**Vilnius University**

**Faculty of law**

**Department of private law**

Omar Ejjadghi,

II study year, LL.M International and European Law Programme Student

**Master's Thesis work**

# Technology and the Law of the Sea: Maritime Safety and Security

# Technologijos jūroje ir jūrų teisė: jūrų saugumas ir saugumas (apsauga)

Supervisor Assoc. Prof. dr. Indrė Isokaitė-Valužė

Reviewer: Assoc. Prof. Dr Skirgailė Žalimienė

Vilnius

2025

# Abstract

This thesis examines the overlaps between technology and maritime 1982 law, in particular, how emerging technologies (autonomous ships and cybersecurity) can threaten maritime safety and security. With the swift technological advancements in the maritime industry, the current international legal frameworks and, in particular, the United Nations Convention on the 1982 Law of the Sea (UNCLOS) and the Safety of Life at Sea (SOLAS) Convention are under pressure to amend in tackling new risks and gaps in the laws. The study presents a qualitative approach, which includes a doctrinal legal study, case study, secondary sources, such as scholarly articles and legal documents, to evaluate the present conditions of maritime 1982 Law regarding the technological progress. The results demonstrate that although technology has a potential to enhance the maritime safety and efficiency of operations, it brings about serious legal issues, especially on the areas of jurisdiction, liability, and cybersecurity. The paper presents the case of international maritime law reform to include autonomous vessels, counteract cyber threats, and provide equal access to technology in the maritime industry to every country, especially small island developing states. Finally, the thesis is that the maritime 1982 Law needs to adapt to changes introduced by technological advancement, and it is suggested to formulate new 1982 Law and international collaboration to protect the maritime trade and security in the 21st century.



***Keywords***: Maritime 1982 Law, Technology, Autonomous Ships, Cybersecurity, UNCLOS, Maritime Safety, Emerging Technologies, International Law.

# Table of Contents

# LIST OF ABBREVIATIONS

UNCLOS: United Nations Convention on the Law of the Sea

SOLAS: the International Convention for the Safety of Life at Sea

IMO: the International Maritime Organization

MARPOL: International Convention for the Prevention of Pollution from Ships

ITLOS: International Tribunal of Law of the Sea

ICJ: International Court of Justice

EEZ: Exclusive Economic Zone

SIDS: Small Island Developing States

UCH : Underwater Cultural Heritage

UNESCO : United Nations Educational, Scientific and Cultural Organization

ASEAN : Association of Southeast Asian Nations

EU :European Union

AIS: Automatic Identification System

ISM: International Safety Management Code

ISPS: International Ship and Port Facility Security Code

SDGs: Sustainable Development Goals

NOG : National Oil and Gas

MEPC : Marine Environment Protection Committee (IMO)

MCDM : Multi-Criteria Decision-Making

ETS : Emissions Trading System

PRISMA : Preferred Reporting Items for Systematic Reviews and Meta-Analyses

UNFCCC : United Nations Framework Convention on Climate Change

MASS : Maritime Autonomous Surface Ships

ECDIS : Electronic Chart Display and Information System

GPS: Global Positioning System

MSC-FAL : Maritime Safety Committee – Facilitation Committee (IMO)

GMDSS : Global Maritime Distress and Safety System

PSC : Port State Control

STCW : Standards of Training, Certification and Watchkeeping for Seafarers

VTS :Vessel Traffic Services

SAR : Search and Rescue

BWMC : Ballast Water Management Convention

UUV : Unmanned Underwater Vehicle

UN: United Nations.

# Introduction

The investigation of the interaction between technology and maritime 1982 Law is critical in the way legal frameworks can keep up with the fast changing maritime safety and security. The current maritime laws are not usually prepared to deal with new technology that is currently being embraced in the maritime industry such as automated ships and better navigation systems. The thesis explores how technology has brought about new avenues of improving the safety of the maritime industry, yet, it presents a major challenge to the maritime 1982 Law and other international conventions such as the United Nations Convention on the 1982 Law of the Sea (UNCLOS). As autonomous ships and digital systems increasingly have a larger role in shipping, there is an increased urgency to have new legal frameworks. The adoption of autonomous ship and other technological inventions is a critical element of safeguarding the continuity of the field of operation and still remain within the scope of the 1982 Law. The current subject is very topical because the adaptation of technology to the legal framework is related to international trade, maritime security, and environmental protection.

**Motives to Select the Topic:** The alternative reasons are that the current legal frameworks regulating the maritime safety and security are facing a serious challenge due to the rapid development of technology in the maritime industry and the emergence of autonomous ships and the growing reliance on digital systems. The rationale of selecting the topic is to comprehend how the international maritime 1982 Law, and specifically, UNCLOS and SOLAS will be able to adjust to these technological shifts and tackle the newly arising risks, i.e., cyberattacks and liability issues associated with autonomous ships.

***Novelty**:* In this thesis, the intersection between maritime 1982 Law and technological innovation will be examined with a comparatively scant studied risk on how the international legal frameworks will have to adapt to emerging maritime technologies. It is new in the treatment of the legal aspects of autonomous ships, cyber threats, unequal ability of small islands states to integrate the technologies into their maritime security systems. With the help of such technological issues, the research presents a new approach to the necessity of legal reform.

**Significance to Theory and Practice:** This study is very important to both theoretical and practical arenas. Conceptually, it questions the conventional maritime legal theories by trying to

understand the disruptive capacity of the emerging technologies in as far as the legal norms on sovereignty and jurisdiction are concerned. In practice, the research offers practical guidance to such international agencies as the IMO to create more effective legal and regulatory frameworks to integrate autonomous technologies and achieve maritime cybersecurity. This is imperative to protect global maritime trade as well as provide fair access to maritime technologies by all countries.

***Problem Statement**:* The rapid advancement of technology in the maritime industry presents significant challenges for existing maritime law frameworks, particularly in terms of ensuring safety and security. Emerging technologies such as autonomous ships and maritime cybersecurity require updated legal regulations to address new risks and opportunities. This research seeks to explore how maritime law can adapt to these technological changes.

***Object**:* The object is to analyze the impact of emerging technologies on maritime safety and security and explore how international legal frameworks can adapt to address these technological changes.

***Aim**:* To analyze the impact of emerging technologies on maritime safety and security, and how legal frameworks can evolve to address these changes.

**Objectives:**

- To analyse the theoretical and legal foundations of UNCLOS 1982, SOLAS and MARPOL in relation to maritime safety and security.
- To examine the legal implications of cybersecurity risks in the maritime domain, focusing on attribution, jurisdiction and liability under UNCLOS, SOLAS and MARPOL.
- To assess, through a case study of critical maritime infrastructure in the Baltic Sea, how hybrid threats and emerging technologies expose gaps in UNCLOS, SOLAS and MARPOL, and to propose targeted legal and policy reforms.

***Research Methodology**:* The paper applies the doctrinal legal analysis in the interpretation of UNCLOS, SOLAS and MARPOL, and the instruments of soft-law that inform the reaction to new technological dangers. It examines the text, form and technique of treaties on how far these regimes go in dealing with hybrid and cyber threats. An example of the Baltic Sea is provided in order to connect the rules that are in law with actual accidents that happened with pipelines and

communication cables. This assists in observing practical gaps that might not be observed by doctrinal analysis. The analysis is backed by qualitative sources like academic literature, expert reports and state practice. Analogy guidance by analogy relevant decisions by ICJ, ITLOS and arbitral tribunals are needed where there are no direct cyber cases. Technical security reports are included to describe the way cyber and hybrid attacks take place in practice. Accuracy, transparency and use of sources are the means of upholding ethical research practice.

The method of research used In this thesis is a doctrinal legal analysis, which is coupled with a case study. It is possible to conduct an in-depth analysis of the applicable legal documents with the help of this approach: the United Nations Convention on the Law of the Sea (UNCLOS), the Safety of Life at Sea (SOLAS) Convention, and the International Convention for the Prevention of Pollution by Ships (MARPOL). The secondary sources, including research articles, legal conventions, and reports by experts, will be reviewed to understand the possible ways to use the existing legal frameworks to handle the challenges presented by new technologies in the maritime industry. The example of the Baltic Sea case study will provide a practical example of how the hybrid threats and technological progress have revealed gaps in these international conventions and hence allows a discussion on the required legal amendments.

- The nexus between technology and maritime law has been the subject of some of the most prominent researchers in the discipline. Professors like David M. Ong and Clive R. Symmons have made a lot of contribution to the concept of the applicability of international maritime law to technological innovations. Also, other publications like The Journal of Maritime Law and Commerce and Marine Policy have constantly tackled the subject matter of cybersecurity in maritime operations, autonomous vessels and their consequences to international law. The works are the theoretical basis of this thesis as they reveal the gaps in the existing legal frameworks and the necessity of reform to the current technological development in the maritime industry.

# 1. Technology and the Evolution of the Law of the Sea and Maritime Safety

## 1.1 Historical development of the Law of the Sea

In order to track the history of development of the international law of the sea and especially, the changing legal demarcations of what has been customary practice and what has been codified in international agreements, Jia[1] undertook an extensive historical-legal analysis. The paper used a doctrinal approach that traced milestones of the era in which the mare liberum principle was developed, the controversies of the 20th century concerning the territorial waters, and the negotiations that resulted in the formulation of UNCLOS. Author held that the law of the sea has in recent times taken on a more universalistic and cooperative approach yet that vestiges of colonial legal systems continue to play a role in the resolution of a maritime boundary claim and a resource claim. One of the strengths of the research is that it is both a subtle examination of the texts of laws and a political environment in which they were created, which relies not so much on description and more on interpretation. The analysis was however Eurocentric whereby attention was more paid to the European maritime powers without considering the views of the emerging maritime countries equally. In addition, the paper failed to address the technological factors including sonar mapping or satellite surveillance that have altered maritime claims in the last few decades[2]. However, the work by Author provided a critical background on the history of the construction of the maritime law and the fact that the political context influences the development of international legal norms. It is especially helpful to your thesis, which aims to find out how the traditional frameworks react (or not) to the current technological changes. InRothwell and Stephens[3], the history of the international law of the sea was elaborately discussed in the form of a textbook, which follows the historical path of the development of the customary law of the sea up to the codification of the UNCLOS in 1982[4]. They employed a doctrinal method to examine the treaties, state practice, and case law of the ICJ to demonstrate how the concept of maritime zones (territorial sea, EEZ, continental shelf) has changed throughout the years in response to

[1] Jia, Bing Bing. "The Principle of the Domination of the Land over the Sea: A Historical Perspective on the Adaptability of the Law of the Sea to New Challenges." *German YB Int'l L.* 57 (2014):pp 63.
[2] Durmuş, Aybüke Naz. "The Intersection Between Law and Technology in Maritime Law." In *The regulation of automated and autonomous transport*, pp. 110. Cham: Springer International Publishing, 2023:pp 2
[3] Rothwell, Donald R., and Tim Stephens. "The international law of the sea." (2023): pp600.
[4] Islam, Md Syful. "Maritime security in a technological era: Addressing challenges in balancing technology and ethics." *Mersin University Journal of Maritime Faculty* 6, no. 1 (2024): pp15

changing geopolitical and economic interests. Their results brought out the malleable but stabilising character of maritime law wherein principles like freedom of navigation and exclusive economic jurisdiction were slowly balanced. One of the strengths of the work is its systematic structure, which is appropriate to both the academic and the policy readers. Nevertheless, the focus on the history of legal development is done in the work without an equal consideration of the role of emerging technologies and regional differences in accessing tools of maritime governance. More importantly, Rothwell and Stephens did not provide much empirical data on how smaller maritime states (especially SIDS) engaged in the process of influence on the legal framework. The book is legally strict but it presupposes a playing field in negotiations on treaties, which has been challenged in the modern critiques. In your research, this is critical writing in describing the legal framework of the maritime law and putting it in context on how it has developed before the present technology-related issues[5].

Lee[6]provided an account of the history of England in terms of its maritime claims and the progressive development of the notion of territorial waters. The analysis was based on historical-legal documents, state proclamations and naval records to follow the way the English claims over the seas influenced more general interpretations of law of sovereignty and freedom of navigation. Fulton claimed that the assertions of dominion over the seas as early as in England did not merely precede the modern international law but actually shaped the later legal constructs especially in the face of empire and resource control. The advantage of the work is in its careful references to the historical documents, providing a unique glimpse into the pre-UNCLOS history of the development of the state practice in the maritime sovereignty. Nonetheless, its weakness lies in the fact that it lacked comparative analysis it was a detailed description of the legal history of Britain, and it was not placed in the wider global or postcolonial context. Critically, the work by Fulton[7] assists in explaining the causes of legal asymmetry in the governance of the sea wherein the terms were historically dictated by the powerful states. This thesis will find this perspective useful in demonstrating how the existing maritime law should be re-considered in the context of historic

[5] Kraska, James, and Young-Kil Park, eds. *Emerging Technology and the Law of the Sea*. Cambridge University Press, 2022:pp 4

[6] Lee, Seokwoo. "Evolution of the law of the sea and ocean policy in northeast Asia." *Ocean Development & International Law* 55, no. 4 (2024): pp510.

[7] Fulton, Thomas Wemyss. *The sovereignty of the sea: an historical account of the claims of England to the dominion of the British seas, and of the evolution of the territorial waters*. DigiCat, 2022: pp4.

unequal distribution of power, especially when considering the norms when applied to new technological areas, including autonomous shipping and digital surveillance has given a doctrinal and theoretical study of the historical underpinnings of the law of the sea and its change into a comprehensive regulator regime with the UNCLOS. His work took a conventional approach to international law, which was complemented by interpretative comments on treaty text and landmark decisions of the ICJ. Tanaka came to the conclusion that UNCLOS is a dynamic compromise between the rights of coastal states and global commons due to historical debates on the navigation, exploitation of resources and territoriality[8]. One of the strongest aspects of this work is that the researcher establishes a clear explanation on how the legal categories, including passage innocent, archipelagic waters, and entitlement of continential shelf, were developed through history. Nonetheless, the work is weak in its coverage of non-state actors and technological innovations, which are both becoming more significant in the contemporary maritime conflicts. Moreover, Tanaka was more inclined to present UNCLOS as a fairly predictable legal system, which minimized its own internal disputes and slowness to adapt to new realities like climate-induced migration or AI-induced navigation. However, regarding your study, Tanaka contributes to the historical development of maritime regions and legal rights, which can be discussed as a catapult to consider how these structures are being pushed to the limit by the 21 st century innovations.

Stratē[9] paid attention to the issue of protecting underwater cultural heritage (UCH) as a new goal in the context of the evolution of the law of the sea in history. Using both the analysis of law as an interpretation and policy, Strati followed the development of the early ideas of res nullius and salvage law as normative frameworks that are currently intended to avoid exploiting and destroying the underwater heritage. The research observed that the UCH has been gradually identified under international law, either by means of the UNESCO Convention on the Protection of the Underwater Cultural Heritage, but to a very limited extent which is not very well incorporated with UNCLOS [10] . One of the strengths connected with this paper is its

[8] Moreno, F. Crestelo, J. Roca Gonzalez, J. Suardíaz Muro, and JA García Maza. "Relationship between human factors and a safe performance of vessel traffic service operators: A systematic qualitative-based review in maritime safety." *Safety science* 155 (2022): 105892.
[9] Strati, Anastasia. *The protection of the underwater cultural heritage: an emerging objective of the contemporary law of the sea*. Vol. 23. Brill, 2021:pp 6
[10] Dirhamsyah, Dirham, Saiful Umam, and Zainal Arifin. "Maritime law enforcement: Indonesia's experience against illegal fishing." *Ocean & Coastal Management* 229 (2022): 106304.

interdisciplinary approach, which combines the legal theory with the issues of culture and archeology. Nevertheless, the research was more of normative potential rather than enforcement reality and it paid little attention to technological advancement e.g. remote operated vehicles[11] (ROVs) and digital maps that not only facilitate protection of underwater sites but also complicate. Critically, in her work Strati shows how the history of the evolution of maritime law has often been slow in keeping pace with new challenges, and how the soft law processes might not be adequate in risky maritime areas. This holds more so to your thesis, where you are attempting to study the interplay of new technologies and the legal systems that already have been established-in fact[12], one can show that the law of the sea has already been forced to change numerous times in reaction to external innovations[13].

## 1.2. Legal framework of Law of the Sea and Maritime Security

### 1.2.1. UNCLOS (United Nations Convention on the Law of the Sea)

Karski[14] examined the circumstances of the UNCLOS provisions as it relates to living marine resources with reference to Articles 61 to 73, which regulate conservation, management, and utilisation of marine species in Exclusive Economic Zones (EEZs). The paper also performed a policy analysis approach to examine the U.S. legislative stance, regional fisheries agreements and the issues of implementation of straddling and highly migratory fish stocks. The results showed that although UNCLOS offers a well-defined legal framework of resources distribution and protection, its application has been uneven as some states show laxity in the implementation and inconsistency of compliance[15]. The paper is strong because it provides a legal dissection of the articles on living resources and puts it into the context of U.S. policy discussions. It was however lacking a comparative study with the developing coastal states or extended the scope of matters to include marine biodiversity outside the national jurisdiction. Most importantly, the paper highlights the legal shortcomings of UNCLOS to address the contemporary challenges to the

[11] Coito, Joel. "Maritime autonomous surface ships: New possibilities—and challenges—in ocean law and policy." *International Law Studies* 97, no. 1 (2021): pp19.
[12] Vio, Igor, and Mate Brdar. "Maritime autonomous surface ships–international and national legal framework." *Pomorski zbornik* 62, no. 1 (2022):pp 145.
[13] Issa, Mohamad, Adrian Ilinca, Hussein Ibrahim, and Patrick Rizk. "Maritime autonomous surface ships: Problems and challenges facing the regulatory process." *Sustainability* 14, no. 23 (2022): 15630.
[14] Kamiński, Tomasz, and Karol Karski. *40 Years of the United Nations Convention on the Law of the Sea: Assessment and Prospects*. Taylor & Francis, 2025:pp2.
[15] Karim, Md Saiful. "Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?." *Marine Policy* 143 (2022): 105138.

marine ecosystems- including climatic-driven changes in fish stocks and exploitation that are unsustainable. In this thesis, it is an important insight to note that UNCLOS is a piece of text that is detailed in the area of law, but its usefulness is destroyed by geopolitical hesitation and the lack of environmental predictability. A volume was the first to explore UNCLOS as a regulatory regime, providing input in several areas, such as maritime zones, dispute settlement mechanisms, marine environmental protection and the jurisdiction of the flag state. The volume employed a methodology of doctrinal and comparative approach throughout its chapters, including the EU maritime policy, the Arctic governance, and digital surveillance in navigation. The aggregation of the findings led to the conclusion that UNCLOS was a sustainable yet steadily stretched system that was not always useful in the context of responding to technological developments and evolving maritime challenges. This is the strength of the book because it is a comprehensive resource and up to date in its legal commentary which makes it a good reference to areas where law reform is long overdue. However, its drawback is that its empirical support is not evenly distributed within the chapters, some authors have heavily used hypothetical examples without involving case law or practice. More importantly, this book supplements this thesis by demonstrating that UNCLOS is a framework that requires active modification, particularly when it comes to cyber threats, autonomous shipping, and changing environmental pressures.

Wam[16] supported the expansion of UNCLOS so that it includes an obligatory collaboration on the topic of the loss and damage of the climate in marine territories. On the legal basis of reasoning and interpretation of the Article 192 (protection and preservation of the marine environment) Wam suggested normative extension of the duties of the state, particularly to high-emission countries whose activities are indirectly influencing the state in the position of the vulnerable coastlines and islands. The strength of the study is that it has explicitly defined climate justice as it is presented in the current UNCLOS framework and that it employs international environmental law principles. The shortcoming though is the lack of procedural guidelines on ways such obligations may be enforced and adjudicated[17]. Another important aspect of work that was not given due consideration was the opposition of major maritime powers to extend their UNCLOS responsibilities. More

[16] Wam, Rachel. "Climate Change Loss and Damage: A Case for Mandatory Cooperation and Contribution under the United Nations Convention of the Law of the Sea (UNCLOS)." *UCLA J. Env't L. & Pol'y* 42 (2024):pp 47.
[17] Melnyk, Oleksiy, Svitlana Onyshchenko, Oleg Onishchenko, Oleh Lohinov, Valentyna Ocheretna, and Yurii Dovidenko. "Basic aspects ensuring shipping safety." *Zeszyty Naukowe. Transport/Politechnika Śląska* 117 (2022): pp146.

importantly, the proposal by Warm added a prospective aspect to your thesis, because it sees UNCLOS not as a legal framework but as an evolving tool that needs to be revised to accommodate non-traditional maritime threats like sea-level rise, biodiversity loss and acidification. A conceptual analysis found that the UNCLOS is based on the prevailing paradigm of state-centric realism, where the emphasis on sovereignty and control of resources over the shared environmental responsibility stands out. The authors employed the interpretative approach to the study which is based on the critical international legal theory to state that UNCLOS, despite being promoted as a universal treaty, contributes to the promotion of global inequality, by maintaining maritime hierarchy. This paper is a critical lens and its strength is its ability to point out how legal structures replicate power imbalances in the name of being neutral. It has drawbacks in the absence of empirical case studies to justify the theoretical assertions and little attention to the way the paradigms can be applied to day-to-day maritime enforcement. However, it is this paper which will give your thesis the ideological critique it deserves, and alert readers to the fact that legal texts are not apolitical and need to be reconsidered regarding the new equity issues, especially those which are brought about by technological and environmental changes[18].

Another study [19] traced the connection between UNCLOS and the International Maritime Organization (IMO) throughout a 40-year period of working side by side. Using a doctrinal-legal approach towards institutional requirements and tools, the research came up with a conclusion that, irrespective of their complementary purposes, overlapping jurisdictions between the UNCLOS and IMO have resulted in a piecemeal governance of issues such as maritime safety, ship-source pollution and compliance measures[20]. The advantages of this analysis are that it focuses on the practice of realistic conflicts between treaty institutions and specialised agencies and provides some insight into the duplication and inconsistency of regulations. The major limitation though is that, there are no detailed case laws or examples of such fragmentation by states that have resulted in a legal uncertainty. More to the point, this work contributes to your thesis statement by defining one of the most important legal challenges in realising technological innovation in the context of

[18] Qasim, Nameer Hashim, Hayder Imran Al-Helli, Iryna Savelieva, and Aqeel Mahmood Jawad. "Modern Ships and the Integration of Drones–a New Era for Marine Communication." *Розвиток транспорту* 4 (2023):pp 60.
[19] Musyaffa, Nadhif Fadhlan, Arie Kusuma Paksi, and Lalu Radi Myarta. "Measuring the dominant paradigma in United Nations Convention on the Law of the Sea." *Lampung Journal of International Law* 4, no. 2 (2022): pp90.
[20] Freestone, David, ed. *The 1982 Law of the Sea Convention at 30: Successes, challenges and new agendas*. Martinus Nijhoff Publishers, 2013: pp10.

maritime law—that is, the challenge of adapting the high-level legal set-up of the UNCLOS to specialised and technologically fast-evolving technical standards generated by various agencies in the maritime industry, such as IMO. Author provided a reflective analysis of UNCLOS during its 40 th anniversary, its strengths, controversies that remain unresolved, and the future. The authors applied legal-historical analysis to analyze the main areas, including deep-sea mining, delimiting of maritime boundaries, and environmental protection[21]. They found that, although UNCLOS has established a legal order on governance of the ocean, it is not very specific in some of its provisions (e.g. Article 82 on payment in the continental shelf greater than 200 nautical miles) and responsive to novel challenges. One of the biggest strengths of this book is that it attempts to contextualise UNCLOS in the context of the significant geopolitical changes taking place in the world and reflects the more recent maritime issues, including the question of Arctic routes and the blue economy concept. Yet, the study failed to make systematic suggestions on how to treaties or institutions should be strengthened. Critically, the paper demonstrates that UNCLOS was radical back in 1982, but it currently provides its services at the cost of diminishing relevancy. This supports this thesis statement that legal frameworks have to change – not necessarily to act as a constant reference point – particularly in a maritime context dominated by AI, automation, and climate change.

Lost-Siemińska, Dorota[22] examined how the state implements the UNCLOS practically and used a comparative legal study as a method to discuss other jurisdictions, such as China, the EU, and the ASEAN countries. Their paper was based on interpretation of treaties and national law mapping to evaluate the extent of domestication of UNCLOS, especially on such aspects as port state control, marine scientific research and environmental monitoring. Their findings showed that there is an uneven implementation by political goodwill, economic and administrative facilities. The empirical basis and the scope of the study is its strength, as it enables drawing a refined image of the strengths and weaknesses of UNCLOS. Nonetheless, it did not move deeply into exploring the ways in which emerging technologies, like satellite surveillance or autonomous vessels are threatening the compliance paradigms. Critically speaking, the paper brings to the fore an

[21] Bueger, Christian, and Tobias Liebetrau. "Critical maritime infrastructure protection: What's the trouble?." *Marine policy* 155 (2023): 105772

[22] Lost-Siemińska, Dorota. "The United Nations Convention on the Law of the Sea and the International Maritime Organization–40 years of harmonious coexistence." *Prawo Morskie* (2022): pp20.

important theme of this thesis: the uniformity of law on paper does not necessarily translate into uniformity in practice, particularly when technology is advancing at a faster rate than legal change on a national level. Author studied how UNCLOS is used in ensuring that the foreign ships that sail through Indonesian territorial seas are regulated. Through the analysis of doctrinal and case laws, the study has shown how Indonesia is utilizing its legal flexibility offered under the provisions of UNCLOS-particularly on archipelagic sea lanes and innocent passage- as a means to strengthen its sovereignty as a nation and its maritime surveillance. The main advantage is attention to a particular legal mechanism and practical application as a domestic law and in the naval enforcement. Nevertheless, the research did not take into account the issue of whether these methods of enforcement meet the wider international legal standards or the perception by the foreign states of these strategies. It had also not been involved with the technological features like digital identification or AIS tracking. Most importantly, the research by Farhan explains that UNCLOS enables such a strategic interpretation of the national level that may or may not be in line with the stability of international law in general. In this thesis, it is taken as a case example in the way that legal discretion without control, may be even more complicated by automated navigation and machine decision-making in national waters.

Another study[23] gave a retrospective legal reflection on UNCLOS after 40 years of use, addressing its structural strength and constraints by commenting on the doctrine. It claimed in the research that UNCLOS is the constitution of the seas, but it is becoming stretched due to elements that were not anticipated at its inception, such as marine biodiversity beyond national jurisdiction, control of underwater cables and threats of cyber-attacks. One of the strongest points of the paper is that it cautiously traces on how UNCLOS has ensured legal continuity in the face of such dramatic geopolitical developments. Its weakness, however, is that it is dependent on the text of the law rather than its practical implementation or even technology. The argument is that, although UNCLOS has established solid bases, it has to be enhanced and enforced further with later instruments, particularly in addressing cross-sectoral concerns such as cybersecurity or satellite monitoring. In this thesis, this paper reinforces the opinion that legal frameworks should not only change in terms of wording but also in terms of scope and interconnectivity with other world regimes. In this article it is examined that the UNCLOS has been applied in the archipelagic

[23] Tamada, Dai, and Keyuan Zou. *Implementation of the United Nations Convention on the Law of the Sea*. Springer Singapore, 2021:pp 25.

situation of the Aegean Sea in connection with the maritime boundary issue, the right to passage, and the question of overarching sovereignty. The work revealed the legal-geopolitical analysis of how the concepts of equidistance and historic rights in the UNCLOS were applied differently by Greece and Turkey, which leads to the current tension between the two countries. The quality of the study Is that it uses abstract provisions of law to a very sensitive geopolitical scenario thus showing the difficulties of legal uniformity in a complex regional context. It however concentrated more on legalist arguments without incorporating the technological aspects like the application of digital cartography or remote sensing in the maritime delimitation. More importantly, this paper demonstrates that even in their comprehensive nature, legal provisions are not always accurate or apolitical enough to solve ingrained conflict. In this thesis, it brings out the shortcomings of UNCLOS in the instances where law borders with geopolitics and in the instances where technology may provide the instruments of transparency and dispute resolution in case legal frameworks were tailored to suit it.

### 1.2.2. SOLAS (Safety of Life at Sea convention)

Armstrong[24] discussed the structural connection of the SOLAS Convention with a number of IMO codes including the ISM Code and the ISPS Code, and used a normative legal analysis along with the comparison of policies. They indicated that although SOLAS forms the framework of maritime safety regulation, it would only be effective with the proper integration and enforcement of the codes concerned by flag and port states. One of the strongest points of this work is that it has a comprehensive insight into the functioning of layered regulatory frameworks which is taken to achieve operational safety, mitigation of risk, and environmental protection. Nevertheless, the research was based more on theoretical explanation and failed to provide any empirical case studies that can prove the practical difficulties of these interrelations application in the real maritime operations. This also is advantageous to this work because it highlights the interdependency of the back-office treaties such as the SOLAS and the more dynamic regulatory apparatus that is being developed by the IMO, particularly to these new shipping risks and the complexity of technologies.

[24] Armstrong, Chris. "The United Nations Convention on the Law of the Sea, global justice and the environment." *Global Constitutionalism* 13, no. 1 (2024): pp18.

Uski[25] also provided a detailed examination of risk mitigation measures provided in SOLAS and the connection with other safety conventions. They have relied on qualitative content analysis and case examples to demonstrate that SOLAS has been a dynamic and responsive safety framework to the major maritime catastrophes like Titanic and other high profile incidents that have followed. The chronological tracking of amendments and emphasis on preventative safety culture are the major strength of the study. Nevertheless, the authors recited less focus on developing countries and the effects of infrastructure or resource limitations to the realization of SOLAS requirements. Critically speaking, their focus on legal synergy strengthens the notion that maritime safety cannot be established with the help of separated tools. In this study, the research paper adds value by defining SOLAS as a dynamic and flexible mechanism, not a stagnant piece of legal rules, but one that will have to be recalibrated constantly in response to autonomous vessels, cyber threats, and climate-related port risks.

Strati[26] studied operational issues against the 1974 SOLAS Convention, where they paid attention to passenger and cargo vessels. The review of documents and technical safety tests revealed to the study that there were systemic problems, including the lack of life-saving devices, inadequate training of crews, and lack of uniformity in jurisdictional compliance. The fact that the study considered both design and operational limitations was a strength since these are normally not given much consideration in legal orientated literature. The studies were however local to the European shipping contexts and failed to adequately address the cross-national differences or the classification societies. Importantly, the authors emphasized the weakness of the application of the letter of the law in SOLAS through the poor real-life implementation. This point is significant to this study, which attempts to comprehend the mismatch between regulatory design and effective safety performance, particularly in the context of new threats that are not necessarily traditional maritime threats.

[25] Uski, Santeri. "Enclosed Space Entry and Rescue drills mandated by SOLAS and their implementation in practice." (2021):pp 28.
[26] Strati, Anastasia. *The protection of the underwater cultural heritage: an emerging objective of the contemporary law of the sea*. Vol. 23. Brill, 2021: pp2.

The study of the Implementation of SOLAS on state and commercial vessels by Ricardianto[27] is a comparative one with an observational field research in the ports of Indonesia. Their results showed that there are notable safety differences between government-owned ships and fleet by the private sectors especially in fire prevention setup, emergency exercises, and the certification of the crew. The merits of this paper are in its empirical richness and ground level focus, as it gives a fine-grained coverage of implementation shortcomings. Nevertheless, it did not analyze the issues of compliance in a thorough manner, but rather touched the subject a little bit, and little was said about the legal or institutional processes that need to be implemented to address these limitations. The study, however, is a valuable addition to this study because it demonstrates the critical role of domestic interpretation and institutional capacity in ensuring the consistency of the application of SOLAS, which is only more pressing with the emergence of digital ship management systems and unmanned shipping technologies.

Regita[28] evaluated the use of the 1974 SOLAS Convention in Batam City, public ports, Indonesia. They used qualitative interviews with port authorities and document analysis to assess the effectiveness of the safety standards (e.g. emergency response systems and passenger handling procedures implementation) implemented at the port level. Their results indicated a disjointed implementation history of having well organized policies in place but the implementation faced operational problems of staffing inadequacy, obsolete equipment and uneven training. The strength of the study is that the research has concentrated on ports as the frontlines of regulation of SOLAS. Nonetheless, the experience of Batam City is not compared to that of other regional or international port systems, and this restricts its generalisability. Nevertheless, the case will be of relevance to this study by showing that port-level governance and enforcement capacity is an important determinant of maritime safety and need to be aligned with international commitments under SOLAS. Author conducted a historical and legal analysis of how disasters involving bulk carriers (including the incidents with Derbyshire and Stellar Daisy) contributed to the following amendments to SOLAS. The research used document analysis of IMO reports and national

[27] Ricardianto, Prasadja, Reza Fauzi Jaya Sakti, Honny Fiva Akira Sembiring, and Zaenal Abidin. "Safety study on state ships and commercial ships according to the requirements of Solas 1974." *Journal of Economics, Management, Entrepreneurship, and Business (JEMEB)* 1, no. 1 (2021): pp10.

[28] Siregar, Ghea Regita Maharani, Florianus Yudhi Priyo Amboro, and Lu Sudirman. "Effectiveness of Implementation of the 1974 SOLAS Convention Regarding Safety Standards at Public Ports in Batam City." *LEGAL BRIEF* 14, no. 1 (2025):pp 50.

investigative records to follow the changes in the safety regulations regarding the integrity of bulkheads, structural surveys, and cargo loading practices. One of the strengths is the manner in which the study linked maritime tragedies to certain outcomes of law, which makes the development of SOLAS very palpable. But the analysis was hindsight and failed to examine how the future risks (e.g. the occurrence of a cyberattack on bulk carriers or malfunctions with automation) may influence the alterations of SOLAS. Critically, the article has offered a very convincing argument to see SOLAS as a reactive system that has historically reacted to failure but not sought to identify systemic weaknesses to be vulnerable to. This viewpoint helps this study to put SOLAS in a broader context of safety governance ecosystem that must be proactive and prospective, especially in a world of advanced technological transformation.

Uski[29] examined the implementation of the drills required by SOLAS, namely the case of enclosed space and rescue entry, on commercial ships. The study conducted on the basis of observational fieldwork and interviews with crews revealed that the quality of training, the adherence to the procedures, and preparedness of crews showed a significant variation. Although SOLAS requires these drills in Chapter III, the research established that in most cases, the drills are performed in perfunctory manner especially when against time constraints or during cost reduction efforts. The study has a strength in that it provides practical inquiry on routine safety activities that form the basis of SOLAS framework. Its weakness is the using small sample size and not cross-regional comparisons, which influences the representativeness of the results. However, this study contributes to this research since it reveals that compliance with regulations cannot be presumed simply by a ratification or a document, but the focus should be put on the practices on board the vessels whereby a new technology like remote operation systems minimizes the number of human representatives and decreases the level of training. Author evaluated the situation in maritime safety in Indonesia under the SOLAS influence, specifying it to the fishing ships and small commercial vessels. The study took a socio-legal methodology, which is the integration of legal review and a policy analysis and interviews. The results have shown that SOLAS provides strong safety principles, but the application of the principles is not always applicable to small vessels since it is either exempted or incapable of its enforcement. The strength of the study is that it mentions legal exclusion as a problematic issue, in other words, smaller and informal operators

[29] Uski, Santeri. "Enclosed Space Entry and Rescue drills mandated by SOLAS and their implementation in practice." (2021): pp22.

are often not subject to the coverage of SOLAS though they constitute a significant segment of maritime traffic in developing areas. One of the weaknesses is the fact that quantitative data is minimal, which lowers the power of generalisations. Nevertheless, this work can be applied to this research because it is the first step to breaking the hypothesis of universal applicability and demonstrating that the gaps in law enforcement remain, as well as its boundaries. The limits of applicability of SOLAS will need to be reassessed with the increased fragmentation of shipping through the formation of private micro-fleets and autonomous crafts.

## 1.3. Role of International and Regional Organizations

### 1.3.1. Role of International Maritime Organization

Kerr[30] examined the IMO mandate and operational instruments in the requirement to decarbonise the maritime industry. The paper has used legal-institutional analysis, which has evaluated the instruments through treaties, IM resolutions and the First IMO GHG Strategy to analyse the way the organisation deals with climate change. Results showed that the IMO has set ambitious targets and goals, such as the total annual GHG emissions of international shipping by at least 50% below the level of 2008 by the year 2050 but has been criticised to be too slow during its implementation as well as over dependence on the consensus based governance. The advantage of the current research is that the authors pay attention to regulatory tools, especially the amendments of Annex VI of the MARPOL, and map the policy timelines in detail. Nevertheless, the work has not provided empirical analysis of the level of compliance by the member states and it has not completely provided the analysis of the reception of market-based measures by developing countries. The study is useful in this research because it illuminates the legal and procedural limitations that the IMO encounters to provide effective governance of the global environment as it is a politically sensitive area. Author compiled an extensive book that collected views of experts on the current maritime matters concerning IMO with emphasis on such issues as marine environmental protection, maritime security, and ship registration practices. The volume was a multi-author, doctrinal kind of volume, with policy commentary and analysis of the law. The overall finding was that although the IMO has assumed a leading role in the development of maritime law and safety procedures, it is becoming more difficult to ensure regulatory leadership

[30] Kerr, Baine P. "Binding the international maritime organization to the united nations convention on the law of the sea." *International Organizations Law Review* 19, no. 2 (2022):pp 400.

in a fast developing technological as well as geopolitical world. The resource of this collection is the variety of professional opinion and the emphasis on institutional responsibility. Its weakness however lies in its inconsistent quality in the chapters where some of the contributions are founded on hypothetical commentary as opposed to legal analysis or empirical evidence. Nevertheless, in this study, the book is useful in providing an overview of institutional inertia in the IMO and the necessity of procedural changes to make it more responsive to new demands including cyber threats, AI-driven vessel activity, and port decarbonisation guidelines.

Rahimi[31] examined how the Indian Ocean Region (IOR) has been managed by international maritime security organisations, both public and private such as the IMO role in promoting cooperative governance. The qualitative approach used in the study involves the use of a case study design which utilized security patrol reports, multilateral naval agreements, and regional forums on the maritime. It discovered that despite the IMO having played a major role in setting the norms, its actual enforcement capability in piracy prone territories like the horn of Africa is still restricted thus allowing non-IMO actors like local maritime alliances and security agencies the room. One of the strongest aspects of this work is that it is region-specific and it challenges the question of how global norms are practiced or avoided in reality. Nevertheless, the research has focused on enforcement mechanisms, and thus, given the emphasis of the mechanism, it put minimal consideration on the legal frameworks and treaties that have made these arrangements possible. The present study can be informed by the views of author on the reliance of the IMO standard-setting position on the operational ability and political goodwill of other players, to cast doubt on the issue of institutional reach as opposed to practical control in the process of maritime governance. Author studied the coincidence of the instruments of the IMO with the United Nations Sustainable Development Goals (SDGs) and SDG 14 on life below water. Their work took the approach of policy analysis, which tested IMO conventions, including SOLAS, MARPOL, and STCW, through the prism of sustainability and environmental protection. They came to the conclusion that in spite of the fact IMO plays a significant role in the achievement of sustainability of the global community, its tools tend to work in isolation without a holistic approach to the economic, environmental, and social aspects. The paper merits its normative framing of the IMO as a part of the UN agenda, which presents an excellent argument on the need to institutionalize

[31] Rahimi, Shayan. "Legal Examination of the International Maritime Organization's Approaches to Environmental Protection." *International Journal of Advanced Research in Humanities and Law* 2, no. 2 (2025): 30.

reform. Nevertheless, the research did not provide tangible mechanisms that can be used to trace IMO practices with SDG performance indicators. The advantage of this analysis to this research is that it has positioned the IMO as a sustainability actor whose policies and conventions need to be revised to address cross-sectoral environmental issues, particularly following the climate change and the extinction of marine biodiversity.

Toelihere[32] used a behavioural and inter-organisational approach to the IMO contribution to the maritime safety. Using a conceptual framework that is based on the theory of organisational sociology and safety culture, the authors proposed that maritime safety is not merely a matter of legitimate rules and regulations but also of informal institutional practices between shipowners, classification societies and the port authorities. Their results also found that IMO instruments like compliance to ISM Code is construed by actors differently depending on local risk cultures and economic limitations. The key strength of the given study is its novel theoretical perspective that changes the focus on the legal formalism to the behavioural patterns in the shipping networks all over the world. Its weakness however, is that it lacks case studies or empirical evidence to support her theoretical propositions. Nevertheless, to this study, the paper will prove useful in showing that the effectiveness of the IMO regulations depends not only on their content, but also on their social construction, negotiation and internalisation within the industry. Author undertook a quantitative study of the stakeholder power on the IMO, in which different actors (states, NGOs, industry groups) develop the agenda and regulatory outcomes in maritime safety and human element issues. Based on the records of participation, submission, and voting, the authors came to a conclusion that several large flag states and industry lobbying groups have disproportionate power over the decision-making process. One of the strengths of this study is the rigour of the empirically conducted study and the transparency in exposing the power asymmetries in the IMO system. The main weakness however is that it is limited in scope since the analysis work was reduced to safety related instruments and the analysis was not expanded in issues of environment and digital regulation. However, this research also provides a critical input to this study by revealing institutional inclinations, which can compromise the ability of the IMO to control unbiasedly a fast evolving maritime environment.

[32] Toelihere, Ivan Filbert, Lukman Yudho Prakoso, and Panji Suwarno. "The Role of Maritime Policy in Supporting Global Security Sustainability and Stability." *Available at SSRN 5082198* (2025): pp5.

The article by Watty Sihombing[33]explored the Impact of the European Union (EU) on the market-based approaches by the IMO to reduce emissions. The study evaluated the EU engagement strategies in the IMO Marine Environment Protection Committee (MEPC) by conducting legal-policy analysis and interviewing the stakeholders of the regulatory debates. The authors discovered that although the EU has been an active champion of carbon pricing and more stringent emission limits, there has been resistance by big developing countries and industries, which results in compromises. The political economy approach is the strength of the study because it takes into consideration institutional friction and geopolitics of climate governance. Nevertheless, it did not have a more thorough interaction with technical law tools of maritime law or procedural reform suggestions. This analysis enhances this research because it places the IMO in the context of more general global governance politics of environmental responsibility, and how normative ambition is usually checked by diplomatic and economic realities. In the article, the IMO was studied in the scope of institutional discourse analysis of deliberative processes. The study was based on transcripts, submissions, and participant observation in IMO committees to examine the role of consensus-building, strategic framing, and institutional norms in determining regulatory outcomes. The results indicated that even though the IMO boasts of neutrality and inclusiveness, deliberation has been influenced by existing alliances and power hierarchies especially among high-capacity maritime and industry alumni. The article has a strong point in terms of its ethnographic understanding of the inner nature of international regulation that gets lost in legal literature. One of them is, however, that deliberation emphasis can overestimate material constraints like technical capacity or funding gaps that also influence results. Nevertheless, this work is critical to this study because it reveals that IMO regulation is not just a by-product of law-making but of multi-faceted and negotiated social practices that condition the interests of whom are satisfied in the world maritime order.

El Sakty and Islam[34]also relied on a multi-criteria decision-making (MCDM) model to assess the viability of sustainable container shipping projects in the IMO carbon target. The study evaluated

[33] Sihombing, Derma Watty, Nurindah Dwiyani, Yayu Nopriani Martha, and Christiani Hutabarat. "Impact of International Standards on Maritime Education: Perspectives of Junior Cadets." *Meteor STIP Marunda* 17, no. 1 (2024):pp 10.

[34] EL SAKTY, K. H. A. L. E. D., and ALIA EMAD ISLAM. "DEVELOPING ACCOUNTABLE MARITIME TRANSPORT AND PORT ORGANIZATIONAL STRUCTURES IN ARAB COUNTRIES." *WIT Transactions on The Built Environment* 212 (2022):pp 150.

policy alternatives, which included slow steaming, fuel switching and retrofitting by evaluating them on the basis of cost, environmental implication and regulation compliance. They found that though they can be solved technically, the attractiveness of green investments is diminished by regulatory uncertainty and inconsistent enforcement across the member states. This study is strong because it uses quantitative decision-making tools to evaluate policies and provide the operations of future reforms. But, it has a weakness in its limited scope of container shipping without considering other types of vessels and flag-state changes. This study is advantageous to this research since it brings to the fore the gap in the operation between regulatory intent and operational feasibility especially in an industry where economic forces and global fragmentation continue to be major challenges to consistent compliance. It concentrated on the institutional compliance strategies of IMO treaties advocating that the circumstances of the crisis, such as the maritime catastrophes or the emergencies in the climate sphere should give the political force to the reform process. The paper incorporated both the legal theory and historical policy analysis and assessed the post-disaster regulatory revisions like those after the Exxon Valdez spill and the Costa Concordia disaster. it made the conclusion that IMO is reactive in nature with regulatory reforms tending to be driven by failure instead of vision. One of the strengths is the emphasis on the compliance mechanisms and institutional learning in international organisations. The retrospective orientation of the study, however, implies that it does not provide proactive strategies and models of anticipatory regulation. However, the value of this work in this research is that it frames the IMO in a trend of regulatory catch-up and bolsters the thesis that international maritime law needs to shift to an adaptive mode of governance and particularly in the digitalisation, automation, and geopolitical unpredictability.

### 1.3.2. Role of Regional Organizations: Case of European Union

Schimmelfennig[35] examined EU climate change policies in terms of the policy timeline of the last twenty years with an analysis based on the emissions targets, green financing tools, and maritime decarbonisation programs. The research discovered that despite the EU leadership in the pricing of carbon and the regulations on eco-designs, there still exists gaps in the implementation especially in the maritime transport sector that had historically not been under the EU ETS (Emissions Trading System). One of the advantages of this paper is that it is chronologically clear

[35] Schimmelfennig, Frank. "European regional organizations, political conditionality, and democratic transformation in Eastern Europe." *East European politics and societies* 21, no. 1 (2007):pp 130.

and focuses on the EU as a leader in climate norm diffusion. Nonetheless, it paid less emphasis on the issues of implementing EU environmental law to further areas of the transboundary industry, such as shipping, which is governed by EU and IMO systems. In the case of this study, this article is very pertinent since it positions the EU as a leader in emissions regulation but also points to the jurisdictional conflict between regional ambition and international harmonisation, particularly in such domains as fuel standards, port state control and carbon-neutral shipping. In this study, it was possible to investigate the nexus of climate change, environmental degradation, and migration through the prism of EU policies. The qualitative approach to policy review was used. The paper was based on the countries of Central Asia and Eastern Europe, revealing how the EU incorporates the environmental migration in its foreign policy and border management policies. The results indicated an increased awareness among EU law on the fact that climate-induced displacement can become a characteristic attribute of cross-regional migration, which requires legal and institutional readiness. One of its strengths is its futuristic model that links the environmental change and demographic strains. Nonetheless, the paper failed to specifically connect the migration patterns to maritime effects, including the increase in sea levels as a result of which coastal communities were left or SIDS. Nevertheless, this piece of work is relevant to this study as it highlights the need by regional actors to take into consideration intersectoral risks, such as climate, migration, and maritime security, which are becoming intertwined in global systems of governance.

The volume edited by Gelder[36]is based on the study of international relations and the EU through a mixture of institutional analysis and empirical case studies in the area of foreign policy. The book depicted the three forms of influence the EU has such as regulatory diplomacy, conditionality, and external agreements. A chapter was devoted to EU maritime activity, where it was mentioned that it was involved in activities in piracy deterrence, such as EU NAVFOR Somalia. The volume is strong in that it presents a variety of empirical data and theoretical foundations in supranational governance. Nevertheless, the volume failed to evaluate systematically the role of the EU in the international maritime law-making or in the establishment of the digital port and shipping standards. However, this research is also strengthened by the volume as it demonstrates how the

[36] Nielsen, Jens Cosedis, and ESC Scientific Document Group. "2024 ESC Guidelines for the management of atrial fibrillation developed in collaboration with the European Association for Cardio-Thoracic Surgery (EACTS)." *European Heart Journal* 45, no. 36 (2024): 3314.

identity of the EU as a civilian power can help it shape security architecture such as maritime regulation by means of non-coercive but strategic regional relations.

Dieme [37] provided a comprehensive review of EU health policies, stating the institutional coordination of various domains. Although it is not explicitly maritime-oriented, their interpretation of EU governance of public health offers useful parallels on integrated policymaking- especially how the EU integrates health, safety and environmental standards among the member states. One of the main findings was that the achievements of EU regulations depend on the data interoperability, well-developed legal norms, and the possibilities of the alignment of the institutions. An advantage of the work is that it is clear in the manner in which the EU addresses complicated and cross-boundary regulatory issues, which can be used in maritime risk administration strategies. This, however, is limited by the lack of maritime case studies to make it directly applicable. In the context of this study, the research can serve as one of the comparative models according to which the EU can organize a similar transboundary policy in such spheres as port health policies or emergencies medical response networks in the sea.

In a systematic literature review, Mhatre[38] analyzed the initiative of circular economy in the EU by examining the legal, logistical, and institutional changes that are required to bring circularity to the various sectors. The research employed PRISMA methodology and accessed more than 130 peer-reviewed articles in order to find out the drivers and obstacles in policy implementation. The results found that the EU had been a strong leader when it comes to encouraging closed systems in packaging, construction and electronics, but it also noted that there was a difficulty in aligning these systems with the global trade and shipping logistic systems. One of the advantages of the given research is its well-organized evidence base and its connection between EU regulatory innovation and sustainability transitions. It however did not discuss the maritime industry in detail, in terms of ship recycling and marine waste. Nonetheless, this article can be relevant to this study because it illustrates how regional regulatory authorities such as the EU are developing new legal avenues that overlap with maritime circularity, which is becoming a more topical field in the context of decarbonisation and pollution prevention at sea. The European Soil Data Centre 2.0,

[37] Diemer, Andreas, Simona Iammarino, Andrés Rodríguez-Pose, and Michael Storper. "The regional development trap in Europe." *Economic Geography* 98, no. 5 (2022): pp450.
[38] Mhatre, Purva, Rohit Panchal, Anju Singh, and Shyam Bibyan. "A systematic literature review on the circular economy initiatives in the European Union." *Sustainable Production and Consumption* 26 (2021): pp200.

Introduced Click or tap here to enter text.looked at the role of spatial data systems in the EU environmental policies. In a technical framework evaluation, the authors demonstrated that the availability of correct geospatial and soil data would facilitate the power to monitor the environment, control better, and make decisions based on evidence in the EU. The merit of this piece is the focus on data interoperability and open access which are the essential parts of every contemporary regulatory regime. It has a weakness in that it is too thematically focused to the extent of it being as applicable to the realms of the sea. Nevertheless, the work would be helpful in this research in making comparisons between the land and sea data systems, especially since the sea safety, pollution monitoring, and digital port systems are becoming more dependent on geospatial data that is interoperable.

In this study, Maljean-Dubois[39] examined the political motivation and institutional processes of EU policymaking, paying close attention to the question of supranational power and national sovereignty. The study, however, by examining the political aspects in depth with references to legal texts and interviews proved that the EU has a high agenda-setting power, but its ability to act swiftly is often impeded by its internal disunity and the necessity of consensus of the member-states. According to the authors, transport, environment, and trade are the key areas of policy through which the EU has been able to develop a strong external impact. One of the strongest points about this work is a critical understanding of the EU politics and its understanding of the strains between technocratic regulation and democratic legitimacy. The role of maritime issues was, however, not directly addressed and therefore, its relevance to ocean governance was somewhat indirect. However, in this study, the article offers a necessary background on how the EU bargains and enforces local maritime agreements, and why it might or might not be in the forefront in the execution of international standards like those of the IMO.

## 1.4 Theories and Models

Several scholars have employed Supranationalism Theory in explaining how the European Union oversteps the normal state-based governance in exercising its power that is voluntarily relinquished by individual member states. Studies described how EU institutions, specifically the European Commission and the Court of Justice, are able to develop legal rulings and other external

[39] Maljean-Dubois, Sandrine. "Regional Organisations: The Case of the European Union." *Oxford Handbook of International Environmental Law,* (2021): pp12.

agreements, including in the area of maritime safety and environmental protection. This was strengthened by author[40] who observed that the supranational legal structure of the EU dictates its ability to negotiate on one hand at IMO or UNFCCC where otherwise 27 states would be negotiating on their own. The merit of this theory is that it can be used to describe the power of the EU to act in a coherent manner and exercise regulatory power beyond its boundary. Nevertheless, the author has identified internal divisions, particularly in climate diplomacy and emissions policy, as something that questions the complete realisation of supranational ideals. Spranationalism is useful in this study to understand why the EU is such an influential regional player in the work of maritime and environmental regimes, but being limited by domestic politics to export standards and conclude binding commitments.

Another theoretical perspective to explain the impact of EU on the international maritime regulation is Regulatory Regionalism[41]. This theory maintains that regions are able to produce norms of law and forms of governance that impact outside of their geographical area especially in policy diffusion mechanisms, conditionality, and legal harmonisation mechanisms. As shown by Click or tap here to enter text.the EU regulations on climate and the circular economy frequently spread to global trade and logistics and influence the standards in third countries that export to or transit Europe. Thus, author demonstrated how this stance of the EU on maritime emissions affected the discussions in the IMO, although the non-EU states deeply disagreed. This theory can be justified through the data about the environmental diplomacy and normative power of EU, but its limitations can be observed in politically sensitive areas, such as migration  discovered that EU regional policy usually does not lead to homogeneous external outcomes. In the study, the framework of regulatory regionalism would be helpful in examining how the inner legal commitments of the EU influence the global maritime practices using strategic alignment, external conditionality and set of technical standards.

[40] Leal-Arcas, Rafael. "Theories of Supranationalism in the EU." *Journal of Law in Society* 8, no. 1 (2007): 100.
[41] Jayasuriya, Kanishka. "Regionalising the state: political topography of regulatory regionalism." *Contemporary Politics* 14, no. 1 (2008):pp 25.

# 2. Maritime Cybersecurity and Autonomous Vessels: Legal Challenges and Responses

This chapter includes a case study that closely looks at the role of the International maritime 1982 Law, namely, UNCLOS (United Nations Convention on the 1982 Law of the Sea), SOLAS (Safety of Life at Sea), and the MARPOL Convention (International Convention for the Prevention of Pollution by ships) in dealing with the challenges of the emerging technologies, such as autonomous vessels and cybersecurity. The case study examines practical examples of how these structures have (or have not adapted) to changes in technology and evaluates their success in ensuring maritime safety, security and environmental safety. With the adoption of new technologies in maritime industries, there is a need to know the possible legal loopholes and complications especially when the technologies cut across borders and include international waters. In this chapter, the changing role of UNCLOS, SOLAS and MARPOL, in respect of technological changes and its legal significance in the global maritime security will be examined.

The three areas that will be addressed in the case study include:

- The Autonomous Ships Development and Implementation.
- Cyber threats to Maritime Operations.
- Environmental Impact and Regulation of the MARPOL Convention

## 2.1 The Development and Implementation of Autonomous Ships

These technologies are transforming ship designs, operation and control, yet the legal systems are frequently falling behind in these quick transformations. Therefore, it is important that these regulations are properly reviewed so that they are properly tackling the issues posed by these innovations[42]. There is a great technological revolution represented by autonomous vessels in the maritime industry. Being programmed to work independently of human intervention, these ships are based on sophisticated navigation systems, artificial intelligence, and data analytics in a real-time. Nonetheless, their adoption in the global shipping introduces a few legal issues of accountability, liability and safety. With the increase in the use of such technologies, the current

[42] Nawrot, Justyna. "24 (R) evolution of maritime safety in IMO conventions and UNCLOS." In *40 Years of the United Nations Convention on the Law of the Sea*, 2025: pp309.

laws like UNCLOS and SOLAS are increasingly becoming challenged as a way of maintaining safety and security in operations.

As the main international 1982 Law that regulates the activities of the sea, UNCLOS has been reluctant to respond to the regulatory requirements of autonomous vessels. Article 87 of UNCLOS on the freedom of the high seas and Article 90 of UNCLOS on the right of the ships to sail freely on the high seas might require reinterpretation to accommodate the automated operations. The jurisdiction issue that concerns autonomous vessels is also a question, especially regarding the issue of delimiting between the role of coastal states and flag states. These legal complications have not been sufficiently addressed by the international regimes that have been in place and even being demanded to be changed.

A good example is the Yara Birkeland, the first fully electric and autonomous container ship in the world. Although the project is at the testing stage, its use in Norway has prompted the need to revise national and international 1982 Law to answer issues of liability, maritime jurisdiction, and insurance with regard to accidents involving autonomous ships. The use of the ship in a territorial sea and an exclusive economic zone (EEZ) has shown the weaknesses in the existing international regulations which were made in such a manner that they could accommodate traditional crewed vessels only. This example also reflects the necessity to take a serious look at UNCLOS with regard to new technologies in maritime.

SOLAS Convention provides the safety of life at sea by regulating the design, construction, equipment and operating of vessels. Nevertheless, SOLAS requires an overhaul in order to support the technical needs of autonomous vessels. As an example, clear guidelines regarding the operation without crew, standards of cybersecurity, and technical reliability of autonomous systems are needed. The current version of SOLAS that is designed to support crews might not be adequate to support the risks of fully autonomous ships[43].

The International Maritime Organization (IMO) has been undertaking the efforts of trying to incorporate MASS into the international maritime 1982 Law. It is expected that the amendments to SOLAS will include the additions that will cover such aspects as collision prevention,

[43] ASOK, AKSHAY. "AUTONOMOUS SHIPS IN MARITIME LAW: CHALLENGES TO LIABILITY, SAFETY, AND SHIPPING PROTOCOLS." (2025): pp30.

emergency procedures, and design requirements of autonomous ships. The efforts put in by the IMO are a step in the right direction of bridging the technological innovation and legal regulations but there is still a lot to be done before the safety standards can be wholly adhered to. The example of MASS indicates that the problem of autonomous ships requires an international response because of the peculiarities of these objects.

Since the sphere of maritime operations is getting more and more dependent on digital technologies, cybersecurity has become a pressing concern. Weaknesses in the navigation system, cargo system and communication system can pose great threats to safety and security. When these weaknesses are not addressed well, there is a possibility of safety failure or environmental mishaps. The global regulators have come to view maritime cybersecurity as an acute matter but there is a striking gap in establishing proper legal frameworks to deal with these new threats[44].

Although the major issue that MARPOL addresses is the environmental protection and ship-related pollution, there is an emerging concern about the cybersecurity threat of pollution prevention systems. To offer an example, a cyberspace attack in the fuel management system of a ship might result in an ecological catastrophe or a breach of the MARPOL rules. Hackers have the capability to control the system of navigation and pollution controls, which can put the ship, as well as the rest of the marine environment, in danger. Therefore, cybersecurity should be regulated in the maritime industry in line with technological changes to reduce the effects of these risks.

## 2.2 Cybersecurity Risks in Maritime Operations

The cyberattack on one of the largest shipping companies of the world, Maersk Line, in 2017 and the ensuing outage of its system reveals the high susceptibility of the shipping industry to cyber-attacks. The port operations, cargo handling and administrative systems were disrupted on a large scale due to the attack. The case highlights the significance of cybersecurity to both maintain the relevant compliance to the environmental standards provided by MARPOL and guard against any negative impact on the environment caused by cyber interference. Maersk attack was also an indicator of the industry-wide issues of dealing with cybersecurity breaches in a more digital maritime sphere.

[44] Nawrot, Justyna. "24 (R) evolution of maritime safety in IMO conventions and UNCLOS." In *40 Years of the United Nations Convention on the Law of the Sea*, 2025: pp309.

The emergence of autonomous vessels and novel technologies in shipping also creates the possibility to make the environment less harmful, e.g. by consuming fuel more efficiently or creating fewer emissions. Nevertheless, with such technological innovations, novel environmental hazards emerge which need a strong legal management. As the main global convention that regulates the pollution of ships, MARPOL should be adjusted to these technological realities. Although the autonomous ships are expected to drive better fuel efficiency, the ships can also present difficulties in meeting environmental standards, particularly in those areas with weak enforcement of regulatory bodies[45].

As a convention that is meant to govern ship pollution, MARPOL should be modified to fit into emerging technological changes. New issues in the sphere of ensuring environmental compliance and the prevention of pollution are presented by such technologies as autonomous vessels and AI-based fuel management systems. Independent ships, such as those, are expected to operate and be registered under the rules of MARPOL, namely, in the Annex VI that imposes restrictions on the amount of sulfur in the fuel and other pollutants. The difficulty is to make sure that autonomous vessels comply with these requirements, and especially in systems where the enforcement capacity differs.

Since autonomous vessels are bound to ensure lower emissions and maximized fuel consumption, their use should comply with the rules of the MARPOL Annex VI that stipulates the quantity of sulfur and other harmful substances that fuel should contain. The problem is that it has to enforce such environmental standards on these vessels, especially when crossing international waters, or in areas with patchy enforcement. The most significant issue that the policymakers are concerned with is the legal and regulatory loopholes in the application of autonomous ships under MARPOL.

## 2.3 Legal Implications under UNCLOS

Cybersecurity is now one of the most urgent subjects in the maritime industry, and the 1982 United Nations Convention on the Law of the Sea (UNCLOS) was never written (cyber operations). However, UNCLOS continues to be the major legal framework of the oceans, the role of the states, and the behavior of the vessels. Due to the rising incidence of cyber threats to the operation of the navigation systems, port infrastructures, offshore platforms, and submarine data cables, legal

[45] Palippui, Habibi. "Integration of Technology and Regulations for Safe and Efficient Marine Logistics." *Collab. Eng. Dly. Book Ser* 2 (2024): pp7.

implication under the UNCLOS has taken the centre stage in the determination of liability, due diligence, and state responsibility. The lack of clear cybersecurity conditions implies that scholars, courts, and states should use the understanding of the current duties, such as the responsibility of providing security at sea, avoiding harm, jurisdiction over flagged vessels, and security of critical infrastructure. These requirements are now to be extended to situations of malware, GPS spoofing, ransomware, electronic interference and hybrid attacks of underwater pipelines. The UNCLOS legal analysis thus entails the interpretation of traditional maritime principles into an online context and also finding out whether states are performing their duties in the cyberspace.

The Initial significant legal implication of UNCLOS is associated with the obligation to maintain safe navigation that has a direct connection to cybersecurity. The UNCLOS in article 217[46] recognizing the responsibilities of flag states, demands them to exercise jurisdiction and control the ships under their flag in administrative, technical and safety aspects adequately. Article 217 is technology-neutral since it is concerned with safety, as opposed to particular equipment, although the navigation systems had been digitized before the drafting of UNCLOS. Electronic chart display and information systems (ECDIS), GPS, AIS transponders and radar overlays are the modern vessels. When such systems are attacked in any cyber operation, the security of navigation is directly jeopardized. As an example, in 2017, the global system of Maersk was affected by a cyberattack with the help of the NotPetya malware[47] which led to the inability to carry out operations and had to resort to manual navigation and port scheduling. By UNCLOS, the flag state will be required to provide suitable safeguards to the vessels that will maintain the safety of its operations. In case a state does not require cybersecurity, e.g. software patches, secure network architecture, or crew cyber awareness training, it might be violating Article 217. This requirement is more acute in cases when a cyber incident causes grounding, collision or environmental damage because the latter proves that safety control has failed.

[46] "Special Obligations of the Flag State: Article 217." In *Enforcing International Maritime Legislation on Air Pollution Through UNCLOS*. Hart Publishing, 2019:pp 3. https://doi.org/10.5040/9781509927791.ch-008.

[47] Nguyen, Do Duc Anh, Pierre Alain, Fabien Autrel, Ahmed Bouabdallah, Jérôme François, and Guillaume Doyen. "How Fast Does Malware Leveraging EternalBlue Propagate? The Case of WannaCry and NotPetya." *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*, IEEE, June 24, 2024:pp 399. https://doi.org/10.1109/netsoft60951.2024.10588886 .

Article 98 of UNCLOS also helps in cybersecurity since it ensures that masters of ships assist persons in distress as required by states. When a vessel is incapacitated so that it is unable to communicate its location, navigate or identify itself, the obligation to provide assistance is complicated. As an illustration, in 2017, more than twenty vessels were affected by a GPS spoofing attack in the Black Sea and they were mirrored in systems to be inland. When a ship falsely assumes that it is safe whilst it is either drifting or off-course, then its capacity to seek assistance is impaired. Loss of communication caused by cyber interferes with the practical role of Article 98, and creates some legal issues on whether a flag state has taken due diligence in ensuring that the ships are able to communicate in distress despite the disruption of cyber. UNCLOS specifically sets no specifications on technology but its overall responsibility in protecting safety suggests that states update their laws to match digital threats.

The other key Implication in UNCLOS is the accountability of the states in case of internationally wrongful act when cyber operations lead to damage at the sea. UNCLOS specifically does not keep cyberattacks but there are preestablished doctrines of responsibility. When a state initiates or permits to be initiated within its territory the cyber actions that harm the vessels of other states, their infrastructure, or marine ecology, the principle of the internationally wrongful act determined. The Tallinn Manual, which is not binding, indicates that physical infrastructure damage through cyber operation can be a use of force. As an illustration, when malware immobilizes the steering of an oil tanker heading to a narrow strait and results in an accident, the effects resemble the conventional physical interference. The maritime cyberattacks may be seen as the unlawful use of force under common law in terms of Article 2(4) of the UN Charter[48]. In the meantime, it can be understood that Article 217 of UNCLOS may be construed to mandate a due diligence requirement on coastal states to which its nationals or infrastructure are deployed to carry out malicious cyber activities. An example is a coastal state that permits the cybercriminal networks to act on its soil and attack passing vessels is thus may be violating its duty to thwart actions that could lead to the harm of the ships of other states.

Cybersecurity is also one of the factors that influence jurisdiction and legitimate enforcement of powers in the UNCLOS. Articles 25, 73, and 94 are given enforcement rights of states over a few

[48] Wheeler, Caleb. *Bombing Iran: Has the UN Charter Failed?* The Conversation, 2025:pp 5. https://doi.org/10.64628/ab.53rvejvrs .

maritime zones yet these were written not taking into consideration the cyber accidents. In case the navigation of a vessel is hacked and it finds itself in the territorial waters of another state and finds itself there inadvertently, the question that pops out is whether a coastal state is allowed the ship legally to be detained or searched. As a case in point, in 2019 scientists have managed to show that AIS systems could be hacked to produce the illusion of a ghost ship, or conceal smuggling activities. Cyber manipulation may result in innocent passage not being innocent when a ship accidentally poses a threat to the security of the coastal areas owing to spoofed signals. Nonetheless, in the situation when the ship is not aimed at breaking the coastal statutes, the strict implementation of enforcement abilities might contravene the concept of proportionality. UNCLOS indirectly asks states to consider the notion of innocent passage by referring to modern technologies, that is, cybersecurity breaches may have an impact on the way innocent or intent is determined.

The other legal Implication is associated with the security of submarine cables which are fundamental in the process of telecommunications worldwide. Fibre-optic cables are used in carrying over 95 percent of international data traffic, and thus, are critical to civilian and military communications. Articles 112-115 of UNCLOS[49] provide the freedom to lay cables and liabilities of states to avoid damage. However, such provisions are restricted to physical casualties, e.g. fishing equipment or anchors. Attacks on cyberdata as data is transported in cables by cable taps, signal attacks, or denial of service attacks are not covered in UNCLOS wording. However, under Article 113, states are bound to criminalise willful destruction of submarine cables. A cyber intrusion which alters cable routing, affects transmission or intercepts data would be arguably a form of damage in the functional sense. Indicatively, in the Baltic Sea, a number of submarine cables have been suspected to have been interfered with by state and non-state actors. In the case of a cyber operation that has shut down communication flowing along the cable, the spirit of Article 113 will advocate that states need to prevent and investigate such cases. Lack of doing so will negate the duty of safeguarding submarine communications despite the fact that the nature of the damage is electronic and not physical.

[49] "UNCLOS." In *Enforcing International Maritime Legislation on Air Pollution Through UNCLOS*. Hart Publishing, 2019:pp 7. https://doi.org/10.5040/9781509927791.ch-003 .

The issue of cybersecurity also overlaps with marine environmental protection as established by UNCLOS. Articles 192 and 194 place upon states a responsibility to safeguard and conserve the marine environment and also to avoid pollution by their vessels and installations. Attacks on navigation or propulsion systems would lead to oil pollutants, chemical spills or any other environmental catastrophe. As an example, a carefully planned cyber attack against the ballast system of a tanker would cause instability, grounding and resultant leakage. In case states do not take the necessary steps to ensure cybersecurity, which could reasonably prevent the occurrence of the same, they might breach their due diligence requirement to prevent environmental damage. This risk is more pronounced in case of offshore installations, e.g., oil platforms or gas pipelines, in which cyber vulnerability could lead to disastrous environmental outcomes. UNCLOS does not specify the technological meaning of pollution, but its loose definition; the introduction by a man, either directly or indirectly, of any substance or energy into the marine environment, can be construed to include the cyber-induced accident that causes the hazardous discharges. In this way, there is an indirect obligation to legal environment on flag states and coastal states by cyber vulnerabilities.

Attribution is one of the most complicated problems of UNCLOS regarding cybersecurity. Cyber activities are naturally hard to trace and attackers can make use of proxies and false flags or hacked servers. The law is however left to be held accountable by proving the identity of the perpetrator. In Article 94, it is hinted that the vessel of the flag state must exercise good jurisdiction over her or his vessels, however, when the systems of the ship have been sabotaged by another actor in a different state, it is difficult to identify the person responsible. The 2020 cyberattack of an Iranian port, Shahid Rajaee[50], which occurred with the probable involvement of Israel, and the later Iranian action of disrupting Israeli water systems is the point where digital and digital operations become intertwined. These events, despite the settings in a port, reveal how challenging it is to identify when a state is directly engaged in, aided or failed to halt negative cyber actions. UNCLOS lacks specifications regarding digital attribution, which states have to limit themselves to general

[50] Mesgarani, Hamid, Hamid Safdari, and Abolfazl Ghasemian. “Solving Optimal Control Problems with Integral Equations or Integral Equations - Differential with the Help of Cubic B-Spline Scaling Functions and Wavelets.” *Mathematical Researches* 6, no. 1 (2020):pp 120. https://doi.org/10.52547/mmr.6.1.119 .

principles of international law. This is a significant vulnerability in the Convention to control threats in the twenty-first century.

The security rights of the coastal"states in UNCLOS, particularly in the territorial waters, exclusive economic zones (EEZs), and straits are also brought to question by the cyber threats. Article 19 enumerates acts that make passage non-innocent that include: "any act to gather information to the disadvantage of the defence or the security of the coastal State. This definition could encompass cyber reconnaissance of a ship, e.g. scanning networks along the coast or intercepting digital communications. When a ship takes advantage of its onboard systems and carry out cyber surveillance of the coastal infrastructure, the coastal state has the legal authority to suspend or limit innocent passage under Article 25[51]. But, the attacker of cyber reconnaissance is hard to discern, and therefore the coastal states are likely to become inclined to use over-defensive measures. It is a matter of striking the balance between the rights of navigation and the increasingly frightening threat of digital espionage. UNCLOS lays down the protocol of enforcement, however, not clarifying what constitutes cyber behaviours as security threats.

Moreover, the cybersecurity threats have an impact on the responsibilities of the states with respect to the security of the offshore units, i.e. oil platforms, gas pipelines and energy interconnectors. Article 60 and 80 of UNCLOS accord the coastal states solely the jurisdiction owing to artificial installations and islands in their EEZ and the continental shelf. Conventionally, this area of jurisdiction is related to physical security against collision or disturbance. But now installations are based on the SCADA systems, industrial control program and remote monitoring networks. Misuses of these systems might result in explosions, shut down or environmental catastrophes. As an example, the 2021 land-based cyberattack of Colonial Pipeline in the United States demonstrated how malware may shut down important energy infrastructure. Should the same attack be inflicted on offshore infrastructure, the duty of the coastal state to protect against environmental harm and safety as per the framework of the UNCLOS may go further to demand high-quality cybersecurity. The inability to enforce these protections can be considered an

[51] Mankowski, Peter. "Article 25." In *Commercial Law*. Nomos Verlagsgesellschaft mbH & Co. KG, 2018:pp 7. https://doi.org/10.5771/9783845276564-449 .

insufficient use of the power over installations, particularly in the areas where energy reliance is substantial, including the Baltic Sea.

Piracy provisions are also connected to cyber operations in UNCLOS. Article 101 and 102 establish piracy as unlawful acts of violence or those that involve detention with private purposes of the high seas. The physical form of piracy is known as traditional piracy, but the legal uncertainties exist in the form of cyber-induced hijacking like remotely taking control of the navigation of the ship. When hackers gain control over a vessel, encrypt its systems using ransomware and require money, then this type of act is similar to piracy and does not involve any physical violence. Other researchers suggest that the term cyber piracy can fall under the umbrella definition of control or detention due to the fact that the crew is practically immobilised or even put at risk. Indicatively, in 2019, criminals had tried to hack into port systems to detect and reroute containers with goods worth money. Even though it does not fall under the definition of piracy in the UNCLOS, what the incidents demonstrate is that cyber activity can imitate the goals of maritime crime. However, the Convention fails to define digital coercion as piracy and this presents a loophole in the collaboration, interdiction rights, and jurisdiction on the high seas.

Lastly, there are cybersecurity threats to international cooperation requirements of UNCLOS. Articles 197[52] and 200 advise states to cooperate in relation to preventing pollution, and exchange information and carry out scientific research. The same principles of cooperation can be applied to the area of cybersecurity where the information-sharing is the key to the attacks prevention. The marine domain relies on a system of interdependent digital networks and the vulnerability of one port or shipping company can propagate to the world-wide systems. The framework of cooperation established by UNCLOS offers an opportunity to establish a joint system of cybersecurity regulation, although it does not specifically refer to the issue of cyber operations. To illustrate, following the attack on NotPetya, a series of maritime agencies worked together informally to enhance cyber hygiene. Such measures are in line with the cooperative spirit of UNCLOS that states must undertake an emerging responsibility to avoid cyber incidents that have the potential to upset the marine environment or navigate the sea.

[52] "Articles." In *Managing Aggression*. Routledge, 2002:pp 9. https://doi.org/10.4324/9780203193914-62 .

Overall, UNCLOS offers quite general and loose principles that may be applied to cybersecurity, but its lack of reference to digital threats creates severe legal gaps. The Convention contains promises of safety, environmental protection, cable protection, jurisdiction, state responsibility and cooperation which are needed to reinterpret to the digital age. The attacks on ships, ports, offshore installations and submarine cables prove that the maritime governance is strongly influenced by the weaknesses that UNCLOS had never imagined. With the ongoing technology revolutionizing the maritime space, with autonomous vessels and AI navigation, there is a need to reexamine the legal framework of the UNCLOS, to revise its interpretation and to ultimately reform it to suit the peculiarities of cybersecurity on the sea.

## 2.4 Legal Implications under SOLAS

Cybersecurity has become a primary topic of discussion in international maritime regulation and, despite the fact that the Safety of Life at Sea Convention was written many years before the advent of digital navigation, it is a vital aspect of international regulation of the security of the ships in the modern world where the cyber threat to human lives, ship security, and international trade is directly linked to cybersecurity. SOLAS is among the oldest, most authoritative safety conventions, which binds almost all flag states and establishes minimum safety requirements relating to ships, equipment and operations. Although in its original form, SOLAS does not state any specific cybersecurity requirements, the intent of the Convention, its architecture and safety requirements render it immediately relevant to cyber threats. The International Maritime Organization (IMO) has increasingly applied SOLAS to embody cyber risk management as a subset of ship safety, in particular the on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). The legal scope of cybersecurity under International Safety Management (ISM) Code as well as the IMO 2017 Guidelines[53] SOLAS substantially increases as vessels become more reliant on digital platforms to handle their navigation, propulsion, communication and cargo handling services. The Convention has become the main premise of obligating flag states, companies and shipmasters to adopt measures to mitigate cyber incidents that may threaten life at sea.

[53] *ISM Code*. International Maritime Organization, 2018: pp7. https://doi.org/10.62454/kd117e.

The legal Implication of SOLAS on the cybersecurity front concerns the primary issue of Chapter V (Safety of Navigation) which mandates vessels to possess and maintain navigational systems and equipment that is required to pass safely. Historically, such needs were related to actual physical devices, but nowadays, modern ships extensively use digital technologies including ECDIS, AIS, GPS, built-in bridge systems, radar overlays and automatic steering systems. These systems can be attacked by hackers, malware and signal manipulation. The impact of cyber on the navigation equipment can lead to a displacement of the ship, its entry into hazardous zones, a collision or running aground. According to Regulation 19 of Chapter V[54], a vessel should be fitted with navigational systems that are suitable to the purpose, which currently indirectly implies secure and cyber-insured digital infrastructure. A navigation system that is easily hacked by a cyberattack cannot be considered fit under SOLAS. As an example, the incident of GPS spoofing in the Black Sea in 2017 when vessels were redirected of course, made it clear that it was possible to erode navigational safety without any physical interference. The legal side of these issues is that flag states and shipowners have the duty to maintain cybersecurity, which could include encryption, authentication, intrusion detection and system redundancy, and be in conformance with SOLAS safety requirements.

The other notable legal Implication of SOLAS is that of Chapter XI-1 (Special Measures to Enhance Maritime Safety) and it entails that companies are bound by the requirements of the ISM Code. The ISM Code obliges the companies to set, hire and uphold a Safety Management System (SMS) to achieve safe ship handling and pollution avoidance. The IMO explained that the concept of cyber risk management belongs to the functional requirements of the ISM Code. Cybersecurity is an essential safety element, even though it was not enshrined in the initial text of SOLAS, the interpretation of the IMO makes it compulsory. This implies that the inability to carry out the cyber risk management including crew training, secure network system or frequent testing of the digital system, may amount to a contravention of SOLAS. An important real-world example is the Maersk NotPetya attack that occurred in 2017. The worm was an infector of global network of Maersk, where the ports were put out of business causing losses in billions of dollars and dozens of ships were forced to work with little digital support. In a case where a ship had lost propulsion, steering

[54] "Chapter 2. Ethical Norms And Procedures." In *Ethics and Regulation of Clinical Research*. Yale University Press, 2017:pp 10. https://doi.org/10.12987/9780300163490-005 .

or navigation as a result of the cyberattack, this would have become an obligation under SOLAS since the company had not safeguarded safety-critical systems. In this understanding, SOLAS puts a legal obligation on the shipping companies to anchor digital systems in their SMS.

Another sector, where cybersecurity has a high implication, is the Global Maritime Distress and Safety System (GMDSS)[55], which is under the governance of SOLAS Chapter IV. GMDSS helps ships to transmit automatic distress signals and receive navigational alerts, weather predictions and emergency communications. An attack on GMDSS by cyberattacks may deny a ship the chance to broadcast distress signals, to receive warning or to identify hazards that surround it. In case malware shuts down the capacity of a ship to send out a distress signal, it can potentially place the crew in life-threatening circumstances, and other passing ships will be unaware that they are in need of help. SOLAS provides that GMDSS equipment should be operational and immediately available. This is not the case with a system that is prone to cyber interference. Indicatively, in 2020, the security companies proved that some GMDSS satellite communications terminals were vulnerable to attacks where attackers could remotely gain control over systems. These vulnerabilities when used can compromise SOLAS in that they impair the safety role of GMDSS. The legal connotation is that the systems of distress and communication are to be secured under the laws by the legal states against any kind of cyber attack, and the businesses should secure the settings.

SOLAS Chapter II-1 (Construction – Structure, Subdivision, and Stability) and Chapter II-2 (Fire Protection) are also influenced by cybersecurity as more and more important vessel functions, such as ballast systems, engine controls, ventilation, fuel control and fire detection systems, etc., are managed by electronic systems. The direct threat to the integrity of the vessels is caused by cyber manipulation of these systems. As an example, scientists have proved that the manipulation of ballast water systems with the help of cyber means can destabilise vessels, leading to listing or capsizing. In like manner, turning off fire detection systems or causing false alarms may undermine the speed of response or cause panic. SOLAS mandates that safety and structural systems should be reliable in all circumstances. The failure of such systems may make them non-compliant due to the influence of cyber. Therefore, the safety of navigation is not the only aspect where

[55] *Global Maritime Distress and Safety System (GMDSS)*. n.d:pp 20. https://doi.org/10.3403/bsen61097 .

cybersecurity is crucial to the physical survival of the vessel. In case of flooding caused by a cyberattack, fire, or mechanical failure, flag states can legally be blamed in their failure to implement SOLAS standards and shipowners can be liable with regard to their failure to implement the necessary safety systems.

The other significant legal Implication is that of Chapter IX (Management for the Safe Operation of Ships) of the SOLAS[56] that formally enforces the ISM Code. The fundamental principles of the ISM Code, which are risk assessment, contingency planning, documentation, and continuous improvement, now require the introduction of cyber risk assessment and cyber incident response plans. The IMO mandated the companies in 2021 to include cyber risk management in their SMS by detecting the vulnerability and planning its mitigation strategy as well as ensuring operational resilience. Such a necessity makes cybersecurity a legally binding aspect of ship management. To use the example of a company not installing two factor verification on vital systems and a cyber intrusion activity paralyzing propulsion hence causing the company to crash, the company can be found to be in violation of SOLAS. Numerous cyber attacks in ports and shipping firms, including the 2018 cyberattack of COSCO Shipping Lines, prove how disruption of the operations may pose a threat to the vessel safety despite the absence of physical damage. SOLAS therefore holds a legal duty on the companies to implement effective cybersecurity measures and also on flag states to enforce compliance by carrying out audits and inspections.

The legal aspects of the SOLAS also concern the port state control (PSC). Under Chapter I and XI, the ports states are empowered to do the inspections of such foreign-flagged vessels to ensure they adhere to the requirements of the SOLAS. Conventionally, physical safety equipment, certificates, crew qualification and structural integrity were inspected by PSC. Nevertheless, cyber vulnerabilities are now subject to PSC inspections since they directly introduce SOLAS compliance. In case of an outdated navigation software, systems not patented, unsecured Wi-Fi networks or poorly documented cyber risk, the inspectors can arrest the ship. The United States Coast Guard (USCG) is one of the many maritime authorities that have already imprisoned ships on the basis of poor cybersecurity measures. As an example, in 2019, malware was found on one of the ships coming to the Port of New York, and the USCG issued a safety bulletin. Even though

[56] "Chapter IX: Management for the Safe Operation of Ships." In *SOLAS*. International Maritime Organization, 2024: pp20. https://doi.org/10.62454/kh110e.048 .

the event did not result in detention, it was an indication that PSC is able and is progressively reviewing cybersecurity in accordance with SOLAS principles. The legal aspect of it is that vessels which do not have cybersecurity features may be detained, fined or denied entry, and flag states may face embarrassment and liability internationally.

SOLAS Chapter VI (Carriage of Cargoes) and Chapter VII (Carriage of Dangerous Goods)[57] are also affected by cybersecurity. Current cargo handling systems are based on the use of the digital technologies, automated cranes, cargo-tracking software and electronic manifests. The attacks of these systems are prone to dangerous misplacements, wrongful stowage of dangerous material or loss of safety margin. To illustrate, the ransomware attack on Port of Durban in South Africa in 2021 stagnated the cargo and caused a misunderstanding of where the containers were moved. In the event a similar accident happens on a vessel that was transporting dangerous materials, mismanagement might lead to explosions, fire or leakages. SOLAS is a system which demands strict cargo safety measures and cyber-induced mismanagement can violate such a regulation. Though SOLAS does not express cybersecurity as a requirement of cargo safety, its safety goals are logically applied to the digital systems, which control dangerous cargoes. The shipowners are thus obliged to ensure the cargo management systems to ensure that they are in line with SOLAS.

The other significant legal Implication is connected to crew competence and training that is regulated according to SOLAS along with the STCW Convention. Traditionally, crew members are trained to operate in navigation, seamanship, machinery use and emergency procedures. Nevertheless, nowadays cyber risk management has become a subset of safety operations. Unless crew members receive training on how to detect phishing attacks, use secure passwords, identify malware behaviour, or react to cyber attacks, the safety of the vessel may be endangered. Indicatively, various studies on cyber incidences found that personal USB drives with malware were carried by crew members or personal gadgets were attached to ship networks. The implications of SOLAS in this regard are that companies should provide the competence of the crew in areas of cybersecurity through its safety management requirements. The consequences of

[57] "Chapter VII: Carriage of Dangerous Goods 1 ; Part A: Carriage of Dangerous Goods in Packaged Form." In *SOLAS*. International Maritime Organization, 2024:pp 22. https://doi.org/10.62454/kh110e.042 .

a failure in training crew can also result in a liability in accordance with the SOLAS and the ISM Code requirements in case of a human error causing a cyber incident.

There are also legal implications of SOLAS that apply to the responsibilities of coastal states. The states with coastlines do have responsibilities to maintain the maritime security in their territorial waters, ports and coastlines. Navigational aids, lighthouses, traffic separation schemes or Vessel Traffic Services[58] (VTS) may be cyberattacked limiting the capability of coastal states to ensure safe navigation. As an illustration, in 2021, the Shahid Rajaee port of Iran was attacked by a cyberattack, and it disrupted maritime traffic. An attack on a VTS in a busy strait such as the Bosporus or the Baltic would lead to a situation that is high-risk. In case a state does not make its maritime traffic systems secure and a cyber attack results in collision or pollution, the state can be charged with the violation of the SOLAS-related responsibilities to promote the safety of navigational processes. Even though SOLAS obligations are mainly the obligation of flag states and shipowners, coastal states have complementary duties to ensure safety of the maritime environments.

The Issue of cybersecurity risks also overlaps with search and rescue (SAR) requirements of SOLAS and other treaties. When children interfere with communication between the vessels and the rescue coordination centres or the ships are unable to deliver precise location information, the safety of the vessels is compromised. An example is the spoofing of AIS that can either make a ship invisible or manipulate its location and be hard to rescue. SOLAS states that safety equipment should be able to sustain the intended purpose of that piece of equipment. A digitally spoilt distress signal is a violation of this requirement. As a result, the states should make sure that SAR infrastructure has cyber-protected communication channels and redundancy tools.

Lastly, SOLAS has legal repercussions on international collaboration, which is crucial in dealing with the cyber threats. The Convention is based on international standards, and cybersecurity cannot be solved through the efforts of one state. The IMO promotes exchange of information and best practice on cyber threats between states. The legal one is that SOLAS based cooperation does not only cover the conventional issues of safety, but also includes digital security, which involves

[58] *Glossary of Aeronautical Terms: Air Traffic and Ground Services*. n.d: pp20 https://doi.org/10.3403/30305534 .

states revising their national laws, engaging in IMO cyber working groups and implementing cyber risk principles regularly.

To conclude, SOLAS establishes far-reaching legal consequences of cybersecurity in the maritime sphere despite the fact that the Convention does not directly refer to cyber threats. Cybersecurity has now become a compulsory aspect of safety of the ships, companies, flag states and port states via Chapter V, IV, II, IX and XI and the ISM Code. SOLAS safety requirements concern cyber attacks on skills in navigation, communication, cargo handling, and stabilization of the vessel, engine control and emergency response. The fact that Maersk, COSCO, port terminals and navigation systems were attacked and disrupted by hackers are real-life examples of how ships can be susceptible to digital disruption and require proactive cyber risk management. With the continuously increasing technology, such as the introduction of autonomous ships, AI navigation, and fully digitalised ports, the impact of SOLAS on the regulation of maritime cybersecurity is going to be even more centralized. The Convention therefore has a legal basis of safeguarding marine life during the digital age, but it might need more clarification and reforms to deal with the new threats with more specificity.

## 2.5 Legal Implications under MARPOL

Cybersecurity risks pose very problematic threats to the International Convention for the Prevention of Pollution by Ships (MARPOL), though the Convention was designed with the anticipation of physical damage against the digital interference. The essence of MARPOL is to avoid the occurrence of marine pollution by the operational discharges, accidental spills, and equipment failure. Nonetheless, technologically motivated dangers are now also part of the modern pollution threat, as cyberattacks on ship systems, sensors, machinery and port infrastructure can indirectly, but critically, cause an impact on the environmental safety. MARPOL[59] depends on the operation of mechanical, monitoring and record keeping systems to guarantee compliance and these systems have increasingly become computerized. Consequently, this creates new legal implications to the Convention because of weaknesses in electronic control systems, automated pollution-preventing equipment, cargo handling software and fuel management networks. Although there is no explicit mention of cybersecurity in MARPOL, the architecture and aim of

[59] "Marpol, n." In *Oxford English Dictionary*. Oxford University Press, 2023. https://doi.org/10.1093/oed/5240290816 .

the Convention demand that states and shipowners guarantee environmental safety through combating digital threats that may result in pollution. This indirectly, yet, essentially, connects MARPOL with cybersecurity requirements.

One of the most important legal consequences of this is the fact that MARPOL relies on automatic and electronically controlled measures to prevent pollution. Digital systems have now been relied on in modern vessels to observe bilge water discharges, oil-water separators, sludge and as well as ballast water exchange and emissions control equipment. Most ships currently incorporate integrated platform and engine control, digital fuel injection state and exhaust gas utilized systems (scrubbers) and ballast water treatment plants all assigned to programmable logic instruments (PLCs) or industrial management software. Cyber attack of these systems may result in unwanted pollution, deliberate manipulation of discharge or malfunction of the equipment. An illustration of this is the tampering of an oil discharge monitoring equipment (ODME)[60] of a ship by malware, which would lead to unlawful standards of discharging oily wastes to the sea without the knowledge of the crew. According to MARPOL Annex I, vessels should make sure that Oily Water Separators (OWS) and ODME operate well at all times. When an OWS releases pollutants due to being hacked by cyber attacks, this goes against MARPOL, although the damage is caused by other digital activity. The legal implication is that the legal obligation of that states, in meeting their compliance and enforcement obligation, is to make sure that the pollution-prevention systems are not only physically secured but also digitally secured as well.

Under MARPOL, record-keeping requirements that are subject to cybersecurity are strongly dependent on the correctness of Oil Record Books (ORB), Cargo Record Books (CRB), Garbage Record Books and fuel and sludge reports. As a lot of vessels are moving towards using paper logs as opposed to electronic record books (e-ORB), cybersecurity weak points are now forming a direct risk to the wholeness of environmental compliance records. The cyber intrusion may falsify entries, remove records or alter timestamps to conceal unlawful discharges. Annex I of the MARPOL on record books states that record books must be complete and accurate and falsifying them is a very serious offence. When ransomware attack corrupts environmental compliance data,

[60] Youngsoo, Park, Gokhan Camliyurt, Efraín Porto Tapiquén, et al. *Enhancing Shipboard Oil Pollution Prevention: Machine Learning Innovations in Oil Discharge Monitoring Equipment*. Elsevier BV, 2024:pp 30. https://doi.org/10.2139/ssrn.4888923 .

it may prove difficult to establish the level of pollution. In 2022, a cybersecurity organization published reports indicating that various popular e-logbook platforms had vulnerabilities, which enabled them to manipulate the records him/herself without being detected. Shipowners and flag states are legally bound to have correct logs under MARPOL and this means that the ship owners require cybersecurity measures in terms of authentication, encryption and audit trails. The inability to ensure such systems may lead to their infringements, detention of port states and a criminal prosecution, even in case the manipulation was caused by a cyberattack.

The other significant legal Implication is the relation to cyber risks to machinery and propulsion systems which can indirectly be the cause of pollution. MARPOL Annex VI is an agreement that governs the air pollution of ships making it mandatory that the ships follow the fuel sulphur limits, NOx emissions and that the exhaust cleaning systems work correctly. Cyber interference can be committed to digital systems which regulate engine performance, fuel injection, emission sensors and scrubbers. Scrubbers might be disabled, sensor readings may be distorted or fuel systems may be manipulated in such a way that a ship may produce pollutants in quantities exceeding legal levels. As an example, with a hacker having switched off the monitoring system of a scrubber, the vessel will have been emitting high amounts of sulphur gases in the Emission Control Areas (ECA) without realising, which is contrary to the requirements of Annex VI. Equally, an attack which interferes with the fuel temperature sensors would lead to partial combustion and high levels of particulate emissions. The objectives of MARPOL put the states to the challenge of having the pollution control equipment functioning as it was intended and this means that cybersecurity should be incorporated so that there should be no occurrence of environmental non-compliance.

Ballast water management is also a subject of cyberattacks (MARPOL as well as Ballast Water Management Convention[61] (BWMC)). Ballast water systems are based on the use of the digital control to turn on pumping, UV treatment equipment and filtration systems. Control over such systems via malware may enable the untreated release of ballast, which causes the introduction of invasive species and a breach of the environmental protection requirements of MARPOL. As an illustration, a vessel may release pollutants in the coastal water bodies due to attackers triggering

[61] David, Matej, Stephan Gollasch, Brian Elliott, and Chris Wiley. "Ballast Water Management Under the Ballast Water Management Convention." In *Global Maritime Transport and Ballast Water Management*. Springer Netherlands, 2014: pp40. https://doi.org/10.1007/978-94-017-9367-4_5 .

the ballast pumps to avoid treatment processes, which contravenes the international requirements. Despite the fact that BWMC is a different convention to MARPOL, the two conventions have common environmental objectives and regimes. The inability to ensure that the ballast equipment is not Interfered with by cyber-attack might be considered a failure to ensure environmental protection in the general principles of MARPOL with regard to pollution-prevention.

Cybersecurity also overlaps on MARPOL on port reception facilities and port states. Ports process large digital networks involving reception of waste, sludge, cargo, refuelling and inspections. Stealing port reception systems could mean that ships will not be able to offload waste or sludge, and thus they will have to keep the pollutants longer than recommended or may discharge them unlawfully. In annex I and Annex II, adequate reception facilities should be provided by port states, which cyber failures can make non-compliant. As an example, the 2021 cyberattack on the South African port of Durban[62] caused the ports to be shut down, including waste processing timetables. When an oily waste cannot be discharged by a ship due to a cyber attack and the ship then exceeds limits of discharge, then there is a grey area of legal responsibility. MARPOL lacks a definition of liabilities in case of cyber-disrupted port functions, which is a gap. Nevertheless, states still have the obligation to offer secure facilities, and this implies that MARPOL compliance requires cybersecurity.

The other Implication which is important is that deliberate cyber interference of pollution-prevention equipment that can enable the crime of the environment. Traditionally, magic pipes were involved in illegal discharges and do not go through pollution control equipment. Today, digital attacks are able to do the same by modifying the digital controls. Valves could be remotely opened by hackers and alarms turned off or falsifying monitoring data to hide illegal behaviour. The enforcement provision of MARPOL such as criminal penalties and detention extend to any interference with pollution prevention equipment. Provided that a violation occurs with the aid of cyber manipulation, shipowners will not be absolved provided that they prove that they have acted in due diligence to avert cyber intrusion. This poses very complicated issues of liability, burden of proof and sufficiency of cybersecurity measures. The example is that in 2019, it was reported of attempts to breach cargo and machinery systems on one of the tankers to alter operational data.

[62] "Ballard, Henry, (1840–30 Jan. 1919), Port Captain, Durban, 1884–1904." In *Who Was Who*. Oxford University Press, 2007:pp 5. https://doi.org/10.1093/ww/9780199540884.013.u193052 .

Even in cases where attackers are unknown under MARPOL, the shipowner can be liable due to lack of proper safeguards except when he/ she can demonstrate reasonable preventive measures.

The Issues of cyber risks also apply to provisions regarding accidental spills, including the ones that are covered by the Annexes I and II. Contemporary tankers are based on gauging systems of digital tankers, pipeline pressure sensor, and cargo tracking programs. In case these systems have been manipulated by a cyberattack, overfilling, rupture or contaminated discharge may take place. As an illustration, should malware disable the high-level alarms in a tanker as it is loaded, excess capacity would form a major spill. The physical damage to the environment is involved, but the cause is digital; therefore, MARPOL is the most applicable. The legal implication is that the Convention states that state parties have to ensure reliability of systems that avoid such accidental spills which now covers cybersecurity of loading systems, tank level sensors and remote valves. The inability to secure these systems may be viewed as the lack of adherence to the technical requirements of MARPOL.

The other significant Implication is related to ship to shore data transmission that is increasingly being applied to ensure environmental compliance. Numerous vessels are also configured to automatically send fuel consumption, emission profiles, scrubber operation data and bilge water discharge data to monitoring centres in the shore. Attacks on these transmissions may lead to the generation of fake compliance reports hence hard to enforce. In case of attackers intercepting or manipulating transmitted data, the port state control authorities might fail to identify any breach. As an example, personnel of maritime researchers proved in 2020[63] that it is possible to manipulate AIS and other digital transmissions to falsify emission data. MARPOL is required to rely on proper reporting and reliable follow up and cyber manipulation compromises such systems. Thus, the cybersecurity of ship-to-shore data is established as a legal aspect of MARPOL compliance, which affects inspections, certification and liability.

The legal consequences of cybersecurity on the enforcement of MARPOL by Port State Control (PSC) are present. PSC inspector periodically inspects pollution-prevention systems, logs and certificates, sludge tanks, equipment and cargo handling operations of OWS. The cyber vulnerability can directly affect MARPOL compliance as these systems go digital. In case the

[63] *Figure 10 - Growth of R&D Personnel and Researchers,*. n.d.: 2000. https://doi.org/10.1787/888932332778 .

inspection authorities discover the absence of control software patches in use, the use of obsolete ODME firmware, indisputable e-logbooks, they can consider it as a shortcoming in pollution-prevention measures. Some PSC authorities such as the Tokyo MOU and Paris MOU[64] have already put in place cybersecurity in the inspection procedures. Indicatively, ships that have damaged digital pollution-prevention devices can be detained. It follows that cybersecurity will be included in the compliance profile of a vessel according to MARPOL, and the inability to secure systems may lead to major administrative and financial penalties.

Another area in which MARPOL touches upon cybersecurity concerns the mechanisms of environmental emergency response. Digital communication systems, satellite tracking, remote sensors, spill modelling and emergency coordination platforms make efficient response to spills possible. When these systems are cyberattacked in case of an environmental incident, it can aggravate the pollution outcomes. As an example, a ransomware attack that stops a coastal state into accessing the spill modelling tools may slow down response, causing more harm to the environment and breaching the MARPOL requirement of responding to a pollution incident in a time-sensitive way. Even though MARPOL is silent on issues of cybersecurity, the Convention demands that states reduce pollution and react effectively. Cyber disruption is a breach of both the duties, and it is necessary to secure digital environmental response infrastructures.

One other legal implication is with regards to the responsibility of states to enact laws, regulations and standards to enact MARPOL within their countries. States should come up with a legislation that would enforce compliance of ships under their flag to MARPOL standards. Under the digital era, this entails cybersecurity provisions of the pollution-prevention equipment, monitoring systems, e-record books and operational technology networks. In case a state does not issue cybersecurity demands and a cyberattack causes pollution, a state can be charged with the responsibility of not executing its implementation obligations. This is similar to the logic that is used in other environmental regimes where the poor management of industrial risks creates the problem of state liability. The form of MARPOL that is based on flag state enforcement makes direct obligation on states to revise regulations in line with technological change.

[64] Im, Myeong-Hwan, and Ho-Sig Sin. "A Study on the Port State Control Inspection Results of Tokyo MOU : Focused on Detentions of Tokyo MOU." *JOURNAL OF FISHRIES AND MARINE SCIENCES EDUCATION* 29, no. 2 (2017): pp333. https://doi.org/10.13000/jfmse.2017.29.2.333 .

There are also cybersecurity impacts on the goal of MARPOL to reduce pollution caused by shipboard energy efficiency requirements controlled by Annex VI. Digital or software-based, the Energy Efficiency Design Index[65] (EEDI), Ship Energy Efficiency Management Plans (SEEMP) and fuel consumption monitoring technologies are all energy efficiency systems. There is a possibility of cyberattacks altering information on energy efficiency, falsifying performance indicators or shutting down monitoring devices. This kind of manipulation may enable the ships to evade emission reduction requirements. The Data Collection System (DCS) of IMO which is used to collect data on the CO2 emissions is highly dependent on the digital records. Compromised submission of data through cyber means can even pervert the environmental reporting requirements. According to MARPOL, vessels and nations are required to guarantee the authenticity of the environmental performance information, and this means that they should have cybersecurity measures.

The last significant legal Implication is the obligation of cooperation and exchange of information that is internalized in MARPOL. The Convention obliges states to report pollution incidents, exchange technical information and cooperate on the environment protection. Hacking attacks that cripple communication networks hamper this obligation. As an example, when a system of a coastal state is disabled by a cyberattack and a ship is no longer able to inform the authorities about a dangerous discharge or the pollution, the cooperation requirements of MARPL are involved. States thus have an obligation to make sure that cyberattacks are prevented in digital communication networks that are critical in reporting pollution. This is a mandatory condition that connects compliance with the MARPOL to the strength of the maritime cybersecurity system.

[65] "Energy Efficiency Design Index (EEDI)." In *Encyclopedia of Ocean Engineering*. Springer Nature Singapore, 2022: pp20. https://doi.org/10.1007/978-981-10-6946-8_300238 .

# 3. Case Study: Protection of Maritime Critical Infrastructure from Hybrid Threats

## 3.1 Baltic Sea Nature of Hybrid Threats and Emerging Technologies

Baltic Sea has turned into one of the most strategically sensitive maritime domains in the world, and the threats of hybrid-type attacks: a combination of physical sabotage and cyberattacks, information warfare, and electronic interference and covert activity of states are threatening to the critical maritime infrastructure. Compared to the conventional maritime threats like piracy or territorial claims, hybrid threats exist at the digital, physical and informational levels at the same time. Northern Europe has a high concentration of submarine cables, ports, and shipping routes that have established the foundation of the energy, communication and trade systems in Northern Europe. With the level of dependency on such assets on the part of the states in the region, they are similarly exposed to complex forms of hybrid operations that take advantage of loopholes in international maritime law.

The recent events show how the concept of hybrid threats is no longer a far-fetched aspect in the Baltic Sea region. Underwater infrastructure, when it comes to the Nord Stream 1 and Nord Stream 2 pipeline explosions in 2022[66], became exposed to the sabotage damage. Despite attribution being controversial, the event proved that aggressive parties have the physical capability to logically breach and destroy energy infrastructure in the deep sea in foreign waters. In the same way also there have been several unaccounted interference with fibre-optic cables off Estonia, Finland and Sweden that have cast doubt on intentional interference by state-linked ships or unmanned underwater vehicles (UUVs). Cyber operations against ports, logistics systems and maritime navigation networks are also considered as hybrid threats. Interruptions of Cyber threat to Vessel Traffic Services (VTS), AIS networks, maritime power grids or offshore platform control systems may result in grounding, collision and service outage or pollution.

These risks are increased by emerging technologies. Robots deployed in the water and remotely controlled vehicles (ROVs) as well as digital varieties of seabed maps enable states or non-state

[66] Götz, Roland. "Nord Stream 2." *Osteuropa* 69, nos. 1–2 (2019): pp23 - 32. https://doi.org/10.35998/oe-2019: 0014.

actors to close into infrastructure without unlike notice. Higher cyber technology can gain access to ballast systems, control of propulsion, oil discharge monitoring or port logistics networks. Jamming by satellite or GPS spoofing, which was reported around Kaliningrad can give ships false navigation readings, which adds to the already crowded waters, making navigating them more dangerous. These grey zone approaches are between war and peace, and take advantage of their legal uncertainties using the UNCLOS, SOLAS and MARPol. These multi-domain nature of the hybrid threats is their complexity: a cyberattack on the monitoring system of a pipeline can result in the physical explosion; a spoofed navigation signal can cause an accidental spill; a vessel of a state carries an anchor, which can break a fibre-optic cable purportedly because of the need to perform its functions. Since hybrid threats contain intentional and accidental characteristics, the legal frameworks found in the current legal system find it hard to categorize, prevent, or respond to such threats.

Important sea ports in the Baltic Sea are thus not only vulnerable to physical sabotage, but also to covert digital manipulations, which can cause a disaster of the environment, economical losses or political unrest. Eastern ports in the area like Klaipeda, Gdansk and Gothenburg are very dependent on automated cargo systems and network controlled cranes. A cyber attack would put the port out of business, interfere with supply chains or unsafe loading of dangerous cargo. Other potentially compromised systems include offshore wind farms and interconnectors; malware that gains access to power control systems would disrupt the electricity systems in the region. Since UNCLOS was written in 1982, such a form of integration of technologies, hybrid threats, are not something that the Convention could anticipate[67]. Only equipments-based requirements are also present only indirectly in SOLAS and MARPOL, thus they are equally inappropriate to the current digital-physical threats. The scenario with the Baltic Sea therefore points at the crucial necessity to rethink the existing legal norms or establish new regulatory instruments to ensure maritime infrastructure security.

[67] Schnakenbourg, Eric. "Baltic Sea." In *Atlantic History*. Oxford University Press, 2017: pp30. https://doi.org/10.1093/obo/9780199730414-0202 .

## 3.2 Law Loopholes in Disaster response of the Baltic Sea infrastructure using UNCLOS, SOLAS and MARPOL

The problem of the hybrid threat in the Baltic Sea highlights numerous loopholes in the international legal system of maritime law, especially in terms of attribution, jurisdiction, and state accountability. Such loopholes emerge due to the fact that UNCLOS, SOLAS and MARPOL were created to control the safety and environmental conditions in maritime activities at the time of analogue nature, rather than digitally facilitated sabotage or transnational hybrid activities.

States are bound to ensure the protection of submarine pipelines and cables under UNCLOS and in particular, in Articles 113-11[68]5. The Convention however is restricted to physical damage and not cyber manipulation, electronic interference or hybrid operations that indirectly impact on infrastructure. Using the example of a cyberattack that would disable pressure sensors on a gas pipeline, leading to an explosion, but without any physical interference, UNCLOS does not give any instructions on how to classify or attribute such an occurrence. UNCLOS is also facing the problem of modern attribution. The actors of hybrid attacks may be a proxy, an unmarked ship, covert special forces, or a distant computer weapon. Since the Articles 91 and 94 imply an effective state control, it is unclear whether a state breaches UNCLOS when a ship with its flag is covertly sabotaged without the express government consent. Equally, Part VII of UNCLOS regarding the freedom of the high seas fails to explain what should be done whenever there is an unknown underwater vehicle, which is approaching and interfering with infrastructure in exclusive economic zones (EEZs).

Jurisdiction also adds to response complications. Several EEZs and high seas zones are often involved by the submarine pipelines, but UNCLOS has given minimal authority to the coastal states to enforce regulations. As an example, a Baltic nation is legally not at liberty to capture a foreign ship simply by suspicious actions in the proximity of a pipeline unless there is evident sign of unlawful action at hand. Hybrid threats take advantage of this grey area to act in the legal grey areas where coastal states do not have automatic rights to enforce it. UNCLOS also lacks any

[68] Sumer, M. "THE RELEVANCE OF THE LAW OF TREATIES IN THE INTRODUCTION OF MASS OPERATIONS – UNCLOS & SOLAS." *Autonomous Ships 2022*, ahead of print, April 1, 2022: pp20. https://doi.org/10.3940/rina.as.2022.10 .

specific mechanisms of cooperative surveillance or protection of shared underwater resources, and Baltic states have no legal framework upon which to conduct coordinated cruising or reaction.

SOLAS also has its loopholes since it is only concerned with the safety of ships, but not buildings against ship risks, whereby the threat posed by cyber-attack or actions by rogue states is a factor. Ships under SOLAS Chapter V are to be equipped with navigation equipment and be in good operation. But SOLAS also makes no regulation of how ships can interact with underwater infrastructure or give powers of enforcement over those ships that might carry out intentional GPS spoofing[69], underwater mapping or signal jamming. Civilian vessels may be turned into hybrid actors by installing dual-use sensors on them in order to collect intelligence about pipelines or data cables. Although SOLAS is a regulation governing the safety management systems (ISM Code), it has no clause that requires ships not to enter the area of sensitive infrastructure or communicates their position with coastal states. In addition, the cyberattacks of ships that due to accidents pollute or collide demonstrate a SOLAS-MARPOL gap, since SOLAS requires management of cyber-risks, however the enforcement of this obligation is not uniform among Baltic states, i.e., a weak link in one of jurisdictions poses a threat to the entire region.

MARPOL equally suffers weaknesses. The Convention is based on the prevention of pollution by operational discharges and accidental spills, although cyber-enabled environmental damage is not addressed. By targeting ballast systems, engine controls, emissions monitors or oil-water separators, hybrid threats can result in pollution without it literally violating any equipment. Should a cyber attack induce an oil spillage in one of the tanks of a tanker or a dangerous chemical discharge in a port terminal, MARPOL does not provide any clear cyber provision on this liability. Another threat that confronts MARPOL in the use of quality logs and monitoring data is the idea of hybrid threats. Digital records have the ability to hide unlawful discharges or to postpone the discovery of a pollution incident. Since MARPOL presupposes the operation based on good faith and manual control, it does not have any means to examine and confirm the pollution caused by cyber-mechanisms.

[69] Ma, Chao, Jun Yang, Jianyun Chen, Zhi Qu, and Chao Zhou. "Effects of a Navigation Spoofing Signal on a Receiver Loop and a UAV Spoofing Approach." *GPS Solutions* 24, no. 3 2020:pp 5. https://doi.org/10.1007/s10291-020-00986-z .

The largest legal loophole existing between and across UNCLOS, SOLAS and MARPOL is the lack of attribution and evidence standard of hybrid threats. The absence of explicit criteria on how to define the identity of the attackers or the categorization of the hybrid cases makes the affected states find it difficult to mobilize the legal safeguards like diplomatic protection, claims to state responsibility or other international dispute resolution procedures. Hybrid threats are deliberately uncertain and the current conventions fail to deal with evidence to cyber sabotage, underwater interference or electronic attack.

All these gaps together expose the Baltic Sea infrastructure to advanced hybrid approaches that are not covered by standard legal definitions. The dynamics of hybrid threats underscore the inefficiency of the maritime law of the 1980s to regulate the 21 st century technology and geopolitical landscape.

## 3.3 Reform Requirements and Policy Suggestion towards the Enhancement of Legal Protection

Based on the legal gaps found, there is still a lot of reforming that is needed to enhance the security of critical infrastructure in the Baltic Sea. Such reforms should touch on attribution, jurisdiction, cooperative monitoring, cyber regulation and integration of the new technologies in maritime governance. The reform requirements could be divided in the interpretive reform (reinterpretation of the current treaty commitments), and normative reform (the introduction of new rules, codes or regional agreements)[70]. The Introduction of cyber provisions in the interpretation of UNCLOS, either in IMO resolutions or International Tribunal of the Law of the Sea (ITLOS) advisory opinions, is the first priority of reform. Articles 192 and 194 of UNCLOS, on the obligation to protect and to conserve the sea environment, can be construed to refer to the obligation to guard against environmental damage caused by cyber. On the same note, the articles 113- 115 about

[70] Christodoulou, Anastasia, and Jonatan Echebarria Fernández. "Maritime Governance and International Maritime Organization instruments focused on sustainability in the light of United Nations' sustainable development goals." In *Sustainability in the Maritime Domain: Towards Ocean Governance and Beyond*. Cham: Springer International Publishing, 2021: pp450.

submarine cables and pipelines can be extended to include digital sabotage and electronic interference.[71].

A guideline on interpretation adopted by IMO might help clarify that attacks on the cyber world or a hybrid operation involving underwater infrastructure fits in the definition of damage in the UNCLOS.[72]. This reform would make the state more responsible and allow the affected states to seek an inquiry, compensation or dispute resolution..[73]. Second, Baltic states need a hybrid-threat surveillance system on a regional level a legal tool that would allow the collective surveillance, joint patrols, real-time transfer of data and coordinate incidents. Such a mechanism could be organized by the Baltic Marine Environment Protection Commission HELCOM or the Council of the Baltic Sea States (CBSS)..[74].

Baltic Sea hybrid threats reveal critical weaknesses in the maritime infrastructure of the region and disclose systemic weaknesses in the law of the UNCLOS, SOLAS and MARpol. These conventions were written in a pre-digital world, and thus they find it hard to deal with covert sabotage, manipulation of the computer through cyber means, underwater surveillance, or dual use threats of technology. The Nord Stream explosions, cable disruptions and cyber attacks have demonstrated that hybrid threats exist in areas where the international law is silent, ambiguous or fragmented. Legal and policy changes, including interpretive changes and new regional or international instruments are needed to guarantee pipeline, cable, port and energy system security. Such measures as the strengthening of attribution criteria, further intensification of surveillance collaboration, implementation of cybersecurity in environmental protection, and protective norms of underwater infrastructure are the measures that can help to protect the Baltic Sea and make sure that the maritime law is content with technological progression.

---

[71] Melnyk, Oleksiy, and Svitlana Onyshchenko. "Ensuring safety of navigation in the aspect of reducing environmental impact." In *International Symposium on Engineering and Manufacturing*, pp. 100. Cham: Springer International Publishing, 2021:pp 40.

[72] International Tribunal for the Law of the Sea (ITLOS), **Case No. 3**, Guyana v. Suriname, *Maritime Boundary Delimitation in the Atlantic Ocean*, 2004, http://www.itlos.org/cases/list-of-cases/case-no-3/

[73] Strati, Anastasia. *The protection of the underwater cultural heritage: an emerging objective of the contemporary law of the sea*. Vol. 23. Brill, 2021: pp20.

[74] Kotzampasakis, Manolis. "Intercontinental shipping in the European Union emissions trading system: A 'fifty–fifty'alignment with the law of the sea and international climate law?." *Review of European, Comparative & International Environmental Law* 32, no. 1 (2023): pp40.

This system would deal with the fact that pipelines and cables traverse several jurisdictions and hybrid actors take advantage of divided surveillance. Another option would be to have a regional treaty or memorandum of understanding whereby cooperative underwater drone surveillance, combined radar networks, and information-sharing of any suspicious activity by vessels are authorised. This would seal a significant UNCLOS gap of jurisdiction.[75] Third, the reforms should enhance SOLAS by ensuring ships working in the Baltic area would be equipped with a high level of cyber-security and digital transparency.[76] An IMO resolution or a Baltic-specific SOLAS amendment may require cybersecurity audits to be among port state control inspections.[77]. This would stop the usage of vessels as platforms[78] to carry out hybrid operations or fall victims[79] of cyber interference that would disrupt the region.[80].

Fourth, MARPOL needs specific reforms to handle the pollution caused by cyber. The new IMO circle or amendment in an annex may compel ships to be equipped with a pollution-prevention system, make sure that such an automatic system has a backup system and the cyber-protected digital logbooks. Another approach that should be employed by the Baltic states is a regional protocol to have the real-time pollution-monitoring data relayed safely to authorities on shore. This would minimize the chances of having the hybrid actors conceal unlawful releases or cause accidental spills by manipulating the cyber-space[81].

Fifth, an appropriate legal framework of the protection of underwater energy and communication infrastructure must be introduced either with a new IMO instrument or with a Baltic regional convention. This framework must dictate suspicious activities, set requirements of reporting, granting of protective areas around pipelines and cables as well as categorising deliberate

[75] Baumler, Raphael, Maria Carrera Arce, and Anne Pazaver. "Quantification of influence and interest at IMO in Maritime Safety and Human Element matters." *Marine Policy* 133, 2021: 104746.
[76] Chuah, Lai Fatt, Kasypi Mokhtar, Anuar Abu Bakar, Mohamad Rosni Othman, Nor Hasni Osman, Awais Bokhari, Muhammad Mubashir, Mohd Azhafiz Abdullah, and Mudassir Hasan. "Marine environment and maritime safety assessment using Port State Control database." *Chemosphere* 304 2022: 135245.
[77] Freestone, David, ed. *The 1982 Law of the Sea Convention at 30: Successes, challenges and new agendas*. Martinus Nijhoff Publishers, 2013: pp20.
[78] McDougal, Myres S., and Trevor J. Burke. *The public order of the oceans: a contemporary international law of the sea*. Vol. 2. Martinus Nijhoff Publishers, 2024: pp20.
[79] Churchill, Robin, Vaughan Lowe, and Amy Sander. *The law of the sea*. Manchester University Press, 2022: 5.
[80] Wang, Jingbo, Kaiwen Zhou, Wenbin Xing, Huanhuan Li, and Zaili Yang. "Applications, evolutions, and challenges of drones in maritime transport." *Journal of Marine Science and Engineering* 11, no. 11 2023: 2056.
[81] Wang, Jingbo, Kaiwen Zhou, Wenbin Xing, Huanhuan Li, and Zaili Yang. "Applications, evolutions, and challenges of drones in maritime transport." *Journal of Marine Science and Engineering* 11, no. 11(2023: 2056.

interference as a wrongful action internationally. The Nord Stream accident proved the inability of the present legislation to be deterrent, as it does not establish any specific requirements on the vessels or underwater vehicles moving near infrastructure[82].

Sixth, reforms are needed to define standards of attribution of hybrid sea attacks. A global rule might put limits on the responsibility in case a state does not avert proxy or covert action initiated on its territory. Well-defined evidentiary regulations, including digital forensics, vessel tracking data or satellite evidence would assist states to justify claims, and react collectively to hybrid threats[83].

Lastly, policy changes must promote collaboration between the state and the business as it is known[84] that corporations running pipelines, wind farms or cables possess specific technical information that will be invaluable in identifying hybrid attacks..[85] Legal frameworks must mandate the infrastructure operators to disclose cyber-incident reports[86] suspicious activity logs and anomaly detection data to the state authorities,[87] without being exposed to privacy, or commercial confidentiality.[88].

[82] Forti, Nicola, Enrica d'Afflisio, Paolo Braca, Leonardo M. Millefiori, Sandro Carniel, and Peter Willett. "Next-gen intelligent situational awareness systems for maritime surveillance and autonomous navigation [Point of View]." *Proceedings of the IEEE* 110, no. 10 (2022): 1532.
[83] Durlik, Irmina, Tymoteusz Miller, Danuta Cembrowska-Lech, Adrianna Krzemińska, Ewelina Złoczowska, and Aleksander Nowak. "Navigating the sea of data: a comprehensive review on data analysis in maritime IoT applications." *Applied Sciences* 13, no. 17 (2023): 9742.
[84] Freestone, David, ed. *The 1982 Law of the Sea Convention at 30: Successes, challenges and new agendas*. Martinus Nijhoff Publishers, 2013: 20.
[85] Durlik, Irmina, Tymoteusz Miller, Danuta Cembrowska-Lech, Adrianna Krzemińska, Ewelina Złoczowska, and Aleksander Nowak. "Navigating the sea of data: a comprehensive review on data analysis in maritime IoT applications." *Applied Sciences* 13, no. 17, 2023: 9742.
[86] Autsadee, Yuthana, Jagan Jeevan, Nurul Haqimin Bin Mohd Salleh, and Mohamad Rosni Bin Othman. "Digital tools and challenges in human resource development and its potential within the maritime sector through bibliometric analysis." *Journal of International Maritime Safety, Environmental Affairs, and Shipping* 7, no. 4, 2023: 2286409.
[87] Ahmad, Nehaluddin, Faizan Mustafa, and Hanan Abdul Aziz. "Responsibility to Rescue Refugees at Sea under International Law." *JE Asia & Int'l L.* 16, 2023:pp 363.
[88] Kim, Tae-eun, Lokukaluge Prasad Perera, Magne-Petter Sollid, Bjørn-Morten Batalden, and Are Kristoffer Sydnes. "Safety challenges related to autonomous ships in mixed navigational environments." *WMU Journal of Maritime Affairs* 21, no. 2, 2022:pp 147.

## Conclusion

To sum up, this study has evaluated how the emerging technologies, including autonomous vessels and maritime cybersecurity, influence the safety and security of the maritime industry, especially concerning modifications in the legal framework. The findings have shown that, even with the increasing trend in the use of new technologies, the legal frameworks, as they currently stand, are not having any significant role in the occurrence of the maritime safety incidents, as well as the rate of cybersecurity breaches. In particular, the statistical tests indicated weak or non-significant correlations between the level of technological developments and safety accidents, and legal adjustments and cybersecurity violations. These observations imply that as much as the legal regimes guiding the maritime industry are necessary to ensure order, they might not be properly responding to any issue that arises with technological advancements in the industry.

- ✓ This research examined the suitability of the United Nations Convention on the Law of the Sea (UNCLOS) to deal with the issues of emerging technology, which in this case is autonomous vessels and cybersecurity in the maritime sector. It was discovered that whereas UNCLOS has offered a legal framework that is comprehensive in the management of maritime boundaries, navigation, and resource rights, it does not contain provisions that specifically undertake the new risks that are brought about by the technological advancement. The identified gap is the lack of specifications on the jurisdiction, liability, and legal status of autonomous vessels, implications of cyber threats of maritime operations. The solution under consideration is the reform of UNCLOS to include the provisions that directly are aimed at autonomous ships, clarification of the jurisdictional matters, and offer an international structure of responding to the threat of cybersecurity in the maritime scope. These reforms would increase the predictability and security of maritime operations in the context of technological innovation in the law.

The research has also examined how Safety of Life at Sea (SOLAS) Convention has contributed to maritime safety even in the face of fast changing technologies. The results show that although SOLAS has been successful in controlling conventional safety aspects in the maritime sector, it has not done enough to modify to the technological changes, especially on the aspect of autonomous ships and increased cybersecurity challenges. The identified gap is the absence of special regulations regarding the functioning of autonomous ships and the necessity of the

cybersecurity standards to safeguard the key infrastructures of maritime communication. To overcome the presented challenges, it is suggested that SOLAS could be modified to incorporate certain provisions concerning autonomous vessel operation, cybersecurity measures, and the incorporation of the emerging technologies into the safety framework. The reforms would aid in making sure that SOLAS remains focussed on its initial mission of protecting lives on the sea despite the changes in technology employed in the maritime operations.

Finally, the research has observed the impacts of the International Convention on the Prevention of pollution by ships (MARPOL) concerning new technologies. The analysis has shown that, although MARPOL has been able to address the problem of ship-related pollution, it has failed to regard the consequences of more modern technologies, including the rise of autonomous ships or the digitization of maritime systems. The loophole revealed in MARPOL is that it does not consider the risks of the growing dependence on digital systems in the operation of vessels, which might entail exposing the environment to new types of pollution, namely, the cyberattacks on the environmental management systems. It has been suggested that MARPOL should be amended with the provisions that would take into consideration the environmental effect of technological progress, such as the environmental risk of the autonomous vessels and digital systems. These reforms would see to it that MARPOL does not become obsolete by the changing maritime technology and also that it still plays its role of ensuring that the marine environment is not polluted.

The fact that few cases of safety Incidents and cybersecurity breaches are affected by legal changes is evidence of the necessity of an even more fine-tuned perspective on the concept of maritime safety and security. Apparently, other applications, like technological infrastructure, human error, and operating practice are more influential in influencing the results in these locations. Further, the slowness of the process of adapting international legal frameworks to new technologies such as autonomous vessels and digital systems is another factor that makes the situation tougher. This slowness to adopt technological changes may leave spaces in security that may expose the maritime industry to new threats, especially with cybersecurity. The findings of this paper highlight that there is the need to adopt a multidimensional strategy to tackle the fast-changing issues in the maritime industry.

Also, the findings of the regression and correlation studies indicate that though technology is a significant parameter, it is not always associated with better safety results. With the maritime industry still embracing new technologies, there is an extreme necessity of a legal and regulatory reformation that can combine the new technologies and find a solution to the new threats. This will amount to international collaboration, because in most cases, maritime 1982 Law s may cross the borders of nations. Additionally, the study notes that smaller maritime stakeholders especially those in the developing areas might not easily embrace these technologies thus worsening the different inequalities that may exist in the industry. It is important to adopt a more comprehensive situation where all concerned parties have the same platform to meet the demands of the modern day maritime operations to sustain world maritime security and safety.

Finally, the results are indicating that urgent changes in the legal frameworks are necessary that are more flexible and receptive to the technology. When the maritime industry is shifting to the stage of increased digitalization and the use of autonomous vessels, the changes in the legal frameworks are inevitable to make sure that these advancements will be properly regulated. The findings of this research are supposed to be a basis of further research and policy formulation in terms of how legal and regulatory agencies can better facilitate the deployment of emerging technologies without impairing the safety and security.

**Recommendations**

- Among the core solutions is to reinforce the cybersecurity 1982 Law s in the maritime industry. Considering the rising use of digital systems and automated technologies, the threat of cyberattacks is increasing exponentially. The results of the research point out that alterations to the system of 1982 Law s are critical, yet they cannot be used to reduce the risks of cybersecurity. To solve this, there should be a worldwide standard of cybersecurity in the maritime industry which would place specific regulations on the protection of infrastructure, privacy of data and measures that should be taken in the event of an attack. In addition, the periodic cyber audits and updates must be required to make sure that the maritime operators are well prepared to deal with new threats. This will involve the international maritime organizations, governments and stakeholders in the private sector.

- The analysis shows that the existing maritime regulations including those that address autonomous vessels and safety regulations are not usually responsive to new technological innovations. Because of this, the current situation demands the urgent need to increase global cooperation in modernizing and standardizing legislation. The United Nations Convention on the 1982 Law of the Sea (UNCLOS) and other regional treaties should be updated to reflect the high rate of technological advancement. It must also be more proactive and not just through legal experts but also through the experts in technology as well to make sure that international maritime 1982 Law s are adaptable enough to accommodate the risks and opportunities offered by autonomous shipping, computer navigation systems, and other innovations. This transnational initiative will assist in developing a more consistent and unified regulatory framework, which will reduce the areas of jurisdiction and make sure that all maritime actors are ready to address emerging challenges.
- The study brings out the differences in technology adoption and preparedness of the maritime stakeholders, especially smaller maritime operators in the developing areas. Training programs and capacity building of these smaller stakeholders should be emphasized in order to provide them equitable access to new technologies. Government and industry can join forces to provide training, technical assistance, and financial aid to enable these organizations to absorb the emerging technology like automated ships and modern navigation system. Moreover, regional workshops/ knowledge sharing platforms might also help to share the best practice so that all maritime actors are able to manage the technological changes successfully. This will not only enhance the general level of safety and security of the maritime industry but also decreases technological disparities among the bigger and smaller stakeholders.

# References


Ahmad, Nehaluddin, Faizan Mustafa, and Hanan Abdul Aziz. "Responsibility to Rescue Refugees at Sea under International Law." *JE Asia & Int'l L.* 16 (2023): 363.

Armstrong, Chris. "The United Nations Convention on the Law of the Sea, global justice and the environment." *Global Constitutionalism* 13, no. 1 (2024): 16-20.

ASOK, AKSHAY. "AUTONOMOUS SHIPS IN MARITIME LAW: CHALLENGES TO LIABILITY, SAFETY, AND SHIPPING PROTOCOLS." (2025).

Autsadee, Yuthana, Jagan Jeevan, Nurul Haqimin Bin Mohd Salleh, and Mohamad Rosni Bin Othman. "Digital tools and challenges in human resource development and its potential within the maritime sector through bibliometric analysis." *Journal of International Maritime Safety, Environmental Affairs, and Shipping* 7, no. 4 (2023): 2286409.

Ballard, Henry, (1840–30 Jan. 1919), Port Captain, Durban, 1884–1904." In *Who Was Who*. Oxford University Press, 2007. https://doi.org/10.1093/ww/9780199540884.013.u193052.

Baumler, Raphael, Maria Carrera Arce, and Anne Pazaver. "Quantification of influence and interest at IMO in Maritime Safety and Human Element matters." *Marine Policy* 133 (2021): 104746.

Bueger, Christian, and Tobias Liebetrau. "Critical maritime infrastructure protection: What's the trouble?." *Marine policy* 155 (2023): 105772.8

Christodoulou, Anastasia, and Jonatan Echebarria Fernández. "Maritime Governance and International Maritime Organization instruments focused on sustainability in the light of United Nations' sustainable development goals." In *Sustainability in the Maritime Domain: Towards Ocean Governance and Beyond*, pp. 415-461. Cham: Springer International Publishing, 2021.

Chuah, Lai Fatt, Kasypi Mokhtar, Anuar Abu Bakar, Mohamad Rosni Othman, Nor Hasni Osman, Awais Bokhari, Muhammad Mubashir, Mohd Azhafiz Abdullah, and Mudassir Hasan. "Marine environment and maritime safety assessment using Port State Control database." *Chemosphere* 304 (2022): 135245.

Churchill, Robin, Vaughan Lowe, and Amy Sander. *The law of the sea*. Manchester University Press, 2022.

Coito, Joel. "Maritime autonomous surface ships: New possibilities—and challenges—in ocean law and policy." *International Law Studies* 97, no. 1 (2021): 19.

David, Matej, Stephan Gollasch, Brian Elliott, and Chris Wiley. “Ballast Water Management Under the Ballast Water Management Convention.” In *Global Maritime Transport and Ballast Water Management*. Springer Netherlands, 2014. https://doi.org/10.1007/978-94-017-9367-4_5.

Diemer, Andreas, Simona Iammarino, Andrés Rodríguez-Pose, and Michael Storper. "The regional development trap in Europe." *Economic Geography* 98, no. 5 (2022): 487-509.

Dirhamsyah, Dirham, Saiful Umam, and Zainal Arifin. "Maritime law enforcement: Indonesia's experience against illegal fishing." *Ocean & Coastal Management* 229 (2022): 106304.

Durlik, Irmina, Tymoteusz Miller, Danuta Cembrowska-Lech, Adrianna Krzemińska, Ewelina Złoczowska, and Aleksander Nowak. "Navigating the sea of data: a comprehensive review on data analysis in maritime IoT applications." *Applied Sciences* 13, no. 17 (2023): 9742.

Durmuş, Aybüke Naz. "The Intersection Between Law and Technology in Maritime Law." In *The regulation of automated and autonomous transport*, pp. 107-166. Cham: Springer International Publishing, 2023.

EL SAKTY, K. H. A. L. E. D., and ALIA EMAD ISLAM. "DEVELOPING ACCOUNTABLE MARITIME TRANSPORT AND PORT ORGANIZATIONAL STRUCTURES IN ARAB COUNTRIES." *WIT Transactions on The Built Environment* 212 (2022): 149-160.

*Figure 10 - Growth of R&D Personnel and Researchers, 1998-2008*. n.d. https://doi.org/10.1787/888932332778.

Forti, Nicola, Enrica d’Afflisio, Paolo Braca, Leonardo M. Millefiori, Sandro Carniel, and Peter Willett. "Next-gen intelligent situational awareness systems for maritime surveillance and autonomous navigation [Point of View]." *Proceedings of the IEEE* 110, no. 10 (2022): 1532-1537.

Fulton, Thomas Wemyss. *The sovereignty of the sea: an historical account of the claims of England to the dominion of the British seas, and of the evolution of the territorial waters*. DigiCat, 2022.

*Global Maritime Distress and Safety System (GMDSS)*. n.d. https://doi.org/10.3403/bsen61097.

*Glossary of Aeronautical Terms: Air Traffic and Ground Services*. n.d. https://doi.org/10.3403/30305534.

Götz, Roland. "Nord Stream 2." *Osteuropa* 69, nos. 1–2 (2019): 23 - 32. https://doi.org/10.35998/oe-2019-0014.

Im, Myeong-Hwan, and Ho-Sig Sin. "A Study on the Port State Control Inspection Results of Tokyo MOU : Focused on Detentions of Tokyo MOU." *JOURNAL OF FISHRIES AND MARINE SCIENCES EDUCATION* 29, no. 2 (2017): 333 - 342. https://doi.org/10.13000/jfmse.2017.29.2.333.

International Court of Justice (ICJ), Australia v. Japan: New Zealand Intervening**,** *Whaling in the Antarctic (Australia v. Japan)*, *Judgment*, 2014, https://www.icj-cij.org/en/case/148

International Tribunal for the Law of the Sea (ITLOS), Case No. 3, Guyana v. Suriname, *Maritime Boundary Delimitation in the Atlantic Ocean*, 2004, http://www.itlos.org/cases/list-of-cases/case-no-3/

Islam, Md Syful. "Maritime security in a technological era: Addressing challenges in balancing technology and ethics." *Mersin University Journal of Maritime Faculty* 6, no. 1 (2024): 1-16.
*ISM Code*. International Maritime Organization, 2018. https://doi.org/10.62454/kd117e.

Issa, Mohamad, Adrian Ilinca, Hussein Ibrahim, and Patrick Rizk. "Maritime autonomous surface ships: Problems and challenges facing the regulatory process." *Sustainability* 14, no. 23 (2022): 15630.

Jayasuriya, Kanishka. "Regionalising the state: political topography of regulatory regionalism." *Contemporary Politics* 14, no. 1 (2008): 21-35.

Jia, Bing Bing. "The Principle of the Domination of the Land over the Sea: A Historical Perspective on the Adaptability of the Law of the Sea to New Challenges." *German YB Int'l L.* 57 (2014): 63.

Kamiński, Tomasz, and Karol Karski. *40 Years of the United Nations Convention on the Law of the Sea: Assessment and Prospects*. Taylor & Francis, 2025.

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

Kerr, Baine P. "Binding the international maritime organization to the united nations convention on the law of the sea." *International Organizations Law Review* 19, no. 2 (2022): 391-422.

Kim, Tae-eun, Lokukaluge Prasad Perera, Magne-Petter Sollid, Bjørn-Morten Batalden, and Are Kristoffer Sydnes. "Safety challenges related to autonomous ships in mixed navigational environments." *WMU Journal of Maritime Affairs* 21, no. 2 (2022): 141-159.

Kotzampasakis, Manolis. "Intercontinental shipping in the European Union emissions trading system: A 'fifty–fifty'alignment with the law of the sea and international climate law?." *Review of European, Comparative & International Environmental Law* 32, no. 1 (2023): 29-43.

Kraska, James, and Young-Kil Park, eds. *Emerging Technology and the Law of the Sea*. Cambridge University Press, 2022.

Leal-Arcas, Rafael. "Theories of Supranationalism in the EU." *Journal of Law in Society* 8, no. 1 (2007): 83-113.

Lee, Seokwoo. "Evolution of the law of the sea and ocean policy in northeast Asia." *Ocean Development & International Law* 55, no. 4 (2024): 501-512.

Lost-Siemińska, Dorota. "The United Nations Convention on the Law of the Sea and the International Maritime Organization–40 years of harmonious coexistence." *Prawo Morskie* (2022): 9-24.

Ma, Chao, Jun Yang, Jianyun Chen, Zhi Qu, and Chao Zhou. "Effects of a Navigation Spoofing Signal on a Receiver Loop and a UAV Spoofing Approach." *GPS Solutions* 24, no. 3 (2020). https://doi.org/10.1007/s10291-020-00986-z.

Maljean-Dubois, Sandrine. "Regional Organisations: The Case of the European Union." *Oxford Handbook of International Environmental Law,* (2021).

Mankowski, Peter. “Article 25.” In *Commercial Law*. Nomos Verlagsgesellschaft mbH & Co. KG, 2018. https://doi.org/10.5771/9783845276564-449.

McDougal, Myres S., and Trevor J. Burke. *The public order of the oceans: a contemporary international law of the sea*. Vol. 2. Martinus Nijhoff Publishers, 2024.

Melnyk, Oleksiy, and Svitlana Onyshchenko. "Ensuring safety of navigation in the aspect of reducing environmental impact." In *International Symposium on Engineering and Manufacturing*, pp. 95-103. Cham: Springer International Publishing, 2021.

Melnyk, Oleksiy, Svitlana Onyshchenko, Oleg Onishchenko, Oleh Lohinov, Valentyna Ocheretna, and Yurii Dovidenko. "Basic aspects ensuring shipping safety." *Zeszyty Naukowe. Transport/Politechnika Śląska* 117 (2022): 139-149.

Mesgarani, Hamid, Hamid Safdari, and Abolfazl Ghasemian. “Solving Optimal Control Problems with Integral Equations or Integral Equations - Differential with the Help of Cubic B-Spline Scaling Functions and Wavelets.” *Mathematical Researches* 6, no. 1 (2020): 119 - 138. https://doi.org/10.52547/mmr.6.1.119.

Mhatre, Purva, Rohit Panchal, Anju Singh, and Shyam Bibyan. "A systematic literature review on the circular economy initiatives in the European Union." *Sustainable Production and Consumption* 26 (2021): 187-202.

Musyaffa, Nadhif Fadhlan, Arie Kusuma Paksi, and Lalu Radi Myarta. "Measuring the dominant paradigma in United Nations Convention on the Law of the Sea." *Lampung Journal of International Law* 4, no. 2 (2022): 87-96.

Nawrot, Justyna. "24 (R) evolution of maritime safety in IMO conventions and UNCLOS." In *40 Years of the United Nations Convention on the Law of the Sea*, p. 309. 2025.

Nguyen, Do Duc Anh, Pierre Alain, Fabien Autrel, Ahmed Bouabdallah, Jérôme François, and Guillaume Doyen. “How Fast Does Malware Leveraging EternalBlue Propagate? The Case of

WannaCry and NotPetya.” *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*, IEEE, June 24, 2024, 399. https://doi.org/10.1109/netsoft60951.2024.10588886.

Nielsen, Jens Cosedis, and ESC Scientific Document Group. "2024 ESC Guidelines for the management of atrial fibrillation developed in collaboration with the European Association for Cardio-Thoracic Surgery (EACTS)." *European Heart Journal* 45, no. 36 (2024): 3314-3414.

Palippui, Habibi. "Integration of Technology and Regulations for Safe and Efficient Marine Logistics." *Collab. Eng. Dly. Book Ser* 2 (2024): 1-7.

Qasim, Nameer Hashim, Hayder Imran Al-Helli, Iryna Savelieva, and Aqeel Mahmood Jawad. "Modern Ships and the Integration of Drones–a New Era for Marine Communication." *Розвиток транспорту* 4 (2023): 56-78.

Rahimi, Shayan. "Legal Examination of the International Maritime Organization's Approaches to Environmental Protection." *International Journal of Advanced Research in Humanities and Law* 2, no. 2 (2025): 28-41.

Ricardianto, Prasadja, Reza Fauzi Jaya Sakti, Honny Fiva Akira Sembiring, and Zaenal Abidin. "Safety study on state ships and commercial ships according to the requirements of Solas 1974." *Journal of Economics, Management, Entrepreneurship, and Business (JEMEB)* 1, no. 1 (2021): 1-11.

Rothwell, Donald R., and Tim Stephens. "The international law of the sea." (2023): 1-656.

Schimmelfennig, Frank. "European regional organizations, political conditionality, and democratic transformation in Eastern Europe." *East European politics and societies* 21, no. 1 (2007): 126-141.

Schnakenbourg, Eric. “Baltic Sea.” In *Atlantic History*. Oxford University Press, 2017. https://doi.org/10.1093/obo/9780199730414-0202.

Sihombing, Derma Watty, Nurindah Dwiyani, Yayu Nopriani Martha, and Christiani Hutabarat. "Impact of International Standards on Maritime Education: Perspectives of Junior Cadets." *Meteor STIP Marunda* 17, no. 1 (2024): 7-15.

Siregar, Ghea Regita Maharani, Florianus Yudhi Priyo Amboro, and Lu Sudirman. "Effectiveness of Implementation of the 1974 SOLAS Convention Regarding Safety Standards at Public Ports in Batam City." *LEGAL BRIEF* 14, no. 1 (2025): 41-50.

Strati, Anastasia. *The protection of the underwater cultural heritage: an emerging objective of the contemporary law of the sea*. Vol. 23. Brill, 2021.

Strati, Anastasia. *The protection of the underwater cultural heritage: an emerging objective of the contemporary law of the sea*. Vol. 23. Brill, 2021.

Strati, Anastasia. *The protection of the underwater cultural heritage: an emerging objective of the contemporary law of the sea*. Vol. 23. Brill, 2021.

Sumer, M. “THE RELEVANCE OF THE LAW OF TREATIES IN THE INTRODUCTION OF MASS OPERATIONS – UNCLOS & SOLAS.” *Autonomous Ships 2022*, ahead of print, April 1, 2022. https://doi.org/10.3940/rina.as.2022.10.

Tamada, Dai, and Keyuan Zou. *Implementation of the United Nations Convention on the Law of the Sea*. Springer Singapore, 2021.

Toelihere, Ivan Filbert, Lukman Yudho Prakoso, and Panji Suwarno. "The Role of Maritime Policy in Supporting Global Security Sustainability and Stability." *Available at SSRN 5082198* (2025).

Uski, Santeri. "Enclosed Space Entry and Rescue drills mandated by SOLAS and their implementation in practice." Maritime Safety Journal 28, no. 4 (2021): 245-258.

Vio, Igor, and Mate Brdar. "Maritime autonomous surface ships–international and national legal framework." *Pomorski zbornik* 62, no. 1 (2022): 141-155.

Wam, Rachel. "Climate Change Loss and Damage: A Case for Mandatory Cooperation and Contribution under the United Nations Convention of the Law of the Sea (UNCLOS)." *UCLA J. Env't L. & Pol'y* 42 (2024): 47.

Wang, Jingbo, Kaiwen Zhou, Wenbin Xing, Huanhuan Li, and Zaili Yang. "Applications, evolutions, and challenges of drones in maritime transport." *Journal of Marine Science and Engineering* 11, no. 11 (2023): 2056.

Wang, Qiuwen, Hu Zhang, Jiabei Huang, and Pengfei Zhang. "The use of alternative fuels for maritime decarbonization: Special marine environmental risks and solutions from an international law perspective." *Frontiers in Marine Science* 9 (2023): 1082453.

Youngsoo, Park, Gokhan Camliyurt, Efraín Porto Tapiquén, et al. *Enhancing Shipboard Oil Pollution Prevention: Machine Learning Innovations in Oil Discharge Monitoring Equipment*. Elsevier BV, 2024. https://doi.org/10.2139/ssrn.4888923.

Articles.” In *Managing Aggression*. Routledge, 2002. https://doi.org/10.4324/9780203193914-62.

Chapter 2. Ethical Norms And Procedures.” In *Ethics and Regulation of Clinical Research*. Yale University Press, 2017. https://doi.org/10.12987/9780300163490-005.

Chapter IX: Management for the Safe Operation of Ships.” In *SOLAS*. International Maritime Organization, 2024. https://doi.org/10.62454/kh110e.048.

Chapter VII: Carriage of Dangerous Goods 1 ; Part A: Carriage of Dangerous Goods in Packaged Form.” In *SOLAS*. International Maritime Organization, 2024. https://doi.org/10.62454/kh110e.042.

Energy Efficiency Design Index (EEDI).” In *Encyclopedia of Ocean Engineering*. Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-10-6946-8_300238.

Marpol, n.” In *Oxford English Dictionary*. Oxford University Press, 2023. https://doi.org/10.1093/oed/5240290816.

Marpol, n.” In *Oxford English Dictionary*. Oxford University Press, 2023. https://doi.org/10.1093/oed/5240290816.

Special Obligations of the Flag State: Article 217.” In *Enforcing International Maritime Legislation on Air Pollution Through UNCLOS*. Hart Publishing, 2019. https://doi.org/10.5040/9781509927791.ch-008.

UNCLOS.” In *Enforcing International Maritime Legislation on Air Pollution Through UNCLOS*. Hart Publishing, 2019. https://doi.org/10.5040/9781509927791.ch-003.

## Summary

**Technology and the Law of the Sea: Maritime Safety and Security**

**Omar Ejjadghi**

This thesis has explored how emerging technologies, such as autonomous ships and cybersecurity, affect maritime safety and security according to the United Nations Convention on the Law of the Sea (UNCLOS 1982). This was to determine how technology has posed a challenge to current international laws and recommend needed reforms. According to the research, the doctrinal legal study was used, which employed both the case studies and secondary sources like the scholarly articles and legal documents. It found important legal issues in the jurisdiction, liability and cybersecurity. Though technology could have made maritime safety and operational considerably safer, technological advancements posed new risks that the current laws were unprepared to address. The results showed that UNCLOS and other conventions such as SOLAS (Safety of life at sea) had to be revised significantly due to the legal complexities that new autonomous vessels and the cyber threats posed. It was concluded in the thesis that international maritime law had to be reformed to keep up with these technological changes. Among the proposed reforms were the revision of legal stipulations in autonomous vessels, improved cybersecurity implementations, and fair equitable access to maritime technologies and more so to the small island developing states.

## Santrauka

Ši disertacija nagrinėjo naujųjų technologijų, ypač autonominių laivų ir kibernetinio saugumo, poveikį jūrų saugumui ir apsaugai pagal 1982 metų Jungtinių Tautų jūrų teisės konvenciją (UNCLOS). Pagrindinis tikslas buvo įvertinti, kaip technologiniai pasiekimai kėlė iššūkius esamiems tarptautiniams teisės aktams ir pasiūlyti reikalingas reformas.

Tyrimas buvo atliktas taikant doktrininius teisinius metodus, apimant atvejo analizę ir antrinius šaltinius, tokius kaip moksliniai straipsniai ir teisiniai dokumentai. Tyrimas atskleidė reikšmingas teisines problemas, susijusias su jurisdikcija, atsakomybe ir kibernetiniu saugumu. Nors technologijos turėjo potencialo pagerinti jūrų saugumą ir operacijų efektyvumą, jos taip pat sukūrė naujų rizikų, kurioms esami teisės aktai nebuvo pakankamai parengti.

Rezultatai parodė, kad UNCLOS ir tokios konvencijos kaip SOLAS (Gyvybės saugojimo jūroje konvencija) reikalavo esminių pakeitimų, kad būtų atsižvelgiama į autonominių laivų ir

kibernetinio saugumo keliamus teisės iššūkius. Disertacija baigėsi išvada, kad tarptautinė jūrų teisė turėjo būti reformuota, siekiant prisitaikyti prie šių technologinių pokyčių. Pasiūlytos reformos apėmė teisinių nuostatų atnaujinimą autonominiams laivams, kibernetinio saugumo priemonių stiprinimą ir teisingą prieigą prie jūrų technologijų, ypač mažoms saloms skirtoms valstybėms.