

Kosmas Pipyros, Assistant Professor

*Department of Computer Science of Philips University,
PhD in Information Systems Security (AUEB),
MSc in Information Systems (AUEB)LLB in Law (AUTH),
email: pipyros.k@philipsuni.ac.cy , 0035799008319*

Leonidas Sotiropoulos, PhD candidate

*in Digitalization AI and Maritime Law at EUC,
LL.M in Shipping Law (Cardiff University), LL.B in Law (AUTH),
email: leon.sotiropoulos@gmail.com, ls231119@students.euc.ac.cy, 0035797534652*

**THE LAW OF THE SEA IN THE AGE OF CYBER THREATS:
PROTECTING MARITIME INFRASTRUCTURE
AND THE MARINE ENVIRONMENT**

Abstract:

The maritime sector's rapid digitalization has resulted in substantial vulnerabilities to the marine ecosystem. Cyber threats have emerged as a critical challenge to global shipping, port operations, and offshore infrastructure. More specifically, the technological advancements in ports, vessels, offshore platforms, and ocean-monitoring systems have created greater risks from cyberattacks, including GPS spoofing, ransomware, and system hijacking, as they depend more on linked technology. These risks might cut off international commerce, put at risk human lives, and impose major ecological harm, involving pollution from compromised systems or oil spills. Notwithstanding these hazards, the United Nations Convention on the Law of the Sea (UNCLOS) lacks specific provisions to address cybersecurity, thereby creating a legal void in maritime governance. Drawing from legal analysis and real-world incidents, the article examines how current international maritime law might be understood or adjusted to address cyber threats. Furthermore, by emphasizing limitations in attribution, jurisdiction, and enforcement, the article proposes pathways to integrate cybersecurity into the broader maritime security and environmental protection agenda. Finally, it assesses the way international organizations—especially the International Maritime Organization (IMO)—may help to advance legislative remedies. The article offers suggestions for modernizing the maritime legal framework to ensure resilient, safe, and environmentally sustainable oceans in the digital era through an analysis of legal texts, current cyber events, and governance practices. The goal is to spark dialogue on modernizing international maritime law for the digital age.

Keywords: *International Maritime Law, Critical Maritime Infrastructure, Cyber Threats, Attribution & Jurisdiction, Maritime Governance*

1. INTRODUCTION

In an era marked by accelerated globalization and economic interdependence, maritime infrastructure has emerged as a cornerstone of global trade and strategic mobility. The strategic and economic importance of maritime infrastructure has intensified on the uninterrupted functioning of ports, shipping lanes, and offshore platforms. According to UNCTAD, maritime transport continues to handle over 80% of the volume of global merchandise trade, with recent figures indicating that global maritime trade reached 12.3 billion tons in 2023 and is projected to grow by 2.4% annually through 2029.¹ This reliance underscores the maritime domain's critical role in sustaining supply chains, ensuring energy security, and enabling international commerce. Concurrently, the digitalization of maritime operations – spanning automated navigation, smart port systems, and integrated logistics platforms – has expanded the sector's cyber-attack surface, exposing critical infrastructure to a growing range of cyber threats.^{2,3} Cyber-attacks targeting maritime systems have increased in frequency and sophistication, with incidents such as the ransomware attack on CMA CGM, the NotPetya incident affecting Maersk (2017), and ongoing GPS spoofing events in the Strait of Hormuz, highlighting the sector's vulnerabilities.^{4,5} These developments signal a pressing need for robust cybersecurity governance tailored to the unique operational and legal complexities of the maritime domain.

Despite the accelerating digital transformation of maritime infrastructure and the corresponding rise in sophisticated cyber threats, the international legal framework, most notably the United Nations Convention on the Law of the Sea (UNCLOS), remains largely silent on cybersecurity concerns. The absence of explicit provisions addressing cyber incidents at sea raises critical questions about the adequacy of existing legal norms in governing emerging technological risks. UNCLOS was drafted in a pre-digital era and is not equipped to address the complexities of cyberattacks on global shipping, port operations, and offshore installations.⁶ Against this backdrop, the central research question guiding this study is *'to what extent is international maritime law, particularly UNCLOS, capable of addressing the evolving threat of cyber-attacks targeting maritime infrastructure, and what legal reforms or governance mechanisms are required to enhance cybersecurity resilience in the sector?'*

To address the core research question, this article pursues four interrelated objectives. First, it critically analyzes the structural and doctrinal limitations of the UNCLOS and related legal instruments in effectively responding to maritime cyber threats, as highlighted in the recent legal scholarship.⁷ Second, it examines the role of international institutions, particularly the International Maritime Organization (IMO), in shaping cybersecurity governance through instruments such as the *Guidelines on Maritime Cyber Risk Management* and the evolving *Maritime Autonomous Surface Ships (MASS) Code*.⁸

1 UNCTAD. (2023). *Review of Maritime Transport 2023*. United Nations Conference on Trade and Development.

2 IMO. (2021). *Guidelines on Maritime Cyber Risk Management*. International Maritime Organization.

3 ENISA. (2023). *Threat Landscape for the Maritime Sector*. European Union Agency for Cybersecurity.

4 Lloyd's List. (2022). *Cyber Risks in Shipping: An Evolving Threat*.

5 Marlink. (2024). *Cyber Threat Intelligence Brief: Maritime Sector Trends*.

6 Kraska, J. (2015). *The Law of the Sea Convention: A National Security Success—Global Strategic Mobility Through the Rule of Law*. Harvard National Security Journal, 6, 1–46.

7 Tanaka, Y. (2023). *The International Law of the Sea* (4th ed.). Cambridge University Press.

8 International Maritime Organization (IMO). (2021). *Guidelines on Maritime Cyber Risk Management*

Third, the study assesses selected cyber incidents, such as the NotPetya attack on Maersk and targeted disruptions to maritime communications systems, to evaluate how current legal and operational frameworks align with best practices in cybersecurity and international law.^{9,10} Finally, it proposes policy and legal recommendations to bridge normative gaps and integrate cybersecurity into the broader framework of maritime safety, environmental protection, and multilateral cooperation. By addressing these objectives, the study contributes to the growing discourse on modernizing maritime legal governance to meet the challenges of technological advancement, and advocates for the development of a more resilient, adaptive, and future-oriented legal framework.

2. THE INTERNATIONAL LEGAL FRAMEWORK FOR THE LAW OF THE SEA. CONTEMPORARY CHALLENGES AND THE COMPREHENSIVE FRAMEWORK OF MODERN MARITIME LAW

The evolution of maritime law from ancient commercial practices to modern international frameworks represents one of the most significant legal developments in human history. The foundational principles of contemporary maritime law can be traced back to the ancient Rhodian Sea Laws, which governed commercial trade and navigation in the Byzantine Empire beginning in the 7th century and established crucial precedents for maritime jurisdiction and dispute resolution.¹¹ These early regulations established a uniform standard for the treatment of merchant ships as they moved from port to port and introduced the revolutionary concept that maritime disputes should be governed by specialized maritime law rather than local territorial courts.¹² The influence of these ancient codes extended far beyond their original Mediterranean context, laying the groundwork for the sophisticated legal architecture that governs today's global shipping industry.

In general, maritime regulations are divided into two main categories. The first is the rules of the law of the sea, which define the rights and obligations of states to regulate and act against foreign ships in various maritime areas. These are mainly contained in the 1982 United Nations Convention on the Law of the Sea (UNCLOS). Second, more detailed technical requirements covering safety, navigation, personnel and monitoring standards are set out in various conventions, which are usually adopted by the International Maritime Organization (IMO). These international regulations are then implemented and, in some cases, supplemented by national regulations (National regulations govern local businesses and regulate local maritime matters.)¹³

(MSC-FAL.1/Circ.3). <https://www.imo.org/en>

9 Marlink. (2024). *Cyber Threat Intelligence Brief: Maritime Sector Trends*. Marlink Maritime Cybersecurity Division.

10 OECD. (2022). *Cybersecurity in Critical Infrastructure: Policy Gaps and Governance Needs*. Organisation for Economic Co-operation and Development. <https://www.oecd.org/>

11 Britannica. "Rhodian Sea Law." Accessed June 25, 2025, <https://www.britannica.com/event/Rhodian-Sea-Law>

12 Maintenance and Cure. "The Intriguing History of Maritime Law." July 12, 2024. <https://maintenanceandcure.com/maritime-blog/the-intriguing-history-of-maritime-law/>

13 <https://eur-lex.europa.eu/EN/legal-content/summary/united-nations-convention-on-the-law-of-the-sea.html>, Tamada, D., & Zou, K. (Eds.). (2021). *Implementation of the United Nations Convention on the Law of the Sea: State Practice of China and Japan*. Springer.

The modern international legal framework for maritime activities reached its culmination with the adoption of the United Nations Convention on the Law of the Sea (UNCLOS) in 1982, which marked the culmination of more than 14 years of work involving participation by more than 150 countries representing all regions of the world.¹⁴ UNCLOS represents a comprehensive legal revolution that lays down a comprehensive regime of law and order in the world's oceans and seas establishing rules governing all uses of the oceans and their resources, fundamentally transforming how nations interact with maritime spaces.¹⁵ The Convention establishes detailed provisions for territorial seas, exclusive economic zones, continental shelves, and the high seas, creating a unified legal framework that balances sovereign rights with the principle of freedom of navigation.¹⁶ This international legal architecture has become indispensable in an era where maritime trade accounts for approximately 80% of global goods movement, providing the essential legal foundation for the complex web of international commerce, environmental protection, and maritime security that defines our interconnected world.

The integration of technological innovations, particularly megaships and autonomous vessels, into existing maritime legal frameworks presents fundamental challenges that current international regulations are ill-equipped to address. New technological development in autonomous and unmanned vessels challenges the international legal framework prevailing at sea, with current regulations applicable to international shipping constituting regulatory barriers preventing their operation on a worldwide scale.¹⁷ Professor Henrik Ringbom of the Scandinavian Institute for Maritime Law argues that “the regulatory framework for autonomous ships is fundamentally flawed because it assumes human decision-making at every critical juncture,” warning that current maritime conventions cannot adequately address liability when artificial intelligence systems make navigation decisions.¹⁸

The international law of the sea represents one of the most ancient and continuously evolving branches of public international law, fundamentally shaped by humanity's enduring relationship with maritime spaces and the practical necessities of regulating oceanic activities. As Professor Yoshifumi Tanaka observes in his authoritative work “The International Law of the Sea”¹⁹, this field has been fully revised to include up-to-date coverage of essential issues, covering new and important matters such as the headline debate of migrant movement across the seas, and the definition of islands in light of the South China Sea Arbitration, while also addressing chapters on conservation of marine living resources and biological diversity, protection of the marine environment, and international peace and security at sea, as well as building further on such topics as the impact of climate change on the oceans.²⁰ The historical development of maritime

14 United Nations Division for Ocean Affairs and the Law of the Sea. “Overview - Convention & Related Agreements.” Accessed June 25, 2025. https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm

15 International Maritime Organization. “United Nations Convention on the Law of the Sea.” Accessed June 25, 2025. <https://www.imo.org/en/ourwork/legal/pages/unitednationsconventiononthelawofthesea.aspx>

16 Tanaka, Y. (2023). *The International Law of the Sea* (4th ed.). Cambridge: Cambridge University Press.

17 Ringbom H., Røsæg E., Solvang T., *Autonomous Ships and the Law* (IMLI Studies in International Maritime Law), (Routledge, 2020)

18 Ibid

19 Tanaka, Y. (2023). *The International Law of the Sea* (4th ed.). Cambridge: Cambridge University Press.

20 Caddell, Richard and Thomas, D.R. (Eds.) (2013). *Shipping, Law and the Marine Environment in the 21st Century: Emerging Challenges for the Law of the Sea - Legal Implications and Liabilities*. Lawtext Publishing Limited.

law reflects the fundamental tension between the freedom of navigation essential for international commerce and the sovereign rights of coastal states over adjacent waters. Unlike many other branches of international law that emerged from specific treaties or diplomatic conferences, the law of the sea evolved organically from customary practices of maritime nations, trade customs, and the practical necessities of regulating navigation, fishing, and maritime commerce. This evolutionary character distinguishes it from more recently codified areas of international law, as it represents centuries of accumulated state practice and *opinio juris* that have been subsequently codified and systematized through multilateral conventions, most notably the 1982.

Modern law of the sea, anchored by UNCLOS as the “constitution for the oceans,” balances sovereignty, cooperation, and maritime commons management.²¹ Contemporary scholarship reveals how foundational principles—like the ICJ’s maxim “The land dominates the sea”—are strained by emerging challenges, particularly sea-level rise threatening maritime boundaries.²² ²³The field’s dynamism is evidenced by ongoing scholarly engagement with climate impacts, delimitation disputes, and technological innovations, demonstrating international law’s capacity to adapt while preserving foundational norms.²⁴

3. CYBER THREATS TO MARITIME INFRASTRUCTURE AND THE MARINE ENVIRONMENT

The increasing reliance of the maritime sector on digital technologies and interconnected systems has significantly widened its vulnerability to sophisticated cyber threats. Critical components of maritime infrastructure – including ports, vessels, and offshore platforms – are now exposed to various forms of cyberattacks that can have severe economic, operational, and environmental consequences. Ports, which function as complex digital ecosystems, are especially at risk. Attacks targeting port IT infrastructure, such as terminal operating systems (TOS), customs databases, and cargo tracking systems, can result in operational paralysis and significant supply chain disruptions. For example, the 2020 ransomware attack on the Chinese shipping giant COSCO resulted in communication

21 See analytically P. Hoagland, J. Jacoby, M.E. Schumacher, *Law Of The Sea*, Editor(s): John H. Steele, Encyclopedia of Ocean Sciences, Academic Press, 2001, Pages 1481-1492, ISBN 9780122274305, <https://doi.org/10.1006/rwos.2001.0415>. <https://www.sciencedirect.com/science/article/pii/B012227430X004153>. Also see thestudentlawyer.com/2024/09/08/autonomous-vessels-and-maritime-law-bridging-the-gap-between-innovation-and-regulation/

22 Mara R Wendebourg, Interpreting the Law of the Sea in the Context of Sea-Level Rise: The Ambulatory Thesis and State Practice, *Journal of Environmental Law*, Volume 35, Issue 3, November 2023, Pages 499–507, <https://doi.org/10.1093/jel/eqad024>

23 U.S. Government Accountability Office. (2024). *Coast Guard: Autonomous Ships and Efforts to Regulate Them*. GAO-24-107059. Washington, D.C.: U.S. Government Accountability Office. Available at: <https://www.gao.gov/products/gao-24-107059>

24 Sun, K., Khan, M., Bibi, A., & Chang, Y.-C. (2025). New Frontiers in the Law of the Sea and Policy Integration. *Water*, 17(3), 444. <https://doi.org/10.3390/w17030444>. Also see New Technology, Equity and the Law of the Sea, <https://www.rifs-potsdam.de/en/blog/2021/09/new-technology-equity-and-law-sea>, Emerging Technology and the Law of the Sea Workshop at <https://www.wmu.se/news/emerging-technology-and-the-law-of-the-sea-workshop>. Also see Khaskheli, Muhammad & Wang, Shumin & Zhang, Xin & Shamsi, Imran & Shen, Chenghuan & Rasheed, Sanobar & Ibrahim, Zakir & Baloch, Dost. (2023). Technology advancement and international law in marine policy, challenges, solutions and future prospective. *Frontiers in Marine Science*. 10. 10.3389/fmars.2023.1258924. And <https://lawclimateatlas.org/resources/maritime-law-and-climate-change/>

outages and operational delays across several global terminals.²⁵

Ships, particularly those equipped with integrated bridge systems, automatic identification systems (AIS), and electronic chart display and information systems (ECDIS), are increasingly susceptible to manipulation. Notable threats include GPS spoofing and AIS manipulation, which can result in false positional data, leading to mis-navigation or collision. Reports of GPS interference in the Black Sea (2017) and the Persian Gulf (2019) highlight the strategic use of such techniques in geopolitically sensitive areas.²⁶ The vulnerability is further amplified in the context of autonomous and remotely operated vessels, which rely heavily on software systems, satellite communications, and artificial intelligence. As Ringbom argues²⁷, these vessels shift the burden of navigation and risk assessment from human seafarers to cyber-physical systems, thereby expanding the potential attack surface.

Furthermore, offshore platforms, such as oil and gas rigs and undersea cable nodes, represent another critical point of vulnerability. A successful cyber intrusion could compromise control systems, trigger environmental disasters, or halt energy production. According to the International Association of Oil & Gas Producers (IOGP), the blending of operational technology (OT) and information technology (IT) systems in offshore facilities creates a cyber risk environment where traditional firewalls and antivirus software are insufficient to threat mitigation.²⁸

Across these infrastructures, common attack vectors include phishing campaigns, ransomware deployment, malware injection via supply chain compromise, and exploitation of unpatched software vulnerabilities. The 2017 Not Petya malware attack that crippled Maersk's global IT network remains one of the most cited examples, causing estimated losses of over \$300 million and disrupting operations in more than 600 ports worldwide.²⁹ These incidents underline the urgent need to bolster cyber resilience in maritime systems and rethink existing risk management strategies to include the full spectrum of digital threats.

Building on the identification of potential cyber threats to ports, ships, and offshore platforms, it is essential to recognize that these threats extend beyond economic and operational disruption, posing significant risks to the marine environment. The integration of digital systems into maritime operations has increased the likelihood that a cyberattack could trigger environmentally damaging events, such as oil spills, chemical leaks, vessel collisions, or unauthorized discharge of pollutants. These outcomes not only violate international maritime safety and environmental standards but also threaten the ecological integrity of marine and coastal ecosystems.³⁰

One of the most concerning scenarios involves the manipulation of navigational systems through GPS spoofing or AIS data tampering. As previously discussed, ships reliant

25 ENISA. (2023). *Threat Landscape for the Maritime Sector*. European Union Agency for Cybersecurity.

26 Humphreys, T. E. (2017). *Statement on the Vulnerability of Civil GPS*. University of Texas at Austin, Radionavigation Laboratory.

27 Ringbom, H. (2019). *Regulating Autonomous Ships—Concepts, Challenges and Precedents*. *Ocean Development & International Law*, 50(2–3), 141–169.

28 IOGP. (2022). *Cybersecurity Guidelines for Upstream Oil and Gas Operations*. International Association of Oil & Gas Producers.

29 Kaspersky Lab. (2018). *NotPetya Report: Lessons Learned from the Maersk Breach*.

30 Simón, L., & Marqués, J. M. (2021). *Cybersecurity, Maritime Safety, and Environmental Protection: A Policy Trilemma*. *European Security*, 30(3), 444–466. <https://doi.org/10.1080/09662839.2021.1936227>

on automated positioning and routing systems are vulnerable to misdirection. A cyberattack that causes a vessel to run around or collide with another ship in an environmentally sensitive area could result in the release of hazardous substances, with devastating ecological consequences. This is not a hypothetical risk – GPS spoofing incidents reported in the Black Sea and Strait of Hormuz illustrate the plausibility of such scenarios.³¹

Similarly, offshore platforms and undersea infrastructure present a high-risk target due to their complex integration of operational technology (OT) systems. A cyber-induced failure in SCADA or pressure control systems could disable blowout preventers or safety valves, leading to uncontrolled hydrocarbon releases. As noted by Peterson et al.³², many offshore rigs still operate on legacy systems that lack modern cybersecurity defences, rendering them particularly susceptible to such attacks. In extreme cases, the environmental impact of a cyber-triggered incident could rival major disasters like the Deepwater Horizon spill, only with far less warning or opportunity for human intervention.

Port facilities also face environmental vulnerabilities from cyber intrusions. A cyberattack that disables monitoring systems for ballast water treatment, waste discharge, or hazardous cargo storage could result in violations of international regulations such as MARPOL (IMO, 1973/1978).³³ Moreover, the disruption of communications between environmental monitoring units and response teams during an incident can delay containment measures, exacerbating environmental harm and increasing the risk of legal liability. As maritime systems grow more automated and reliant on digital coordination, the environmental consequences of cyberattacks become more profound and multifaceted. Simón and Marqués³⁴ argue that cyber risks must be explicitly integrated into maritime environmental protection regimes, as the convergence of digital vulnerabilities with ecological hazards creates a complex regulatory challenge. This underscores the urgent need for international legal and policy frameworks that do not treat cybersecurity and environmental protection as separate domains, but rather as interdependent pillars of maritime governance in the digital age.

4. THE IMO MASS CODE AND CYBERSECURITY AT SEA: REGULATING AUTONOMOUS VESSELS IN AN ERA OF DIGITAL VULNERABILITIES

The deployment of autonomous vessels promises to reduce maritime accidents—notably human error, which contributes to ~75% of insurance losses—while enhancing operational efficiency. However, these advancements introduce novel vulnerabilities, termed collectively as ‘cyber risks’, encompassing software malfunctions, navigational failures, and cyber piracy,³⁵ defined by the IMO as threats compromising data or systems to precipitate

31 Goward, D. (2017). *GNSS Spoofing in the Black Sea: Test or Attack?* GPS World. <https://www.gpsworld.com>

32 Peterson, G., Clarke, R., & Kalil, T. (2020). *Cybersecurity of Offshore Oil and Gas Infrastructure: Challenges and Mitigation Strategies*. MITRE Corporation.

33 International Maritime Organization (IMO). (1973/1978). *International Convention for the Prevention of Pollution from Ships (MARPOL)*.

34 Simón, L., & Marqués, J. M. (2021). *Cybersecurity, Maritime Safety, and Environmental Protection: A Policy Trilemma*. *European Security*, 30(3), 444–466. <https://doi.org/10.1080/09662839.2021.1936227>

35 HC Burmeister et al., ‘Can unmanned ships improve navigational safety?’ (2014) Transport Research Arena <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.846.5385&rep=1&type=pdf> accessed 09/10/2018

safety/operational failures. Consequently, cybersecurity is a key component of the modern maritime industry, as the digitalization of ports and vessels creates new threats.³⁶ These vulnerabilities (e.g., software malfunctions, cyber piracy) fundamentally disrupt maritime law's anthropocentric foundations. Consequently, integrating autonomous cyber defense systems on ships will enable automatic detection and blocking of cyberattacks.³⁷ Artificial intelligence and machine learning will ensure constant monitoring of the ship's digital environment and the application of protective measures without human intervention.³⁸

The IMO has addressed these challenges through systematic institutional adaptation.³⁹ Beginning with a 2021 Regulatory Scoping Exercise (RSE) to assess existing treaties' applicability,⁴⁰ it developed a roadmap culminating in a goal-based MASS Code. Originally slated for 2024 adoption, the timeline was revised to accommodate regulatory complexity: a **non-mandatory Code** will enter force in 2025, transitioning to a mandatory instrument by 2028. This phased approach reflects the IMO's recognition that autonomous vessels require foundational legal innovation—not incremental adjustments—to reconcile emerging technologies with maritime safety frameworks.⁴¹

5. LEGAL GAPS AND REGULATORY CHALLENGES

The increasing exposure of maritime infrastructure to cyber threats has revealed significant gaps and inconsistencies in the existing international legal framework. Despite the rapid digitalization of the sector, the cornerstone of maritime law – the United Nations Convention on the Law of the Sea (UNCLOS) – offers no explicit provisions addressing cybersecurity. This legal void presents challenges across several key dimensions: attribution of cyberattacks, jurisdiction over digital incidents, enforcement mechanisms, and liability for environmental or economic damages.

First, attribution remains a central challenge. Cyberattacks are frequently conducted through anonymized networks or proxy actors, making it difficult to identify responsible parties with the confidence required under international law.⁴² When a ship is affected by GPS

36 Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cyber-security in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. *Lex Portus*, 11(1), 7–19. <https://doi.org/10.62821/lp11101>. Also see Neumann, T. (2024). Cybersecurity in maritime industry. *TransNav*, 18(4), 765–774. <https://doi.org/10.12716/1001.18.04.02>

37 Karim, Md Saiful (2022) Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, 143, Article number: 105138.

38 Chupkemi, D. C., & Mersinas, K. (2024). Challenges in Maritime Cybersecurity Training and Compliance. *Journal of Marine Science and Engineering*, 12(10), 1844. <https://doi.org/10.3390/jmse12101844>

39 See analytically at International Maritime Organization. (2018, May 23). IMO Doc. MSC/C 99/WP.9, Annex 1, para. 4. Also see Aldo Chircop, (2019) “Maritime Autonomous Surface Ships in International Law: New Challenges for the Regulation of International Navigation and Shipping” in Myron H Nordquist, John Norton Moore & Ronán Long, *Cooperation and Engagement in the Asia-Pacific Region* (Leiden: Brill) 18.

40 <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx>

41 Kouroupis, Konstantinos and Leonidas Sotiropoulos, „Cyber Challenges amid the Digital Revolution in Maritime Transport”, *Juridical Tribune - Review of Comparative and International Law* 14, no. 2 (June 2024): 321–340.

42 Pipyros, K. (2016). Legal and technical difficulties of attributing cyberattacks under international law. *Information & Computer Security*, 24(1), 108–123.

spoofing or a port suffers a ransomware attack, determining whether the perpetrator is a state actor, a criminal group, or an individual hacker is rarely straightforward.⁴³ This ambiguity impairs the ability of states to respond under established international legal doctrines such as the state responsibility of self-defense under Article 51 of the UN Charter.⁴⁴

Second, jurisdictional complexities further hinder effective legal responses, Cyberattacks can traverse multiple jurisdictions instantaneously, involving vessels flagged under one state, ports operated by another, and infrastructure or cloud services hosted in yet other territories. This fragmentation creates uncertainty regarding which state has the competence to investigate, prosecute, or demand reparations. The concept of flag state jurisdiction, traditionally robust in maritime law, becomes less effective when dealing with cross-border digital operations that may not involve any physical intrusion.⁴⁵

Third, there are significant enforcement challenges. The International Maritime Organization (IMO) has made notable strides through the issuance of the *Guidelines on Maritime Cyber Risk Management* and the development of the *Maritime Autonomous Surface Ships (MASS) code*.⁴⁶ However, these instruments are largely non-binding and rely on voluntary compliance. Furthermore, national implementation remains uneven, particularly among flag states with limited cybersecurity expertise or resources.⁴⁷

Finally, liability mechanisms and compensation procedures for maritime cyber incidents remain inadequately defined. Existing liability regimes, such as those established under the *International Convention on Civil Liability of Oil Pollution Damage (CLC)* or *MARPOL*, are centered on physical damage and pollution, with no clear provisions addressing cyber-induced harm. Consequently, victims of cyber incidents, whether they are port authorities, shipowners, or environmental entities, may find it difficult to seek compensation or hold perpetrators accountable under current maritime law.⁴⁸

6. EVALUATION OF THE LEGAL AND PRACTICAL CHALLENGES IN RESPONDING TO MARITIME CYBER INCIDENTS

As noted above, legal challenges in addressing maritime cyber incidents stem from jurisdictional ambiguities, fragmented regulatory frameworks, and liability attribution complexities. Existing international maritime law, primarily the United Nations Convention on the Law of the Sea (UNCLOS), lacks explicit provisions for cyber threats,⁴⁹ creating

43 Pipyros K, Thraskias C, Mitrou L, Gritzalis D, Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of the Tallinn Manual. *Computers & Security* 74:371-383

44 Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

45 Papagiannakis, K., & Apostolidis, K. (2022). *Flag State Jurisdiction in the Age of Cyber Threats: Reassessing Legal Boundaries*. *Journal of Maritime Law & Commerce*, 53(2), 145–171.

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

47 Chircop, A. (2021). *The IMO and Maritime Cybersecurity: Governance Challenges in the Age of Digital Threats*. *Ocean Yearbook*, 35, 219–241.

48 van Ginkel, B., & van der Voet, L. (2022). *Legal Remedies for Victims of Maritime Cyber Incidents: Gaps in International Liability Regimes*. *Netherlands International Law Review*, 69(1), 89–108.

49 Barney, S. M. (2001) "Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of cyberspace." *Naval Law Review*. Vol. 48.: 61., <https://www.diplomacy.edu/blog/law-sea-law-internet-inspiring-analogy/>

gaps in governing state responsibilities and victim redress.⁵⁰ For instance, incidents like Iranian GPS spoofing near the Strait of Hormuz blur jurisdictional lines—whether such acts constitute “use of force” or “interference with navigation” under UNCLOS remains contested. Similarly, attributing liability for attacks involving state-sponsored actors⁵¹ (e.g., Houthi cyber operations against Saudi ports) or third-party technology providers proves difficult, as current liability regimes prioritize physical damage over data compromise. Regulatory fragmentation exacerbates these issues; while the EU’s NIS Directive⁵² and IMO’s cybersecurity guidelines offer baseline standards, their non-binding nature and uneven adoption across flag states hinder cohesive legal enforcement.⁵³

Practical challenges arise from the maritime sector’s technical vulnerabilities, resource constraints, and coordination deficits. Legacy systems—exemplified by Maersk’s unsegmented IT infrastructure during NotPetya—remain pervasive, impeding rapid threat containment. Resource limitations, particularly among smaller operators, delay investments in advanced defenses like multi-factor authentication or system redundancy, leaving critical infrastructure exposed.⁵⁴ Coordinating incident response across stakeholders (e.g., shipowners, ports, insurers)⁵⁵ is further complicated by geopolitical tensions, as seen in the April 2024 global ransomware attack, where conflicting national protocols slowed information sharing. Moreover, evolving threats like AI-driven botnets (reported in Marlink’s 2024 data) outpace static defense strategies, demanding continuous adaptation.⁵⁶ Without harmonized international protocols and scalable public-private partnerships, the industry’s reactive posture risks perpetuating operational disruptions and safety hazards.

7. CONCLUSION

The digital transformation of the maritime sector has significantly improved operational efficiency, yet it has also exposed critical vulnerabilities to cyberattacks targeting ships, ports, and offshore infrastructure. This study has revealed that the existing international legal framework—particularly UNCLOS—is ill-equipped to address the unique challenges posed by cyber threats. Key issues include the lack of explicit legal provisions for cybersecurity, difficulties in attributing cyberattacks, jurisdictional fragmentation, and outdated liability regimes that do not account for data-related or environmental damages caused by cyber incidents. Although the IMO has taken steps

50 Jiménez, W. G., & Lodder, A. R. (2015). Analyzing approaches to internet jurisdiction based on a model of harbors and the high seas. *International Review of Law, Computers & Technology*, 29(2-3), 266-282

51 See Characteristically Sotiropoulos, L. (2024). *Geopolitics and maritime terrorism: Challenges and the legal complexities in the Red Sea*. XXI međunarodni naučni skup Pravnički dani - Prof. dr Slavko Carić, na temu: Odgovori pravne nauke na izazove savremenog društva - zbornik radova.

52 <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>, <https://www.hilldickinson.com/insights/articles/cyber-security-regulations-applicable-maritime-transport-sector>, <https://gtg.com.mt/cybersecurity-and-maritime-in-the-eu-technology-lawyers/>

53 <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>

54 Clavijo Mesa, M. V., & Patino-Rodriguez, C. E. (2024). *Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains*. MDPI.

55 Ingasio de la Peña Zarzuelo, I. (2021). *Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on This Issue*. Transport Policy, Elsevier.

56 <https://www.porttechnology.org/news/marlink-reports-increase-in-maritime-cyber-threats/>, <https://smartmaritimetwork.com/2025/05/21/ai-driven-maritime-cyber-threats-on-the-rise-report/>

through non-binding guidelines and the development of the MASS Code, enforcement remains inconsistent, and legal harmonization is lacking.

To address these challenges, this paper recommends a multi-pronged strategy for reforming international maritime governance. First, cybersecurity provisions should be codified either through a new protocol to UNCLOS or a standalone binding instrument addressing digital threats at sea. Second, international cooperation should focus on developing reliable attribution mechanisms and protocols to facilitate coordinated legal and technical responses. Third, the IMO should accelerate the transition of voluntary instruments—such as the MASS Code—into binding standards, coupled with a global compliance and reporting mechanism. Fourth, liability regimes must be updated to explicitly recognize cyber-induced harm, including data breaches, operational paralysis, and indirect environmental consequences. Additionally, capacity-building programs for developing maritime states and enhanced public-private collaboration are essential to ensure global resilience and equitable implementation of cyber safeguards.

Looking ahead, future research should focus on empirical mapping of maritime cyber incidents, comparative analyses of national legal frameworks, and the evolving role of AI and automation in maritime liability. Moreover, interdisciplinary studies are needed to assess the environmental implications of cyberattacks and to explore new cooperative models—such as cyber peacekeeping or regional cyber incident response frameworks—that can support the secure and sustainable governance of the maritime domain in the digital era.



Dr Kosmas Pipiros, vanredni profesor

Odeljenje za računarstvo Philips univerziteta, doktor nauka iz bezbednosti informacionih sistema (AUEB), master iz informacionih sistema (AUEB), diplomirani pravnik (AUTH)

Leonidas Sotiropoulos, doktorand

iz oblasti digitalizacije veštačke inteligencije i pomorskog prava na EUC, master iz pomorskog prava (Cardiff University), diplomirani pravnik (AUTH)

ZAKON MORA U DOBA SAJBER PRETNJI: ZAŠTITA POMORSKE INFRASTRUKTURE I MORSKOG OKRUŽENJA

Apstrakt:

Brza digitalizacija pomorskog sektora dovela je do značajnih ranjivosti morskog ekosistema. Sajber pretnje su postale ključni izazov za globalni pomorski saobraćaj, lučke operacije i priobalnu infrastrukturu. Preciznije rečeno, tehnološki napredak u lukama, plovilima, priobalnim platformama i sistemima za nadzor okeana povećao je rizike od sajbernapada, uključujući lažiranje GPS signala, ucenu putem zlonamernog softvera i preuzimanje sistema, budući da oni sve više zavise od međusobno povezanih tehnologija. Ovi rizici mogu dovesti do prekida međunarodne trgovine, ugrožavanja ljudskih života i

izazivanja značajne ekološke štete uključujući zagađenje iz kompromitovanih sistema ili izlivanja nafte. Uprkos ovim opasnostima, Konvencija Ujedinjenih Nacija o pravu mora (UNCLOS) ne sadrži posebne odredbe koje regulišu sajber-bezbednost, što dovodi do pravne praznine u oblasti pomorskog upravljanja. Polazeći od pravne analize i stvarnih incidenata, članak istražuje na koji način se trenutno međunarodno pravo može tumačiti ili prilagoditi kako bi se odgovorilo na sajber pretnje. Štaviše, naglašavanjem ograničenja u atribuciji, nadležnosti i sprovođenju, članak predlaže načine za uključivanje sajber-bezbednosti u širu agendu pomorske bezbednosti i zaštite životne sredine. Konačno, članak ocenjuje na koji način međunarodne organizacije – posebno Međunarodna pomorska organizacija (IMO) – mogu doprineti unapređenju zakonodavnih mera. Članak pruža predloge za modernizaciju pomorskog pravnog okvira radi obezbeđivanja otpornijih, bezbednijih i ekološki održivih okeana u digitalnom dobu, kroz analizu pravnih tekstova, aktuelnih sajber događaja i praksi upravljanja. Cilj je da se podstakne dijalog o modernizaciji međunarodnog pomorskog prava za digitalno doba.

Ključne reči: Međunarodno pomorsko pravo, kritična pomorska infrastruktura, sajber pretnje, atribucija i nadležnost, pomorsko upravljanje.

LIST OF REFERENCES

1. Barney, S. M. (2001). Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of cyberspace. *Naval Law Review*, 48, 61. <https://www.diplomacy.edu/blog/law-sea-law-internet-inspiring-analogy/>
2. Britannica. (2025). Rhodian Sea Law. *Encyclopedia Britannica*. <https://www.britannica.com/event/Rhodian-Sea-Law>
3. Caddell, R., & Thomas, D. R. (Eds.). (2013). *Shipping, Law and the Marine Environment in the 21st Century: Emerging Challenges for the Law of the Sea*. Lawtext Publishing Limited.
4. Chircop, A. (2021). The IMO and Maritime Cybersecurity: Governance Challenges in the Age of Digital Threats. *Ocean Yearbook*, 35, 219–241.
5. Chupkemi, D. C., & Mersinas, K. (2024). Challenges in Maritime Cybersecurity Training and Compliance. *Journal of Marine Science and Engineering*, 12(10), 1844. <https://doi.org/10.3390/jmse12101844>
6. ENISA. (2023). *Threat Landscape for the Maritime Sector*. European Union Agency for Cybersecurity.
7. Goward, D. (2017). GNSS Spoofing in the Black Sea: Test or Attack? *GPS World*. <https://www.gpsworld.com>
8. Humphreys, T. E. (2017). Statement on the Vulnerability of Civil GPS. *University of Texas at Austin, Radionavigation Laboratory*.
9. IMO. (2021). *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3). International Maritime Organization.
10. International Maritime Organization (IMO). (1973/1978). *International Convention for the Prevention of Pollution from Ships (MARPOL)*.
11. International Maritime Organization. (2025). United Nations Convention on the Law of the Sea. <https://www.imo.org/en/ourwork/legal/pages/unitednationsconventiononthelawofthesea.aspx>
12. IOGP. (2022). *Cybersecurity Guidelines for Upstream Oil and Gas Operations*. International Association of Oil & Gas Producers.
13. Jiménez, W. G., & Lodder, A. R. (2015). Analyzing approaches to internet jurisdiction

- based on a model of harbors and the high seas. *International Review of Law, Computers & Technology*, 29(2–3), 266–282.
14. Kaspersky Lab. (2018). *NotPetya Report: Lessons Learned from the Maersk Breach*.
 15. Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, 143, Article 105138.
 16. Kouroupis, K., & Sotiropoulos, L. (2024). Cyber Challenges amid the Digital Revolution in Maritime Transport. *Juridical Tribune – Review of Comparative and International Law*, 14(2), 321–340.
 17. Kraska, J. (2015). The Law of the Sea Convention: A National Security Success—Global Strategic Mobility Through the Rule of Law. *Harvard National Security Journal*, 6, 1–46.
 18. Lloyd's List. (2022). *Cyber Risks in Shipping: An Evolving Threat*.
 19. Maintenance and Cure. (2024). The Intriguing History of Maritime Law. <https://maintenanceandcure.com/maritime-blog/the-intriguing-history-of-maritime-law/>
 20. Marlink. (2024). *Cyber Threat Intelligence Brief: Maritime Sector Trends*. Marlink Maritime Cybersecurity Division.
 21. Melnyk, O., Drozdov, O., & Kuznichenko, S. (2025). Cyber-security in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures. *Lex Portus*, 11(1), 7–19. <https://doi.org/10.62821/lp11101>
 22. Neumann, T. (2024). Cybersecurity in Maritime Industry. *TransNav*, 18(4), 765–774. <https://doi.org/10.12716/1001.18.04.02>
 23. OECD. (2022). *Cybersecurity in Critical Infrastructure: Policy Gaps and Governance Needs*. Organisation for Economic Co-operation and Development.
 24. Papagiannakis, K., & Apostolidis, K. (2022). Flag State Jurisdiction in the Age of Cyber Threats: Reassessing Legal Boundaries. *Journal of Maritime Law & Commerce*, 53(2), 145–171.
 25. Peterson, G., Clarke, R., & Kalil, T. (2020). *Cybersecurity of Offshore Oil and Gas Infrastructure: Challenges and Mitigation Strategies*. MITRE Corporation.
 26. Pipyros, K. (2016). Legal and technical difficulties of attributing cyberattacks under international law. *Information & Computer Security*, 24(1), 108–123. <https://doi.org/10.1108/ICS-12-2014-0081>
 27. Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security*, 74, 371–383. <https://doi.org/10.1016/j.cose.2017.03.004>
 28. Ringbom, H. (2019). Regulating Autonomous Ships—Concepts, Challenges and Precedents. *Ocean Development & International Law*, 50(2–3), 141–169.
 29. Ringbom, H., Røsæg, E., & Solvang, T. (2020). *Autonomous Ships and the Law* (IMLI Studies in International Maritime Law). Routledge.
 30. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
 31. Simón, L., & Marqués, J. M. (2021). Cybersecurity, Maritime Safety, and Environmental Protection: A Policy Trilemma. *European Security*, 30(3), 444–466. <https://doi.org/10.1080/09662839.2021.1936227>
 32. Sun, K., Khan, M., Bibi, A., & Chang, Y.-C. (2025). New Frontiers in the Law of the Sea and Policy Integration. *Water*, 17(3), 444. <https://doi.org/10.3390/w17030444>
 33. Tanaka, Y. (2023). *The International Law of the Sea* (4th ed.). Cambridge University Press.
 34. Tamada, D., & Zou, K. (Eds.). (2021). *Implementation of the United Nations Convention on the Law of the Sea: State Practice of China and Japan*. Springer.
 35. U.S. Government Accountability Office. (2024). *Coast Guard: Autonomous Ships and Efforts to Regulate Them* (GAO-24-107059). <https://www.gao.gov/products/gao-24-107059>

107059

36. UNCTAD. (2023). *Review of Maritime Transport 2023*. United Nations Conference on Trade and Development.
37. Wendebourg, M. R. (2023). Interpreting the Law of the Sea in the Context of Sea-Level Rise: The Ambulatory Thesis and State Practice. *Journal of Environmental Law*, 35(3), 499–507. <https://doi.org/10.1093/jel/eqad024>