

UNCLOS establishes a comprehensive framework of dispute resolution mechanisms designed to address maritime conflicts between states. These include specialized forums such as the International Tribunal for the Law of the Sea (ITLOS), broader judicial bodies like the International Court of Justice (ICJ), and various arbitration tribunals with specific judicial jurisdictional competencies. Despite this institutional diversity, significant uncertainty remains regarding the applicability of these mechanisms to maritime cyberattacks. As of early 2025, no

precedent currently exists to determine whether a state alleging a cyberattack against its submarine cables, vessels, or offshore installations by another state can successfully initiate and sustain proceedings under the established maritime law framework.

The evidentiary challenges in maritime cybersecurity disputes present formidable obstacles to effective adjudication. Technical identification of attack sources encounters numerous methodological limitations and evidentiary blind spots that complicate attribution. The construction of legally sufficient evidence chains faces substantial procedural hurdles, as digital forensics techniques that might be acceptable in domestic settings may not satisfy the rigorous evidentiary standards required in international tribunals. This evidentiary deficit significantly undermines the practical utility of UNCLOS dispute resolution mechanisms in cyber contexts.

The international cooperation necessary for effective investigation and adjudication of maritime cyberattacks remains problematic. States frequently invoke exemptions based on "national security considerations" or "intelligence confidentiality" to avoid disclosure of information critical to resolving such disputes. These sovereign prerogatives, while legitimate within the existing international legal framework, create substantial impediments to the fact-finding processes essential for adjudication. International tribunals currently lack specific procedural rules or technical expertise to address these unique challenges presented by maritime cyber operations.

Furthermore, the applicability of UNCLOS dispute resolution mechanisms to cyber incidents raises fundamental questions regarding subject-matter jurisdiction (ratione materiae). Many states maintain that certain cyber operations fall outside the substantive scope of UNCLOS altogether, particularly when they do not result in physical damage to maritime infrastructure. This interpretive disagreement regarding the convention's subject matter jurisdiction creates additional uncertainty about whether existing maritime tribunals possess the legal authority to adjudicate cyber-related disputes, even when they clearly affect maritime interests and activities regulated under UNCLOS. This creates an accountability gap, where victims (states or private entities) may have little recourse for damages or to compel cessation of harmful activities.

3.4 Cyber-legal synergies: Tallinn Manual 2.0 insights and limitations

The Tallinn Manual 2.0, while not possessing binding legal authority, provides significant analytical frameworks for addressing maritime cyber operations through its systematic exploration of principled approaches to cyber conflicts. The Manual's expert interpretations offer valuable reference points for extending existing maritime legal norms to cyber contexts in three critical areas:

First, regarding the Freedom of the High Seas in relation to cyberattacks, the Tallinn Manual establishes an important interpretive principle: when cyberattacks substantially disrupt or impede normal navigation or communication freedoms on the high seas, the attacking entity may be deemed to have violated fundamental principles established in UNCLOS. Such violations potentially trigger state responsibility under international law, even when the attacks do not cause physical damage to vessels or infrastructure. This interpretation meaningfully extends traditional maritime freedom protections to the cyber domain while respecting the underlying purposes of UNCLOS provisions.

Second, concerning Exclusive Economic Zones and Coastal State Countermeasures, the Manual suggests that coastal states may possess legitimate authority to respond when cyberattacks directly compromise their sovereign rights within EEZs. Under this interpretation, when cyber operations interfere with a coastal state's ability to protect marine resources or environmental integrity, the affected state may implement appropriate protective measures under UNCLOS frameworks. However, significant ambiguity remains regarding the precise threshold of impact necessary to justify enforcement actions or countermeasures, particularly when effects are primarily digital rather than physical in nature.

Third, on the crucial issues of Use of Force and Self-Defense, the Tallinn Manual articulates a consequentialist approach that evaluates cyber operations based on their effects rather than their methods. Specifically, Rule 69 ("Use of Force") suggests that a cyber operation constitutes a use of force when its scale and effects are comparable to those of a non-cyber operation rising to the level of a use of force. Applied to MCOs, this could mean a cyberattack causing widespread disruption to shipping or port operations might be considered a use of force. Similarly, Rule 4 (Violation of sovereignty) posits that a cyber operation that infringes upon another State's inherently governmental functions or causes damage or injury within its territory may violate sovereignty, even if it does not amount to a use of force. The implications of these rules for activities like GNSS spoofing or interference with submarine cable data flows are significant but remain subject to diverse state interpretations, as discussed in Section 2.2.6. When maritime cyberattacks reach certain severity thresholds—particularly if they cause significant operational disruption, economic damage, or endanger human safety—they may constitute a "use of force" under international law. This classification would potentially entitle the victim state to claim self-defense rights, though proportionality requirements would still apply. This interpretive position continues to generate substantial debate in both academic and operational circles, requiring further validation through evolving state practice or judicial determinations before achieving widespread acceptance in the international community.

While the Tallinn Manual's interpretations offer valuable analytical frameworks, their practical implementation in maritime contexts requires further development through formal international agreements, authoritative judicial decisions, or consistent state practice that demonstrates emerging consensus on these complex enforcement and judicial jurisdictional and enforcement questions. Its non-binding nature and the controversies surrounding some of its interpretations, particularly regarding sovereignty and use of

force thresholds, limit its direct applicability as a definitive legal guide.

3.5 Summary

The accelerating digitization of maritime operations presents unprecedented challenges to the existing legal governance frameworks. UNCLOS and related maritime legal instruments face mounting pressure to effectively address the complex and evolving nature of MCOs. While the international community has reached general consensus that established principles of international law apply to cyberspace, significant operational and enforcement jurisdictional gaps persist specifically within maritime contexts.

These regulatory deficiencies stem from three interconnected factors. First, enforcement and judicial jurisdictional disputes arise from the transnational nature of cyber operations that frequently transcend traditional maritime boundaries. Second, technical limitations in attribution and evidence collection undermine effective enforcement mechanisms. Third, the absence of specific provisions addressing cyber threats within UNCLOS creates fundamental interpretive challenges for maritime authorities and judicial bodies.

The existing legal framework requires substantial adaptation to address these emerging threats, whether through innovative interpretation of current UNCLOS provisions, formal amendments to the convention, or the development of complementary legal instruments. Establishing clear thresholds for when cyberattacks constitute use of force, developing coherent enforcement and judicial jurisdictional frameworks for maritime cyber incidents, and creating effective dispute resolution mechanisms have become urgent priorities for maintaining maritime security and order.

Addressing these structural gaps within the UNCLOS framework has emerged as a critical task for the international community. The development of comprehensive legal responses must balance technological innovation with maritime security imperatives while respecting established principles of navigational freedom and sovereign rights. The following section will examine the current landscape of international cooperation in maritime cybersecurity governance and explore potential pathways toward resolving these fundamental legal challenges.

4 Pathways to global governance: a multi-level framework

This section reviews the current maritime cybersecurity governance landscape and proposes a multi-level framework to fill gaps in international cooperation. By critically examining existing mechanisms, legal principles, and emerging practices, we outline pathways to stronger protection of maritime digital infrastructure. We begin by assessing present cooperation efforts and political–legal obstacles, then present multi-level governance recommendations and evaluate their potential effectiveness and limitations.

4.1 Current state of international cooperation

The maritime cybersecurity governance landscape remains fragmented, with various international organizations and regional bodies addressing cyber threats but facing significant limitations in their approaches. This section examines international cooperation at global and regional levels, highlighting both contributions and shortcomings in addressing maritime cybersecurity challenges.

4.1.1 UN and NATO frameworks

At the United Nations level, both the UNGGE and the OEWG have established foundational principles for applying international law to cyberspace and suggested voluntary norms, such as not attacking critical infrastructure of other states in peacetime. However, these initiatives have focused primarily on terrestrial critical infrastructure — power grids, financial systems, telecommunications — leaving maritime cybersecurity largely overlooked. Within NATO, the Tallinn Manual 2.0, developed under the Cooperative Cyber Defence Centre of Excellence (CCDCOE), offers comprehensive theoretical analysis on the legal applicability of cyber operations. Despite its analytical depth, the manual lacks legal binding force and predominantly reflects NATO member states' perspectives rather than representing a global consensus on maritime cybersecurity governance. NATO exercises now include cyber elements in maritime scenarios, contributing indirectly to norm development among allies.

4.1.2 The IMO and regional cooperation mechanisms

The IMO plays a significant role in enhancing global shipping cybersecurity. In 2017, it issued the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3), which were subsequently revised in 2021 and 2022 to address escalating cyber threats. These guidelines were integrated into the International Safety Management (ISM) Code via IMO Resolution MSC.428(98), recommending that cyber risks be addressed in safety management systems by January 2021 (IMO, 2022). These guidelines urge shipping companies and port authorities to strengthen cyber defenses, raise awareness, and emphasize submarine cable security. Despite these efforts, the IMO's role remains limited to setting industry standards and providing training guidance, as it lacks enforcement authority over cyberattacks (Yoo and Park, 2021; Dimakopoulou and Rantos, 2024).

Regionally, the European Union is advancing maritime cybersecurity by considering the integration of ports and shipping into its critical infrastructure protection framework under the EU Network and Information Security Directive (NIS2, adopted 2022), which explicitly lists maritime transport as a critical sector requiring cybersecurity measures (Karamperidis et al., 2021; EU, 2022;

Kanwal et al., 2024). Similarly, ASEAN states are gradually developing maritime cybersecurity cooperation, though progress remains slow. This trend reflects a broader principle in maritime governance: just as massive physical infrastructure projects like the Maritime Silk Road create new demands for environmental regulation, the increasing digitization of maritime transport necessitates the development of unified cybersecurity frameworks (Heinl, 2014; Wang et al., 2025).

In the Indo-Pacific region, allies such as the United States, Australia, and Japan conduct cooperative exercises focused on military defense and intelligence sharing. These initiatives, however, primarily center on naval operations and have not yet evolved into a globally inclusive civilian maritime cybersecurity framework (Karamperidis et al., 2021; Vosse, 2022). Given these limitations in existing mechanisms, academics and policymakers propose that the IMO could develop a legally binding Cybersecurity Code modeled after the Polar Code to strengthen global maritime cybersecurity governance.

4.2 Political, legal, and procedural barriers to major reform

Any proposal to strengthen governance must grapple with significant obstacles. Amending UNCLOS faces immense procedural hurdles (for example, the Article 313 simplified amendment process requires zero state objections, while the Article 312 conference route is lengthy and could unravel existing compromises (Pedrozo, 2010)). Politically, major powers are reluctant to accept new constraints on their cyber capabilities, and divergent views on internet governance and national security make global consensus difficult. Legally, ongoing uncertainties in defining and thresholding cyber operations complicate any treaty negotiations. Finally, overlapping mandates between law-of-the-sea bodies and cyber governance forums can stall progress. These barriers show that formal UNCLOS reform will be protracted, so interim multi-layered solutions are crucial.

4.3 Proposed multi-level governance framework

Drawing on the foregoing analysis and existing international practices, this paper proposes the following framework recommendations at global, regional, and national levels to guide future maritime cybersecurity governance. An integrated approach across these three dimensions will be essential for establishing comprehensive protection mechanisms that address the complex and evolving nature of maritime cyber threats. Figure 3, presented below, offers a visual representation of this proposed multi-level governance framework, illustrating the interconnectedness of initiatives at the global, regional, and national levels and highlighting key areas of focus for each level.

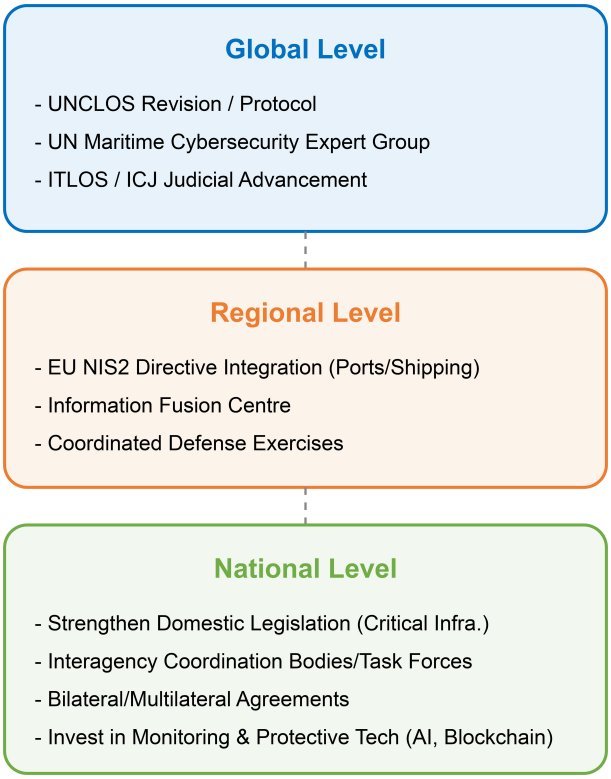

FIGURE 3
Proposed multi-level governance framework for maritime cybersecurity.

4.3.1 Global level—strengthening legal and institutional innovation

Revising or Supplementing UNCLOS represents a foundational approach to addressing maritime cybersecurity gaps. If the international community reaches a consensus on the harmfulness of maritime cyberattacks, adding provisions to UNCLOS or developing subsequent instruments like an UNCLOS Implementing Agreement or Protocol on Maritime Cybersecurity could comprehensively address critical issues such as submarine cable protection, the legal characterization of maritime cyberattacks, and the delineation of cyber enforcement rights in EEZs. While the amendment process may be complex and protracted, UNCLOS's global authority could fundamentally resolve existing legal gaps. To bridge these gaps in the interim, an UNCLOS Cybersecurity Supplementary Protocol could be promoted, focusing on three key areas.

First, such a protocol would define the constitutive elements of "maritime cyberattacks," establishing clear distinctions between "cybercrime," "cyber espionage," and "cyber warfare" in the maritime domain. For instance, it could provide criteria based on intent, effect, and actor type to differentiate these categories, thereby clarifying thresholds for different legal responses. Second, it would establish balanced rules enabling coastal states to exercise limited enforcement jurisdiction over cyberattacks within their EEZs while avoiding sovereignty disputes with flag states. This might involve, for

example, clauses allowing coastal state investigation of cyber incidents significantly impacting their EEZ resources or environment, contingent on notification to the flag state and established cooperation mechanisms. Third, it would create robust mechanisms for state responsibility and private sector joint liability, including requirements for flag states to exercise oversight or provide compensation for cyber activities originating from their registered vessels. This could entail specific due diligence obligations for flag states regarding the cybersecurity posture of their flagged vessels and mechanisms for attributing responsibility when such vessels are used in MCOs. The negotiation of such a protocol would undoubtedly face political challenges in reconciling differing national interests regarding sovereignty, intelligence activities, and economic considerations; however, focusing on shared threats to maritime safety and security could provide common ground for progress.

Judicial advancement offers another pathway for clarifying maritime cybersecurity governance. Should maritime cyberattack disputes arise between parties that accept judicial jurisdiction, submitting these cases to the ITLOS or the ICJ could provide valuable precedential guidance for applying UNCLOS principles in the digital age. While this approach is inherently reactive rather than preventive, judicial decisions carry significant authority in shaping international legal norms.

Establishing a dedicated "Maritime Cybersecurity" Expert Group within the UN framework represents a third strategic approach. Modeled after the UNGGE, this specialized body would coordinate state positions, develop technical standards, and monitor the implementation of agreements specifically within the maritime cybersecurity domain. Drawing inspiration from the International Atomic Energy Agency (IAEA) model, such a group could enhance transparency through regular reviews and reporting mechanisms. This institutional framework could foster meaningful cooperation or, at minimum, establish soft law consensus on critical issues including high seas freedoms, submarine cable protection, and the exercise of cyber enforcement jurisdiction within EEZs.

4.3.2 Regional level—enhancing technical standards, early warning, and joint response mechanisms

The development of robust regional frameworks represents a critical intermediate layer in effective maritime cybersecurity governance. Regional approaches can provide more targeted and contextually appropriate mechanisms while maintaining sufficient coordination across multiple nations. Three key regional initiatives merit particular consideration:

The European Union should integrate maritime cybersecurity comprehensively into the revised Network and Information Security (NIS) Directive. This integration would establish uniform regulatory standards across member states, with enforcement authority vested in maritime safety agencies or specialized cybersecurity bodies. A concrete implementation step would involve formally designating ports and shipping companies as "critical entities" within the European regulatory framework. This designation would establish mandatory requirements for vessels entering EU ports to implement cybersecurity systems that meet ISO/IEC 27001 standards, creating a consistent security baseline modeled on other successful regulatory frameworks like Emission Control Areas (ECAs), which enforce specific technical standards within defined maritime zones (Xiao et al., 2025).

Within ASEAN, member states should establish a maritime cybersecurity center (perhaps expanding the Information Fusion Centre in Singapore). This specialized institution would focus on addressing the region's most prevalent maritime cyber threats, particularly ransomware attacks and unauthorized data access affecting vessels operating in Southeast Asian waters. The Centre would facilitate a real-time threat intelligence-sharing platform connecting all member states and coordinate annual exercises to enhance collective response capabilities.

Beyond these formal institutional arrangements, coastal states and stakeholder nations should organize regular maritime cyber defense exercises. These scenarios should simulate realistic threats including AIS spoofing, GPS signal jamming, and coordinated attacks causing port operational paralysis. Such exercises would strengthen response capabilities across multiple sectors—enforcement agencies, naval forces, and civilian maritime operators—while providing valuable operational insights. Each exercise should conclude with comprehensive review sessions identifying systemic vulnerabilities and establishing improved communication protocols for future incidents.

However, it is crucial to acknowledge that unharmonized regional technical standards or significant disparities in national capacities for implementation could lead to fragmented enforcement and create new vulnerabilities; thus, capacity-building and efforts towards interoperability must accompany such regional initiatives.

4.3.3 National level—improving domestic law, interagency coordination, and public-private collaboration

At the national level, effective maritime cybersecurity governance requires a comprehensive approach encompassing legislative frameworks, institutional coordination, international agreements, and technological innovation. This multi-faceted strategy ensures that individual states can protect their maritime interests while contributing to the broader international security architecture.

Strengthening maritime cybersecurity legislation constitutes a foundational element of national governance. States should enact or amend critical infrastructure protection laws to explicitly designate submarine cables and port automation systems as national critical infrastructure. These legal frameworks should establish mandatory protection standards, including specific requirements for data encryption levels, intrusion detection capabilities, and incident response timeframes. Furthermore, legislation should address cross-border transfers of sensitive maritime data, such as seabed mapping results, implementing appropriate restrictions to prevent unauthorized intelligence collection or data exploitation.

The establishment of interagency coordination mechanisms represents an essential institutional component. National governments should create dedicated coordination bodies or task forces that integrate representatives from maritime authorities,

cybersecurity agencies, intelligence services, naval forces, and relevant private sector entities. These bodies would be responsible for developing comprehensive contingency plans, coordinating responses to transnational incidents, and maintaining regular communication channels with shipping companies and port operators. Such institutional arrangements ensure a whole-of-government approach to maritime cybersecurity challenges, like the US Coast Guard Cyber Protection Team (U.S. Coast Guard, 2025).

In parallel with domestic initiatives, states should actively pursue bilateral and multilateral agreements to address immediate operational needs. In the absence of global consensus on maritime cybersecurity governance, these agreements can preemptively establish protocols for cooperation in maritime cyberattack investigations, evidence collection procedures, and extradition arrangements. The experiences gained through these more limited agreements could subsequently inform the development of broader international cooperation frameworks.

Technological innovation constitutes the fourth pillar of effective national response. States should invest in developing advanced monitoring systems for submarine cable infrastructure, such as AI-based anomaly traffic detection capabilities that can identify potential data theft in real time. Norway's Tampnet "Smart Cable Guardian" project exemplifies this approach. Additionally, emerging technologies like blockchain offer promising applications for maritime security, enabling the creation of immutable records of vessel communication data that could significantly enhance attack attribution capabilities, as demonstrated by Maersk and IBM's TradeLens platform. Furthermore, technological innovation can directly harden port infrastructure by replacing vulnerable physical guidance systems with resilient, AI-based visual navigation for automated vehicles, thereby reducing the attack surface for both physical and cyber threats (Chen et al., 2025).

4.4 Evaluation and limitations of the proposed framework

The proposed maritime cybersecurity governance frameworks provide a comprehensive approach to addressing emerging threats in this critical domain. However, several significant challenges constrain their practical implementation and effectiveness.

Political will represents a fundamental obstacle to international cooperation on maritime cybersecurity. Many states consider their cyber capabilities strategic assets, approaching them with a level of secrecy and competitiveness that impedes genuine transnational intelligence sharing and collaborative defense. This protective stance directly undermines the trust-based mechanisms essential for effective international governance frameworks. This reluctance is particularly acute when considering binding legal reforms or extensive information sharing that could compromise perceived national security advantages.

Legal processes introduce additional complications. Amending UNCLOS or developing new international conventions requires consensus among major maritime powers with divergent interests and priorities. These diplomatic processes are inherently protracted and struggle to keep pace with rapidly evolving threats. The timeline for developing binding legal instruments typically extends far beyond the operational window in which new threats emerge and proliferate. Therefore, while pursuing long-term legal reforms, emphasis must also be placed on more agile soft-law mechanisms, regional arrangements, and technically-driven standards as interim or complementary measures.

Technological disparities between nations further complicate governance efforts. Developing countries often lack the resources, technical expertise, and infrastructure necessary to implement sophisticated maritime cybersecurity measures. These capability gaps create vulnerabilities that could be exploited across interconnected maritime systems. Addressing these disparities necessitates substantial capacity-building investments and sustained funding commitments from more developed nations. This digital divide can lead to uneven implementation of both legal frameworks and technical standards, creating weak links in the global maritime cybersecurity chain and potentially exacerbating existing inequalities.

The dynamic nature of maritime cyber threats poses perhaps the most persistent challenge. As technologies such as unmanned underwater vehicles, artificial intelligence, and quantum communications continue to advance, maritime cyberattack vectors and methodologies will evolve accordingly. This technological progression places legal frameworks and enforcement mechanisms in a perpetual state of adaptation, consistently struggling to address novel threat categories.

These limitations indicate that while the proposed governance frameworks offer valuable direction, they must be implemented with sufficient flexibility to accommodate rapid technological change and evolving geopolitical realities in maritime security. Success will require ongoing reassessment and adaptation rather than static regulatory approaches.

5 Conclusions and prospects

The key findings of this study underscore the governance challenges posed by maritime cyber operations and lay the groundwork for strengthening maritime cybersecurity as the sector becomes increasingly digitized.

5.1 Key research findings

Our analysis reveals four primary conclusions:

1. MCOs are a frontier challenge at the intersection of cybersecurity and maritime governance, featuring ever-expanding attack methods and targets that threaten global shipping and strategic stability. Our study addresses this by categorizing MCOs and using case studies to show their tangible cross-domain impacts, thereby moving beyond purely theoretical discussion.
2. Current maritime law (particularly UNCLOS) has no direct provisions for cyberattack scenarios, resulting in major

gaps in enforcement jurisdiction, state accountability, and dispute resolution. Our analysis highlights how specific UNCLOS articles (e.g., 19, 92, 110, 113–115) are strained by different types of MCOs across various maritime zones, revealing concrete areas of legal ambiguity or outright gaps.
3. While international awareness is rising—evidenced by the Tallinn Manual 2.0 and IMO initiatives—a unified, legally binding global framework remains absent. Our analysis critically assesses the limitations of existing soft-law approaches and identifies the specific political, legal, and interpretative hurdles to achieving broader consensus and more effective governance.
4. Effective governance will require multi-level cooperation: revising UNCLOS at the global level, bolstering technical standards at the regional level, and improving domestic laws and coordination at the national level—employing both soft-law and hard-law measures to balance sovereignty with security. Accordingly, we propose an integrated multi-level governance framework (Figure 3) that charts a coordinated path for global, regional, and national actions to build layered resilience (defense-in-depth) against maritime cyber threats.

5.2 Future research and action recommendations

Moving forward, we make the following recommendations:

1. Expanding case studies and technical monitoring of maritime cyberattacks, with particular focus on emerging technologies like UUVs, quantum communications, and AI automation. States and industry should collaborate to document and share anonymized incident data to facilitate trend analysis and inform risk assessments.
2. Pursuing legislative or judicial breakthroughs under UNCLOS, potentially through landmark legal interpretations (e.g., via ITLOS advisory opinions or contentious cases if states consent) or a dedicated UNCLOS Cybersecurity Supplementary Protocol protecting maritime digital infrastructure. Practically, this involves states proactively championing negotiations, focusing on achievable consensus points first, such as enhanced protection for submarine cables against cyber threats, and clarifying due diligence obligations for flag states.
3. Enhancing regional coordination through initiatives like EU's NIS2 Directive and Asia-Pacific multilateral security exercises. The application of our findings suggests that regional bodies could use the MCO typologies developed here to tailor exercises and capacity-building programs to address the most pertinent threats in their specific maritime environments, fostering interoperability and shared situational awareness.
4. Fostering interdisciplinary research and talent development across maritime law, computer science, and international relations to support governance initiatives. Specifically, our research underscores the need for policymakers and legal experts to gain greater technical literacy regarding MCOs, and for technical experts to understand the legal and geopolitical context of their work. Governments and academia should invest in specialized educational programs and joint training exercises.

Furthermore, interim measures such as developing robust soft-law agreements, promoting regional regulatory coherence, and advancing technically driven standard-setting mechanisms should be prioritized to address immediate vulnerabilities while longer-term legal reforms are pursued. The proposed multi-level governance framework provides a roadmap for how these different types of initiatives can be mutually reinforcing.

5.3 Research limitations and outlook

This study has several limitations. First, data on maritime cyber incidents are often limited or classified, resulting in significant information gaps. Second, the rapid pace of technological evolution can outstrip the development of legal and policy responses. Third, uncertainty in international political dynamics complicates the formulation of long-term governance solutions. While our study relies on qualitative legal analysis and case studies, future work would benefit from more empirical data (e.g., on MCO frequency, economic impacts, and attribution) as better incident reporting becomes available. Such data would help quantify the urgency and scale of the problem. As maritime digitization deepens, integrating maritime law with cyber law will only grow more critical for effective governance. This paper contributes to that integration by providing a clear framework and practical recommendations to help policymakers and stakeholders navigate the "digital seas" safely.

Author contributions

YJ: Conceptualization, Writing – original draft, Writing – review & editing, Supervision. YF: Writing – review & editing, Conceptualization, Writing – original draft. CL: Writing – original draft, Writing – review & editing, Conceptualization. SL: Supervision, Writing – review & editing.

Funding

The author(s) declare financial support was received for the research and/or publication of this article. This work was supported by the National Social Science Fund of China (grant number 23BGJ048).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Alweqyan, D. (2024). Cyberattacks in the context of international law enforcement. *J. Financial Crime* 31, 1052–1066. doi: 10.1108/JFC-07-2023-0164

Androjna, A., Brcko, T., Pavic, I., and Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.* 8, 776. doi: 10.3390/jmse8100776

Androjna, A., Perkovič, M., Pavic, I., and Mišković, J. (2021). AIS data vulnerability indicated by a spoofing case-study. *Appl. Sci.* 11, 5015. doi: 10.3390/app11115015

Bai, L., Sun, C., Dempster, A. G., Zhao, H., and Feng, W. (2024). GNSS spoofing detection and mitigation with a single 5G base station aiding. *IEEE Trans. Aerosp. Electron. Syst.* 60, 4601–4620. doi: 10.1109/TAES.2024.3382074

Banks, W. C., and Criddle, E. J. (2016). Customary constraints on the use of force: article 51 with an american accent. *Leiden J. Int. Law* 29, 67–93. doi: 10.1017/S0922156515000655

Barnsby, R. E., and Reeves, S. R. (2017). Give them an inch, they'll take a terabyte: how states may interpret tallinn manual 2.0's international human rights law chapter. *Tex. Law Rev.* 95, 1515–1530.

Bueger, C., and Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemp. Secur. Policy* 42, 391–413. doi: 10.1080/13523260.2021.1907129

Caprolu, M., Pietro, R. D., Raponi, S., Sciancalepore, S., and Tedeschi, P. (2020). Vessels cybersecurity: issues, challenges, and the road ahead. *IEEE Commun. Mag.* 58, 90–96. doi: 10.1109/MCOM.001.1900632

Chae, C.-J., Kim, I.-C., Baumler, R., and Ahn, Y.-J. (2024). Ship cybersecurity risk assessment for safe operation with human involvement: an experimental case study. *WMU J. Marit. Aff.* doi: 10.1007/s13437-024-00353-6

Chen, X., Ma, F., Wu, Y., Han, B., Luo, L., and Biancardo, S. A. (2025). MFMDepth: MetaFormer-based monocular metric depth estimation for distance measurement in ports. *Comput. Ind. Eng.* 207, 111325. doi: 10.1016/j.cie.2025.111325

Chen, X., Wei, C., Xin, Z., Zhao, J., and Xian, J. (2023). Ship Detection under Low-Visibility Weather Interference via an Ensemble Generative Adversarial Network. *J. Mar. Sci. Eng.* 11, 2065. doi: 10.3390/jmse11112065

Cimpanu, C. (2018). Maersk reinstalled 45,000 PCs and 4,000 servers to recover from notPetya attack. *BleepingComputer*.

Clark, B. (2016). Undersea cables and the future of submarine competition. *Bull. At. Sci.* 72, 234–237. doi: 10.1080/00963402.2016.1195636

Council of Europe (2024). The convention on cybercrime (Budapest convention, ETS no. 185) and its protocols. *Cybercrime*.

De Hert, P., Parlar, C., and Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Comput. Law Secur. Rev.* 34, 327–336. doi: 10.1016/j.clsr.2018.01.003

Diaz, J. (2020). Maritime industry rocked by cyber attacks. *Customs Int. Trade Law Blog.*

Dimakopoulou, A., and Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *J. Mar. Sci. Eng.* 12, 919. doi: 10.3390/jmse12060919

Ducheine, P. A. L., and Pijpers, P. B. M. J. (2021). Chapter 13: The notion of cyber operations. Available online at: https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00024.xml (Accessed May 28, 2025).

Efrony, D., and Shany, Y. (2018). A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice. *Am. J. Int. Law* 112, 583–657. doi: 10.1017/ajil.2018.86

Eichenhofer, J. O., Heymann, E., Miller, B. P., and Kang, A. (2020). An in-depth security assessment of maritime container terminal software systems. *IEEE Access* 8, 128050–128067. doi: 10.1109/ACCESS.2020.3008395

Elhaw, A. E. M. (2023). The right of legitimate defense against cyberattacks in public international law. *Migr. Lett.* 20, 954–966. doi: 10.59670/ml.v20iS5.4115

EU (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 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) (Text with EEA relevance). Available online at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Accessed May 22, 2025).

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York, NY: Knopf Doubleday Publishing Group).

Guilfoyle, D., Paige, T. P., and McLaughlin, R. (2022). The final frontier of cyberspace: the seabed beyond national jurisdiction and the protection of submarine cables. *Int. Comp. Law Q.* 71, 657–696. doi: 10.1017/S0020589322000227

Guo, R., Xiao, G., Zhang, C., and Li, Q. (2025). A study on influencing factors of port cargo throughput based on multi-scale geographically weighted regression. *Front. Mar. Sci.* 12. doi: 10.3389/fmars.2025.1637660

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law Innov. Technol.* 9, 159–189. doi: 10.1080/17579961.2017.1377914

Haataja, S., and Akhtar-Khavari, A. (2018). Stuxnet and international law on the use of force: an informational approach*. *Camb. Int. Law J.* 7, 99–121. doi: 10.4337/cilj.2018.01.05

Hao, Y., Shi, C., Xu, A., Sui, X., and Xia, M. (2023). Revealing methods of GNSS spoofing mitigation through analyzing the spoofing impacts on adaptively robust estimation-based RTK/INS tightly coupled integration. *IEEE Sensors J.* 23, 25165–25178. doi: 10.1109/JSEN.2023.3303199

Heering, D. (2020). Ensuring cybersecurity in shipping: reference to Estonian shipowners. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* 14, 271–278. doi: 10.12716/1001.14.02.01

Heinl, C. H. (2014). Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime. *Asia Policy* 18, 131–159. doi: 10.1353/asp.2014.0026

Hong, N., and Ng, A. K. Y. (2010). The international legal instruments in addressing piracy and maritime terrorism: A critical review. *Res. Transp. Econ.* 27, 51–60. doi: 10.1016/j.retrec.2009.12.007

Honniball, A. N. (2020). Port states, coastal states and national security: A law of the sea perspective on the 2017 Qatar-Gulf crisis. *Mar. Policy* 116, 103817. doi: 10.1016/j.marpol.2020.103817

Hutchins, T. E. (2020). The legality of nearshore cyber-related operations: breaching the peace, innocent passage, or something else? *Univ. Hawai'i Law Rev.* 43, 4.

IMO (2022). Maritime cyber risk. Available online at: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (Accessed May 22, 2025).

ISA (2019). Technical Study 23: Towards the Development of a Regional Environmental Management Plan for Cobalt-Rich Ferromanganese Crusts in the Northwest Pacific Ocean - International Seabed Authority. Available online at: https://www.isa.org.jm/wp-content/uploads/2022/06/Technical-Study-23-amazon-Jan-2020-eversion.pdf (Accessed May 22, 2025).

Jenisch, U. K. (2012). Old laws for new risks at sea: mineral resources, climate change, sea lanes, and cables. *WMU J. Marit. Aff.* 11, 169–185. doi: 10.1007/s13437-012-0018-1

Jin, J., and Techera, E. (2021). Strengthening universal jurisdiction for maritime piracy trials to enhance a sustainable anti-piracy legal system for community interests. *Sustainability* 13, 7268. doi: 10.3390/su13137268

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., and Chang, C.-H. (2024). Maritime cybersecurity: are onboard systems ready? *Marit. Policy Manage.* 51, 484–502. doi: 10.1080/03088839.2022.2124464

Karamperidis, S., Kapalidis, C., and Watson, T. (2021). Maritime cyber security: A global challenge tackled through distinct regional approaches. *JMSE* 9, 1323. doi: 10.3390/jmse9121323

Kim, S. K. (2024). An approach to maritime cyber security risks: nature and countermeasures. *Int. J. Mar. Coast. Law* 1, 1–22. doi: 10.1163/15718085-bja10200

Kraska, J. (2011). *Maritime Power and the Law of the Sea:: Expeditionary Operations in World Politics* (Oxford, UK: Oxford University Press).

Kshetri, N. (2022). Economics of supply chain cyberattacks. *IT Prof.* 24, 96–100. doi: 10.1109/MITP.2022.3172877

Liao, X. (2021). The road not taken: submission of disputes concerning activities in undelimited maritime areas to UNCLOS compulsory procedures. *Ocean Dev. Int. Law* 52, 297–324. doi: 10.1080/00908320.2021.1959772

Liu, C., and Feng, Y. (2025). Navigating uncharted waters: Legal challenges and the future of unmanned underwater vehicles in maritime military cyber operations. *Mar. Policy* 171, 106430. doi: 10.1016/j.marpol.2024.106430

Liu, H., Tian, Z., Huang, A., and Yang, Z. (2018). Analysis of vulnerabilities in maritime supply chains. *Reliab. Eng. Syst. Saf.* 169, 475–484. doi: 10.1016/j.ress.2017.09.018

Lymperopoulos, V. (2024). Regional maritime security limitations under UNCLOS. *Rev. Contemp. Sci. Acad. Stud.* 4. doi: 10.55454/rcsas.4.02.2024.009

Marten, B. (2011). The enforcement of shipping standards under UNCLOS. *WMU J. Marit. Aff.* 10, 45–61. doi: 10.1007/s13437-011-0005-y

Matis, M. S. (2012). The Protection of Undersea Cables: A Global Security Threat. Available online at: https://agris.fao.org/search/en/providers/122415/records/647368fb2c1d629bc9808343 (Accessed February 26, 2025).

McCabe, R., and Flynn, B. (2024). Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure. *Eur. Secur.* 33, 324–344. doi: 10.1080/09662839.2023.2248001

McGeachy, H. (2022). The changing strategic significance of submarine cables: old technology, new concerns. *Aust. J. Int. Aff.* 76, 161–177. doi: 10.1080/10357718.2022.2051427

Morel, C. (2016). Threats beneath the seas: Vulnerabilities in the global cable network. *Herodote* 163, 33–43. doi: 10.3917/her.163.0033

Newberry, M. E. (2014). Maritime critical infrastructure cyber risk. *Coast. Guard J. Saf. Secur. Sea Proc. Mar. Saf. Secur. Counc.* 71, 42–44.

Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. *Calif. Law Rev.* 101, 1079.

Nguyen, C. L., and Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: '*Law on the books*' vs '*law in action.*'. *Comput. Law Secur. Rev.* 40, 105521. doi: 10.1016/j.clsr.2020.105521

Pedrozo, R. (2010). Is it time for the United States to join the law of the sea convention. *J. Marit. Law Commer.* 41.

Petrig, A. (2020). "The commission of maritime crimes with unmanned systems: an interpretive challenge for the United Nations Convention on the Law of the Sea," in *Maritime Security and the Law of the Sea* (Cheltenham, UK: Edward Elgar Publishing), 104–131. Available online at: https://www.elgaronline.com/edcollchap-oa/book/9781788971416/book-part-9781788971416-10.xml.

Roach, J. A. (2021). "Excessive Maritime Claims: Fourth Edition," in *Excessive Maritime Claims* (Leiden, Netherlands: Brill Nijhoff). Available online at: https://brill.com/display/title/59191.

Ross, M. (2014). Understanding interconnectivity of the global undersea cable communications infrastructure and its implications for international cyber security. *SAIS Rev. Int. Affairs* 34, 141–155. doi: 10.1353/sais.2014.0014

Schmitt, M., Schmitt, M., Schmitt, M., and Vihul, L. (2017). Respect for sovereignty in cyberspace. *Tex. Law Rev.* 95, 1639–1671.

Shires, J. (2024). Career connections: transnational expert networks and multilateral cybercrime negotiations. *Contemp. Secur. Policy* 45, 45–71. doi: 10.1080/13523260.2023.2274775

Simon, J., and Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *Eur. J. Oper. Res.* 282, 161–171. doi: 10.1016/j.ejor.2019.09.017

Spector, P. (2017). In defense of sovereignty, in the wake of tallinn 2.0. *AJIL Unbound* 111, 219–223. doi: 10.1017/aju.2017.56

Spravil, J., Hemminghaus, C., Von Rechenberg, M., Padilla, E., and Bauer, J. (2023). Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. *J. Mar. Sci. Eng.* 11, 928. doi: 10.3390/jmse11050928

Tabish, N., and Chaur-Luh, T. (2024). Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access* 12, 17114–17136. doi: 10.1109/ACCESS.2024.3357082

Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Mind. Mach.* 29, 187–191. doi: 10.1007/s11023-019-09504-8

Tanodomdej, P. (2019). The tallinn manuals and the making of the international law on cyber operations. *Masaryk Univ. J. Law Technol.* 13, 67–86. doi: 10.5817/MUJLT2019-1-4

Todorov, Y. (2021). Maritime cyber(in)security: A growing threat imperils EU countries. *Connections QJ* 20, 73–91. doi: 10.11610/Connections.20.3-4.04

Trevisanut, S. (2014). Efthymios papastavridis. The interception of vessels on the high seas, contemporary challenges to the legal order of the oceans. *Eur. J. Int. Law* 25, 616–619. doi: 10.1093/ejil/chu044

UN OEWG (2021). Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security_Final Substantive Report. Available online at: https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (Accessed May 22, 2025).

U.S. Coast Guard (2025). Maritime Cyber Readiness Branch. Available online at: https://www.dco.uscg.mil/Our-Organization/CGCYBER/Maritime-Cyber-Readiness-Branch/ (Accessed May 22, 2025).

Vosse, W. (2022). A conceptional broadening of the security order in the indo-pacific: the role of EU-Japan cooperation in ICT and cybersecurity. *Asian Aff.* 53, 561–582. doi: 10.1080/03068374.2022.2090683

Wang, T., Xiao, G., Li, Q., and Biancardo, S. A. (2025). The impact of the 21st-Century Maritime Silk Road on sulfur dioxide emissions in Chinese ports: based on the difference-in-difference model. *Front. Mar. Sci.* 12. doi: 10.3389/fmars.2025.1608803

Warwick, A. (2017). NotPetya attack cost up to $300m, says Maersk | Computer Weekly (ComputerWeekly.com). Available online at: https://www.computerweekly.com/news/450424559/NotPetya-attack-cost-up-to-300m-says-Maersk.

Wu, Z., Zhang, Y., Yang, Y., Liang, C., and Liu, R. (2020). Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access* 8, 165444–165496. doi: 10.1109/ACCESS.2020.3022294

Xiao, G., Amamoo-Otoo, C., Wang, T., Li, Q., and Biancardo, S. A. (2025). Evaluating the impact of ECA policy on sulfur emissions from the five busiest ports in America based on difference in difference model. *Front. Mar. Sci.* 12, 1609261. doi: 10.3389/fmars.2025.1609261

Yoo, Y., and Park, H.-S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *J. Mar. Sci. Eng.* 9, 565. doi: 10.3390/jmse9060565

Zorri, D., and Kessler, G. (2024). Position, navigation, and timing weaponization in the maritime domain: orientation in the era of great systems conflict. *Jt. Force Q.* 112, 12–21.