

Article

The Law the Sea Left Behind: Reforming Maritime Criminal Law

Selina Wai-Ming Robinson 

School of Criminology and Criminal Justice, University of Portsmouth, Portsmouth PO1 2DZ, UK;
selina.robinson@port.ac.uk

Abstract

This article examines the legal inadequacy of traditional piracy frameworks in responding to contemporary maritime threats. The legal definition of piracy, rooted in Articles 101 and 105 of the United Nations Convention on the Law of the Sea (UNCLOS), was designed for a narrower category of maritime violence than now exists, and this definitional gap produces enforcement failures across criminal, international, and maritime governance law. Drawing on interdisciplinary literature spanning maritime security, criminology, international law, cybersecurity, and organised crime research, the article identifies five principal threat categories that fall outside existing piracy law: organised maritime crime, maritime terrorism, cyber-enabled disruption, illegal fishing, and state-linked hybrid maritime activity. It further identifies structural legal vulnerabilities, including jurisdictional fragmentation, the high seas/territorial waters divide, the private gain requirement, and the absence of a unified cyber-maritime legal instrument, that prevent existing frameworks from adequately regulating contemporary maritime criminality. The article concludes with a normative argument for an expanded, adaptive legal framework integrating cybersecurity, grey zone activity, and organised crime into maritime law, alongside improved international coordination, intelligence-sharing obligations, and governance capacity. The paper contributes directly to ongoing debates about the fitness for purpose of UNCLOS and the need for supplementary legal instruments to address twenty-first-century maritime threats.

Keywords: maritime piracy; UNCLOS; maritime law reform; hybrid threats; maritime cybersecurity; organised crime; maritime terrorism; legal frameworks; blue crime

1. Introduction

Maritime security has become one of the defining legal and security challenges of the twenty-first century. The global economy depends heavily on maritime transport, with shipping routes connecting producers, consumers, energy markets, food systems, and industrial supply chains across continents. Disruption at sea, whether through a hijacked vessel, a blocked chokepoint, a cyberattack on a port, or an attack on offshore infrastructure, can produce cascading consequences across trade, insurance, food security, energy markets, and national security, as seen in the blockage of the Strait of Hormuz during the Iran conflict (2026), or the grounding of the Ever Given container vessel in the Suez Canal on 23 March 2021.

The legal response to maritime crime has historically been organised around the concept of piracy. Piracy is defined in Article 101 of UNCLOS as any illegal act of violence, detention, or depredation committed for private ends by the crew or passengers of a private ship, directed against another ship, persons, or property on the high seas. This definition



Academic Editor: James C. Simeon

Received: 25 May 2026

Revised: 31 July 2026

Accepted: 1 August 2026

Published: 4 August 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

has remained the cornerstone of international maritime criminal law for decades. However, this article argues that UNCLOS Article 101 is no longer legally adequate to address the full range of contemporary maritime threats, and that its continued dominance as the organising framework of maritime criminal law produces significant enforcement gaps with real-world consequences. While the limitations of the UNCLOS piracy framework have been widely recognised in relation to specific issues, including maritime terrorism, cyber-enabled threats, and illegal, unreported and unregulated fishing, these challenges have largely been examined in isolation. This article argues that they instead reveal a broader structural inadequacy within the existing international maritime legal framework and asks whether the legal architecture centred on UNCLOS Article 101 remains capable of regulating contemporary maritime criminality.

That broader structural inadequacy is reflected in three principal legal deficiencies. First, the private requirement in piracy law excludes politically motivated maritime violence, meaning that a wide category of maritime terrorism falls outside the legal definition of piracy and into a fragmented patchwork of domestic law and the 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention). Second, the high seas limitation in UNCLOS means that maritime crimes committed in territorial waters or exclusive economic zones, including armed robbery, illegal fishing, and smuggling, fall under domestic jurisdiction, producing inconsistent and often inadequate legal responses. Third, and most importantly, there is currently no binding international legal instrument that addresses cyber-enabled maritime threats, even though cyberattacks can have consequences comparable to or exceeding those of physical maritime violence. Beyond these doctrinal failures, contemporary maritime criminality increasingly operates through overlapping and hybrid modalities that resist categorisation within existing legal frameworks. Criminal groups engage in piracy, smuggling, trafficking, and illegal fishing using the same routes, networks, and corrupt facilitators. State-linked actors use proxy groups, shadow fleets, and grey-zone tactics that fall below the threshold of armed conflict but above that of ordinary crime. Cyber actors manipulate navigational data, disrupt port systems, and enable physical maritime crime without setting foot on a vessel (Chatterjee 2014). None of these activities fit neatly within the existing piracy legal framework, and the absence of an adequate legal response leaves enforcement agencies without the statutory tools they need.

This article proceeds as follows. Section 2 describes the methodology. Section 3 examines the historical foundations and legal architecture of maritime piracy law. Section 4 analyses five categories of evolving maritime threats and the legal gaps each exposes. Section 5 examines why maritime spaces are structurally vulnerable to legal arbitrage. Section 6 considers the legal implications of technological transformation. Section 7 develops the normative argument for legal reform and Section 8 concludes.

2. Methods

This article uses doctrinal legal analysis and a qualitative literature review. This combined methodological approach is appropriate because the research question concerns the adequacy of the existing legal framework rather than the prevalence of particular forms of maritime crime, and thus requires critical analysis of legal instruments alongside an evaluation of the contemporary academic literature. The doctrinal analysis examines key primary legal instruments, including UNCLOS, the 1988 SUA Convention, the Cape Town Agreement, and relevant International Maritime Organisation (IMO) instruments, to assess what existing maritime criminal law covers and, critically, where it falls short.

The literature review drew on searches across multiple academic databases and publisher platforms, including Scopus, Web of Science, Google Scholar, Taylor & Francis Online,

Sage Journals, Wiley Online Library, SpringerLink, and JSTOR. Search terms included: maritime piracy, UNCLOS, maritime terrorism, SUA Convention, organised maritime crime, maritime cybersecurity, illegal fishing, IUU fishing, hybrid threats, blue crime, maritime governance, maritime jurisdiction, flag state jurisdiction, and the law of the sea. The searches were conducted between March and May 2026.

Sources were included where they engaged substantively with legal frameworks, jurisdictional questions, criminal law, governance, or the normative dimensions of maritime security. Sources were excluded where they addressed maritime security in purely technical or operational terms without legal or governance relevance, or where they could not be verified through accessible academic repositories. Priority was given to peer-reviewed journal articles, though book chapters, legal analyses, and credible policy documents were included where they made a direct contribution to the legal arguments developed in this article. The regional examples discussed throughout the article were selected because they illustrate distinct categories of legal challenge rather than to provide an exhaustive geographical survey. Somalia demonstrates the operation of universal jurisdiction under the traditional piracy framework; the Gulf of Guinea illustrates the jurisdictional limitations arising from offences committed within territorial waters; the Straits of Malacca and Singapore provide an example of emerging cyber–physical maritime vulnerabilities; and the Strait of Hormuz illustrates the increasing significance of hybrid and state-linked maritime threats. Collectively, these case studies are intended to demonstrate how different forms of contemporary maritime criminality expose common structural weaknesses within the existing international legal framework.

No primary data was collected, no datasets were generated, and no human participants were involved. Ethical approval was not required.

All sources drawn upon are publicly available. There are no restrictions on materials or information associated with this publication.

3. Historical Foundations and Legal Architecture of Maritime Piracy Law

Piracy is one of the oldest forms of maritime criminality, and its legal definition has deep roots in customary international law. The classical characterisation of the pirate is as ‘hostis humani generis’, the enemy of all humanity, and reflects the historical view that piracy was a universal crime justifying universal jurisdiction. This principle, articulated by Grotius and developed in subsequent centuries of state practice, forms the foundation of the modern legal approach to piracy (Galgano 2023). The rationale for universal jurisdiction was that piracy occurred on the high seas, beyond the territorial jurisdiction of any state, and that pirates had therefore placed themselves outside the protection of any legal order. The contemporary legal definition of piracy is codified in Articles 100–107 of UNCLOS, which represents the most authoritative statement of international piracy law. Article 101 defines piracy as comprising illegal acts of violence, detention, or depredation committed for private ends by the crew of a private ship on the high seas or in a place outside the jurisdiction of any state. Article 105 grants all states the right to seize pirate ships and prosecute pirates, giving effect to the principle of universal jurisdiction (Bellamy 2020). These provisions reflect a deliberate legal design: piracy law was constructed to address a specific type of criminal who conducts private, economically motivated, maritime violence in international waters (Khaerany and Maskun 2016). This deliberate legal design has, however, generated sustained academic debate regarding whether the definitional boundaries of Article 101 remain appropriate for contemporary maritime security challenges. While the traditional interpretation reflects the historical purpose of piracy law, commentators have increasingly questioned whether concepts such as “private ends” and the restriction to the high seas continue to provide an adequate legal basis for

responding to modern forms of maritime criminality. Rather than treating these criticisms as isolated doctrinal issues, this article argues that they collectively expose broader structural limitations within the existing international maritime legal framework.

This legal architecture has significant consequences for how piracy is enforced and prosecuted. The requirement that acts be committed for “private ends” has proved one of the most contested elements of Article 101. Although traditionally interpreted to exclude politically or ideologically motivated violence, thereby placing maritime terrorism outside the scope of piracy law, this limitation has generated considerable doctrinal debate over whether a broader functional interpretation is justified in light of evolving patterns of maritime violence. Regardless of the preferred interpretation, the continuing disagreement illustrates that the existing legal framework was not designed to accommodate the increasingly blurred distinction between politically motivated and economically motivated maritime offending. Similarly, the geographical limitation of Article 101 to the high seas reflects the historical rationale for universal jurisdiction, namely that piracy occurred beyond the territorial jurisdiction of any state. Contemporary maritime criminality, however, increasingly occurs within territorial waters or exclusive economic zones, where responsibility rests primarily with coastal states. While this jurisdictional division was intended to preserve state sovereignty, it has also been criticised for creating fragmented enforcement arrangements and significant disparities in national responses to functionally similar forms of maritime violence. Conduct that would constitute piracy on the high seas may therefore fall outside UNCLOS Article 101 when committed in territorial waters, where it is instead treated as “armed robbery against ships” under IMO definitions.

This category lacks the same universal jurisdiction and international legal machinery as the former (Li and Yang 2023). These distinctions matter enormously in practice: the same crew, attacking the same vessel and using the same method, may be pirates (subject to universal jurisdiction) or domestic criminals (subject only to local jurisdiction) depending entirely on the geographic coordinates of the attack.

The rise of Somali piracy in the 2000s tested and exposed several of these legal tensions. Piracy off Somalia demonstrated how local grievance, weak governance, environmental harm, and organised criminal entrepreneurship could interact to produce a sustained maritime threat (Weldemichael 2012). More importantly for present purposes, it revealed the procedural and jurisdictional difficulties of prosecuting pirates under UNCLOS. Naval forces from multiple states operating under international mandates captured suspected pirates. However, prosecution proved considerably more complex than exercising interdiction powers at sea. Questions concerning applicable domestic law, evidentiary standards, transfer agreements, regional prosecutorial capacity, and compliance with international human rights obligations demonstrated that universal jurisdiction under Article 105 was not, in itself, sufficient to ensure effective criminal accountability (Alsawalqa and Venter 2021; Ghosh 2014). The legal response to Somali piracy required significant improvisation, such as bilateral transfer agreements and improvised prosecution frameworks. It expanded regional court capacity, demonstrating that UNCLOS Article 101 was not self-executing but required substantial institutional infrastructure to be legally effective. The Gulf of Guinea illustrates a further legal complication. Maritime crime in this region has often involved oil theft, kidnapping, and cargo theft linked to onshore criminal and political economies, much of it occurring within territorial waters rather than on the high seas (Adesanya 2023; Denton and Harris 2019; Kamga 2024). Because UNCLOS Article 101 does not apply to territorial waters, this conduct falls outside international piracy law and into the domestic criminal jurisdiction of coastal states—many of which lack the institutional capacity, legislative framework, or political will to prosecute effectively (He et al. 2023). The result is not merely an operational enforcement gap but a structural legal limitation arising from the allocation

of jurisdiction within the existing law of the sea framework. Consequently, conduct that may be operationally indistinguishable from piracy can attract markedly different legal treatment depending solely upon the maritime zone in which it occurs.

Traditional piracy law can therefore be characterised as: geographically restricted to the high seas; limited to private, economically motivated actors; dependent on universal jurisdiction as its enforcement mechanism; and designed for direct physical attacks on vessels. Each of these characteristics represents a legal boundary that contemporary maritime threats have surpassed or rendered legally insufficient.

4. The Legal Gaps Exposed by the Evolution of Maritime Criminality

4.1. *Organised Maritime Crime and the Limits of Piracy Law*

Contemporary maritime crime increasingly operates through organised and transnational networks. Bueger and Edmunds (2020) describe this wider field as “blue crime,” capturing the convergence of different illicit maritime activities and emphasising that maritime criminality cannot be reduced to a single offence category. This convergence exposes a fundamental limitation of the existing international legal framework, which continues to regulate piracy, smuggling, trafficking, illegal fishing, and cargo theft as legally distinct phenomena, even though they increasingly operate as interconnected manifestations of organised maritime criminality (Aishwarya 2021).

The legal significance of this categorical approach lies in its inability to accommodate the operational reality of organised maritime crime, where different forms of offending frequently overlap and reinforce one another. Criminal networks operating in maritime spaces do not respect legal categories. The same routes, corrupt facilitators, financial systems, ports, and weak enforcement environments may support piracy, drug trafficking, human smuggling, and fuel theft simultaneously. In the Gulf of Guinea, armed robbery at sea has intersected with oil bunkering operations and kidnapping for ransom, involving actors who shift between legally distinct offence categories depending on opportunity (Adesanya 2023; Denton and Harris 2019). However, maritime law and domestic criminal law typically address each category of offence through separate statutory provisions, separate agencies, and separate jurisdictional rules. Consequently, organised maritime crime is often fragmented into discrete legal offences, each attracting different jurisdictional rules and enforcement mechanisms, rather than being addressed as a coherent transnational criminal enterprise.

Shadow fleets represent a particularly significant legal challenge within this category. Vessels operating through opaque ownership structures, flags of convenience, and complex corporate arrangements to evade sanctions or conceal cargo origins exploit a structural feature of international shipping law: the separation between flag-state jurisdiction, port-state authority, and coastal-state rights. Because the flag state exercises primary jurisdiction over a vessel on the high seas, and because flags of convenience are readily available to operators who wish to minimise regulatory scrutiny, shadow fleet operators can legally register vessels in jurisdictions with limited capacity or willingness to enforce maritime law (Papastavridis 2016). This is not a gap in enforcement—it is a gap in law. The current legal architecture of flag-state jurisdiction, designed in an era when flags reflected genuine national connections, actively facilitates the legal evasion that shadow fleets depend on. The difficulty, therefore, lies not simply in the capacity of states to enforce existing rules, but in the fact that the existing jurisdictional architecture permits these practices to develop within the boundaries of international law.

Trafficking and smuggling via maritime routes further illustrate the limitations of piracy-centred law. These activities exploit weak port controls, limited maritime domain awareness, and the practical impossibility of inspecting more than a small fraction of

maritime cargo. Legal responses primarily depend on domestic criminal law and on bilateral or multilateral agreements, such as the Palermo Protocol (Miloš et al. 2023). The consequence is a persistent legal gap in which maritime trafficking and smuggling are governed by a fragmented mix of domestic criminal law and international agreements not designed to address the jurisdictional and operational complexities of contemporary organised maritime crime. The inadequacy, therefore, lies not merely in enforcement but in the absence of an integrated legal framework capable of addressing maritime criminality as a connected transnational phenomenon.

4.2. Maritime Terrorism and the SUA Convention's Limitations

Maritime terrorism represents the clearest example of conduct that falls categorically outside the UNCLOS definition of piracy. Because UNCLOS Article 101 requires that piracy be committed “for private ends,” politically or ideologically motivated maritime violence, however similar in method to piracy, cannot legally constitute piracy under international law. This is not merely a semantic distinction. It has direct consequences for the legal machinery available to states: universal jurisdiction under UNCLOS Article 105 does not apply, naval forces operating under anti-piracy mandates may lack authority to intercept and prosecute, and prosecution must instead rely on domestic terrorism law or the SUA Convention.

The SUA Convention of 1988, developed in response to the hijacking of the *Achille Lauro* in 1985, was designed to address the legal gap left by the private-ends requirement in piracy law. It criminalises a range of acts that endanger maritime navigation, including the seizure or control of a ship by force, violence against persons on board, and the placement of devices on a ship likely to destroy or damage it. The 2005 Protocol to the SUA Convention extended its scope to cover acts involving weapons of mass destruction and offences committed by or against persons on ships. The SUA Convention therefore complements, rather than replaces, the piracy regime established under UNCLOS by criminalising conduct that falls outside Article 101 while relying upon a fundamentally different jurisdictional and enforcement model (Luft and Korin 2004; Murphy 2009; Osadtsa 2025).

However, the SUA Convention has significant limitations as a counterterrorism instrument. It operates through an obligation to extradite or prosecute (*aut dedere aut judicare*) rather than through universal jurisdiction, meaning that prosecution depends on state cooperation and the domestic legislative implementation of SUA obligations. It also lacks the automatic enforcement mechanism that UNCLOS Article 105 provides for piracy, under which any state may seize a pirate vessel (Li 2023). In practice, these limitations mean that the effectiveness of the SUA Convention depends less upon the existence of international legal obligations than upon the willingness and capacity of individual states to incorporate, investigate and prosecute offences through their domestic legal systems. Unlike the piracy regime under UNCLOS, the Convention does not, by itself, create a comprehensive international enforcement framework capable of responding to maritime terrorism wherever it occurs (Papastavridis 2016).

The operational overlap between piracy and maritime terrorism creates further legal difficulty. Groups may shift between economically and politically motivated maritime violence depending on the circumstances. A group may engage in smuggling to finance political violence, use piracy-style tactics to support insurgency, or attack maritime targets for both profit and strategic disruption (Khan 2020; Lehr 2006). When conduct is legally ambiguous as to motive, the choice between piracy law and terrorism law and their different jurisdictional bases, enforcement mechanisms, and procedural requirements becomes contested. The attack on the *USS Cole* in 2000 and the activities of groups such as Hezbollah

in the Mediterranean illustrate the difficulty of applying stable legal categories to hybrid maritime political violence (Luft and Korin 2004; Murphy 2009). The persistence of this ambiguity illustrates a broader structural limitation within the existing legal framework. Where the legal classification of maritime violence depends upon establishing motive, jurisdiction and the applicable enforcement regime, these may themselves become contested, reducing legal certainty and complicating effective international cooperation. Taken together, UNCLOS and the SUA Convention illustrate the fragmented nature of the current international legal response. Rather than operating as complementary components of a coherent framework, they regulate different forms of maritime violence through distinct jurisdictional principles and enforcement mechanisms, leaving uncertainty where contemporary maritime threats blur the traditional distinction between piracy and politically motivated violence.

4.3. Cyber-Enabled Maritime Threats and the Absence of Legal Frameworks

One of the most significant legal gaps in contemporary maritime law is the absence of a binding international framework governing cyber-enabled maritime threats. Modern shipping depends on digital systems, including port management software, navigation systems, satellite communications, Automatic Identification System (AIS), Global Navigation Satellite System (GNSS), electronic charts, and logistics platforms. Cyberattacks can target ships, ports, offshore infrastructure, and communication networks, resulting in consequences ranging from data manipulation to physical collisions, cargo delays, and environmental disasters. However, despite growing recognition of maritime cyber risk within the International Maritime Organisation (IMO), including cyber risk management guidance and recommendations for integration within existing safety management systems, there remains no binding international legal instrument specifically regulating cyber-enabled maritime threats or establishing uniform obligations relating to prevention, investigation or enforcement (Afenyo and Caesar 2023; Ashraf et al., 2023). The IMO's current approach, therefore, recognises the problem but remains focused primarily on operational risk management rather than on binding criminal, jurisdictional or enforcement rules for cyber-enabled maritime attacks.

This legal lacuna has significant jurisdictional and enforcement consequences. If a cyberattack causes a vessel to ground, collide, or spill cargo, the legal response must be cobbled together from general principles of international law, domestic criminal statutes, and maritime liability conventions that were not designed with cyber incidents in mind (Otto and Jernberg 2020). Attribution of cyberattacks is difficult in any domain, and it is especially complex in maritime contexts where vessels operate across multiple jurisdictions, IT systems may be managed by third-party providers, and flag state capacity to investigate may be limited. Fenton (2024) demonstrates the scale of this vulnerability through analysis of the Straits of Malacca and Singapore, one of the world's most critical maritime choke-points, where a successful cyber-physical attack could cause physical collisions, blockages, and cascading supply chain consequences.

AIS spoofing and GNSS interference are particularly concerning because they directly undermine the navigational integrity of maritime systems. AIS manipulation can conceal vessel identity, falsify location data, and facilitate sanctions evasion, smuggling, and illegal fishing, while making it legally impossible to establish a vessel's position at a given time—a fundamental requirement for jurisdictional attribution and prosecution (Sosnowski et al. 2024). This illustrates that cyber-enabled interference challenges not only navigational safety but also the evidential foundations upon which existing maritime jurisdiction and criminal accountability depend.

GNSS interference can increase the risk of collisions for vessels and disrupt traffic management in congested waterways. They are not speculative threats; they are documented, recurring practices that current maritime law lacks a specific framework to address. Ransomware attacks on ports present a further legal challenge. Ports are critical nodes in global supply chains, and their digital systems coordinate vessel arrivals, cargo movements, customs processing, and logistics networks (Pandey 2023). A cyberattack on a major port can create cascading delays across international trade. However, port cybersecurity incidents are currently governed primarily by domestic law, with no international obligation on states to report, investigate, or share information about cyber incidents affecting their port infrastructure.

The absence of mandatory reporting obligations means that the true scale of maritime cyber incidents remains uncertain, limiting both the development of consistent state practice and the ability of states and industry to assess the threat environment and formulate proportionate legal responses (Fenton 2024; Tachie-Menson 2023).

4.4. *Illegal Fishing, Fisheries Crime, and the Limits of Environmental Law*

Illegal, unreported and unregulated (IUU) fishing occupies a peculiar position in maritime law. It is regulated primarily through fisheries law rather than criminal law, and its connections to organised crime, forced labour, corruption, and maritime insecurity are frequently overlooked in legal responses. Witbooi et al. (2020) argue compellingly that organised crime in the fisheries sector poses a fundamental threat to a sustainable ocean economy, involving document fraud, violence, bribery, tax evasion, and links to trafficking networks. Belhabib and Le Billon (2022) similarly demonstrate that fish crimes constitute a significant and underappreciated global problem. However, IUU fishing is rarely treated as a criminal justice issue; it is typically addressed through administrative sanctions, licence revocations, and port and state control measures that are inadequate to deter organised criminal operators.

The legal gap here is as much one of characterisation as of enforcement. IUU fishing conducted through shadow fleets, using fraudulent documentation, exploiting forced labour, and linked to broader criminal networks, is functionally indistinguishable from organised crime, yet it is rarely prosecuted as such. The legal significance of this distinction is that conduct exhibiting many of the characteristics commonly associated with organised criminality continues to attract predominantly administrative sanctions, limiting the availability of investigative powers, international cooperation mechanisms and criminal penalties that would ordinarily accompany comparable transnational offences.

This is not to suggest that all instances of IUU fishing should be criminalised, but rather that the most serious forms, linked to organised criminal networks, require legal responses that extend beyond administrative fisheries enforcement. The Cape Town Agreement on fishing vessel safety, which has not yet entered into force due to insufficient ratifications, illustrates the broader problem of treaty ratification gaps in maritime law: international instruments addressing maritime problems exist but lack the universal participation necessary for effectiveness (Phayal et al. 2022). The result is that the most harmful forms of maritime environmental crime fall into enforcement voids that neither fisheries law nor criminal law adequately fills (Okafor-Yarwood et al. 2024; Phayal et al. 2024).

The connection between IUU fishing and piracy further underscores the problem of legal fragmentation. Desai and Shambaugh (2021) and Phayal et al. (2024) show that depletion of local fish stocks through illegal fishing correlates with increases in maritime piracy, suggesting that fisheries crime creates the conditions for maritime violence. This interaction between legally regulated environmental harm and a legally categorised criminal offence is precisely the kind of cross-domain relationship that current law is poorly equipped to

address. Addressing these interconnected harms requires a legal framework that integrates fisheries governance with criminal justice and maritime security rather than treating each as an isolated regulatory domain. This would require closer cooperation between fisheries regulators, criminal justice agencies, customs authorities and naval forces. Although existing international instruments encourage such cooperation, they do not establish the integrated legal mechanisms necessary to respond effectively to IUU fishing as part of wider organised maritime criminality.

4.5. Hybrid Threats, Grey-Zone Activity, and the Gaps in International Law

The emergence of state-supported hybrid maritime threats represents perhaps the most challenging legal frontier in contemporary maritime law. Hybrid threats involve the blending of conventional and unconventional methods, state and non-state actors, criminal and political motives, and physical and digital operations (Sanz Caballero 2023). In maritime contexts, this may take the form of state-sponsored proxy groups disrupting shipping lanes, shadow fleets conducting sanctions evasion under de facto state protection, or state actors using cyber tools to interfere with port or navigation systems while maintaining plausible deniability. These activities are designed to operate in the legal grey zone between armed attack (which may trigger the application of the law of armed conflict) and ordinary crime (which would attract domestic criminal law)—a space in which international law currently provides no coherent framework.

The legal problem is that existing maritime law was designed for a world of clearer distinctions: between state and non-state actors, between war and peace, between public violence and private criminality. Hybrid maritime threats deliberately exploit these distinctions. When a state uses a private fishing fleet to contest territorial waters, a corporate-structured shadow fleet to evade sanctions, or proxy militias to harass commercial shipping, such conduct does not neatly fall within either the law of state responsibility or the piracy regime under UNCLOS. Under the law of state responsibility, however, responsibility only arises where the conduct of private actors can be attributed to a state. Hybrid maritime operations are often deliberately structured to avoid meeting that threshold, allowing states to influence events while maintaining plausible deniability. The resulting accountability gap is not accidental; rather, it is frequently exploited as a strategic feature of hybrid maritime operations (Kotman 2020; Fenton 2024; Bueger and Liebetrau 2023).

Although widespread or systematic attacks against civilians at sea may, in limited circumstances, engage the jurisdiction of the International Criminal Court (ICC) under the Rome Statute, the Court has only a limited role in addressing the broader spectrum of maritime criminality considered in this article.

Chokepoints are particularly vulnerable to hybrid exploitation for precisely this reason. The Straits of Malacca and Singapore, the Bab el-Mandeb, the Strait of Hormuz, and the Suez Canal are essential to global trade. As demonstrated by the current disruption around the Strait of Hormuz and the Houthis' attacks on Red Sea shipping since late 2023, these spaces can be subjected to sustained disruption by state-linked actors using a combination of physical attacks, drone strikes, and information warfare in ways that resist legal classification and therefore resist legal response. Hybrid actors do not need to control maritime chokepoints; they need only to create sufficient legal uncertainty, insurance risk, and operational disruption to achieve strategic effects. Although elements of international law, including the law of state responsibility, the law of the sea and, in some circumstances, the law of armed conflict, may apply to particular incidents, no single legal framework provides a coherent response to hybrid maritime activity operating below the threshold of armed conflict while extending beyond ordinary criminality (Fenton 2024; Sanz Caballero 2023).

5. Why Maritime Spaces Are Structurally Vulnerable to Legal Arbitrage

Maritime spaces are not merely physically difficult to police; they are legally structured in ways that create systematic enforcement gaps. The architecture of the law of the sea was built around flag, state jurisdiction, coastal state rights, and the freedom of the high seas and was designed to balance state sovereignty against freedom of navigation. In practice, this balance creates significant opportunities for legal arbitrage that criminal and hybrid actors exploit deliberately and systematically.

Jurisdictional fragmentation is the most fundamental structural problem. A vessel may be owned in one country, flagged in another, crewed by nationals of several others, insured in a different jurisdiction, and operated through a corporate structure registered in yet another. Each jurisdictional layer creates potential for accountability gaps. Taken individually, each jurisdictional rule serves a legitimate purpose within the law of the sea. Collectively, however, they create opportunities for legal arbitrage that increasingly exceed the assumptions underlying the existing framework.

Flag state jurisdiction over vessels on the high seas means that the state with primary enforcement authority may be a small island jurisdiction with no maritime enforcement capacity, selected precisely because of its regulatory minimalism. Port state control provides a secondary enforcement mechanism, but it is applied inconsistently and does not address crimes committed at sea (Papastavridis 2016).

The territorial waters and high seas distinction creates a further structural vulnerability. UNCLOS Article 101 piracy law applies only on the high seas, but much contemporary maritime crime occurs in territorial waters or exclusive economic zones. Armed robbery against ships in territorial waters is not piracy under international law; it is a domestic criminal matter. This means that the legal response depends entirely on the capacity and will of the coastal state, which may be precisely the state whose weakness or corruption enables crime in the first place. In the Gulf of Guinea, coastal state institutional capacity has been identified as a key determinant of maritime crime rates, with weaker states showing higher rates of maritime criminal activity (Denton and Harris 2019; Adesanya 2023). The law does not compensate for this governance deficit; it depends on its absence.

Criminological theory helps explain how legal vulnerability translates into criminal opportunity. Routine activity theory, which holds that crime occurs where motivated offenders, suitable targets, and absent guardianship converge, maps onto the maritime context with clarity (Alsawalqa and Venter 2021). Motivated offenders include pirates, traffickers, cyber actors, and state-linked proxies. Suitable targets include vessels, cargo, ports, offshore platforms, and digital systems. Moreover, guardianship is frequently absent or legally constrained: naval forces may lack jurisdiction, coast guards may lack capacity, and police may lack extraterritorial authority. The law, in other words, actively structures the guardianship gaps that criminal actors exploit.

The global economy's dependence on uninterrupted maritime trade intensifies these structural vulnerabilities. Because maritime systems are designed for efficiency, disruption can be costly and disproportionate to the legal resources deployed against it. Just-in-time logistics, port congestion, energy dependence, and global supply chains mean that even modest maritime disruption can cause significant economic harm. Criminal and hybrid actors understand that even legally ambiguous, below-threshold conduct can produce disproportionate strategic and economic effects. The inability of the existing legal framework to respond effectively to these dynamics is itself a structural vulnerability that contemporary maritime actors increasingly exploit.

6. The Legal Implications of Technological Transformation

Whereas the previous section examined cyber-enabled threats as a contemporary category of maritime offending, this section considers how wider technological developments are reshaping established legal concepts, including jurisdiction, criminal responsibility and evidential standards.

Technological transformation is reshaping maritime security in ways that existing legal frameworks are increasingly ill-equipped to address. These challenges are not unique to maritime law. Across international law, developments such as artificial intelligence, autonomous systems, cyber operations and hybrid conflict are exposing similar questions concerning jurisdiction, attribution, liability and criminal responsibility. The maritime domain nevertheless presents a particularly acute example because these technologies interact with an already fragmented jurisdictional framework. The legal status of autonomous vessels is illustrative. UNCLOS and related maritime conventions were drafted on the assumption that human crews operate vessels. Questions of flag, state jurisdiction, seafarer rights, collision liability, and criminal responsibility all depend, in different ways, on the presence of human actors making navigational decisions. An autonomous vessel hacked to cause a collision, or remotely commandeered to transport illicit cargo, does not fit neatly within these legal frameworks. The IMO's regulatory scoping exercise on Maritime Autonomous Surface Ships (MASS) has identified significant gaps in existing conventions. However, although the IMO has begun considering the regulatory implications of Maritime Autonomous Surface Ships (MASS), no binding international instrument has yet addressed the criminal law implications of autonomous vessel operation or clarified questions of criminal responsibility where autonomous systems are used to facilitate maritime offending (Ashraf et al. 2023).

Smart ports compound this legal uncertainty. A smart port is not only a physical logistics hub but also a digital ecosystem—a complex network of automated systems, sensors, data platforms, and communications infrastructure. Cybersecurity incidents at smart ports may involve actors across multiple jurisdictions, targeting systems operated by private companies under public concession arrangements, causing harm that spans criminal, commercial, and public law. The absence of mandatory cybersecurity standards for port infrastructure—and the absence of any international obligation to report or investigate cyber incidents at ports—means that vulnerabilities in smart ports are systematically underregulated. The result is a fragmented legal framework in which responsibility for preventing, reporting and responding to cyber incidents remains unevenly distributed between states, port authorities and private operators (Fenton 2024; Okafor-Yarwood et al. 2024).

AIS manipulation and GNSS interference raise specific legal questions about the rules of evidence and attribution in maritime criminal prosecutions. AIS data is routinely used in maritime investigations as evidence of vessel position, movement, and identity. If AIS data can be systematically falsified, its evidentiary value is undermined. Similarly, if GNSS interference can cause vessels to display false positions, investigations of maritime incidents may be unable to establish the basic jurisdictional facts, where the vessel was, in whose waters, and on which criminal prosecution depends (Premarathna 2021). These are not merely technical challenges; they are legal ones, requiring both evidentiary reform and the development of alternative means of establishing jurisdictional facts in maritime criminal proceedings.

Technology also affects criminal adaptability in ways that the law has not kept pace with. Criminal groups use encrypted communication, satellite imagery, AIS monitoring, drones, and digital payment systems to identify targets, coordinate attacks, and conceal proceeds. The same technologies that support legitimate maritime commerce are repurposed for illicit activity. Although anti-money laundering law, sanctions law, and the law

governing digital evidence can address aspects of these activities, they operate largely in parallel rather than as part of an integrated legal framework for combating technologically enabled maritime crime (Sosnowski et al. 2024; Tachie-Menson 2023). Beyond these existing technologies, emerging developments such as quantum computing are also likely to reshape the maritime security landscape. Quantum computing has the potential to challenge current approaches to encryption, cybersecurity, digital communications and evidential integrity, creating new legal and regulatory questions that extend beyond those considered by existing maritime conventions. Although these capabilities are still developing, they reinforce the need for legal frameworks that are sufficiently adaptable to respond to future technological change rather than only existing threats.

7. The Case for Legal Reform: Towards an Integrated and Adaptive Maritime Legal Framework

The analysis in this article supports a normative argument for significant legal reform. Current maritime legal frameworks are too reactive, too fragmented, and too anchored in the UNCLOS piracy paradigm to address the full spectrum of contemporary maritime threats. Reform is needed at multiple levels: doctrinal, institutional, and governance.

First, the definition of maritime crime in international law must be expanded. The UNCLOS definition of piracy is not wrong, but it is insufficient. The international community requires a supplementary legal instrument that builds upon as well as goes beyond the SUA Convention. One that creates binding obligations with respect to cyber-enabled maritime attacks; organised maritime crime involving two or more states; maritime hybrid threat activity by state-linked actors; and the criminal dimensions of IUU fishing and fisheries crime. Such an instrument should establish clearly defined jurisdictional bases for the most serious forms of transnational maritime crime. Depending upon the nature of the offence, this could include carefully circumscribed universal or quasi-universal jurisdiction, while preserving the primary jurisdiction of coastal and flag states where appropriate. Any extension of jurisdiction would require clear thresholds and safeguards to ensure consistency with state sovereignty and the existing law of the sea framework.

The model of the SUA Convention—an instrument that fills a specific gap left by UNCLOS—provides a useful template. However, any successor instrument would need to address the SUA Convention's own shortcomings regarding its enforcement mechanism and state participation (Psarros et al. 2011).

Second, the jurisdictional architecture of maritime law requires reform. The territorial waters/high seas divide was designed to protect coastal states' sovereignty, not to create enforcement gaps for maritime criminals. A reformed framework should strengthen obligations on coastal states to cooperate with flag-states, port states, and third-state naval forces in investigating and prosecuting maritime crimes occurring within their territorial seas, with provisions for international assistance where coastal-state capacity is limited. The existing framework of bilateral agreements and ad hoc arrangements, illustrated by the improvised prosecution mechanisms developed for Somali piracy, is insufficiently systematic and unsustainable as a model for global maritime criminal justice (Ghosh 2014; Alsawalqa and Venter 2021).

Third, maritime law must be brought into the digital era through binding international cybersecurity obligations. The IMO's non-binding guidance on maritime cyber risk management is inadequate. Whether developed through the IMO or a dedicated multilateral treaty process, a binding international framework for maritime cybersecurity should include: mandatory minimum cybersecurity standards for vessels of specified tonnage and for designated port infrastructure; mandatory reporting obligations for cyber incidents with maritime safety or security consequences; mutual legal assistance mechanisms for

the investigation of cyber-maritime crimes across jurisdictions; and provisions addressing the evidentiary challenges posed by AIS manipulation and GNSS interference. Such a framework should be developed under the auspices of the IMO or through a dedicated multilateral treaty process, with participation by states, representatives of the shipping industry, and cybersecurity authorities (Afenyo and Caesar 2023; Ashraf et al. 2023; Fenton 2024).

Fourth, the treatment of hybrid maritime threats requires the development of new legal concepts rather than simply applying existing ones. The grey zone between armed conflict and ordinary crime does not disappear because international law does not address it; it simply allows harmful conduct to proceed without legal consequence. Rather than creating an entirely new legal doctrine, further development of the existing law of state responsibility may provide a more realistic basis for addressing hybrid maritime threats. In particular, greater clarification of the principles governing attribution, proxy actors and state-supported maritime disruption would reduce the legal uncertainty currently exploited by hybrid threat actors. The development of such a doctrine would require engagement among international lawyers, maritime security practitioners, and state actors in multilateral forums and would likely need to be expressed through a combination of soft-law guidance and hard-law treaty commitments (Sanz Caballero 2023; Kotman 2020).

Fifth, legal reform must be accompanied by institutional reform. Effective maritime criminal law depends not only on adequate legal instruments but also on capable enforcement institutions (Sosnowski et al. 2024). Maritime governance suffers from the same fragmentation as maritime law: coast guards, navies, customs agencies, police, fisheries authorities, cyber agencies, and international organisations all hold partial information and partial authority. Legal reform should strengthen mechanisms for intelligence sharing, facilitate the establishment of joint investigation teams in multi-jurisdictional maritime cases, and establish clear lines of authority for maritime enforcement operations. Existing international initiatives, including INTERPOL's maritime crime programme and the United Nations Office on Drugs and Crime (UNODC) Global Maritime Crime Programme, demonstrate the value of coordinated international cooperation, capacity building and operational support. The UNODC's Maritime Crime: A Manual for Criminal Justice Practitioners (United Nations Office on Drugs and Crime 2017) further recognises the need for integrated investigative and prosecutorial approaches to maritime crime. However, these initiatives remain dependent upon existing legal frameworks and cannot, by themselves, resolve the structural legal deficiencies identified throughout this article.

Finally, legal reform must address the human and institutional capacity dimensions of maritime criminal justice. Surveillance systems, maritime domain awareness tools, and digital platforms are only effective when supported by trained personnel, legal authority, institutional trust, and maintenance capacity. Okafor-Yarwood et al. (2024) make this point clearly with respect to maritime security technology in Africa, and it applies equally to cyber forensics, evidential standards for maritime prosecutions, and the legal training of maritime enforcement officers (Tsailas 2025). Capacity building in maritime criminal justice—including legal reform at the domestic level, training of prosecutors and judges in maritime law, and development of regional prosecution frameworks—is as important as the development of new international instruments.

8. Conclusions

Maritime criminality has evolved significantly from traditional piracy into a complex spectrum of hybrid and transnational threats. The legal framework for addressing maritime crime, anchored in UNCLOS Article 101 and imperfectly supplemented by the SUA Convention and domestic criminal law, was designed for a narrower category of maritime violence than now exists. This article has argued that the definitional boundaries of piracy

law—the private ends requirement, the high seas limitation, and the focus on physical violence—produce systematic enforcement gaps that contemporary maritime criminals, terrorists, cyber actors, and hybrid threat operators deliberately exploit.

These legal gaps have real consequences. They allow organised maritime criminal networks to fragment their activities across legal categories and jurisdictions. They exclude politically motivated maritime violence from the machinery of universal jurisdiction under piracy law. They leave cyber-enabled maritime attacks without a binding international legal framework capable of providing consistent rules for prevention, investigation and enforcement. Moreover, they provide state-linked hybrid actors with significant accountability gaps for below-threshold maritime disruption.

The normative argument advanced in this article is therefore for an integrated programme of legal reform. This includes developing supplementary international instruments where existing frameworks are inadequate, strengthening jurisdictional cooperation between states, establishing binding obligations for maritime cybersecurity, clarifying the application of the law of state responsibility to hybrid maritime threats, and reinforcing the institutional capacity needed to investigate and prosecute increasingly complex forms of maritime crime.

Maritime criminality can no longer be adequately addressed through traditional piracy law. The law must therefore evolve alongside the changing character of maritime criminality. If international maritime law is to remain effective, it must provide legal frameworks capable of responding coherently to threats that increasingly transcend traditional distinctions among piracy, organised crime, terrorism, cyber operations, and hybrid activities.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The author would like to thank colleagues within the School of Criminology and Criminal Justice at the University of Portsmouth for their support and feedback during the development of this article.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
EEZ	Exclusive Economic Zone
GNSS	Global Navigation Satellite System
IMO	International Maritime Organisation
INTERPOL	International Criminal Police Organisation
IoT	Internet of Things
IUU	Illegal, Unreported and Unregulated (fishing)
MASS	Maritime Autonomous Surface Ships
SUA	Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation
UNCLOS	United Nations Convention on the Law of the Sea
UNODC	United Nations Office on Drugs and Crime

References

- Adesanya, Olusegun Paul. 2023. Maritime crimes and the Gulf of Guinea. *Cogent Social Sciences* 9: 2241263. [CrossRef]
- Afenyo, Mawuli, and Livingstone D. Caesar. 2023. Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management* 236: 106493. [CrossRef]
- Aishwarya, R. J. 2021. Maritime terrorism in the Indian Ocean Region. *Electronic Journal of Social and Strategic Studies* 2: 385–96. [CrossRef]
- Alsawalqa, Rulah Odeh, and Denis Venter. 2021. Piracy and maritime security in the North, Western Indian Ocean: From the Gulf of Oman to the waters off the Somali coast. *Insight on Africa* 14: 88–103. [CrossRef]
- Ashraf, Imran, Yongwan Park, Soojung Hur, Sung Won Kim, Roobaea Alroobaea, Yousaf Bin Zikria, and Summera Nosheen. 2023. A survey on cybersecurity threats in the IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems* 24: 2677–90. [CrossRef]
- Belhabib, Dyhia, and Philippe Le Billon. 2022. Fish crimes in the global oceans. *Science Advances* 8: eabj1927. [CrossRef] [PubMed]
- Bellamy, Chris. 2020. What are maritime crime and maritime security? *International Journal of Maritime Crime and Security* 1: 17–22. [CrossRef]
- Bueger, Christian, and Timothy Edmunds. 2020. Blue crime: Conceptualising transnational organised crime at sea. *Marine Policy* 119: 104067. [CrossRef]
- Bueger, Christian, and Tobias Liebetrau. 2023. Critical maritime infrastructure protection: What's the trouble? *Marine Policy* 155: 105772. [CrossRef]
- Chatterjee, Aditi. 2014. Non-traditional maritime security threats in the Indian Ocean Region. *Maritime Affairs: Journal of the National Maritime Foundation of India* 10: 77–95. [CrossRef]
- Denton, Ginger L., and Jonathan R. Harris. 2019. Maritime piracy, military capacity, and institutions in the Gulf of Guinea. *Terrorism and Political Violence* 34: 1–27. [CrossRef]
- Desai, Raj M., and George E. Shambaugh. 2021. Measuring the global impact of destructive and illegal fishing on maritime piracy: A spatial analysis. *PLoS ONE* 16: e0246835. [CrossRef] [PubMed]
- Fenton, Adam James. 2024. Preventing catastrophic cyber–physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the Straits of Malacca and Singapore. *Journal of Marine Science and Engineering* 12: 510. [CrossRef]
- Galgano, Francis A. 2023. Hostis humani generis: Pirates and global maritime commerce. *Research in Globalisation* 8: 100188. [CrossRef]
- Ghosh, Probal Kumar. 2014. Strategies for countering Somalian piracy: Responding to the evolving threat. *India Quarterly* 70: 15–31. [CrossRef]
- He, Zhaoyang, Chengjin Wang, Jianbo Gao, and Yongshun Xie. 2023. Assessment of global shipping risk caused by maritime piracy. *Heliyon* 9: e20988. [CrossRef] [PubMed]
- Kamga, Gerard Emmanuel Kamdem. 2024. Troubled sea off the coast of West and Central Africa: Insights into the Gulf of Guinea's upsurge in maritime (in)security and its impact on human rights and the rule of law. *South African Yearbook of International Law* 49: 20. [CrossRef] [PubMed]
- Khaerany, Radillah, and Maskun Maskun. 2016. Global cooperation in combating sea piracy: The factors behind global piracy trends. *Hasanuddin Law Review* 1: 213–24. [CrossRef]
- Khan, Khalil Ur Rahman. 2020. Piracy and maritime terrorism: Serious perils to sea security. *Global Strategic and Securities Studies Review* V: 34–42. [CrossRef]
- Kotman, Türkay. 2020. Maritime hybrid threat. Maritime security centre of excellence. Available online: <https://www.marseccoe.org/wp-content/uploads/2021/08/Maritime-Hybrid-Threat.pdf> (accessed on 12 June 2026).
- Lehr, Peter. 2006. *Violence at Sea: Piracy in the Age of Global Terrorism*. New York: Routledge. [CrossRef]
- Li, Huanhuan, and Zaili Yang. 2023. Towards a safe navigation environment: The imminent role of spatio-temporal pattern mining in maritime piracy incidents analysis. *Reliability Engineering & System Safety* 238: 109422. [CrossRef]
- Li, Lingqun. 2023. Building up a sustainable path to maritime security: An analytical framework and its policy applications. *Sustainability* 15: 6757. [CrossRef]
- Luft, Gal, and Anne Korin. 2004. Terrorism goes to sea. *Foreign Affairs* 83: 61–71. [CrossRef]
- Miloš, Frane, Jakša Mišković, and Ivica Pavić. 2023. Analysis of current threats to ships from 2019 to 2022 in selected regions. *Naše More* 70: 126–36. [CrossRef]
- Murphy, Martin N. 2009. *Small Boats, Weak States, Dirty Money: Piracy and Maritime Terrorism in the Modern World*. New York: Columbia University Press.
- Okafor-Yarwood, Ifesinachi, Oliver Eastwood, Noleen Chikowore, and Lucas de Oliveira Paes. 2024. Technology and maritime security in Africa: Opportunities and challenges in the Gulf of Guinea. *Marine Policy* 160: 105976. [CrossRef]
- Osadtsa, Roman. 2025. Maritime Piracy and Terrorism Emerged as Legal Categories. *New Ukrainian Law*. [CrossRef]
- Otto, Lisa, and Leaza Jernberg. 2020. Maritime piracy and armed robbery at sea. In *Global Challenges in Maritime Security*. Cham: Springer, pp. 95–110. [CrossRef]

- Pandey, Shivam Kumar. 2023. A comprehensive classification system of non-traditional maritime security threats: A step towards enhancing maritime security. *International Journal of Scientific and Research Publications* 13: 227–34. [CrossRef]
- Papastavridis, Efthymios D. 2016. Crimes at sea: A law of the sea perspective. In *The Centre for Studies and Research in International Law and International Relations Online*. Buckinghamshire: Brill, pp. 3–52.
- Phayal, Anup, Aaron Gold, and Brandon Prins. 2022. Interstate hostility and maritime crime: Evidence from South East Asia. *Marine Policy* 143: 105134. [CrossRef]
- Phayal, Anup, Aaron Gold, Curie Maharani, Maria Lourdes D. Palomares, Daniel Pauly, Brandon Prins, and Sayed Riyadi. 2024. All maritime crimes are local: Understanding the causal link between illegal fishing and maritime piracy. *Political Geography* 109: 103069. [CrossRef]
- Premarathna, P. K. B. Isuru. 2021. Maritime security challenges in the Indian Ocean: Special reference to Sri Lanka. *International Journal of Research and Innovation in Social Science* 5: 158–73. [CrossRef]
- Psarros, George Ad., Alexander F. Christiansen, Rolf Skjong, and Gjermund Gravir. 2011. On the success rates of maritime piracy attacks. *Journal of Transportation Security* 4: 309–35. [CrossRef]
- Sanz Caballero, Susan. 2023. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications* 10: 1–8. [CrossRef]
- Sosnowski, Monique, Gohar Petrossian, Thanaphon Nunphong, and Eric Piza. 2024. Crimes at sea: Exploring the nexus of maritime crimes across global EEZs. *Marine Policy* 166: 106161. [CrossRef]
- Tachie-Menson, Elsie Amelia. 2023. Investigating the intersection of maritime and cybercrime in the Gulf of Guinea. *Scientia Militaria* 51: 89–112. [CrossRef]
- Tsailas, Demetrios N. 2025. Risks and threats in 21st-century maritime security. *Security Science Journal* 6: 106–44. [CrossRef]
- United Nations Office on Drugs and Crime. 2017. Maritime Crime: A manual for Criminal Justice Practitioners. United Nations. Available online: https://www.unodc.org/documents/Maritime_crime/19-02087_Maritime_Crime_Manual_Second_Edition_ebook.pdf (accessed on 12 June 2026).
- Weldemichael, Awet T. 2012. Maritime corporate terrorism and its consequences in the western Indian Ocean: Illegal fishing, waste dumping and piracy in twenty-first-century Somalia. *Journal of the Indian Ocean Region* 8: 110–26. [CrossRef]
- Witbooi, Emma, Kamal-Deen Ali, Mas Achmad Santosa, Gail Hurley, Yunus Husein, Sarika Maharaj, Ifesinachi Okafor-Yarwood, Inés Arroyo Quiroz, and Omar Salas. 2020. Organised crime in the fisheries sector threatens a sustainable ocean economy. *Nature* 588: 48–56. [CrossRef] [PubMed]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.