CYBER PIRACY ON THE HIGH SEAS: RETHINKING THE TWO-SHIP REQUIREMENT UNDER UNCLOS

Anavi, Mahi Yadav & Dhulipudi Hema Sruthi, Alliance University, Bangalore

ABSTRACT

The maritime industry is undergoing rapid digitalization that is changing how ships operate, improving navigation, communication, cargo management and operational efficiency. But this growing reliance on digital systems has also made vessels more vulnerable to cyber assaults. Countermeasures against attacks like GPS spoofing, manipulation of the Automatic Identification System (AIS), malware intrusions and interference with satellite communications can have a devastating effect on maritime operations, safety of navigation and global trade without the need to physically board or involve another vessel. These developments pose a challenge to the traditional legal framework for piracy under the United Nations Convention on the Law of the Sea (UNCLOS), drafted primarily to deal with physical attacks by one vessel on another on the high seas. The study discusses the 'two-ship requirement' and its relevance in light of the increasing technological threats and asks if maritime cyberattacks can be categorized as piracy under Article 101 of UNCLOS. This research uses doctrinal research technique. The study takes into account the relevant sections of the UNCLOS, international treaties on cybercrime, marine cybersecurity recommendations and recent legal literature to evaluate whether the current framework is sufficient. It also utilizes the 2024 Red Sea cyber operation as a case study to show how remote hacks can allow physical harm even when they do not fit under the existing legal framework of piracy. Building upon this research, this article argues that the current regime is inadequate to address the contemporary hazards of maritime cyber, and offers a multi-layered solution to narrow the legal gap. Recommendations include requesting an advisory opinion from the International Tribunal for the Law of the Sea (ITLOS), amending the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) to explicitly criminalize maritime cyber-attacks, and strengthening the International Maritime Organization's cyber-risk framework through mandatory and independently auditable standards of compliance. Such measures would allow international maritime law to better address new cyber assaults, while maintaining the core values of the high seas.

Keywords: Cyber Piracy, Maritime Cybersecurity, UNCLOS, High Seas, Article 101, Two-Ship Requirement, ITLOS, SUA Convention, Maritime Cyberattacks, International Maritime Law.

1. Introduction

1.1. Maritime Trade and The Concept of High Seas

Maritime trade is the backbone of economic growth in many nations.[1] The maritime trade operates throughout the globe, setting up the structure of the global marketplace. It plays a key role in many fields, mainly in trade. Maritime trade has given rise to many international trade relationships, whether it is friendly or neutral. This also attracts unwanted threats and security challenges from the foe.

A major part of maritime trade operated through the high seas. Freedom of the seas is also known as the High Seas. High seas are labeled as international marine waters outside of any jurisdiction of any nation or country. High seas start from 200 nautical and extend beyond that. Part VII of the UNCLOS regulates the High Seas, stating the permissible and non-permissible acts.[2] Many freedoms are granted on high seas like freedom of navigation, freedom of over flight, freedom of fishing and many more. Even though UNCLOS allows certain freedoms, it prohibits the nation from subjecting any part of high seas in its sovereignty.[3]

1.2. Digitalization and emerging cyber threats

With emerging technology, the maritime sector is also evolving at the same pace. Maritime field is heavily reliant on technology. Digitalizing port logistics, shipping and navigation systems for achieving more efficiency has made it easily reliant on digital systems and automated systems. Through this water bodies have become more prone to maritime cyber threats. Disrupting, interfering, and manipulating maritime infrastructure is known as cyber-attack.[4]

---

[1] "Maritime Security: A Pillar for Economic Development," https://www.imo.org/en/mediacentre/pages/whatsnew-2157.aspx.
[2] "1982 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA," *Centre for International Law*, https://cil.nus.edu.sg/wp-content/uploads/2019/02/1982-United-Nations-Convention-on-the-Law-of-the-Sea.pdf.
[3] "High Seas," LII / Legal Information Institute, https://www.law.cornell.edu/wex/high_seas.
[4] Yongming Jin et al., "Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations," Frontiers in Marine Science 12 (August 29, 2025), https://doi.org/10.3389/fmars.2025.1616906.

1.3. Research Problem

Even though the growing developments in technology have helped us achieve efficiency and connectivity on the next level through cargo management, navigation, automated control systems, and operational safety. It has exposed ships or vessels to cyber threats like manipulating data and interfering in maritime operations. Unlike conventional acts of piracy where there is another pirate vessel needed, this act is done remotely.

The international convention which governs piracy is mentioned under the United Nations Convention on the Law of the Sea. The piracy under this convention is defined as any illegal acts of violence, detention or any act of depredation committed by a crew or passengers of a private ship or private aircraft on high seas against another ship.

This raises a significant issue whether cyber-attacks can be regarded as piracy if there is no other vessel in the existing legal framework. This gives rise to a gap between conventional provisions and emerging cyber threats. This study analyses whether the two-ship requirement under UNCLOS is adequate or if there should be development needed in the convention due to emerging threats.

1.4. Research Objectives

- To identify a gap in existing international legal framework regarding cyber-attacks against a ship on high seas.
- To examine the definition of piracy established under UNCLOS
- To understand the importance of traditional legal definition of piracy under international maritime law.
- To examine that if the cyber-attacks against a vessel on high seas, can be labeled as piracy.

1.5. Research Questions

Are cyber-attacks against ships on high seas considered piracy when no pirate vessel is involved, particularly the two-ship requirement for an adequate definition of piracy under UNCLOS?

To what extent can cyberattacks against vessels on the high seas be legally classified as piracy under current UNCLOS, and what regulatory developments are required to address these emerging threats?

1.6. Methodology

This research paper adopts a 'doctrinal legal research paper'. Which focuses on interpreting and analyzing the existing international maritime law in accordance with cyber-attacks on high seas. This paper primarily involves analysis and interpretation of existing legal provisions, treaties and scholarly literature related to cyber security of the law of the sea.

This study exclusively relies on secondary sources like international conventions, academic journal articles, legal commentaries, reports of the International Maritime Organization (IMO), International Tribunal for the Law of the Sea (ITOLS) materials, maritime cyber security publications and international legal documents. A case study of the 2024 Red Sea operation is used to demonstrate the practical limitations of the current legal framework. Also considering the convention of UNCLOS as the center of this paper. Through this, the paper evaluates whether a two-ship requirement is necessary and whether the cyber-attacks on high seas on a vessel fall under UNCLOS. And to provide the appropriate legal solution if not.

2. Legal Framework of Piracy under UNCLOS and its limitations

2.1. Overview of UNCLOS

The main challenge with marine territory is that it is indivisible unlike land territory. During the age of exploration, dominant maritime powers like Spain and Portugal sought exclusive sovereignty over vast areas of the seas. To address this, Mare Liberum (1609), laid the foundation for the principle of freedom of navigation which challenged the notion of exclusive control over the oceans. This principle suggested a limited coastal control from the territorial claims. Beyond this is the area of common territory, open to all called High seas.[5]

In 1967, Arvid Pardo of Malta addressed the General Assembly of UN and stated the need for international regime that governs the oceans beyond the defined national jurisdiction.[6] Over

[5] Prapti Dheeraj, "Critical Analysis of the Evolving Concept of Maritime Boundaries in Light of UNCLOS," IJLSSS, July 20, 2024, https://ijlsss.com/critical-analysis-of-the-evolving-concept-of-maritime-boundaries-in-light-of- unclos/.
[6] "UNCLOS," International Tribunal for the Law of the Sea, https://www.itlos.org/en/main/the-

the years, the United Nations Convention on the Law of the Sea (UNCLOS) was entered into force in 1994, is a primary international legal framework that governs the maritime activities and the ocean's resources. It lays down the law and order for the world's oceans and also established rules over the state's sovereignty over the water bodies.[7]

Here are the key Maritime zones established by UNCLOS: - [8][9][10]

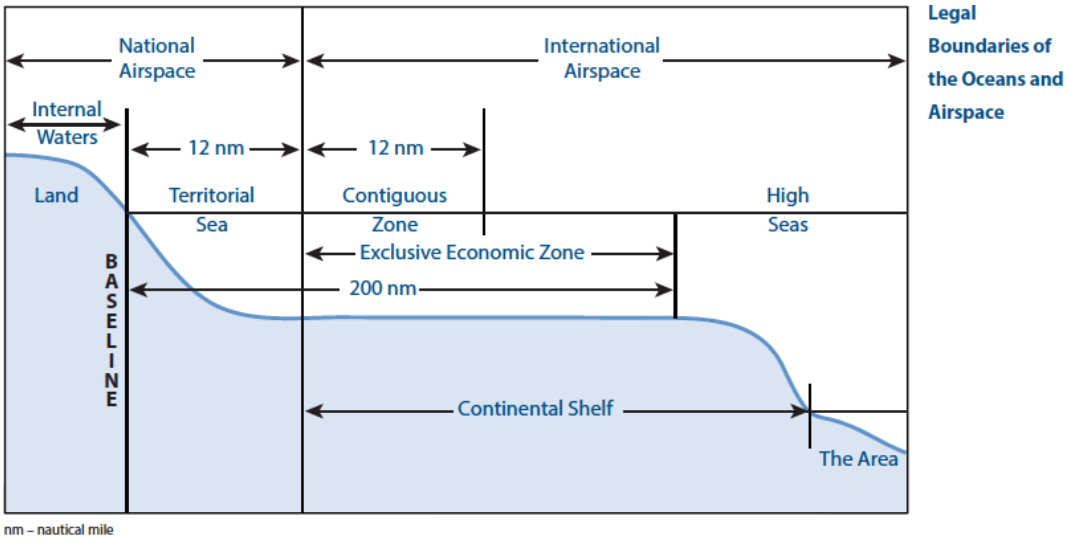

Image: Division of the maritime zones set by UNCLOS[11]

- Internal Waters *(Article 2-32)*- Includes rivers, bays, ports and waters landward of the baseline. The state enjoys complete sovereignty, and foreign vessels have no automatic right of passage.

- Territorial Sea *(Article 3)*- The state has full sovereignty extending to the air space over to the water, seabed, subsoil, up to 12 nautical miles from the baseline.

- Contiguous Zone *(Article 33)*- Up to 24 nautical miles, has limited enforcement

tribunal/unclos/#c4986.

[7] "United Nations Convention on the Law of the Sea," https://www.imo.org/en/ourwork/legal/pages/unitednationsconventiononthelawofthesea.aspx.

[8] Prapti Dheeraj, "Critical Analysis of the Evolving Concept of Maritime Boundaries in Light of UNCLOS," July 20, 2024.

[9] "Overview - Convention & Related Agreements," https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm.

[10] "UNCLOS - Table of Contents," https://www.un.org/Depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm.

[11] "Chapter 2: Maritime Zones – Law of the Sea," https://sites.tufts.edu/lawofthesea/chapter-two/.

powers.

- Exclusive Economic Zone (EEZ) *(Article 55-75)*- Extends up to 200 nautical miles, granting the state sovereign rights to explore and exploit natural resources such as fish, oil, gas and minerals.

- Continental Shelf *(Article 76-85)*- Refers to seabed and subsoil beyond the territorial sea that extends up to 200 nautical miles.

- High Seas *(Article 86-120)*- Areas beyond national jurisdiction, open to all states for navigation, fishing, scientific research and laying submarine cables.

One of the main challenges of high seas is the continuing trends of cyber-attacks on the ship vessel. It is a result of widespread digitalization of the maritime sector that brought significant changes in the way ships operate. Thus, cybersecurity emerges as a critical issue as the modern ships are equipped with interconnected information systems and operating systems.[12] However, the current UNCLOS code has limitations in the face of growing cyber and AI threats.[13]

2.2. Article 100: Duty to Cooperate

Article 100 of UNCLOS[14] establishes the duty of all states to cooperate in the suppression of piracy on the high seas. The key idea is international cooperation and not restricted to the flagged ships in which piracy has occurred. This obligation only applies when piracy occurs on the high seas or outside national jurisdiction.

2.3. Article 101: Definition of Piracy

Article 101 of UNCLOS[15]provides the official legal definition of piracy under UNCLOS. It defines piracy as "any illegal acts of violence or detention, or any act of depredation,

[12] Apostolos Kapsalis, "Cybersecurity and Cyberattacks in Maritime Shipping," *ResearchGate*, November 2025, https://www.researchgate.net/publication/397642565_Cybersecurity_and_Cyberattacks_in_Maritime_Shipping.
[13] John Snyder, "Cyber Criminals and Bad Actors Roam on the High Seas," Riviera, August 11, 2025, https://www.rivieramm.com/news-content-hub/cybercriminals-and-bad-actors-roam-on-the-high-seas-85653.
[14] United Nations Convention on the Law of the Sea, 1982, Article 100.
[15] United Nations Convention on the Law of the Sea, 1982, Article 101.

committed for private ends" on the high seas. This article lays down the foundation of "two ship requirements" in which a crew or passenger of a private ship or private aircraft (Pirate Ship) go against another ship or aircraft or against persons or property on board (Victim ship). This is a limitation of the modern legal cyber-attack scenarios that occur from land to the ships on high seas.

Moreover, the term 'violence' under this section is traditionally interpreted as physical forces. However, this term does not extend to harm caused through cyber means leaving a notable gap in the legal framework governing maritime security.

Furthermore, the term 'depredation' is not explicitly defined within the convention itself. This term is characterized as destructive conduct that includes plundering, destroying and devastating, indicating tangible conduct. However, a progressive interpretation may argue that interference with a ship's digital systems such as GPS spoofing, hacking of navigational controls or disabling of onboard communication systems, could constitute depredation if it causes destruction to the ship's operations. This draws on the Functional Equivalence Theory, where the acts caused through cyber space rather than physical harm can have legal consequences. This lack of modern interpretation and ambiguity highlights a critical legal gap in UNCLOS that has yet to be formally addressed by either state practice or international tribunal decisions. [16][17]

2.4. Article 105: Seizure of Pirate Ships

Article 105 of UNCLOS[18] reflects the principles of universal jurisdiction as it authorizes any state to seize pirate ships or aircraft on the high seas, arrest offenders and confiscate the property on board. Piracy is treated as a threat to an international community. However, this provision primarily addresses traditional piracy involving physical vessels, making it difficult to apply to modern cyberattacks on ships where no pirate vessel is involved.

[16] Oleksiy Melnyk, Oleksandr Drozdov, and Serhii Kuznichenko, "Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures," *Lex Portus* 11, no. 1 (March 11, 2025), https://doi.org/10.62821/lp11101.
[17] Anne Veerpalu, "Functional Equivalence: An Exploration Through Shortcomings to Solutions," *ResearchGate*, December 2019, https://www.researchgate.net/publication/339931469_Functional_Equivalence_An_Exploration_Through_Shortcomings_to_Solutions.
[18] United Nations Convention on the Law of the Sea, 1982, Article 105.

3. Legal Gap: Cyber Piracy Without a Vessel

The rapid digitalization of maritime operations has introduced new vulnerabilities in the shipping industry. Modern ships heavily rely on digital navigation systems, interconnected technologies, and more. With these advancements, there are more opportunities for the interference with the maritime operations by cyber criminals. These maritime technologies are susceptible to the attacks, allowing hackers to remotely disrupt navigation, communication and operational systems even from land-based locations

3.1. Why did the two-ship requirement existed historically?

Historically, piracy was perceived as an act committed by one private vessel against another vessel on high seas. The beginning of the development of international maritime law began with the Harvard Draft Convention on Piracy 1932 which heavily influenced the piracy provisions of the Geneva Convention on the High Seas 1958. At that time, piracy primarily involved armed pirate ships intercepting merchant ships for violence, detention, robbery and other types of acts.[19][20]

One of the most significant reasons for the two-ship requirement was the exclusive flag State Jurisdiction. Somalia was a primary state suffering through Piracy and also one of states to established the two-ship requirement.[21]

Criminal acts committed solely within a single vessel like hijacking, violence by crew members or mutiny were considered a matter of the vessel's flag state rather than a matter of an international community. Attacks which included one vessel attacking the other threatening the freedom of navigation of high seas were considered piracy and therefore universal jurisdiction was justified.[22]

---

[19] Tullio Treves, "1958 Geneva Conventions on the Law of the Sea - Main Page,"https://legal.un.org/avl/ha/gclos/gclos.html.
[20] Mick P. Green, Douglas R. Burnett, and Nternational Cable Protection Committee, Ltd, "Security of International Submarine Cable Infrastructure: Time to Rethink?," *BRILL*, n.d., https://brill.com/display/book/edcoll/9789047440406/Bej.9789004164277.v-594_021.xml?language=en&srsltid=AfmBOorLxjvSLb7wnGQPmFlHEzoJfbtaOwOLATkp673cVcaCuquRZDIx.
[21] Santiago Iglesias Baniela and Juan Vinagre Ríos, "Piracy in Somalia: A Challenge to the International Community," *Journal of Navigation* 65, no. 4 (June 15, 2012): 693–710, https://doi.org/10.1017/s0373463312000185.
[22] Douglas Guilfoyle, "Shipping Interdiction and the Law of the Sea," https://www.academia.edu/31002094/Shipping_Interdiction_and_the_Law_of_the_Sea.

The historical requirements of two vessel system were established by Harvard draft convention on Piracy 1932 and Geneva Convention on the High Seas 1958 which became an integral part in establishing UNCLOS.

3.2. The Two ship requirement problem

The major limitation of the piracy framework of UNCLOS is the traditional "two ship requirement" established in Article 101.[23] This definition is limited to piracy that occurs through physical confrontation between two vessels. However, the modern cyber piracy does not necessarily involve a pirate vessel. These cyber-attacks can take place from land-based hackers. In this way, the attacks can interfere with the ships' operating system without ever approaching the ship vessel physically. Moreover, the Article 101 further requires that these attacks occur on the high seas or outside the jurisdiction of any state. In cyber-attacks, the criminal may be situation within the national boundaries, further complicating the framework.

One such incident that illustrates this legal gap that occurred in 2024 when Iran linked hacking group accessed maritime AIS tracking systems and vessel CCTV feeds to gather data about the commercial ship before it was targeted by a missile strike in the Red Sea. The attackers operated from land or remotely controlled the digital networks rather than from a pirate vessel. This shows how cyber operations targeting ships may fall outside the traditional piracy definition under UNCLOS.[24]

3.3. Consequences of the Legal gap

There is limited legal interpretation on the regulation of the maritime cyber attacks that happens on the high seas. One of the main issue is the prosecution of cyber attackers who target ships operating on the high seas. Since these actions don't fit into the definition of Article 101, authorities would often rely on domestic cybercrime laws, which vary widely between countries.[25]

[23] "Piracy and Undersea Cables: An Overlooked Interpretation of UNCLOS?," EJIL: Talk!, February 27, 2025, https://www.ejiltalk.org/piracy-and-undersea-cables-an-overlooked-interpretation-of-unclos/.
[24] The Hacker News, "Iran-Linked Hackers Mapped Ship AIS Data Days Before Real-World Missile Strike Attempt," https://thehackernews.com/2025/11/iran-linked-hackers-mapped-ship-ais.html.
[25]"Top Content on LinkedIn," https://www.linkedin.com/pulse/aidriven-cyber-piracy-sea-legal-%20challenges-maritime-kotor-kamara-%20xqjxf?utm_source=share&utm_medium=member_ios&utm_campaign=share_via.

Another major issue is uncertainty in the jurisdiction. A cyber-attack may originate from land in one country, targeting a ship in another state and affecting the operation on the high seas. These situations complicate the jurisprudence of the state over the legal issues that arise from these crimes.

3.4. Should Maritime Cyber Attacks be Governed by Cybercrime Law Instead of Piracy Law?

A plausible explanation is that maritime cyberattacks do not need to be forced into piracy framework because a dedicated body of cybercrime law already exists to address them. The most widely known and developed international framework is the Council of Europe's Convention on Cybercrime (Budapest convention, EST No. 185), which addresses internet and computer-related crimes likw illegal access to computer system, data interference, system interference and misuse of devices.[26];[27]

However, cybercrime law alone is insufficient for the governance of cybercrimes that occurs in high seas. There are specific conditions that needs to be addressed when this occurs in high seas. The major limitation is due to the uneven ratification and fragmented substantive law. The Budapest Convention binds only its parties and even if it has been adopted by many states not all of them are ready to join the convention due to concerns over loss of national sovereignty or ratify their domestic laws which makes it unevenly distributed.[28] Whether a cyberattack on a ship is considered a crime or not and how it is pursued depends on the domestic law of the country. This creates a legal uncertainty as to whether the international framework aims to provide a uniform legal framework rather than relying on the laws of individual states. As a result, cybercrime laws differ from one country to another.

Another limitation is the complexity of jurisdiction on the high seas. The cybercrime laws usually allow countries to prosecute the offences based on where the crime occurred, the

[26] Council of Europe, "CONVENTION ON CYBERCRIME Budapest, 23.XI.2001," *Council of Europe*, https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.
[27] "Budapest Convention on Cybercrime – Treaty 185," https://statesassembly.je/getmedia/baff60aa-468b-4914-8420-d3fc58f1698d/Research%20-%20Briefing%20Paper%20on%20Council%20of%20Europe%20Convention%20on%20Cybercrime%20-%2031%20October%202018.pdf.
[28] Kenneth Propp and DeBrae Kennedy-Mayo, "From Budapest to Hanoi: Comparing the Council of Europe and United Nations Cybercrime Conventions," *United Nations General Assembly*, 2024, https://www.crossborderdataforum.org/wp-content/uploads/2025/05/From-Budapest-to-Hanoi-Comparing-the-Council-of-Europe-and-United-Nations-Cybercrime-Conventions.pdf.

nationality of the offender or the victim. However, the maritime cybercrime laws involve multiple countries like the attacker may be from one country, the registered ship in another and the server used to attack maybe in elsewhere. Due to this several countries may claim the right to prosecute creating legal uncertainty as to which state has the legal authority. As a result, it makes it difficult to enforce the law on high seas.[29]

Lastly, the two laws protects different interests. While the cybercrime law protects the confidentiality, integrity and availability of computer systems and data, piracy law protects the security of navigation and freedom of the high seas as a shared global resource.[30] [31] This is governed by UNCLOS, which provides for the seizure and universal prosecution of the pirate ship. But this does not involve the crimes related to computer which is a limitation of UNCLOS.

4. Cyber Attacks Against Ships

4.1. Nature of Maritime Cyber Attacks

Maritime cyber-attacks are unauthorized digital intrusions into the technological systems used on ships. Modern vessels rely on interconnected digital systems for navigation, cargo management, communication, and onboard computer operations, making these systems potential targets for cyber interference.

Cyber attackers may target navigation systems, cargo management systems, communication networks, and onboard computer systems that control or support ship operations. Because these systems are digitally connected, interference with them can disrupt the normal functioning of a vessel.

The perpetrators of maritime cyber-attacks may include cybercriminal groups, organized criminal networks, or hostile state actors. These actors exploit weaknesses in shipboard

[29]Paul Arnell and Bukola Faturoti, "The prosecution of cybercrime: why transnational and extraterritorial jurisdiction should be resisted.," *International Review of Law, Computers & Technology*, 2023, https://rgu-repository.worktribe.com/preview/1694891/ARNELL%202022%20The%20prosecution%20of%20cybercrime%20%28VOR%29.pdf.

[30] Council of Europe, "CONVENTION ON CYBERCRIME Budapest, 23.XI.2001."

[31]Yongming Jin et al., "Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations," *Frontiers in Marine Science* 12 (August 29, 2025), https://doi.org/10.3389/fmars.2025.1616906.

technologies and maritime digital networks to gain unauthorized access or interfere with operations.[32]

4.2. Examples of Maritime Cyber Attacks

4.2.1. Hacking Navigation Systems

Among the most dangerous marine cyber risks is the manipulation of navigation systems. Attackers can jam ships' navigation systems, which rely on Global Positioning System transmissions. This is called GPS spoofing, when attackers send out fake signals to trick navigation devices into displaying the wrong position or path.

4.2.2. AIS Spoofing

The Automatic Identification System (AIS) sends the identification, position, speed and heading of the ship to surrounding ships and to monitoring authorities. AIS spoofing is where attackers transmit false identification or location information, forcing ships to appear to be somewhere they are not, or creating fictitious ships in tracking systems, leading to confusion in maritime monitoring.

4.2.3.Malware Attacks

Malware assaults are corrupt malware that enters ship or company networks via infected devices, phishing emails, or compromised upgrades. Once installed, malware may interfere with the ship's operations, corrupt data or even allow illegal control over digital systems. Some assaults utilize ransomware to limit access to crucial systems until a payment is made.

4.2.4. Satellite Communication Interference

Ships communicate with control centres and logistics networks on land through satellite communications. These satellite links could be targeted by cyber attackers to interrupt communications or intercept important data, affecting coordination with ports and safe sailing.

5. Case Study: The 2024 Red Sea Cyber Operation Against Commercial Shipping

[32] "Maritime Cyber Risk,"https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx?utm.

5.1. Background

In 2024, commercial vessels in international waters increasingly faced cyberattacks in Red Seas. Reports indicate a hostile hacking group hacked into maritime digital systems prior to kinetic attacks on merchant vessels, according to reports released by the United Kingdom Maritime Trade Operations (UKMTO), maritime cybersecurity firms and the United States Cybersecurity and Infrastructure Security Agency (CISA). Rather than use another ship to get close to the ships, the attackers hacked into Automatic Identification System (AIS) data, vessel CCTV feeds and other digital information remotely to track ship movements and gather intel.[33]

5.2. Nature of the Attack

The attackers did not physically board or intercept the targeted vessel but instead used digital maritime infrastructure from land-based locations. The operation involved the collection of navigational and surveillance data that enabled subsequent missile strikes on commercial ships in the Red Sea. The cyber element of the operation was completely remote, via access to digital networks, showing how maritime attacks can now be carried out without any physical interaction between ships.[34] [35]

5.3. Legal Analysis under UNCLOS.

Article 101 defines piracy as any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship.

Consequently, despite direct threatening the safety and security of maritime navigation, cyber operation does not satisfy the traditional "two-ship requirement" stated in Article 101. Also, because the attackers were allegedly linked to a state-affiliated group, the "private ends" requirement presents an additional obstacle to classify the conduct as piracy under UNCLOS.[36]

---

[33] United States Maritime Administration, Maritime Security Communications with Industry (MSCI) Advisory 2024-006: Threats to Commercial Vessels, https://www.maritime.dot.gov/msci/2024-006-southern-red-sea-bab-el-mandeb-strait-gulf-aden-indian-ocean-somali-basin-arabian-sea.

[34] International Maritime Organization, Maritime Cyber Risk, https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx.

[35] United States Maritime Administration, MSCI Advisory 2024-006, https://www.maritime.dot.gov/msci/2024-006-southern-red-sea-bab-el-mandeb-strait-gulf-aden-indian-ocean-somali-basin-arabian-sea.

[36] United Nations, United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397, arts. 101 & 105, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

5.4. Critical Analysis of the Case Study

The 2024 Red Sea cyber operation highlights the limitations of Article 101 of UNCLOS in addressing modern maritime cyber threats. Although the attack targeted a commercial vessel on the high seas, it was carried out remotely without the use of a pirate vessel. Consequently, it does not satisfy the traditional "two-ship requirement," exposing a significant legal gap in the definition of piracy.[37]

The event also raises questions about the “private ends” rule. But the attack was purportedly related to a state-sponsored group pursuing strategic aims, thus it doesn't qualify as piracy under UNCLOS. This reveals that the Convention is not geared to handle state-sponsored marine cyber activities.

Moreover, the case shows the jurisdictional problems that cyberattacks provide where the hackers, digital infrastructure and affected vessel may be located in separate jurisdictions. This limits the exercise of jurisdiction available for piracy under Article 105.

5.5. Relevance to the Research Problem

The event suggests that today’s marine cyber assaults have outgrown the concepts that supported the 1982 UNCLOS framework. A cyber attack can have a serious impact on marine operations, undermine the safety of navigation and enable physical attacks without a single pirate vessel being involved.” This kind of action has similar repercussions to those of traditional pirate attacks, but does not fit under the purview of traditional piracy.

This case is a case in point of the main thesis of this study, namely that the existing legal definition of piracy under article 101 is not sufficient to deal with modern marine cyber operations. It strengthens the need for regulatory reform through an interpretative measure, such as an advisory opinion from the ITLOS, or legislative developments, such as modifications to the SUA Convention or the establishment of a specific international framework for maritime cybersecurity.[38][39]

[37] International Maritime Organization, Maritime Cyber Risk, https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx.
[38] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention), Mar. 10, 1988, https://www.imo.org/en/About/Conventions/Pages/SUA-Treaties.aspx.
[39] International Tribunal for the Law of the Sea, Advisory Proceedings,

5.6. Key Takeaway

The 2024 Red Sea cyber operation shows that cyberattacks on ships in high seas can affect navigation and maritime security without engaging a second ship. This exposes a fundamental legal vacuum in UNCLOS and supports the claim that the traditional two-ship rule no longer appropriately represents the realities of current maritime cyber threats.[40]

6. Regulatory Alternatives and Legally Viable Solutions

6.1. Seek an International Tribunal for the Law of the Sea *(ITLOS) Advisory Opinion to Clarify Article 101 UNCLOS.*

Since it is politically and procedurally difficult to change Article 101 of the UNCLOS, a more realistic temporary option would be to seek an advisory opinion to the ITLOS through a competent authority or accord. Such an opinion may shed light on whether cyber operations that have effects functionally equal to acts of violence or depredation against ships, may be considered to fall within the ambit of pirate under Article 101. While ITLOS advisory opinions are not obligatory in law, they do have important weight and have contributed to the gradual development and consistent interpretation of international law. The Tribunal has previously dealt with complicated legal issues in its 2015 Advisory Opinion concerning the Sub-Regional Fisheries Commission (SRFC) and its 2024 Advisory Opinion on Climate Change and International Law, showing its capacity to interpret emerging questions under the law of the sea. Thus, an advisory opinion on maritime cyber activities would give governments with the interpretative guidance they desperately need, while bypassing the lengthy and politically taxing process of formally revising UNCLOS.

6.2. Expand the SUA Convention to Explicitly Criminalize Maritime Cyberattacks

States should consider amending the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation or adopting an additional protocol to explicitly criminalize cyberattacks against a vessel's digital systems, rather than relying solely on the piracy provisions under UNCLOS. Unlike Article 101 of UNCLOS, the SUA Convention does not require the involvement of a second vessel. The Convention already criminalizes activities

https://www.itlos.org/en/main/cases/advisory-proceedings

[40] United Nations, United Nations Convention on the Law of the Sea, art. 101.

that undermine the safe navigation of ships, such as damage to vessels, destruction of navigational facilities, and the dissemination of false information. Expanding these rules to explicitly cover hostile cyber operations will fill the existing jurisdictional gap while maintaining the current legal framework on piracy. This change should also be backed by wider ratification and effective implementation, especially by large flag States.

6.3. Transform IMO Cyber Risk Management into a Mandatory Auditable Compliance Standard

The International Maritime Organization should reinforce its existing cyber-risk framework by mandating compliance with marine cybersecurity regulations and having them independently audited. The International Safety Management (ISM) Code requires shipping companies to include cyber risk in their safety management systems through IMO Resolution MSC.428(98). Detailed guidance on cyber risk management is provided in MSC-FAL.1/Circ.3/Rev.1, but implementation seems inconsistent as the framework is largely guidance-based rather than enforceable. Introducing mandatory third-party audits and allowing Port State Control authorities to verify cyber-risk compliance during inspections would promote consistent implementation, enhance maritime cyber resilience, and improve cybersecurity standards across flag states.[41]

7. Conclusion

As the technological transformation of maritime sector is evolving, the nature of threats is also evolved involving vessels on high seas. Even though the advancements which improve efficiency in maritime trade, it changes the industry and shifts it to vulnerability to cyber attacks. This attacks are very different from conventional attacks of piracy because this attacks can be carried out remotely without any physical presence of pirate ship.

The existing convention on sea UNCLOS states that there should be two-ship requirement and any form of physical violence namely illegal acts of violence, detention or any act mentioned under Article 101 to be considered as an act of piracy.

The traditional two-ship requirement, together with the convention's view of physical acts of violence, reflects the history of maritime piracy. But this gives rise to challenges to emerging

[41] 53. MSC-FAL.1/Circ.3/Rev.1: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

cyber attacks like GPS spoofing, AIS manipulation, malware attacks, and satellite communication interference which can damage ship and cause disruption without any pirate ship.

The analysis of the convention and rising cyber threats suggests that the two-ship requirement under UNCLOS is inadequate for addressing the modern threats. Which consequently opens a significant legal gap in the framework.

To address this gap this paper suggests a multi-layered approach. Rather than relying solely on UNCLOS, this paper emphasizes on obtaining a logical clarification of article 101 through the International Tribunal for the Law of the Sea (ITLOS) and expanding the scope of SUA convention to expressly address maritime cyberattacks. Also strengthening the International Maritime Organization's cybersecurity through mandatory auditable compliance standards. Altogether, these measures will enable international maritime law to respond more efficiently to emerging cyber threats while preserving the fundamental principle of navigation, security and cooperation on the high seas.

BIBLIOGRAPHY:

1. "1982 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA." *Centre for International Law*, https://cil.nus.edu.sg/wp-content/uploads/2019/02/1982-United-Nations-Convention-on-the-Law-of-the-Sea.pdf.

2. Apostolos Kapsalis. "Cybersecurity and Cyberattacks in Maritime Shipping." *ResearchGate*, November 2025. https://www.researchgate.net/publication/397642565_Cybersecurity_and_Cyberattacks_in_Maritime_Shipping.

3. Anne Veerpalu. "Functional Equivalence: An Exploration Through Shortcomings to Solutions." *ResearchGate*, December 2019. https://www.researchgate.net/publication/339931469_Functional_Equivalence_An_Exploration_Through_Shortcomings_to_Solutions.

4. Baniela, Santiago Iglesias, and Juan Vinagre Ríos. "Piracy in Somalia: A Challenge to the International Community." *Journal of Navigation* 65, no. 4 (June 15, 2012): 693–710. https://doi.org/10.1017/s0373463312000185.

5. "Budapest Convention on Cybercrime – Treaty 185," https://statesassembly.je/getmedia/baff60aa-468b-4914-8420-d3fc58f1698d/Research%20-%20Briefing%20Paper%20on%20Council%20of%20Europe%20Convention%20on%20Cybercrime%20-%2031%20October%202018.pdf.

6. Bhatti, Jahshan, and Todd E. Humphreys. "Hostile Control of Ships via False GPS Signals: Demonstration and Detection." *NAVIGATION Journal of the Institute of Navigation* 64, no. 1 (March 1, 2017): 51–66. https://doi.org/10.1002/navi.183.

7. Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. "A security evaluation of AIS automated identification system." *ACM Digital Library*, December 8, 2014, 436–45. https://doi.org/10.1145/2664243.2664257.

8. "Chapter 2: Maritime Zones – Law of the Sea," https://sites.tufts.edu/lawofthesea/chapter-two/.

9. Douglas Guilfoyle. "Shipping Interdiction and the Law of the Sea," https://www.academia.edu/31002094/Shipping_Interdiction_and_the_Law_of_the_Sea.

10. EJIL: Talk! "Piracy and Undersea Cables: An Overlooked Interpretation of UNCLOS?," February 27, 2025. https://www.ejiltalk.org/piracy-and-undersea-cables-an-overlooked-interpretation-of-unclos/.

11. International Maritime Organization,"Maritime Security: A Pillar for Economic Development," 10 October 2024, https://www.imo.org/en/mediacentre/pages/whatsnew-2157.aspx.

12. International Tribunal for the Law of the Sea. "UNCLOS," https://www.itlos.org/en/main/the-tribunal/unclos/#c4986.

13. Jin, Yongming, Yuan Feng, Chaomin Liu, and Shibo Li. "Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations." *Frontiers in Marine Science* 12 (August 29, 2025). https://doi.org/10.3389/fmars.2025.1616906.

14. LII/Legal Information Institute. "High Seas," https://www.law.cornell.edu/wex/high_seas.

15. Melnyk, Oleksiy, Oleksandr Drozdov, and Serhii Kuznichenko. "Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures." *Lex Portus* 11, no. 1 (March 11, 2025). https://doi.org/10.62821/lp11101.

16. Mick P. Green, Douglas R. Burnett, and Nternational Cable Protection Committee, Ltd, "Security of International Submarine Cable Infrastructure: Time to Rethink?," *BRILL*, n.d., https://brill.com/display/book/edcoll/9789047440406/Bej.9789004164277.v-594_021.xml?language=en&srsltid=AfmBOorLxjvSLb7wnGQPmFlHEzoJfbtaOwOLATkp673cVcaCuquRZDIx.

17. "Overview - Convention & Related Agreements," https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm.

18. Prapti Dheeraj. "Critical Analysis of the Evolving Concept of Maritime Boundaries in Light of UNCLOS." IJLSSS, July 20, 2024. https://ijlsss.com/critical-analysis-of-the-evolving-concept-of-maritime-boundaries-in-light-of-unclos/.

19. Propp, Kenneth, and DeBrae Kennedy-Mayo. "From Budapest to Hanoi: Comparing the Council of Europe and United Nations Cybercrime Conventions." *United Nations General Assembly*, 2024. https://www.crossborderdataforum.org/wp-content/uploads/2025/05/From-Budapest-to-Hanoi-Comparing-the-Council-of-Europe-and-United-Nations-Cybercrime-Conventions.pdf.

20. Paul Arnell, and Bukola Faturoti. "The prosecution of cybercrime: why transnational and extraterritorial jurisdiction should be resisted." *International Review of Law, Computers & Technology*, 2023. https://rgu-repository.worktribe.com/preview/1694891/ARNELL%202022%20The%20prosecution%20of%20cybercrime%20%28VOR%29.pdf.

21. Snyder, John. "Cyber Criminals and Bad Actors Roam on the High Seas." Riviera, August 11, 2025. https://www.rivieramm.com/news-content-hub/cybercriminals-and-bad-actors-roam-on-the-high-seas-85653.

22. Tullio Treves, "1958 Geneva Conventions on the Law of the Sea - Main Page," https://legal.un.org/avl/ha/gclos/gclos.html.

23. The Hacker News. "Iran-Linked Hackers Mapped Ship AIS Data Days Before Real-World Missile Strike Attempt," n.d. https://thehackernews.com/2025/11/iran-linked-hackers-mapped-ship-ais.html.

24. Top "Content on LinkedIn," n.d. https://www.linkedin.com/pulse/aidriven-cyber-piracy-sea-legal-%20challenges-maritime-kotor-kamara-%20xqjxf?utm_source=share&utm_medium=member_ios&utm_campaign=share_vi.

25. "United Nations Convention on the Law of the Sea," n.d. https://www.imo.org/en/ourwork/legal/pages/unitednationsconventiononthelawofthesea.aspx.

26. Yongming Jin et al. "Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations." *Frontiers in Marine Science* 12 (August 29, 2025). https://doi.org/10.3389/fmars.2025.1616906.

27. "Budapest Convention on Cybercrime – Treaty 185," https://statesassembly.je/getmedia/baff60aa-468b-4914-8420-d3fc58f1698d/Research%20-%20Briefing%20Paper%20on%20Council%20of%20Europe%20Convention%20on%20Cybercrime%20-%2031%20October%202018.pdf.

28. Kenneth Propp and DeBrae Kennedy-Mayo, "From Budapest to Hanoi: Comparing the Council of Europe and United Nations Cybercrime Conventions," United Nations General Assembly, 2024, https://www.crossborderdataforum.org/wp-content/uploads/2025/05/From-Budapest-to-Hanoi-Comparing-the-Council-of-Europe-and-United-Nations-Cybercrime-Conventions.pdf.

29. Paul Arnell and Bukola Faturoti, "The prosecution of cybercrime: why transnational and extraterritorial jurisdiction should be resisted.," International Review of Law, Computers & Technology, 2023, https://rgu-repository.worktribe.com/preview/1694891/ARNELL%202022%20The%20prosecution%20of%20cybercrime%20%28VOR%29.pdf.

30. Council of Europe, "CONVENTION ON CYBERCRIME Budapest, 23.XI.2001."

31. Yongming Jin et al., "Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations," Frontiers in Marine Science 12 (August 29, 2025), https://doi.org/10.3389/fmars.2025.1616906.

32. "Maritime Cyber Risk,"https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx?utm.

33. United States Maritime Administration, Maritime Security Communications with Industry (MSCI) Advisory 2024-006: Threats to Commercial Vessels, https://www.maritime.dot.gov/msci/2024-006-southern-red-sea-bab-el-mandeb-strait-gulf-aden-indian-ocean-somali-basin-arabian-sea.

34. International Maritime Organization, Maritime Cyber Risk, https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx.

35. United States Maritime Administration, MSCI Advisory 2024-006, https://www.maritime.dot.gov/msci/2024-006-southern-red-sea-bab-el-mandeb-strait-gulf-aden-indian-ocean-somali-basin-arabian-sea.

36. United Nations, United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397, arts. 101 & 105, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

37. International Maritime Organization, Maritime Cyber Risk, https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx.

38. United Nations, United Nations Convention on the Law of the Sea, Montego Bay, Jamaica, December 10, 1982, art. 101 and 105, 1833 U.N.T.S. 397. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

39. Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention), Mar. 10, 1988, https://www.imo.org/en/About/Conventions/Pages/SUA-Treaties.aspx.

40. International Tribunal for the Law of the Sea, Advisory Proceedings, https://www.itlos.org/en/main/cases/advisory-proceedings

41. United Nations, United Nations Convention on the Law of the Sea, art. 101.

42. MSC-FAL.1/Circ.3/Rev.1: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.