Ars Iuris Salmanticensis
ESTUDIOS
Vol. 12, doi: https://doi.org/10.14201/AIS20241221139
Diciembre 2024
eISSN: 2340-5155

For a Future-Proofed Law of the Sea: Challenges and Opportunities Emerging from the Rapid Development of Technology

Hacia una legislación marítima a prueba de futuro: desafíos y oportunidades derivadas del rápido desarrollo tecnológico

Dina QASMI NABIL
Phd candidate Abdelmalek Essaadi University, the Faculty of Legal, Economic and Social Sciences, Center for Doctoral Studies. Tangiers, Morocco
dina.qasmi@gmail.com
https://orcid.org/0009-0007-3970-4637

Recibido: 24/10/2024
Aceptado: 04/11/2024

Abstract

In light of the recent technological developments such as artificial intelligence, space exploration technologies, etc., the urgent need to adopt a sustainable approach to laws and policies is now widely recognized. It is undoubtedly a contentious issue to make the law of the sea

Resumen

A la luz de los recientes avances tecnológicos, como la inteligencia artificial y las tecnologías de exploración espacial, se reconoce de manera general la urgente necesidad de adoptar un enfoque sostenible en las leyes y políticas. Hacer que la legislación marítima

future-proofed and future-focused. The need to re-evaluate the maritime legal system is, however, more pressing than ever.
This paper will analyze the current and future intersection between the law of the sea and new technologies and will focus on ways to develop a forward-looking and more future-proofed framework for the law of the sea.
The study will raise questions about the extent and the capability of the legal imagination to match technological development. It will suggest how to rethink the current legal framework in a way that lawmakers and scientists closely work together to prevent maritime security issues. Consequently, it will not only focus on how to make the law of the sea future-proofed but also how to make its provisions future-oriented and in line with technological advances.

Keywords: law of the sea; maritime security; sustainable approach; resilience; legal imagination; artificial intelligence.

esté a prueba de futuro y orientada al futuro es, sin duda, un tema polémico. Sin embargo, la necesidad de reevaluar el sistema jurídico marítimo es más apremiante que nunca.
Este documento analizará la intersección actual y futura entre la legislación del mar y las nuevas tecnologías, y se centrará en cómo desarrollar un marco más proactivo y adaptado a los cambios del entorno. La investigación planteará interrogantes sobre la capacidad de la imaginación jurídica para seguir el ritmo del desarrollo tecnológico. Sugerirá maneras de repensar el marco legal actual para que legisladores y científicos colaboren estrechamente en la prevención de problemas de seguridad marítima. Así, no solo se buscará cómo hacer que la legislación marítima esté a prueba de futuro, sino también cómo alinear sus disposiciones con los avances tecnológicos.

Palabras clave: legislación marítima; seguridad marítima; enfoque sostenible; resiliencia; imaginación jurídica; inteligencia artificial.

1. INTRODUCTION

Oceans and seas are essential not only for global security but also for the economic well-being of nations, as activities like commercial shipping, navigation, and various forms of maritime exploration serve as crucial sources of sustenance for many states. Despite their importance, the maritime domain encounters a myriad of complex challenges and threats, encompassing both legal and ethical dimensions. In this context, the Law of the Sea provides a comprehensive legal framework that is fundamental to tackle these issues.

Time and the changes it brings is has become a significant concern highlighting the need for a more resilient body to protect seas and maritime activities from emerging threats and challenges while preserving resources. As a consequence, maritime security started to resonate, now more than ever, on both national and international levels. Although the expression is not new, it resurfaced with new technologies, specifically Artificial Intelligence (AI) among others.

Perceptions and awareness regarding the concept of maritime security have changed in the last few years from a specialized and constrained viewpoint to one that is more comprehensive in its analysis of the relevant problems.

It is worth noting that no universal definition or consensus on maritime security has emerged yet[1]. The United Nations Convention on the Law of the Sea UNCLOS as the reference legal framework for the use of maritime spaces and resources, does not refer to or define maritime security[2]. However, even if UNCLOS does not specifically refer to maritime security, it serves as a foundation for it in its broad conceptualization by outlining the rights and responsibilities of states. The absence of a universal definition is nonetheless supplemented by other treaties, UN resolutions, and customary international law related to major security threats in the maritime domain regulated directly or indirectly under UNCLOS[3].

Maritime security can be seen as a nexus of various state and non-state concerns. The issues related to maritime security are often addressed in multiple provisions and bodies such as UNGA[4] resolutions or UNSC[5] periodic reports. In this regard, these two United Nations bodies contributed significantly to identifying challenges that qualify as maritime security threats and proposing measures to enhance the safety and security of maritime activities worldwide.

In this spirit, maritime security can be described as a general term that draws attention to new challenges[6] and threats that prevail in the maritime domain[7] and rallies support for tackling them. As highlighted by Rao, maritime security represents a relatively modern notion that differs from traditional naval security projections and embodies an

1. KLEIN, N. 2011: *Maritime Security and the Law of the Sea*. Oxford University Press, 8.
2. In general, science depends heavily on exact definitions of ideas, concepts and parameters that are widely accepted. This is because having explicit definitions promotes standardization, improves communication, and enables the unambiguous sharing of knowledge. Thus the importance of standardization and commonly agreed upon definitions of concepts.
3. UK Parliament. *UNCLOS: The Law of the Sea in the 21st Century*. 2nd Report of Session 2021-22, published 1 March 2022, HL Paper 159.
4. UN General Assembly Resolution A/RES/73/292 (2019).
5. UN Security Council Resolution 2383 (2017).
6. BUEGER, C. 2015: «What is Maritime Security?». *Marine Policy*, 2015, 53: 159.
7. KRASKA, J. and PEDROZO, R. 2013: *International Maritime Security Law*. Martinus Nijhoff Publishers.

evolving comprehensive construct encompassing several interconnected aspects of the maritime domain[8].

In light of these rapid technological developments, maritime security is facing multiple threats and challenges. States have to handle the positive but also and especially the negative use of these new technologies especially given their proliferation and accessibility. Hence, the need to adopt a sustainable and resilient approach to laws and policies. The question that arises is: Can smart technologies help decision-makers develop a robust and more resilient framework that ensures maritime security?

In this context, the working hypothesis of this study is that the rapid pace of smart technologies, particularly AI, can significantly enhance maritime security by improving threat detection, response strategies, and resource management. However, the existing legal framework under the United Nations Convention on the Law of the Sea (UNCLOS) must be adapted and integrated with these technologies to ensure a sustainable, resilient, and future-proof maritime security regime that effectively addresses both emerging and traditional maritime threats.

This paper will analyze the current and future intersection between the law of the sea and new technologies and will focus on ways to develop a forward-looking and more future-proofed framework for maritime security. In addition, the study will also focus on the extent and the capability of the legal imagination[9] to match the current technological era. It will suggest how to rethink the current legal framework in a way that lawmakers and scientists closely work together to better address and prevent maritime security issues.

To be able to address the main research question, it is essential to first lay a foundational understanding of the complexity and multidimensional nature of maritime security, providing a holistic approach that integrates traditional threats with emerging concepts. By examining the relationships between seapower, marine safety, the blue economy, and human security (2). Following this, we will explore the evolving concept of maritime security in the digital era, by examining the emerging threats and the role of technology in reshaping security strategies at sea (3). The following section will then look towards the future, exploring a forward-looking approach to maritime security, where we discuss potential innovations and strategic adaptations for the maritime domain (4). Finally, in Section (5), the paper will conclude with a summary of the key findings and provide recommendations for policy-makers and stakeholders. Through this, we aim to gain a comprehensive understanding of maritime security and contribute towards its future-proofing.

8. RAO, I. A. (retd). 2023: *Maritime Security: Challenges & Responses in a Changing World*. 1st ed. IPS Press.

9. WHITE, J. B. 1985: *The Legal Imagination*. 2nd ed. Abridged Edition.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

2. UNDERSTANDING THE MULTIFACETED NATURE OF MARITIME SECURITY: KEY CONCEPTS AND THEIR INTERCONNECTIONS

Instead of examining the scope of maritime security through the classic conceptualization method consisting of exploring the different security threats related to it (e.g., piracy, Illegal, Unreported, and Unregulated Fishing IUUF, marine pollution…), another approach of concept analysis will be adopted in this chapter, focusing on the multifaceted nature of maritime security and connecting it to various key concepts.

This approach allows the analysis of maritime security while taking into consideration the complexity of the concept and its ever-changing and context-dependent nature[10]. This method can also provide a more holistic and future-oriented approach where in addition to the above-mentioned threats, emerging challenges can also be included in the concept.

Since no universal definition of maritime security exists and as concepts usually acquire their meaning from their interference with other concepts, the notion of maritime security could be intended at large as a term that refers to a comprehensive architecture of a minimum of four different concepts presenting some form of correlation to the secure use of maritime spaces and resources including but not exclusively: seapower, marine safety, blue economy, and human security.

Each of these concepts highlights different facets of maritime security. The terms «seapower» and «marine safety» reflect traditional views on dangers at sea. However, blue economy, and human security are closely connected to the rise of maritime security.

This maritime security matrix, «organizes a web of relations, replaces or subsumes older established concepts, as well as relates to more recently developed ones»[11] and by examining the links between these concepts, we can understand the term maritime security from a holistic approach.

The concept of seapower has been discussed in various scientific, political, and international relations domains. It was first introduced by Mahan[12] as a strategic concept. Mahan invented the term 'seapower', but he could not clearly and succinctly articulate his strategic concepts.

10. See More on the approach followed by the author in analysing the concept of maritime security through connected concepts BERENSKOTTER, F. 2016: «Approaches to Concept Analysis». *Millennium: Journal of International Studies*, 2016, 45. https://doi.org/10.1177/0305829816651934

11. BUEGER, 2015, 160.

12. MAHAN, A. T. 2010: *The Influence of Sea Power upon History, 1660-1783*. Cambridge: Cambridge University Press.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155

At that time, seapower meant the sum of naval power and transport capabilities[13]. However, Mahan's perspectives on seapower went beyond military considerations. Economic considerations also constituted the core of his reasoning. If «seapower is a part of the national power that arises from the characteristics of the sea and ocean environment»[14], the sea environment, however, has changed functionally since the emergence of the concept.

The concept of seapower has taken into consideration new parameters that go beyond the mere ability to control sea space as pointed out by Geoffrey Till[15] «Seapower must be defined as an input, that is the sum of the various naval and maritime related assets, as well as output, that is, the ability to influence the behavior of other actors». Stated differently, the application of sea power is not just significant at sea, but it also has an impact on land-based processes and behaviors.

One of the key connections between seapower and maritime security is the role of naval forces in maintaining security at sea. Armed forces, especially navies, are often at the forefront of maritime security efforts. Their ability to project power, defend shipping lanes, conduct anti-piracy operations, and maintain a presence in international waters is crucial in upholding maritime security. In this sense, naval forces are both a primary actor in ensuring maritime security and a central component of seapower.

Another connection between seapower and maritime security lays in the discourse on military presence and operations beyond national waters. There is ongoing debate about how far the armed forces of a nation should operate outside its territorial waters, whether in international waters or in the exclusive economic zones (EEZ) of other states. Some argue that a strong, proactive naval presence globally is essential for safeguarding maritime security, deterring potential threats, and asserting national influence. Others question the risks and ethical implications of such international military engagement, considering potential sovereignty disputes.

This focus on securing maritime domains inevitably intersects with the broader concept of marine safety, another term for which no universal definition exists, but there is some sort of a consensus on its scope. According to the Oxford Dictionary, the word safety means «the condition of being protected from or unlikely to cause danger, risk, or injury»[16].

Respectively, marine safety can be understood as the protection of life[17] and property of all forms of waterborne transportation. In other words, it means «all measures

13. For more on the concept, see Sekine, D. 2011: *Seapower and Japan's maritime coalition building*.

14. Allahverdizadeh, R. and Karimi, M. 2023: «A New Approach to the Theory of Seapower in the 21st Century (In Times of War and Peace)», 386.

15. Till, G. 2009: *Seapower: A Guide for the Twenty-first Century*. Routledge, 21.

16. *Oxford Dictionary of English*. 3rd ed. Oxford: Oxford University Press, 2010.

17. Particularly in terms of training for the safety of activities onboard and search and rescue.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

taken for the safety of ships and offshore installations, their crews, their passengers, the safety of navigation and the facilitation of maritime traffic, maritime facilities and maritime environment»[18].

The frequent interchange between marine security and maritime safety can create confusion in terms of the scope of each one of these concepts which is why it is worth noting that to achieve maritime security, safety at sea is required. They are two interconnected aspects of ensuring the protection and well-being of the maritime domain and its resources and securing the flow of maritime trade and transport.

As we have seen, marine safety is a critical component in ensuring the stability and security of maritime domains. However, to fully understand the broader implications of maritime security, it is essential to consider the economic and environmental aspects that also shape the future of our oceans. One of the most significant developments in this regard is the concept of the Blue Economy, which emerged as a key focus at the 2012 United Nations Conference on Sustainable Development (UNCSD)[19].

The blue economy was defined as an economy «that results in improved human well-being and social equity, while significantly reducing environmental risks and ecological scarcities» [20]. Blue economy tends to encourage economic growth and development by offering a friendly and risk-free environment in which the economy can operate.

The relationship between Blue Economy and maritime security can be seen through the socio-economic and environmental externalities produced by the unsustainable use of marine spaces and resources. For instance, the overexploitation of marine resources can lead to a decline in fish stocks, affecting the livelihoods and income of coastal communities reliant on fishing. This could result in social unrest, IUU fishing, and conflicts[21] between different user groups, impacting the overall security situation in the maritime domain[22].

18. AFRICAN UNION. 2016: *African Charter on Maritime Security and Safety and Development in Africa*.

19. Or Rio +20 Conference.

20. United Nations Environment Programme. 2012: UNEP 2011 Annual Report, https://wedocs.unep.org/20.500.11822/8053

21. MACKINNON, J. 2019: «Fishery Depletion and the South China Sea». *Fisheries*, 2019, 9(1).

22. Overfishing in the South China Sea has led to tensions between countries like China, Vietnam, and the Philippines. These tensions have escalated to confrontations between fishing vessels, threatening stability and security in the region leading to a substantial conflict dynamic in the form of piracy.

Legal provisions like UNCLOS[23], SDG 14[24], and maritime spatial planning frameworks provide guidance and instruments to tackle these risks, promote sustainable development, and safeguard maritime security.

In this context of growing considerations of the human element and the well-being of individuals and communities, particularly in maritime regions, human security becomes a critical lens through which the protection and prosperity of people, particularly those dependent on the ocean, must be considered.

The concept of human security was established by The United Nations Development Programme (UNDP) in its Human Development Report of 1994. The paper re-examined the idea of security and made a distinction between national security and individual citizen security, with a focus on the latter. As stated in the research, many conflicts are now within nations rather than between nations[25].

Despite the notions established by UNDP, defining human security remains a complex task[26]. The Report recognizes two human security aspects. The first aspect includes being safe from long-term issues like hunger, disease, and repression. The second aspect involves being protected from unexpected disruptions that can negatively affect everyday life, such as disruptions in homes, jobs, or communities.

By understanding that human security includes various dimensions beyond just safety at sea, the misconception that maritime safety is a component of human security can be avoided. Human security highlights the linkage and interdependence of different factors that contribute to ensuring the well-being and prosperity of individuals and states in maritime areas.

In summary, the concept of maritime security has no definite meaning. Its definition depends on the involved actors and their attempts to relate it to other concepts and fields, forming an interconnected matrix where other elements can be added to adjust it to the test of time and the changes it brings about.

As a result, maritime and international law specialists will always be challenged when it comes to harmonizing the practical and theoretical definitions of maritime security. In other words, the practical definition of the concept will always differ among actors[27], across time and geography, and most importantly due to the emerging threats

23. UNCLOS establishes the legal framework for the sustainable use and conservation of marine resources. Article 192 emphasizes the obligation of states to protect and preserve the marine environment, which indirectly contributes to maritime security.

24. For instance, SDG 14 focuses on conserving and sustainably using the oceans, seas, and marine resources. It recognizes the interlinkages between the Blue Economy, environmental sustainability, and maritime security, emphasizing the need for integrated, science-based management approaches.

25. UNDP (UNITED NATIONS DEVELOPMENT PROGRAMME). (1994). *Human Development Report 1994: New Dimensions of Human Security*. New York, 22.

26. ROSSELLO, M. 2022: «Fisheries and the Law of the Sea in the Anthropocene Era». In Pierandrea Leucci e Ilaria Ianiello (eds.): *Ascomare Yearbook on the Law of the Sea*, vol. 2.

27. With their different geopolitical interests and world views.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

that come with technological developments. Hence, «striving for a unanimous definition of maritime security is an unproductive quest»[28].

Having provided some preliminary details and remarks on the concept of maritime security and other connected concepts in the preceding chapter, we will be focusing next on maritime security in the digital era as the transformation of society by digital technology has permeated various aspects of our lives, including the maritime domain.

3. MARITIME SECURITY IN A DIGITAL ERA

Apart from the traditional challenges, the resurgence of wars in recent years, the illegal activities such as piracy, smuggling, and trafficking as well as environmental hazards and potential security impacts of natural or man-made disasters, technology has had a tremendous effect on maritime security, underscoring the significance of our maritime environment.

Automation and technology created new opportunities but also significantly increased remote hijacking risks and other emerging threats. Our oceans have become a battleground not only for physical threats but also for invisible, yet potent, cyber-threats.

The digital era has introduced a new set of risks to the maritime domain, as Sarah PERCY has argued[29] various maritime security challenges are not «traditional security issues, in the sense that they are often lower-order, unconventional threats... that straddle the border between crime and international security»[30]. The main question here is to know if the maritime domains are ready for an era of smart technologies such as AI.

With the growing use of new technologies, the maritime domain is no longer a far playground for hackers and other technology-related threats that can seriously affect the four components of the maritime security matrix. Legally speaking, UNCLOS, which entered into force in 1994, is the main international legal framework governing the use and protection of the world's oceans and marine resources. Various maritime concerns, including maritime security, are covered by UNCLOS by acknowledging that, subject to certain restrictions, every state has the right to conduct maritime security operations within its maritime zones.

UNCLOS is undoubtedly an essential framework in promoting maritime security by ensuring that maritime operations are carried out in compliance with international law and with respect for human rights and by providing states with a legal framework for cooperation in the prevention and suppression of illegal maritime activities. However, primarily designed to address traditional maritime security concerns, covering and

28. BUEGER, 2015, 163.

29. PERCY, Sarah. 2016: «Counter-piracy in the Indian Ocean: A New Form of Military Cooperation». Journal of Global Security Studies, 2016, 1:4: 270-284.

30. AVANT, David D.; P. O. I. R. D. and WESTERWINTER, Oliver (eds.). 2016: The New Power Politics: Networks and Transnational Security Governance. Oxford: Oxford University Press.

keeping up with all the technological and geopolitical changes can be very challenging for an over thirty-year-old text, hence the need for a multi-faceted approach.

Technological advancements have revolutionized maritime activities, including navigation systems, deep-sea exploration, and the use of remotely operated vehicles. These advancements raise new legal and regulatory questions that UNCLOS may not be specifically able to address[31].

The future of maritime security will most likely involve increased dependency on technology, including artificial intelligence and automation[32]. In the following subsections, we will be highlighting some of the rapidly emerging threats that will exacerbate the already harmful effects of traditional sources of pollution, global warming, and overfishing on our oceans as well as the legal framework governing it (or not).

3.1. Maritime cybersecurity: a challenge to international law

Each time brings something of its own, and the rise of the 21st century witnessed major transformation due to substantial technological developments in various fields such as Information Technology (IT) and AI, profoundly affecting the maritime domain.

Cyber-security is defined by the International Telecommunication Union as «the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization, and user's assets»[33].

Although there is no universally agreed definition, the term «maritime cyber security can be defined as cyber-security in the maritime domain which involves safeguarding the sector's Critical Information Infrastructure (CII), guarding against cyber-attacks and/or other unintended errors that may disable, disrupt and take-control of OT[34] infrastructure»[35].

31. H. O. L. 2022: UNCLOS: *The law of the sea in the 21st century*. International Relations and Defence Committee, 2nd Report of Session 2021-22.

32. International Relations and Defence Committee. 2021: Response by Dr Alexandros X. M. Ntovas: UNCLOS: Fit for purpose in the 21st century? University of Southampton, 12.11.2021. for the following questions: What are the main challenges facing the effective implementation of UNCLOS in 2021? Focusing on: Autonomous maritime vehicles (both commercial and military), cybersecurity, and other new technologies. In light of these challenges, is UNCLOS still fit for purpose? Can or should UNCLOS be renegotiated to better address these challenges?

33. INTERNATIONAL TELECOMMUNICATION UNION. 2008: «Overview Cybersecurity».

34. Operational technology is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

35. FITTON, O.; PRINCE, D. and GERMOND, B. 2015: *The Future of Maritime Cyber Security*. Lancaster University.

The information and operational technology systems on board a ship are just as susceptible to hacking as systems on land. These breaches of security could seriously jeopardize the safety and security of ships, ports, marine facilities, and other components of the maritime transportation system. Since the majority of the new systems operate autonomously and are heavily dependent on IT and data flows, the probability of cyberattacks is more significant than ever.

To better illustrate this threat, it is worth noting that in the first few months of the COVID-19 pandemic, attempted cyber attacks rose by 400 % and the costs of global cybercrime are expected to increase by 15 % per year between 2021 and 2025, and reaching USD 10.5 trillion by 2025, compared to USD 3 trillion in 2015[36].

Cyber incidents in the maritime sector might have catastrophic effects[37] on human life, the economy, and the environment. For instance, the massive maritime firm Maersk was the target of a significant cyberattack in June 2017. Malicious spyware prevented employees' computers from opening files, which brought an end to Maersk's port operations. 76 port terminals were shut down by the attack, and despite Maersk's ostensibly prompt response, the corporation ultimately suffered a $300 million loss.

While there are some similarities between cybersecurity challenges in the marine sector and cybersecurity in general, the distinctive features of the maritime industry necessitate a specialized international legal response due to its unique challenges and implications. Furthermore, institutions that are primarily responsible for marine cybersecurity differ from general ones in terms of the applicable international law.

The main question here is to know if the current public international law is fit enough to qualify cybersecurity as a violation and an internationally unlawful act. The answer to that is not as simple as it might seem.

Cyber attacks, in general, don't resemble traditional criminal activities. In Cyber attacks, in contrast with traditional crimes such as terrorism, it is often difficult to establish that the conduct of the issue is criminal[38] as they do not conform to the basic dichotomous threat model that has evolved over the last few centuries[39]. Cyberattacks defy even the simple categorization of weaponry, used in international law, making it very challenging for nations to apply conventional criteria.

Moreover, cyberattacks must first be attributable to a country to qualify as a violation of public international law. However, legal responsibility attribution is always a challenge because it requires a fairly high degree of certainty, and this is not always possible

36. According to Cybersecurity Ventures 2020 report: «Cybercrime to Cost the World $10.5 Trillion Annually by 2025». Accessed November 2024.

37. Even the United Nations' International Maritime Organization was cyber-attacked in September 2020.

38. BRENNER, Susan W. 2009: *Cyberthreats: The Emerging Fault Lines of the Nation State*, 6-7.

39. BRENNER, S. W. 2007: ««At Light Speed»: Attribution and Response to Cybercrime/Terrorism/Warfare». *The Journal of Criminal Law and Criminology*, 2007, 97(2): 379-475.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

in such cases. This leads us to wonder whether there are international obligations that prohibit cyberattacks in the maritime field.

UNCLOS does not specifically govern cyber-security threats. However, navigational rights and freedoms are listed in the provisions regarding the general duty to protect the marine environment without any specific explanation. For instance, the interference with a merchant ship's navigation and damage to that merchant ship constitutes a violation of UNCLOS, mainly under articles 17,19 and 57.

Although UNCLOS does not directly govern cybersecurity threats, some provisions within the convention indirectly address related aspects such as freedom of communication and the protection of undersea cables, it provides protection and preservation measures for communication channels and pipelines against possible physical damage but does not directly address the cybersecurity risks they might face.

UNCLOS recognizes the principle of sovereign immunity, which means that warships, government vessels, and other state-owned ships are immune from the jurisdiction of foreign states. This immunity extends to their communication systems and ensures their protection from unauthorized intrusion.

As Governments and organizations realize the lack of an international law framework regarding cybersecurity threats as well as the urgent and increasing need for protection against cyber attacks, cybersecurity standards and best practices started to see the light.

3.2. Developing a Tailored Framework for Cybersecurity

During the years 2017 and 2018, the maritime industry encountered an unprecedented surge in fraudulent activities, particularly through email scams, phishing attempts, and other deceptive strategies. This trend has been coupled with a growing concern as «Port and shipping line networks are increasingly vulnerable to what appears to be increasingly targeted attacks against maritime systems»[40].

The cybersecurity framework refers to a set of guidelines and best practices that nations, organizations, and other stakeholders ought to follow to strengthen their cybersecurity posture. It aims to help organizations identify, protect, detect, respond to, and recover from cyber threats and incidents.

Cyber-attacks can be carried out by different individuals or groups, each with their motives. These can range from non-state actors trying to cause significant disruptions to state-sponsored programs having widespread international consequences[41]. Thus, there is a need for a tailored framework for cybersecurity.

The need for a tailored framework for cybersecurity specific to each country arises from the fact that every country has unique characteristics, such as legal, cultural, and

40. KESSLER, G. C. 2019: «Cybersecurity in the Maritime Domain». *USCG Proceedings of the Marine Safety & Security Council*, 2019, 76(1).

41. HILLER, A. L. 2017: *The challenge of cybersecurity in the maritime domain: Senior capstone thesis*. California State University Maritime Academy.

technological aspects, which can impact their cybersecurity needs and challenges. A one-size-fits-all approach to cybersecurity would not be effective as different countries face distinct threats and have varying levels of security infrastructure.

Similarly, it is important to have tailored frameworks for cybersecurity at the regional level as maritime activities often occur in regional clusters, such as ports, shipping lanes, or economic zones. These regions may face common cybersecurity risks and encounter similar threats. Developing a framework specific to each region enables collaboration among neighboring countries to address shared risks and vulnerabilities more effectively. It also provides a platform for information exchange, best practices sharing, and collective response to emerging threats.

In this regard, multiple states have their laws and regulations related to maritime cybersecurity in an individual approach or a regional one.

Morocco, for instance, adopted Law No. 05-20 on cybersecurity which aims to establish a legal framework that advocates for a set of rules and security measures to ensure and enhance the security and resilience of information systems in state administrations as well as critical infrastructures with sensitive information systems, that applies to the Moroccan maritime domain as well[42].

In the European Union (EU), the Network and Information Security Directive (NIS Directive) establishes cybersecurity requirements for operators of essential services, including maritime ports and related entities.

While individual countries and regions have unique cybersecurity requirements, cyber threats are not constrained by borders, and malicious actors can target countries indiscriminately therefore, it is equally important to promote interregional and worldwide cooperation.

Various international bodies, such as the IMO and International Electro-Technical Commission (IEC), have developed cybersecurity guidelines and standards for the maritime sector.

Globally speaking and after realizing the growing threat that cyberattacks pose to the maritime sector, the IMO has taken action to create a framework to address cybersecurity concerns through several regulations and guidelines developed by the IMO's Maritime Safety and Maritime Security Committees[43].

Cybersecurity in the maritime field has not been exclusively regulated by the IMO. The IEC has also developed international standards for the electrical and electronic industries with specific cybersecurity standards for maritime systems, such as IEC 62443[44].

42. KINGDOM OF MOROCCO, ADMINISTRATION OF NATIONAL DEFENSE. إدارة الدفاع الوطني المملكة المغربية. [Presentation of Law No. 05-20 on Cybersecurity]. Retrieved from https://www.dgssi.gov.ma/fr/loi-ndeg-0520-relative-la-cybersecurite

43. Such as Resolution MSC.428(98), the International Ship and Port Facility Security (ISPS) Code, the Guidelines on Maritime Cyber Risk Management and Maritime Domain Awareness.

44. While the standard was originally developed for the industrial sector, its principles can be applied to various domains. In the maritime domain, the implementation of IEC 62443 can help protect critical systems and infrastructure against cyber threats as ships and offshore facilities heavily rely on interconnected systems for navigation, communication, and other essential functions.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155

In addition to this, several entities have developed guidelines for cybersecurity in general that can also apply to the maritime field. The Tallinn manual is a good example in this regard.

The Tallinn Manual is a set of guidelines for states in the field of cyberspace. It was published in 2013 by the NATO Cooperative Cyber Defence Centre of Excellence[45] in Tallinn, Estonia.

The manual serves as a comprehensive guide for the legal analysis of cyberspace activities, particularly those conducted by nation-states. It is focused on how international law applies to cyberspace and provides recommendations for state behavior in the cyber domain.

The Tallinn Manual is not legally binding, but it has been influential in shaping international norms. It has been widely referenced by governments, policy-makers, and legal experts around the world to develop their cyber policies and strategies[46].

It is noteworthy that the regulatory framework for cybersecurity in maritime sectors is in a state of constant evolution, with new norms and guidelines actively being formulated to counter emerging threats within this field.

Having examined the challenges and implications of maritime security in the digital era, it is important to shift our focus towards proactive measures that can effectively future-proof the maritime domain legal provisions. As maritime activities continue to evolve amidst technological developments, it is evident that traditional security frameworks must adapt to safeguard against emerging threats. In this regard, the following chapter will be dedicated to the exploration of innovative means to enhance legal provisions for maritime security, highlighting new ways of thinking, futuristic and holistic approaches, and frameworks that can be employed to ensure the durability and adaptability of these regulations in a constantly changing environment.

4. TOWARDS A FUTURISTIC AND FORWARD-LOOKING APPROACH

Given the major transformations occurring in the maritime domain, it is anticipated that the legal framework governing this domain will experience substantial modifications. The advent of digital developments has profoundly influenced the maritime arena, introducing both emerging threats — some of them have already emerged and some will emerge to the surface maybe shortly — and promising opportunities[47]. As humanity

45. The NATO Cooperative Cyber Defence Centre of Excellence.

46. SCHMITT, M. N. 2013: *Tallinn Manual 2.0: On the International Law Applicable to Cyber Operations*, vol. 14. Cambridge University Press.

47. For instance, in the field of Search and Rescue (hereinafter SAR) Unmanned Aerial Vehicles (UAVs) and drones are taking a more prominent role. Drones are being used as the «first response» to analyze accident scenes, determine emergency routes and locate potential survivors.

enters a new era of digitalization, it is crucial to ensure that the law of the sea is prepared for emerging challenges and can withstand them.

In this regard, the complexity of maritime activities has increased major concerns about liability, safety regulations, and the sustainability of the actual legal framework and its resilience in the face of these major transformations.

In response to these concerns, it is crucial for the legal framework governing maritime space to evolve and establish more robust and forward-looking regulations to ensure its resilience.

Future-proofing is much more than simply adjusting the legal provision once it is outdated. It means taking proactive measures ahead to prepare for emerging challenges and opportunities, rather than simply handling them when they arise. The following lines will focus not only on the need to expand the legal imagination to match the evolution of technology but also on ways to develop a much more futuristic and forward-looking approach to reshaping maritime activities and the law of the sea.

4.1. Expanding the legal imagination to align with technological developments

The concept of expanding the legal imagination aims to balance the evolving nature of technology and the existing legal systems. By embracing innovation and envisioning new legal frameworks, it becomes possible to effectively address emerging challenges and opportunities brought about by technological developments[48].

The development of the law of the sea has forced legislatures to reflect upon new concepts, rules, and principles. This is because the maritime domain is not only confined to two parties bound by an agreement that defines their obligations and rights. It is rather a vast space where multiple parties are involved. Legal imagination is, as a consequence, required to establish a corpus that responds to this reality of multiple interconnected parties, scientific uncertainties, different interests, and geopolitical conflicts[49].

Imagination has gained popularity as a referent in recent decades in the context of modern international legal discourse[50,51.] This rising popularity of imagination in

48. CAPLAN, R. L. 1980: «Review of Legal Reasoning and Legal Theory, by N. MacCormick». *Harvard Law Review*, 1980, 93(4): 817-831. https://doi.org/10.2307/1340528

49. FISHER, Elizabeth. 2017: «Expanding Legal Imagination». In *Environmental Law: A Very Short Introduction*. Oxford, online edn, Oxford Academic, 26 Oct. https://doi.org/10.1093/actrade/9780198794189.003.0005 [7 Nov. 2023].

50. CARTY, A. 1986: *The Decay of International Law? The Limits of Legal Imagination in International Affairs* (republished with a new introduction in 2019).

51. D'ASPREMONT, J. 2022: «Legal Imagination and the Thinking of the Impossible». *Leiden Journal of International Law*, 2022, 35(4): 1017-1027.

international law in general and in the law of the sea and maritime law, in particular, can prove surprising for two major reasons. First of all, it is an empirical exercise before anything else and it is as old as the international legal discourse[52]. Second, the act of envisioning itself can be regarded as an integral component of the process of law-making. In this sense, imagination can be seen as a means of engagement with the world[53].

In today's international legal discourse, «imagination often refers to an act of denaturalizing what comes naturally»[54] for jurists and decision-makers, especially following recent technological developments. The following steps can help broaden the legal imagination to match technological developments in the maritime field.

The expansion of legal imagination is a concept that involves pushing the boundaries of conventional legal thinking. It involves adopting a flexible approach, one that allows for innovative ideas, creative interpretations, and imaginative solutions to legal challenges. This flexible approach is necessary to keep up with the social, technological, and cultural changes. It enables legal professionals to effectively address emerging legal issues, adapt to new circumstances, and ensure that the law remains relevant and accessible to all.

By embracing a flexible approach, the expansion of legal imagination allows for the development of a more dynamic and inclusive maritime framework[55].

Putting the maritime legal framework against the test of time can be very challenging because predicting the changes that time will bring is not an easy matter. The main difficulty is predicting future disturbances and changes.

In this sense, the resilience of the law derives from its capacity for flexibility[56]. The term resilience[57] describes the amount of disturbance a system could take before its

52. Regarding the notion that Grotius provided a pioneering act of creativity in the area, refer to KOSKENNIEMI, M. 2019: «Imagining the Rule of Law: Rereading the Grotian 'Tradition'». *European Journal of International Law*, 2019, 30: 17-52, at p. 22.

53. WINTER, S. L. 2001: *A Clearing in the Forest: Law, Life and Mind*, 67.

54. On the idea of naturalistic necessity see Butler, J. 2007: *Gender Trouble: El feminismo y la subversion de la identidad*. Paidós.

55. WARNER, R. 2003: «Flexibility in the law of the sea: A new dimension for UNCLOS». *Marine Policy*, 2003, 27(6): 499-513.This paper explores the concept of flexibility in UNCLOS and argues for its importance in addressing the dynamic nature of maritime disputes. It discusses the potential benefits and challenges of incorporating flexibility into the legal framework of UNCLOS.

56. FENWICK, M. and WRBKA, S. 2016: *The Flexibility of Law and Its Limits in Contemporary Business Regulation*. Also see ROOSEVELT, Kermit. 2019: «Certainty vs. Flexibility in the Conflict of Laws». In F. Ferrari and D. Fernández Arroyo (eds., Elgar 2019): *Private International Law: Contemporary Challenges and Continuing Relevance*. University of Pennsylvania Law School. Public Law Research Paper No. 18-40.

57. For more on the term «resilience» see FOLKE, C.; BIGGS, R.; NORSTRÖM, A. V.; REYERS, B. and ROCKSTRÖM, J. 2016: «Social-ecological resilience and biosphere-based sustainability science». *Ecology and Society*, 2016, 21(3).

controls shifted to a set of variables and relationships thus dominating another stability region.

Whereas flexibility can be defined as «the ability [of a system] to transform itself to improve its insertion into the environment and thus increase its probability of survival»[58]. In other words, flexibility is a way to deal with uncertainty[59].

GERWIN notes that flexibility has been generally proposed as the adaptive response to environmental uncertainty, specifically as a set of responses to different manifestations of uncertainty[60].

DE TONI and TONCHIA[61], in a comprehensive literature review, find that flexibility is defined as 1) the characteristic of the relationship between a system and its environment, where it operates as a buffer for uncertainty; 2) the degree of homeostatic control of a system, that is, the degree of cybernetic adaptation; 3) the capacity for change and adaptation.

These statements aim at what could be called the general characteristics of flexibility, and they seem to converge in identifying it as «the capacity for adaptation and the purpose of coping with uncertainty»[62].

The main question here is to explore how policymakers and jurists can incorporate flexibility in their approaches.

Drafting a legal framework calls upon a more predictive approach that brings together lawmakers and scientists and encourages them to work hand in hand for the legal and scientific imaginations to match and be synchronized with one another[63]. Only after reaching this harmony and synchronization both legally and technologically, a more flexible corpus can be reached.

There is no denying the pressing necessity for lawmakers to collaborate with scientists and researchers to increase the resilience and flexibility of the legal corpus. The reaction of policymakers to the coronavirus pandemic is the perfect illustration of the importance of maintaining strong ties between scientific and political communities.

58. TARONDEAU, J.-C. 1999a: «La flexibilité est un moyen de faire face à l'incertitude». *Revue française de gestion*, dossier «Les flexibilités», 1999a, 123: 66-71.

59. REIX, R. 1997: «*Flexibilité*». In Y. Simon and P Joffre (dirs.): *Encyclopédie de gestion*, vol. 2. 2.ª ed. Paris: Economica.

60. GERWIN, D. 1987: «An agenda for research on the flexibility of manufacturing processes». *International Journal of Operations & Production Management*, 1987, 7(1): 38-49.

61. DE TONI, A. and TONCHIA, S. 2001: «La flessibilità dei sistemi produttivi: concettualizzazioni e misurazioni sul campo». In *Atti del 2nd Workshop di Organizzazione aziendale*. Università di Padova, CD-Rom.

62. MAGGI, B. 2006: «Critique de la notion de flexibilité». *Revue française de gestion*, 2006, 162(3): 35-49.

63. KHASKHELI, M. BILAWAL; WANG, S.; HUSSAIN, R. Y.; JAHANZEB BUTT, M.; YAN, X. and MAJID, S. 2023: «Global law, policy, and governance for effective prevention and control of COVID-19: A comparative analysis of the law and policy of Pakistan, China, and Russia». *Front Public Health*, 2023, 10:1035536. doi: 10.3389/fpubh.2022.1035536

Whether in times of crisis or not, the integration of science experts into decision-making processes strengthens policies, improves the resilience of legal texts, and leads to robust, forward-looking, flexible, and sustainable outcomes.

Privileging multidisciplinary coordination that encourages collaboration between legal professionals, technology experts, maritime industry stakeholders, and researchers can ensure a more comprehensive understanding of the potential impacts of technological developments on the legal framework. This multidimensional collaboration can also boost the involved parties' ability to anticipate challenges and detect opportunities and thus be more flexible and forward-looking.

In addition to this, developing legal education training and programs that involve incorporating technology-related modules will help create the next generation of maritime jurists and professionals. This is the first step towards ensuring the provision's flexibility while keeping up with the digitalization era as it can help identify gaps in the existing framework.

Moreover, encouraging innovation and experimentation hubs through regulatory sandboxes or pilot programs that allow testing and experimenting with new technologies in a controlled environment can enable lawmakers to better understand how new technologies may require legal adaptation, especially AI as it can be very challenging to comprehend the relationship between AI and the law of the sea, which subsequently brings us to our next point.

4.2. Exploring the potential of artificial intelligence in future-proofing the law of the sea

Connecting AI and the maritime domain can lead to many misunderstandings and disagreements not only regarding the use of AI but also its ethical use. These misconceptions run the potential of further straining already unstable maritime relations, particularly in light of the way that legal ambiguities jeopardize established legal provisions, especially under UNCLOS. For instance, the legal status of unmanned vehicles[64] is considered a serious ambiguity because it is not clear how unmanned vehicles are governed by the Law of the Sea — or whether they are effectively regulated at all[65].

According to the United Nations Secretary-General's AI Advisory Body's Latest report:

> Artificial intelligence increasingly affects us all. Though AI has been around for years, capabilities once hardly imaginable have been emerging at a rapid, unprecedented pace. AI offers extraordinary potential for good — from scientific discoveries that expand the

64. Commonly known as maritime drones.

65. BARTLETT, Matt. *Game of Drones: Unmanned Maritime Vehicles and the Law of the Sea*. SSRN: https://ssrn.com/abstract=4155356

> bounds of human knowledge to tools that optimize finite resources and assist us in everyday tasks. It could be a game changer in the transition to a greener future … Yet, there are also risks. AI can reinforce biases or expand surveillance; automated decision-making can blur the accountability of public officials even as AI-enhanced disinformation threatens the process of electing them. The speed, autonomy, and opacity of AI systems challenge traditional models of regulation, even as ever more powerful systems are developed, deployed, and used[66].

4.2.1. Artificial Intelligence: The opportunities

AI has the potential to change the way we approach and sustainably manage ocean resources, which is crucial for future-proofing the Law of the Sea. AI can significantly enhance our understanding of marine ecosystems and enable efficient monitoring and assessment of ocean health.

Through data analysis and machine learning algorithms, AI can process vast amounts of oceanographic and biological data collected from various sources, including satellites, underwater sensors, and research expeditions. This analysis contributes to a better understanding of ocean dynamics, biodiversity distribution, and ecological connectivity. By recognizing patterns and predicting trends, AI can assist in identifying emerging threats to marine environments, equipping policymakers and stakeholders with valuable information for data-driven and effective strategies for ocean governance.

In addition, AI can support legal processes and ensure the fair application of international maritime law. The Law of the Sea addresses various issues, including territorial boundaries, navigation rights, resource management, and environmental protection. The complexity of these legal frameworks often poses challenges for interpretation and enforcement. AI systems can simplify this process by providing legal professionals with assistance in searching and analyzing vast amounts of relevant data, such as international treaties, court precedents, and national legislation. This can streamline the research phase and lead to more accurate legal interpretations and analyses.

In this regard, AI can enhance dispute resolution by leading to a more efficient and fair resolution of disputes by offering unbiased guidance based on past cases and precedents. AI algorithms can analyze legal precedents, international conventions, and relevant case laws, providing insights to support courtrooms or arbitration proceedings.

The digitalization of maritime disputes can thus be conducted more transparently by automating parts of the arbitration process and supporting the evaluation of evidence, ultimately ensuring equitable outcomes for all parties involved.

66. UNITED NATIONS SECRETARY-GENERAL'S AI ADVISORY BODY. (2023, December 21). *Interim Report Governing AI for Humanity.*

AI offers significant potential for future-proofing the Law of the Sea. By using AI technologies, we can better understand and manage ocean resources, protect marine biodiversity, and ensure the fair implementation of international maritime law.

4.2.2. The use of AI: Ethical Considerations

AI is a double-edged sword, and despite its multiple benefits, the use of AI in the maritime domain brings several ethical concerns that will be unfolded in the following lines.

Some AI benefits can also come with downsides. It is the case for the potential risk of bias[67] when AI systems are used in the maritime industry. AI algorithms are trained on vast amounts of historical data, including information related to performance, accidents, and incidents. If this data is biased or reflects discriminatory practices, the AI systems may perpetuate and even amplify these biases. For instance, if AI algorithms favor certain shipping routes or vessel types based on historical data that is not representative of equitable distribution, it may reinforce inequalities and disadvantage marginalized regions or communities.

Relying on AI in the maritime domain raises concerns regarding accountability and liability[68]. When AI systems are integrated into critical maritime operations, such as autonomous vessels or port security systems, questions arise about who is responsible for accidents or errors caused by these technologies. Unlike human operators, AI systems are not capable of moral reasoning or exercising judgment, which makes it challenging to assign blame in the event of an incident.

In this sense, the European Commission's Comparative Law Study on Civil Liability for Artificial Intelligence notes that:

> The procedural and substantive hurdles along the way of proving causation coupled with the difficulties of identifying the proper yardstick to assess the human conduct complained of as faulty may make it very hard for victims of an AI system to obtain compensation in tort law as it stands.

The EU has also proposed the AI Liability Directive which is designed to ensure that liability rules are appropriately applied to AI-related claims[69]. In addition, the EU's General Data Protection Regulation (GDPR) also plays a crucial role in ensuring that

67. The European Parliament has also recognised that AI has the potential to create and reinforce bias.

68. BUITEN, M.; DE STREEL, A. and PEITZ, M. 2023: «The law and economics of AI liability». *Computer Law & Security Review*, 2023, 48. The paper identifies the challenges of AI for liability and assesses how liability rules should be adapted to address these issues.

69. The AI Liability Directive is in draft form and is yet to be considered by the European Parliament and Council of the EU. Timing remains uncertain.

AI applications in maritime security comply with data privacy standards, especially in the handling of sensitive information related to vessel tracking, cargo operations, and maritime surveillance.

Another ethical concern in the maritime domain lies in the effects of automation on human employment[70]. As AI technology advances, there is a fear that it may replace human jobs[71] on ships, ports, and maritime operations. If uncontrolled, generalized automation could lead to significant job losses[72] and socio-economic imbalances[73].

Ensuring transparency and privacy in the use of AI technologies in the maritime sector is essential. AI systems rely on big amounts of data collected from sensors, cameras, or communication devices. This data can include highly personal[74] or sensitive information about individuals, vessels, or cargo. Without robust safeguards in place, the misuse or unauthorized access to this data could have severe implications for privacy[75] rights and national security.

While the use of AI in the maritime domain offers numerous benefits, it also presents various ethical concerns that need to be addressed. The potential for unfair judgments, accountability, and liability issues, impacts on human employment, transparency, and privacy concerns, as well as cybersecurity vulnerabilities all require careful consideration. Balancing between keeping up with technological developments and addressing the associated ethical concerns is crucial for ensuring responsible and sustainable use of technology in the maritime sector.

This balance can be reached by implementing a neutral technological architecture. This means that the LOS, in addressing technology, should not regulate the use of a particular type of technology.

Adopting a technology-neutral approach creates a prosperous environment for massive technological developments to be embraced rather than be in competition with the provisions leading to its obsolescence.

70. GULIYEV, H. 2023: «Artificial intelligence and unemployment in high-tech developed countries: New insights from dynamic panel data model». *Research in Globalization*, 2023, 7.

71. According to OECD, the share of employment in manufacturing in many OECD countries has declined dramatically over the past couple of decades, as robots have taken over the jobs of lower-skilled workers. OECD. 2023: *OECD Employment Outlook 2019: The Future of Work*. Paris: OECD Publishing. https://doi.org/10.1787/19991266

72. GLOBERMAN, Steven (contributing editor). 2019: *Technology, Automation, and Employment: Will this Time be Different?* Fraser Institute. http://www.fraserinstitute.org

73. SUSSKIND, R. E. and SUSSKIND, D. 2015: *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. United Kingdom: Oxford University Press.

74. SARTOR, G. 2020: *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Study*. European Parliament.

75. BUTTARELLI, G. (EDPS). 2016: «Privacy in an Age of Hyper Connectivity». Keynote speech to the Privacy and Security Conference 2016, Rust am Neusiedler See, 7 November 2016.

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

4.2.3. The EU-AI framework

The European Union (EU) has established a comprehensive regulatory framework for AI, which aims to foster technological innovation while safeguarding human rights, privacy, and public safety. This approach has profound implications for sectors like maritime security, where AI technologies are increasingly utilized for navigation, logistics, and monitoring.

The cornerstone of the EU's regulatory approach to AI is the Artificial Intelligence Act[76] (AI Act), proposed in April 2021. It is a comprehensive, first-of-its-kind regulation aimed at ensuring that AI systems used in the EU are safe, ethical, and respect fundamental rights. The AI Act establishes a risk-based approach to AI regulation, categorizing AI systems into four risk levels: minimal risk[77], limited risk[78], high risk[79], and unacceptable risk[80].

On September 5, 2024, the Council of Europe's Framework Convention on AI was signed by Andorra, Georgia, Iceland, Norway, the Republic of Moldova, San Marino, the United Kingdom, Israel, the United States, and the European Union. The Convention is the first legally binding international agreement on AI and it is fully in line with the EU AI Act, the first comprehensive AI regulation in the world[81].

In terms of regulation and ethics, the European Union has positioned itself as a global leader in AI governance compared to other AI-Key regions. For instance, the AI Act and the ethical guidelines put forward by the EU are much more comprehensive and legally binding compared to the US approach. The US is primarily focused on promoting innovation, with voluntary guidelines rather than mandatory rules for AI development.

Mirroring the US approach, the post-brexit UK developed its own AI strategy avoiding the implementation of strict regulatory frameworks. Although it has established AI ethics principles, the UK's approach is more about creating a supportive environment for innovation.

76. The EU AI Act was published in the *EU Official Journal* on July 12, 2024, and is the first comprehensive horizontal legal framework for the regulation of AI across the EU. The EU AI Act enters into force on August 1, 2024, and will be effective from August 2, 2026. See Convention text here: https://rm.coe.int/1680afae3c

77. Minimal-risk AI faces no regulatory requirements. e.g., AI for entertainment or online shopping recommendations.

78. Limited-risk AI systems have moderate regulatory requirements, such as transparency and user notification.

79. High-risk AI systems are subject to strict requirements, including transparency, accountability, and human oversight (e.g., biometric identification, critical infrastructure management like ports).

80. Unacceptable risk AI is banned (e.g., social scoring systems or AI systems used in mass surveillance).

81. The treaty will enter into force on the first day of the month following three months after five signatories, including at least three Council of Europe Member States, have ratified it. Countries from all over the world will be eligible to join and commit to its provisions.

In the maritime sector, this *laissez-faire* approach could potentially lead to the unregulated use of AI in areas like autonomous ships, port security, and maritime surveillance.

The EU-AI framework was also strengthened by the Digital Services Act[82] (DSA), introduced by the European Union in 2020. While the DSA primarily targets online environments such as social media, e-commerce, and search engines, its principles and mechanisms can have far-reaching implications for the maritime domain, particularly in areas involving digital technologies, cybersecurity, and maritime logistics. Key implications could include:

- Cybersecurity and Data Protection: The DSA emphasizes stricter accountability for digital platforms used in maritime navigation, logistics, and communication, aligning with EU regulations like the GDPR. Maritime companies must ensure robust cybersecurity and data protection measures to prevent cyber threats.
- Third party digital Platforms in Maritime Operations: Platforms that provide digital services for vessel tracking, port operations, and maritime logistics (e.g., shipping marketplaces, port community systems, or remote monitoring systems) would be required to adhere to the DSA's transparency and accountability provisions[83].
- Navigational Tools and AI: AI-driven tools, such as autonomous vessels or route optimization systems, will need to meet DSA standards for transparency and safety, ensuring clear explanations of their algorithms and decision-making processes.
- Cross-Border Regulatory Impact: The DSA's extraterritorial scope means maritime companies operating in the EU or interacting with EU-based platforms must comply with its requirements. This could create challenges for international maritime companies and raise questions about compliance across different jurisdictions[84].
- Platform Liability and Maritime Safety: If a digital platform fails to secure vital safety information, or if it provides misleading information that leads to accidents or operational disruptions, it may be held accountable under the DSA. This raises important questions about the liability of service providers in the maritime sector, particularly when relying on third-party platforms for crucial operational data.

82. The Digital Services Act (DSA) is an EU regulation adopted in 2022 that addresses illegal content, transparent advertising and disinformation. It updates the Electronic Commerce Directive 2000 in EU law and applies to online platforms and intermediaries such as social networks, marketplaces and app stores.

83. For instance, shipping companies that use third-party platforms for logistics would need to ensure that these platforms disclose their algorithmic decisions and provide mechanisms for handling complaints, increasing trust and transparency in maritime commerce.

84. Companies operating within the EU, or interacting with EU-based platforms, may need to adjust their operations and practices to align with the DSA's requirements, even if their primary operations are outside the EU.

4.2.4. Towards a UN-AI Governance

On the 21st of December 2023, the UN Secretary-General's AI Advisory Body launched its Interim Report, *Governing AI for Humanity*. The report emphasizes the need for an international framework to govern the integration and deployment of AI in global practices.

The UN Advisory Body[85] is a multi-stakeholder High-level Advisory Body on AI convened by the UN Secretary-General to undertake analysis and advance recommendations for the international governance of AI.

The report shed light on the Global Governance Deficit even though several AI regulatory and policy initiatives have emerged. It is also a call for a more inclusive engagement to create a level-playing field as many communities have been largely missing from high-level discussions on AI governance. For this purpose, the report suggests measures to ensure fair representation for all nations.

The report states that norms including commitments to the UN Charter, the Universal Declaration of Human Rights, and international law including environmental law and international humanitarian law, apply to AI.

The UN AI Advisory Body interim report presents a plan to strengthen the global regulation of AI through several guiding principles and institutional functions.

In terms of guiding principles, the report identified 5 essential principles for shaping the establishment of future global AI governance institutions: Inclusivity, Public Interest, Centrality of Data governance, Universal, networked, multi-stakeholder, and International Law.

As for institutional functions, the Body identified what functions should be incorporated into an AI governance framework. They include, regularly assessing the state of AI and its trajectory, harmonizing standards, safety, and risk management frameworks, promoting international multi-stakeholder collaboration to empower the Global South, monitoring risks and coordinating emergency response, and developing binding accountability norms.

5. CONCLUSION AND RECOMMENDATIONS

There is no doubt that international Law in general and the Law of Sea in particular are facing a lot of changes due to digitalization. This new reality invites reflection on the adaptability and sustainability of the maritime domain legal framework, particularly in how existing legal frameworks can adapt to technological advancements.

85. The UN Advisory Body is Co-chaired by Carme Artigas, Secretary of State for Digitalisation and Artificial Intelligence of Spain and James Manyika, Senior Vice President of Google-Alphabet, President for Research, Technology and Society.

As previously examined, the digital era offers many promising opportunities for the responsible use of our oceans. The integration of smart technologies, such as AI, in the maritime domain promises to enhance situational awareness, improve decision-making, and streamline responses to security threats. However, alongside the opportunities, these innovations bring several challenges, complexities and emerging threats that need to be addressed urgently.

One of the key challenge is the difficulty of reconciling the rapid pace of technological evolution with the more gradual development of legal systems. Technologies like AI can have far-reaching implications across various areas of international law, from human rights to cyber threats, liability, and ethical considerations. This is probably because even one technology can have multiple consequences in several legal fields. But this shouldn't be an excuse to refrain from using the technology and developing a robust framework that ensures its safe use.

A future-oriented framework for maritime security must be resilient to technological disruptions and adaptable to the rapid advancements in AI and other smart technologies. It should not only address current threats but also anticipate and mitigate future risks. To achieve this anticipation, adaptability and flexibility maritime jurists, professionals, and scientists are encouraged to work hand in hand for a more holistic approach. Only a multidimensional approach can help expand the legal imagination to match the rapid technological developments.

The anticipation-based approach that will result from interdisciplinary strategy-making can significantly help reduce vulnerabilities and enhance the overall resilience of maritime security systems by prioritizing the use of predictive analytics smart technologies and real-time monitoring systems.

The potential for smart technologies to aid decision-makers in developing such a framework depends on several factors. The most important factor in our personal opinion would be technological reliability and safety. This means that the AI used or other smart systems must function reliably under different maritime conditions/scenarios and be trusted under high-stakes security situations.

In addition to reliability, the world needs to start considering negotiating new amendments to the existing legal framework, mainly UNCLOS. Updating the international law of the sea to account for the new realities that smart technologies bring can make the legal framework more resilient, durable and future oriented. These Amendments can include provisions that encourage global standards and fosters collaboration among states, international organizations, the tech-industry and all the maritime domain stakeholders to create a cohesive, holistic and effective maritime security strategy.

In conclusion, while smart technologies hold significant promise for enhancing maritime security, their successful integration into a resilient and future-oriented framework requires careful planning and ongoing evaluation to ensure that technological advancements are aligned with maritime domain legal and ethical standards. In this spirit, it is worth noting that the emerging challenges that arise from the technological shift can

Ars Iuris Salmanticensis,
vol. 12, Diciembre 2024, 11-39
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-SA

have worldwide implications thus the need for a global response and a collective effort to overcome a global threat.

In this spirit, Governments and different stakeholders should consider the creation of an interoperable «Smart Maritime Domain Mechanism». A sort of Global Maritime Network that serves as a centralized and reliable real-time data-sharing platform connecting vessels, maritime infrastructures, coastguards and maritime agencies globally. This ecosystem however, could constitute the perfect target for hackers, thus the need for a robust and highly secure management system, a high level of coordination and the most advanced resources capable of neutralizing cyberattacks on critical maritime infrastructures. This could be done through a «Global Maritime Cybersecurity Task Force» which accompanies the «Smart Maritime Domain Mechanism». Combining the mechanism and the task force would allow maritime security efforts to become more proactive (time and cost), transparent and efficient.

The idea of a Task force can start as a Maritime Security Innovation Lab, that Governments and maritime agencies could fund to allow start-ups, academic institutions, and tech companies to pilot new smart technologies in a controlled environment which would foster innovation and novel solutions[86] without jeopardizing operational security.

Implementing these innovative recommendations could transform maritime security into a proactive, highly adaptable system, that is not only stronger and more resilient but also better equipped to anticipate and address emerging threats and challenges.

6. REFERENCES[87]

AFRICAN UNION. 2016: *African Charter on Maritime Security and Safety and Development in Africa*.

ALLAHVERDIZADEH, R. and KARIMI, M. 2023: «A New Approach to the Theory of Seapower in the 21st Century (In Times of War and Peace)». *Geopolitics Quarterly*, 2023, 18:4: 383-411. https://doi.org/20.1001.1.17354331.1401.18.68.17.9

ANDREONE, G. (ed.). 2018: *The Future of the Law of the Sea: Bridging Gaps Between National, Individual and Common Interests*. Springer International Publishing.

AVANT, David D.;, P. O. I. R. D. and WESTERWINTER, Oliver (eds.). 2016: *The New Power Politics: Networks and Transnational Security Governance*. Oxford: Oxford University Press.

AYLAK, B. L. «The Impacts of the Applications of Artificial Intelligence in Maritime Logistics». *European Journal of Science and Technology*, 2022, (34): 217-225.

86. For instance, incorporating Augmented Reality (AR) into maritime decision-making tools to train maritime experts and to improve situational awareness. By combining AR with AI for dynamic threat analysis, operators could visualize potential risks and plan responses more effectively.

87. All internet sources were last accessed in August 2024.

BALDÉ, C. P.; D'ANGELO, E.; LUDA, V.; DEUBZER, O. and KUEHR, R. 2022: *Global Transboundary E-waste Flows Monitor - 2022*. Bonn: United Nations Institute for Training and Research (UNITAR).

BARTLETT, M. 2018: *Game of Drones: Unmanned Maritime Vehicles and the Law of the Sea*. University of Auckland - Faculty of Law, November 22. Retrieved from https://ssrn.com/abstract=4155356

BASKAR, K. and BALAKRISHNAN, M. 2019: «Cyber Preparedness in Maritime Industry». *International Journal of Scientific and Technical Advancements*, 2019, 5:2: 19-28.

BRAMER, M. and PETRIDIS, M. (eds.). 2016: *Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV*. Springer International Publishing.

BRENNER, S. W. Cyberthreats: The Emerging Fault Lines of the Nation State. Oxford: Oxford University Press, 2009.

BUEGER, C. «What is Maritime Security?». *Marine Policy*, 2015, 53: 1-8. https://doi.org/10.1016/j.marpol.2014.12.005

BUEGER, C.; EDMUNDS, T. and RYAN, B. J. «Maritime Security: The Uncharted Politics of the Global Sea». *International Affairs*, 2019, September: 971-978.

BUITEN, M.; DE STREEL, A. and PEITZ, M. «The Law and Economics of AI Liability». *Computer Law & Security Review*, 2023, 48: 1-18.

BUTLER, J. 2007: *Gender Trouble: El feminismo y la subversion de la identidad.* Paidós.

CAPLAN, R. L. 1980: «Review of Legal Reasoning and Legal Theory, by N. MACCORMICK». *Harvard Law Review*, 1980, 93:4: 817-831. https://doi.org/10.2307/1340528

CUSTERS, B. (ed.). 2016: *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*. T.M.C. Asser Press.

DE TONI, A. F. and TONCHIA, S. 2001: *La flessibilità dei sistemi produttivi: concettualizzazioni e misurazioni sul campo* [Atti del 2nd Workshop di Organizzazione aziendale, Università di Padova].

EUROPEAN UNION. 2021: *AI Act: Proposal for a Regulation on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts*. COM/2021/206 final, European Commission..

EUROPEAN UNION. 2022: «Digital Services Act (DSA) Regulation (EU) 2022/2065». *Official Journal of the European Union*.

EUROPEAN UNION. 2022: *AI Liability Directive: Proposal for a Directive on Liability for Artificial Intelligence*. COM/2022/495 final, European Commission.

EVANS, M. D. and GALANI, S. (eds.). 2020: *Maritime Security and the Law of the Sea: Help or Hindrance?* Edward Elgar Publishing Limited.

FENWICK, M. and WRBKA, S. (eds.). 2016: *Flexibility in Modern Business Law: A Comparative Assessment*. Springer Japan.

FISHER, E. C. 2017: *Environmental Law: A Very Short Introduction*. Oxford: Oxford University Press. https://doi.org/10.1093/actrade/9780198794189.003.0005

FITTON, O.; PRINCE, D.; GERMOND, B. and LACY, M. 2015: *The Future of Maritime Cybersecurity*. Lancaster University.

FOLKE, C. 2016: Social-ecological Resilience and Biosphere-based Sustainability Science. *Ecology and Society*, 2016, 16: 1-6.

GERWIN, D. 1987: «An Agenda for Research on the Flexibility of Manufacturing Processes». *International Journal of Operations & Production Management*, 1987, 7:1: 1-5.

GERWIN, D. 1993: «Manufacturing Flexibility: A Strategic Perspective». *Management Science*, 1993, 39:4: 1-10.
GILL, T. D.; GEISS, R.; HEINSCH, R.; MCCORMACK, T.; DORSEY, J. and PAULUSSEN, C. (eds.). 2012: *Yearbook of International Humanitarian Law*, vol. 15. T.M.C. Asser Press.
GLOBERMAN, S. (ed.). 2019: *Technology, Automation, and Employment: Will This Time Be Different?* Fraser Institute.
GOUVEIA, J. B. 2018: *Direito da segurança: cidadania, soberania e cosmopolitismo: segurança, Estado e comunidade internacional, direito estadual e direito supraestadual, direito fundamental à segurança...* Almedina.
GRASSO, M. E. 2021: *Resilience and Sustainability in Law: Theoretical and Critical Approaches*. Cambridge: Cambridge Scholars Publisher.
GULIYEV, H. 2023: «Artificial Intelligence and Unemployment in High-tech Developed Countries: New Insights from Dynamic Panel Data Model». *Research in Globalization*, 2023, 7.
HASSAN, D. and HASAN, S. M. 2017: «Origin, Development, and Evolution of Maritime Piracy: A Historical Analysis». *International Journal of Law, Crime, and Justice*, 2017, 49: 1-9. https://doi.org/10.1016/j.ijlcj.2017.01.001
HILLER, A. L. 2017: *The Challenge of Cybersecurity in the Maritime Domain: Senior Capstone Thesis*. California State University Maritime Academy.
HOLLING, C. S. 1973: Resilience and Stability of Ecological Systems. *Annual Review of Ecology, Evolution and Systematics*, 1973, 4: 1-23.
KERMIT, R. 2019: Certainty vs. Flexibility in the Conflict of Laws. *University of Pennsylvania Law School*, Public Law Research Paper No. 18-40.
KESSLER, G. C. 2019: «Cybersecurity in the Maritime Domain». *USCG Proceedings of the Marine Safety & Security Council*, 2019, 76(1). Retrieved from https://commons.erau.edu/publication/1318
KINGDOM OF MOROCCO, ADMINISTRATION OF NATIONAL DEFENSE. بية، إدارة الدفاع الوطني المملكة المغر. [Presentation of Law No. 05-20 on Cybersecurity]. Retrieved from https://www.dgssi.gov.ma/fr/loi-ndeg-0520-relative-la-cybersecurite
KITTICHAISAREE, K. 2001: «A Code of Conduct for Human and Regional Security Around the South China Sea». *Ocean Development & International Law*, 2001, 32(2): 131-147. https://doi.org/10.1080/00908320151100262.
KLEIN, N. 2011: *Maritime Security and the Law of the Sea*. Oxford: OUP Oxford.
KOOPS, B.-J. (ed.). 2006: *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners*. T.M.C. Asser Press.
KOSKENNIEMI, M. 2021: *To the Uttermost Parts of the Earth: Legal Imagination and International Power 1300-1870*. Cambridge: Cambridge University Press.
KRASKA, J. and PARK, Y.-K. (eds.). 2023: *Emerging Technology and the Law of the Sea*. Cambridge: Cambridge University Press.
LAVROV, S. and SARI, A. 2021: «Hybrid Threats and the Law: Building Legal Resilience». *Hybrid CoE*, 2021, November 24. Retrieved from https://www.hybridcoe.fi/wpcontent/uploads/2021/10/20211104_Hybrid_CoE_Research_Report_3_Hybrid_threats_and_the_law_WEB.pdf
LEUCCI, P. and VIANELLO, I. (eds.). 2023: *Ascomare Yearbook on the Law of the Sea 2022*. Luglio (Trieste).
LIU, Y.-H. and LIANG, T.-P. 2018: «A Bibliometrics Study on the Research Landscape of Business Intelligence and Big Data Analytics». *Expert Systems with Applications*, 2018, 111: 2-10.

LOTT, A. 2022: *Hybrid Threats and the Law of the Sea: Use of Force and Discriminatory Navigational Restrictions in Straits*. Brill Nijhoff.
MACKINNON, J. 2019: «Fishery Depletion and the South China Sea». *Fisheries*, 2019, 9(1): 10.26443/firr.v9i1.8
MAGGI, B. 2006: «Critique de la notion de flexibilité». *Revue française de gestion*, 2006, 162(3).
MAHAN, A. T. 2010: *The Influence of Sea Power upon History, 1660-1783*. Cambridge: Cambridge University Press.
NORDQUIST, M. H.; MOORE, J. N. and LONG, R. (eds.). *Challenges of the Changing Arctic: Continental Shelf, Navigation, and Fisheries*. Brill.
OUE ELFERINK, A. G. (ed.). 2005: *Stability and Change in the Law of the Sea: The Role of the LOS Convention*. Brill.
PERKUŠIĆ, M.; JOZIPOVIĆ, Š. and PIPLICA, D. 2020: «The Need for Legal Regulation of Blockchain and Smart Contracts in the Shipping Industry». *Transactions on Maritime Science*, 2020, 9:2: 365-373.
RANCHORDÁS, S. and ROZNAI, Y. (eds.). 2020: *Time, Law, and Change: An Interdisciplinary Study*. Bloomsbury Academic.
RAO, V. A. I. A. 2023: *Maritime Security: Challenges & Responses in a Changing World*. IPS Press.
REIX, R. «Flexibilité». *Encyclopédie de gestion*, 1997, 2(2).
ROSSELLO, M. 2022: «Fisheries and the Law of the Sea in the Anthropocene Era». In Pierandrea Leucci and Ilaria Ianiello (eds.): *Ascomare Yearbook on the Law of the Sea*, vol. 2.
SARTOR, G. 2020: *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Study*. European Parliament.
SCHMITT, M. N. (ed.). 2017: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
SEKINE, D. 2011: Seapower and Japan's Maritime Coalition Building. *University of Wollongong Thesis Collection*. Retrieved from https://ro.uow.edu.au/theses/3565/. STANTON, N. (ed.). 2020: *Advances in Human Aspects of Transportation: Proceedings of the AHFE 2020 Virtual Conference on Human Aspects of Transportation, July 16-20, 2020, USA*. Springer International Publishing.
SUSSKIND, R. E. and SUSSKIND, D. 2015: *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. Oxford: Oxford University Press.
TANAKA, Y. 2006: Predictability and Flexibility in the Law of Maritime Delimitation. Bloomsbury Academic.
TILL, G. 2009: *Seapower: A Guide for the Twenty-first Century*. Routledge.
UNITED NATIONS ENVIRONMENT PROGRAMME. 2012: *UNEP 2011 Annual Report*. Retrieved from https://wedocs.unep.org/20.500.11822/8053
UNITED NATIONS SECRETARY-GENERAL'S AI ADVISORY BODY. 2023: *Interim Report Governing AI for Humanity*. December 21.
UNITED NATIONS UNIVERSITY (UNU). *The Global E-waste Monitor 2020*. United Nations University.
WHITE, J. B. 1985: *The Legal Imagination*. 2nd ed. Abridged Edition.