MARITIME SECURITY CENTRE OF EXCELLENCE

Working Together for Maritime Security

5th MARITIME SECURITY CONFERENCE PROCEEDINGS

THE IMPACT OF TECHNOLOGY ON MARITIME SECURITY

(24-25 JUNE 2025)

5th Maritime Security Conference Proceedings:

The Impact of Technology on Maritime Security

Maritime Security Centre of Excellence Publication

ISBN: 978-625-93502-0-2

Editor in Chief

Assoc. Prof. Dr. Mürsel DOĞRUL / National Defence University

Editor

LCDR. (TUR-N) Ata Aziz YILMAZ / MARSEC COE

Office of Primary Responsibility and Co-OPR

CAPT. (TUR-N) Dr. Levent BAHADIR / Turkish Navy Forces

CDR. (TUR-N) Selim BAHÇEKAPILI / Turkish Navy Forces

Published By

Maritime Security Centre of Excellence (MARSEC COE)

Academic Advisor

Prof. Raul A. PEDROZO / U.S. Naval War College

Cover and Graphic Designer

ENS. (TUR-N) Furkan ŞİŞMAN / MARSEC COE

Text Designer

ENS. (TUR-N) Fatih ÖZÇELİK / MARSEC COE

MARITIME SECURITY CENTRE OF EXCELLENCE

"Working Together for Maritime Security"

Adress: Deniz Güvenliği Mükemmeliyet Merkezi Komutanlığı, Milli Savunma Üniversitesi Yerleşkesi, 34330, Yenilevent – İstanbul / Türkiye

Phone: +90 212 398 01 00 (5885)

E-Mail: info@marseccoe.org

Publication Date: December 2025

Printed by
Çözüm Baskı Merkezi Ticaret Limited Şirketi
Emniyetevleri Mahallesi Güvercin Sokak No: 7/1 KAĞITHANE / İSTANBUL
Phone: (0212) 281 49 48 **/ Gsm**: +90 543 297 43 59

Director's Remarks

It is with great honour that I present the official proceedings of the 5th Maritime Security Conference, MARSEC COE's flagship "diamond" event, convened on 24–25 June 2025.

The 2025 conference was dedicated to the critical and timely theme "The Impact of Technology on Maritime Security." The event convened approximately 250 participants from 22 nations, supported by 19 distinguished panelists and four expert moderators, and conducted under the Academic Advisor Professor Dr. Raul Pedrozo. This diverse and high-level participation ensured a comprehensive and multidisciplinary examination of contemporary maritime security challenges.

The conference provided a rigorous forum for in-depth analysis and strategic dialogue on the evolving influence of technology across the maritime domain. Discussions addressed a wide spectrum of interrelated issues, including cyber threats, the rapid proliferation of unmanned and autonomous systems (UXS) and counter-UXS measures, as well as the corresponding legal and regulatory implications. The exchange of concepts, lessons identified, and operational experiences highlighted the increasingly complex, contested, and technologically driven nature of maritime security, underscoring the pressing need for innovative, coordinated, and interoperable approaches to counter multidimensional and hybrid threats.

I wish to express my sincere appreciation to all those who contributed to the successful planning and execution of this conference. In particular, I acknowledge the valuable contributions of the panelists, moderators, and participants, as well as the dedicated MARSEC COE staff, whose professionalism, discipline, and operational expertise were instrumental in achieving the conference objectives.

As readers engage with these proceedings, they are encouraged to critically reflect upon the analyses, perspectives, and proposed solutions presented herein. Through shared understanding, strengthened cooperation, and collective resolve, the maritime security community can enhance resilience and effectiveness in addressing the growing complexity of the global maritime environment.

Respectfully,

Mehmet Cengiz EKREN
Captain (TUR-N)
Director, MARSEC COE

5th MARITIME SECURITY CONFERENCE PROCEEDINGS:

THE IMPACT OF TECHNOLOGY ON MARITIME SECURITY

(24-25 JUNE 2025)

TABLE OF CONTENTS

Preface: The Impact of Technology on Maritime Security

The main theme of the 5th Maritime Security Conference, hosted by the NATO Maritime Security Center of Excellence, was The Impact of Technology on Maritime Security. Experts from around the world gathered in Istanbul, Türkiye, to discuss various topics on how new technologies can be used to improve maritime security, including unmanned maritime systems, artificial intelligence, maritime cybersecurity, and space-based and underwater technologies. Additionally, the conference addressed traditional maritime security threats.

Maritime Unmanned Systems (MUS) and Artificial Intelligence

The application of new and advanced technologies in the maritime industry has resulted in the rapid development (both commercially and militarily) of unmanned and autonomous maritime systems (MUS). The International Maritime Organization (IMO) is working to ensure that commercial MUS can operate safely at sea. In 2019, IMO promulgated Interim Guidelines for Maritime Autonomous Surface Ships (MASS) trials. IMO completed a regulatory scoping exercise on MASS in 2022 to assess the applicability of existing IMO instruments to ships utilizing four degrees of automation. Notably, IMO recognized that a MUS could qualify as a ship even though the master and crew are not physically onboard, provided the master can intervene when necessary and the MUS can be operated by qualified crew members from a remote operation center. The next step is to adopt a nonbinding code by 2026 and a mandatory code by 2032, regulating the safe and secure operation of MASS.

Militarily, for the first time in history, MUS have been used during an international armed conflict to conduct offensive strikes against the enemy. Both Russia and Ukraine have used MUS to attack ships at sea, as well as land-based targets (e.g., bridges, ports). MUS are ideally suited to perform dull (e.g., intelligence, surveillance, and reconnaissance), dirty (e.g., detect chemical, biological, nuclear material), and inherently dangerous (e.g., mine clearing) military missions. The use of MUS in wartime raises important domestic and international legal issues, such as their status as warships, naval auxiliaries, weapons systems, or devices.

Advancements in artificial intelligence (AI) have transformed every sector of modern society, including the defense sector. The military application of AI can include autonomous target recognition and engagement, autonomous navigation, and accelerating the decision-making cycle (e.g., out-sense, out-decide, and out-fight the enemy) to complete targeting solutions and close the kill chain. AI enables the handling of massive amounts of multi-source data in near real-time, which can be utilized during the planning process to support the development of courses of action and enhance the ability of naval forces to conduct distributed maritime operations in a high-end, contested environment. These new technologies, however, are susceptible to cyberattacks. Operators must be able to identify, protect, detect, respond to, and recover from these attacks to minimize operational disruptions.

Combating Traditional Maritime Security Threats

Despite the impact of new technologies on maritime security, the international community must remain vigilant and committed to combating traditional maritime security threats, such as drug trafficking, maritime piracy and terrorism, and interference with freedom of navigation. The Single Convention on Narcotic Drugs of 1961 (as amended by the 1972 Protocol), the Convention on Psychotropic Substances of 1971, and the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Convention) provide the legal architecture to combat illicit drug trafficking. The 1988 Convention also provides a legal framework for international cooperation to prevent precursor chemical diversion. Yet these instruments have not designated drug trafficking as a crime of universal jurisdiction, so coordination among flag states is essential to effective interdiction.

The Indian Ocean Region has emerged as an active corridor for the movement of drugs, particularly hashish and heroin. The Makaran coast is used as a primary route by criminal organizations to smuggle drugs through boats, dhows, and fishing vessels. Use of these commercial vessels poses a significant challenge for local law enforcement, many of which lack capacity and capabilities and sometimes legal authority, to interdict illicit drugs on the high seas. The increasing use of sea routes in the Indian Ocean by drug traffickers presents a growing challenge for regional security, maritime governance, and regional cooperation. Long-term progress in combating these threats requires closer regional partnerships, enhanced maritime domain awareness, and the strategic application of new technologies, such as satellite tracking.

Piracy and armed robbery at sea continue to threaten commercial shipping and regional security. Although there has been a decline in piracy attacks along the Gulf of Guinea in West Africa and in the South China Sea, the number of incidents in the Malacca Strait is rising. Additionally, as attacks on tankers have declined, the number of incidents involving bulk carriers is increasing.

Since 2023, there has been a resurgence in acts of piracy off the Horn of Africa, in part, because of the Houthi attacks on commercial shipping in the Red Sea. Tactics employed by the Houthis range from the use of small boats and helicopters used to board merchant vessels, as well as attacks using heavy suicide drones and anti-ship cruise missiles and even anti-ship ballistic missiles, weapons traditionally held only by states. These attacks have significantly disrupted maritime trade, forcing commercial vessels to reroute via the Cape of Good Hope, a longer and more costly alternative than the Suez Canal. These assaults also pose a significant threat to the safety and security of seafarers. Some of the relevant international legal instruments used to address Houthi interference with international maritime trade include the United Nations Convention on the Law of the Sea (UNCLOS) and the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA Convention). These peacetime law enforcement authorities have proved effective to counter Somali piracy, but not Houthi drone and missile attacks on international shipping.

Maritime Cybersecurity

The shipping industry is increasingly reliant on digitized and interconnected systems. Ships have complex networks of Information Technology (IT) and Operational Technology (OT). OT networks on vessels control critical functions such as navigation, propulsion, and cargo operations, which can be prime targets for cyber-attacks. Disruption of these systems can result in loss of life and property, environmental damage, and significant financial loss.

The emergence of "shadown fleets" poses additional risk to maritime order. Russia (and other States) operate formidable "shadow fleets" that engage in illicit operations, such as circumventing sanctions; intentionally avoiding flag and port State control inspections; evading compliance with international safety or environmental regulations, as well as industry standards and best practices; failing to maintain adequate liability insurance; intentionally taking measures to avoid ship detection (e.g., switching off automatic identification systems (AIS) or long-range identification and tracking (LRIT) system transmissions); concealing the ship's actual identity (e.g. changing flag or name); or engaging in other illegal activities. Most recently, Russian and Chinese "shadow fleet" vessels have engaged in intentional damage and suspected sabotage of critical undersea infrastructure (CUI), jamming and spoofing of the Global Navigation Satellite Systems (GNSS), and electronic warfare (EW). Existing international law, including UNCLOS, does not provide an effective legal basis to combat these illicit activities beyond the territorial sea.

E-navigation harmonizes marine navigation systems and supports shore services by providing digital information and infrastructure that benefits maritime safety, security, and the protection of the marine environment, thereby reducing administrative burdens and increasing the efficiency of maritime trade and transport.

The IMO defines e-navigation as “the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment.” The member States of the International Hydrographic Organization (IHO) developed the S-100 Universal Hydrographic Data Model, a hydrographic geospatial data standard that supports a wide variety of hydrographic-related digital data sources and aligns with mainstream international geospatial standards. This alignment enables easier integration of hydrographic data and applications into geospatial solutions.

The maritime industry is increasingly vulnerable to cybersecurity threats due to the widespread integration of advanced IT and OT systems. Ships, ports, and offshore installations are becoming vulnerable to cyberattacks that can pose significant risks to national security, the marine environment, and supply chain resilience. Cybersecurity challenges are expected to intensify as the maritime industry progresses toward commercial use of MASS. The regulatory landscape is fragmented, not mandatory, and maritime authorities lack enforceability. The International Association of Classification Societies Unified Requirements for Cyber Resilience apply only to new ships, leaving older ships vulnerable to cyber-attacks. The absence of a harmonized international regulatory regime, coupled with varying levels of infrastructure and technical capacities among nations hinders effective implementation of an existing regulatory framework. Unclear mandates among national maritime agencies and port authorities, and lack of a single point on contact further complicate coordinated responses to cyber threats. The existing regulatory framework, as well as multi-layered cooperation, must be strengthened to address emerging cyber threats in the maritime industry.

GNSS jamming and spoofing affect navigation performance on manned and unmanned ships. Launch and recovery operations of manned and unmanned systems are dependent on GNSS availability. There are pros and cons of operating in a GNSS-denied environment, which may require mitigation or augmentation alternatives. Examples include Controlled Reception Pattern Antennas, alternative terrestrial navigation candidates, stellar navigation, terrain aided navigation, and vision aided navigation methods and systems.

GNSS/GPS is central to maritime navigation, providing precise positioning, route planning, and collision avoidance. The growing number of GPS spoofing and jamming attacks, however, represents a considerable threat to ships’ operational safety and cybersecurity. A system thinking approach can be used to create and analyze the interconnection between technical vulnerabilities, human factors, organizational responses, and external threat vectors relation to GNSS disruptions in the maritime sector. Systems thinking focuses on comprehending entire systems and their interactions, rather than examining separate components in isolation. Principal leveraged points, including crew training, hybrid navigation, and incident reporting processes, can be used to mitigate risks and enhance system resilience. There is a pressing requirement for coordinated cyber-physical risk management strategies with maritime security operation center analysts for responding to GPS-dependent dangers in maritime operation, in congested or geopolitically restricted waters.

The Maritime Cyber Attack Database (MCAD), developed by the Maritime IT Security Research Group, catalogues cyber incidents in the maritime domain dating back to 2001. The database provides valuable insight into threats targeting the Global Maritime Transportation System. MCAD has identified over 380 incidents from public sources that directly threaten vessels and offshore platforms.

Leveraging Space-based and Underwater Technologies

To prevent unintended damage by ships, the location of submarine cables and pipelines is publicly available. This transparency makes it more difficult and expensive for States and private companies to protect critical undersea infrastructure (CUI) from rogue States and non-State actors that seek to disrupt the system. Intentionally dragging a ship's anchor can easily sever a cable or pipeline at minimal cost. The existing international legal framework (including UNCLOS) governing the protection of CUI is adequate to prevent foreign-flagged vessels from negligently or intentionally damaging CUI beyond the territorial sea.

The protection of critical energy infrastructure has attracted increased attention following the sabotage of the Nord Stream pipelines in 2022 in the Baltic Sea, Russia's attacks on Ukraine's energy infrastructure, and the cooperation between the European Union and NATO to safeguard Allied energy infrastructure. The targeting of the Nord Stream pipeline highlights the importance and difficulty of protecting energy infrastructure on land, underground, and at sea. Close monitoring, surveillance, and collective efforts are key to deterring attacks against critical energy infrastructure. Attacks on energy infrastructure allow for plausible deniability for rogue actors and can cause significant economic and logistical damage at low costs. Threats to energy infrastructure range from cyber and hybrid attacks to climate change to kinetic attacks. As Europe phases out its reliance on Russian oil and gas imports, it will need to develop new infrastructure for alternative supplies.

China has elevated maritime critical infrastructure protection (MCIP) to a matter of national strategy. China has fused military capabilities with civilian assets to build an expansive, layered approach to MCIP. This fusion—coordinated activities of the People's Liberation Army-Navy (PLAN), China Coast Guard (CCG), and state-aligned commercial entities (COSCO Shipping Corporation, Huawei Marine)—reflects China's broader ambition to project power, secure strategic dependencies, and shape international maritime norms. China's protection of undersea communications cables, energy corridors, and distant-water fishery zones using submarines, high-end surveillance platforms, and large-displacement patrol vessels supports both defensive objectives and geopolitical signaling. China's overseas deployments in the Indian Ocean reveal a proactive MCIP posture extending well beyond its immediate periphery. China's approach to MCIP is altering the balance of influence in key maritime regions and introducing new dynamics into the global security architecture.

The rise of hybrid threats to CUI has led to new efforts to protect underwater installations such as pipelines and electricity and data cables. Examples of such threats include the intentional damage to the Eastlink 2 undersea cable between Finland and Estonia, the attack on the Nord Stream pipelines in the Baltic Sea, and the drone attack on the MT Mercer Street off the coast of Iran. Deployment of varying degrees of sensor technologies can be used to detect subsea threats to CUI.

Emerging technologies can be used to conduct offensive seabed warfare operations. For example, in 1971, the USS Halibut (SSGN-587) was deployed to the Sea of Okhotsk. Its mission—Operation Ivy Bells—was to tap the submarine cable that connected the Soviet Union's Pacific Fleet headquarters at Vladivostok with the ballistic missile submarine base at Petropavlovsk on the Kamchatka Peninsula. Similarly, Deep Submergence Vessel NR-1 (Nerwin) was used by the United States to (inter alia) recover Soviet military hardware from the deep seabed and gather intelligence. The Russian Navy deploys the ARS-600, a deep diving manned submersible that is designed for searching, examining, and lifting various underwater objects from the seabed; sustaining life activity of crews in distressed submarines; and docking other rescue facilities with distressed submarines. China recently developed a device for cutting deep-sea cables at depths of up to 4,000 meters. The cable-cutting device is designed for use with China's sophisticated submersibles (e.g., Fendouzhe and Haidou series). Italy's naval special forces (COMSUBIN) also operate a swimmer delivery vehicle (AE-90). These undersea and seabed activities presage the future of warfare. The surface has become so vulnerable to long range missile attack that assets are being driven underwater. Technology is enabling distributed fleets of unmanned systems, complicating naval decision-making.

Conclusion

The 5th Maritime Security Conference, hosted by the NATO Maritime Security Center of Excellence in Istanbul, Türkiye, underscored the transformative role of technology in shaping the future of maritime security while emphasizing the persistent need to address traditional threats. MARSEC COE is at the forefront of thinking about the changes brought about by new technologies at sea and considering programmatic, operational, and legal responses to protect the interests of the NATO alliance.

The discussions highlighted the dual-use potential of emerging technologies, such as MUS, AI, space-based and underwater capabilities, and e-navigation, in enhancing maritime safety, operational efficiency, and military effectiveness. These advancements enable real-time data processing, autonomous operations, and enhanced situational awareness, fundamentally reshaping naval strategies and distributed maritime operations. However, they also introduce new vulnerabilities, particularly in maritime cybersecurity, as digitized systems and CUI become prime targets for cyberattacks, jamming, and hybrid threats.

The conference also reaffirmed the importance of combating enduring challenges like drug trafficking, piracy, terrorism, and interference with freedom of navigation, which continue to threaten global maritime trade and regional stability. The resurgence of piracy off the Horn of Africa, illicit drug trafficking in the Indian Ocean, and Houthi attacks in the Red Sea highlight the need for robust international cooperation and legal frameworks, such as UNCLOS and the SUA Convention, though gaps in enforceability and universal jurisdiction persist.

To navigate this complex landscape, the maritime community must prioritize regional partnerships, enhance maritime domain awareness, and strategically integrate new technologies, such as satellite tracking and sensor systems, to deter and respond to both conventional and hybrid threats. Strengthening cybersecurity frameworks, harmonizing international regulations for autonomous systems, and protecting critical infrastructure are imperative to ensure resilience against evolving risks. The conference illuminated a path forward: leveraging technological innovation while fostering collaborative, adaptive strategies to safeguard the global maritime commons for the future.

As NATO's Center of Excellence for Maritime Security, the 5th Annual Conference demonstrated that military officers and leading experts can collaborate to produce meaningful and tangible progress in safety, security, and stability at sea. From the Baltic Sea to the Black Sea and the South China Sea, MARSEC COE is a thought leader in advancing ideas and solutions for NATO commanders and their forces.

Prof. Raul A. Pedrozo
U.S. Naval War College

Part I

Maritime Unmanned Systems (MUS) and Artificial Intelligence

Prof. (em.) Dr. Wolff Heintschel von Heinegg
Europa-Universität Viadrina, Germany

Abstract

As expected, the first panel proved to be an appropriate basis for the ensuing discussion and the panels to follow. The distinguished panelists addressed various, though interrelated, topics by providing an in-depth insight into the activities within the International Maritime Organization (IMO) aimed at the adoption of a Code on maritime autonomous surface ships (MASS), the legal status of unmanned maritime vehicles as warships under the law of naval warfare, the military application of artificial intelligence (AI) for a variety of purposes, including autonomous unmanned maritime vehicles, and, last but not least, on the various aspects necessary for an improvement of cyber security in the maritime domain.

Keywords

Unmanned Maritime Vehicles, Warships, Autonomous Ships, Military Applications of Artificial Intelligence, Maritime Cyber Security

Introduction

The four topics, although dealt with separately by the distinguished panelists, are quite interrelated. Autonomous systems/vessels, whether employed for commercial or military purposes, not only give rise to questions as to their legal status and their compatibility with the existing international legal framework of maritime law, the law of the sea, and the law of naval warfare. Their operation also highly depends on advanced cyber technology, including Artificial Intelligence (AI), which begs the question whether the respective technology is sufficiently reliable, in particular in light of the various vulnerabilities that are known or that still must be identified. If AI systems, whether decision-support or fully autonomous systems, are developed and employed for naval engagements, i.e., attack purposes, the legality of their use under the law of naval warfare is a highly contested issue that is not yet fully resolved. Finally, the same holds for the continuing debate on whether and to what extent there must be a human in or at least on the loop.

Presentations

Mrs. Maria Pia V. Benosa from the Legal Affairs Office of the International Maritime Organization (IMO) opened the panel by providing a comprehensive overview of the IMO's activities and discussions on maritime autonomous surface ships (MASS) that were initiated by the United Kingdom's information on its national approach to marine autonomous systems in 2015. After the adoption of a Regulatory Scoping Exercise (RSE) aimed at identifying the implications of MASS for IMO convention and regulations in 2017, the IMO issued interim guidelines for Mass trials, followed by discussions in the Maritime Safety Committee on the development of a MASS Code expected to be adopted in 2030. Within the IMO there was agreement on the necessity of compliance of MASS with the United Convention on the Law of the Sea (UNCLOS) and on the principal applicability of IMO conventions and regulations, subject to necessary amendments. The work on the prospective MASS Code covers a variety of issues related to the IMO Conventions and regulations, including special measures to enhance maritime security. Accordingly, MASS are expected to also comply with SOLAS and the ISPS Code. The legal issues at stake relate to the requirement of effective exercise of flag State jurisdiction, as required by Article 94 UNCLOS; the application of equivalences for current and new roles in MASS operation; the reconciliation of divergent interests and challenges for coastal States, port States, and flag States; and the implications for the liability and compensation conventions of MASS operation. However, the discussions and the work of the IMO focus on cargo ships that are subject to SOLAS chapter I. Accordingly, the expected MASS Code will not apply to high-speed craft, passenger ships, and warships. Nevertheless, the IMO's work will have an indirect impact on the ongoing discussion on the legal status of unmanned maritime systems/vehicles (UMS/UMV) operated by the armed forces.

That topic was dealt with in depth by Captain (TUR Navy) Levent Bahadir, PhD, currently assigned to the MARSEC COE. After an overview of the development of UMVs in military operations from World War II, the Cold War and the post-Cold War, until the present, Capt. Bahadir provided a summary of the various current uses of UMVs – defense operations (coastal defense, harbor protection, and mine countermeasures), intelligence and surveillance (reconnaissance in critical maritime areas and oceanographic data collection), combat operations (anti-submarine, anti-surface, and anti-air warfare), and support functions (communication nodes, electronic warfare, and SOF support –, thus showing that UMVs have become an integral component of contemporary naval operations. According to the law of naval warfare, only warships as defined by international law are entitled to exercise belligerent rights (i.e., attacks against lawful targets at sea, in the air, and on land, and visit, search, diversion and capture of enemy or neutral merchant vessels under prize law). There is, however, no consensus on whether UMVs can be classified as warships, as defined in Article 29 UNCLOS.

This begs the question on how to synchronize the slow-moving law and the rapidly advancing technology, because the definition of Article 29 UNCLOS inter alia requires the ships to be under the command of a commissioned officer and manned by a crew under regular armed forces discipline. Capt. Bahadir discussed potential approaches to the clarification of the legal status of UMVs by the adoption of a specific legal instrument, the application and evolutionary interpretation of the existing legal framework, or the development of customary international law by State practice. As to the second approach, Capt. Bahadir rejected the assimilation of UMVs to auxiliary vessels/ships because, as such, they would not be entitled to exercise belligerent rights. Considering UMVs as "organic components" of the launching warship would not apply to UMVs operating independently from a surface platform or submarine. Their classification as either "devices/equipment" or "craft" would be either too ambiguous or counter-productive because then UMVs would not enjoy navigational rights, and they would not be entitled to exercise belligerent rights. Another possible solution was discussed by Capt. Bahadir could be leveraging upon the recognized classification of unmanned aerial vehicles (UAVs) as military aircraft, if they are operated by the regular armed forces of a State, marked as such, and operated under military command and control. Capt. Bahadir concluded by proposing to assess UMVs as equivalent to manned platforms in size, tonnage, and functionality, maintaining, however, that human oversight remains crucial.

Autonomous Surface and Underwater Vehicles depend upon artificial intelligence (AI). Prof. Bleda Riza Kurtdarcan from the Galatasaray University did not limit his presentation to that aspect but discussed the military application of AI from a broader perspective. Starting from the OODA loop (Observe, Orient, Decide, Act), he explained that the various decision cycles in military operations can be considerably accelerated by the use of AI systems with a view of out-sensing, out-deciding, and out-fighting an adversary. The data provided by various sources (satellites, drones, intercepted communications) enable naval forces to create a "transparent battlefield", but the sheer quantity and complexity of such data can no longer be processed by human beings.

The resulting delays in data processing and, thus, of operational decisions can only be avoided and overcome by the introduction of AI-enabled ISR systems. In the same vein, the use of AI systems enables commanders to compromise the adversary's OODA loop and to act faster and in a distributed manner, thus gaining decisional superiority. As regards the out-fighting of the enemy, Prof. Kurtdarcan recognized the positive impact of AI systems resulting in the improvement of Automatic Target Recognition (ATR), autonomous navigation, and a recognized maritime picture. Because AI systems have already become a reality in military naval operations, he took the view that the use of AI systems is an unavoidable military necessity. AI and AI enabled systems enhance data analysis, reduce human error, provide situational awareness, and support optimal decision-making. Nevertheless, the delegation of operational decisions to machines and AI systems is, according to Prof. Kurtdarcan, limited by the law of armed conflict/international humanitarian law, which obliges the parties to an armed conflict to take precautions in attack, including constant care to spare the civilian population, civilians and civilian objects. He, therefore, advocated for an inclusion of human operators into all stages of military decision-making process.

The panel's last topic on the application of the National Institute of Standards and Technology (NIST) framework to maritime security, was prepared by Prof. Haydar Yalçın from Ege University and Prof. Mursel Doğrul from the Turkish National Defense University and presented by Prof. Doğrul. It provided an in-depth report about the methodology and results of an impressive research project and recommendations for the improvement of maritime cybersecurity.

The research project, after having identified the various cyber threats in the maritime domain (navigational safety threats, cargo logistics vulnerabilities, and port infrastructure), applied the NIST Cybersecurity Framework, which aims at identifying cybersecurity threats, protecting critical infrastructure and services, detecting potential cybersecurity events, responding to such events, and recovering affected systems and capabilities.

By employing large language models (LLMs) to classify maritime cybersecurity concepts, the researchers analyzed data from 30,279 publications. The research revealed that the functions of the NIST framework have been dealt with maturely and sufficiently.

This, however, did not hold for the recovery function. Accordingly, the stagnation of research with regard to that important aspect of maritime cybersecurity indicated a lack of academic and industrial interest that could result in considerable vulnerabilities. Accordingly, Professors Yalçın and Doğrul advocated for the development of AI-enabled response doctrines, the implementation of scenario-based recovery drills, the allocation of targeted research funding, and the improvement of real-time information sharing. They took the view that, by addressing the said gaps, "the maritime sector could develop more balanced cybersecurity strategies that not only prevent and detect threats but also ensure rapid recovery when incidents occur".

Comments By The Moderator

The work within the IMO on MASS cannot be underestimated. It has shown a remarkably flexible, realistic, and efficient approach to a new technology that is about to become a reality and that is crucial for the global maritime supply chains. The MASS Code, expected to be adopted in 2030 will most likely reflect that approach. Although it will only apply to cargo ships to which SOLAS chapter I applies, it has already had an impact on national approaches to the classification of unmanned maritime vehicles as warships.

Since many navies already rely on UMVs for a variety of military purposes they cannot but clarify their legal status. Of course, every sovereign decision to include UMVs into the national registries of warships and to use them for the exercise of belligerent rights is limited by international law, in particular by the definition of the term 'warship' in Article 29 UNLOS, which arguably is reflective of customary international law. However, the requirement of being manned by a crew subject to regular armed forces discipline does not mean that a ship to qualify as a warship needs to be manned. This follows from the historic background of that definition, i.e., the 1856 Paris Declaration prohibiting privateering.

That prohibition aims at outlawing the exercise of belligerent rights, in particular capture under prize law, by crews composed of civilians, some of whom had a criminal background. Accordingly, the definition of 'warship' must be interpreted as emphasizing the element of the crew being subjected to military discipline and not as requiring the ships to be manned by a crew.

Accordingly, States are free to designate UMVs as warships and to make use of them for the exercise of belligerent rights. Nevertheless, States should as soon as possible clarify their positions on such classification, because it is still unsettled whether certain coastal States are willing to recognize that UMVs qualify as warships and whether they enjoy the freedom of navigation to the same extent as manned naval platforms.

The use of AI systems in naval operations is a reality. Such AI systems are as vulnerable as other cyber technology vis-à-vis a variety of cyber threats. It is, therefore, crucial to enhance their resilience and to ensure that they can recover as quickly as possible, as rightly emphasized by Professors Yalçın and Doğrul. If AI or AI-enabled systems are employed in naval operations, including targeting of enemy military objectives, they must be sufficiently reliable. Otherwise, the delegation of operational decisions to such systems may prove to be highly problematic. While it continues to be a contentious issue whether targeting decisions must by necessity be ultimately taken by a human operator, it must be emphasized that the law of naval warfare distinguishes between attacks against objects at sea and in the air on the one hand, and attacks against targets on land on the other hand. AI and AI-enabled systems are expected to have the capacity of a sufficiently reliable identification of platforms qualifying as lawful targets. Whether they have such capacity when it comes to attacks against targets on land, i.e., in a far more complex environment, will have to be seen. It is, however, to be expected that at least AI-enabled decision-support systems will result in improved targeting decisions by the responsible commander.

Concluding Remarks

Technological developments cannot be prevented. However, every technological innovation must not only comply with applicable rules and principles of international law it must also be reliable. Reliability presupposes that those expected to employ such new technology have sufficient trust and confidence. It is not enough to merely equip the armed forces with new technologies developed by industry and to have them apply it in military operations. Rather, operators must be integrated into every stage of their development and testing with a view to ensuring that they have at least a basic understanding and that the respective technology meets their needs.

About the Author

Prof. (em.) Dr. Wolff Heintschel von Heinegg / Europa-Universität Viadrina, Germany / heinegg[at]outlook.de

Until April 1, 2025, Professor Dr. Wolff Heintschel von Heinegg was the Chair of Public Law, in particular Public International law, European Law and Foreign Constitutional Law at the Europa-Universität Viadrina in Frankfurt (Oder), Germany. Since May 2018 he has been the President of the International Society for Military Law and the Law of War. He was a member of the groups of experts who produced the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, Manual on Air and Missile Warfare (2010) and the Tallinn Manuals on the International Law Applicable to Cyber Warfare (2013) and to Cyber Operations (2016), the Oslo Manual on Select Topics of the Law of Armed Conflict (2020) and the Newport Manual on the Law of Naval Warfare (2nd ed. 2025).

Preliminary steps toward MASS Regulation at the International Maritime Organization

Maria Pia Benosa
International Maritime Organization

Abstract

At IMO, the UN specialized agency for the safety, security and environmental performance of international shipping, member States and observer organizations have been identifying solutions for adapting its regulatory framework to the increasing use of autonomous ship technologies, if not the advent of uncrewed, remotely operated, or even fully autonomously navigated commercial and passenger vessels alongside conventional vessels. Led primarily by its Maritime Safety Committee (MSC), IMO is on track to adopting in 2026, as an initial step, a goal-based non-mandatory code to set high-level standards for the safe operation of maritime autonomous surface ships (MASS Code), with the aim of later adopting a mandatory code under the SOLAS Convention. This article will look at the work done so far under IMO's MSC, Legal and Facilitation Committees, and the key issues explored when determining whether MASS can be accommodated under the Organization's existing instruments.

Keywords

IMO, Maritime Autonomous Surface Ships, MASS Code, SOLAS, remote operations

Introduction

Since 2015, the International Maritime Organization (IMO) has been engaged in work to assess the potential implications of autonomous technologies on the current regulatory framework for international shipping. Eventually termed "maritime autonomous surface ships" (MASS), the Organization, through its Maritime Safety Committee and working groups, is now at work on a goal-based non-mandatory MASS Code, with a target entry into force in 2032.

As one such competent international organization under the UN Convention on the Law of the Sea, IMO is the forum for the development of generally accepted international rules and standards with respect to the safety of maritime navigation and the protection of the marine environment from vessel-sourced pollution. The Organization's work is supported by five Committees, each with their own areas of competence, and ascribed, to varying extents, with legislative and/or regulatory authority by the different conventions adopted under their auspices. With respect to MASS, the Maritime Safety (MSC), Legal (LEG) and Facilitation (FAL) Committees, have so far been engaged in related work to ascertain the new roles and responsibilities that increased autonomy in commercial shipping might entail. The Marine Environment Protection Committee (MEPC), which is currently at the helm of negotiations for maritime decarbonization, could potentially undertake complementary activities in the coming years, upon the submission of relevant proposals by interested delegations.

IMO's substantive work on MASS began with the conduct of regulatory scoping exercises (RSE) to determine how MASS might be introduced in IMO instruments (IMO, 2017). The first to embark on such an exercise was the MSC, which has several key instruments in maritime safety under its purview, including the SOLAS[1] Convention, STCW Convention[2], COLREG[3], Load Lines Convention[4], and the SAR Convention[5]. The Legal Committee followed suit in 2019 with a review of the key conventions on liability and compensation following incidents of marine pollution damage, such as the BUNKERS[6], Civil Liability[7], and Athens[8] Conventions. The FAL Committee, which is responsible for the Facilitation Convention[9], was the last to commence its RSE in 2021.

[1] International Convention on the Safety of Life at Sea, 1974. Amended by the Protocols of 1978 and 1988.
[2] International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978.
[3] Convention on the International Regulations for Preventing Collisions at Sea, 1972.
[4] International Convention on Load Lines, 1966, and the Protocol of 1988 relating to the International Convention on Load Lines, 1966. In relation to the LL Convention, the RSE also included the IMO Instruments Implementation Code (III Code) and Part A of the International Code on Intact Stability, 2008.
[5] International Convention on Maritime Search and Rescue, 1979.
[6] International Convention on Civil Liability for Bunker Oil Pollution Damage, 2001.
[7] International Convention on Civil Liability for Oil Pollution Damage, 1969, and its Protocols of 1976 and 1992.
[8] Athens Convention relating to the Carriage of Passengers and their Luggage by Sea, 1974, and its Protocols of 1976 and 2002.
[9] Convention on Facilitation of International Maritime Traffic, 1965.

Regulatory Scoping Exercises

The RSEs entailed separate assessments by each of the Committees, through the work of the respective volunteering delegations, of whether the operation of MASS could be easily accommodated under their existing instruments, and if this was not the case, the extent to which such instruments may need amendments or interpretation. Cognizant of the number of commercial research and development initiatives relating to autonomous technologies, it was acknowledged early on that IMO should take a leading role with respect to the development of MASS. The RSEs provided an opportunity for a wide range of shipping stakeholders to express their views on the prospective advent of crewless and increasingly intelligent ships alongside those that are conventionally manned, and revealed the diverse interests of States in their capacities as coastal, port and flag States.

While there was acknowledgment that there was already a high degree of automation in technologies onboard existing ships, some delegations held reservations on, among others, the ability of MASS at higher degrees of autonomy to satisfy the standards set in UNCLOS, to comply with requirements under the different IMO conventions, and to assure that in their operational context, they pose no greater risk of collisions or pollution of the marine environment. In this context, suggestions have been made on disallowing MASS operations until there are applicable regulations, or a potential ban on the entry of MASS, specifically, into specific ports. Meanwhile, States which were at advanced levels of developing autonomous technologies for use in commercial navigation likewise shared information from early trials and the corresponding national legislation they have adopted.

In their RSEs, the three Committees' work were anchored on the same framework for degrees of autonomy. First, MASS was provisionally defined as a ship which, to varying degrees, can operate independent of human interaction. As for the specific degrees of autonomy, Degree One ships were those ships with automated processes and decision support; at Degree Two were remotely controlled ships *with* seafarers on board; at Degree Three were remotely controlled ships *without* seafarers on board; and at Degree Four were fully autonomous ships. In this regard, priority was given to considering how ships of Degrees Two and Three of autonomy would interact with the IMO instruments, while also acknowledging that a ship could be operating at different degrees in the course of a voyage.

After its RSE, MSC agreed that the best way forward would be through the development of a goal-based MASS instrument (IMO, 2021). Given the Committee's extensive experience in developing specialized instruments that expand the technical scope of the SOLAS Convention (e.g. ISPS and IMDG Codes), it was decided that a non-mandatory MASS Code would be developed, with a view to the eventual development of a Code that will be made mandatory under a specific chapter of SOLAS.

In the Legal Committee, the emergence of new roles in the operation of MASS was among the most crucial elements for determining whether the current instruments relating to liability and compensation following marine pollution damage incidents could accommodate MASS. Foremost of these are the remote operators that will be charged with the control of MASS, whether in one location or at different remote operations centres across the world. Instruments like the Civil Liability Convention and the Bunkers Convention traditionally accorded strict liability to shipowners in case of pollution incidents – that is, compensation must be paid to victims affected by such incidents irrespective of a finding of fault, to the prescribed limits of liability.

One line of inquiry would therefore be whether the application of strict liability should be maintained for MASS operations, and whether such liability could be channelled against remote operators upon a finding of the latter's fault in causing a pollution incident. Another question, insofar as the relevant conventions provide for exonerations that shipowners can invoke against the imposition of such strict liability, is whether remote operators can similarly invoke certain exceptional circumstances. There have also been questions on whether further recourse can be had against the software developers or programmers of such intelligent systems, should the incident have been caused by the malfunctioning of the respective operating systems. Following its RSE, the Legal Committee eventually concluded that MASS could be accommodated within the framework of its instruments without need for major adjustments, although some conventions may require additional interpretations or amendments to address potential gaps and themes.

Like the MSC and LEG RSEs, the FAL RSE concluded with the finding that the FAL Convention can address MASS operations without major amendments (IMO, 2022, p. 5). Amendment or interpretation may thus be required on operational matters such as the ships' provision of information upon arrival and departure at port, ensuring continuous connectivity with ROCs during a voyage, and contingencies in case of specific situations such as the rescue of persons or refugees at sea, or the presence onboard of stowaways.

Interim Guidelines for MASS Trials

Pending the completion of work on the development of the draft MASS Code, MSC deemed it necessary in 2019 to approve Interim Guidelines for MASS Trials (IMO, 2019), to ensure that even in the absence of mandatory regulations, some form of guidance exists that prescribes consistency with the current legal framework for conventionally operated ships.

This is with regard to matters such as risk management, emergency planning, minimum manning requirements, personnel qualification, safe infrastructure and reporting requirements, among others. The Interim Guidelines likewise encourage IMO Member States to share information and report on their experience from their respective MASS trials.[10]

[10] See for example, IMO documents MSC 102/INF.8 (Japan), MSC 104/INF.4 (China), MSC 104/INF.19 (France); MSC 108/4/3 (Russian Federation), MSC 109/INF.14 (Republic of Korea).

Development of the MASS Code

Following its RSE, MSC 105 began to embark on the development of a goal-based instrument on MASS. Goal-based regulation aims to chart high-level standards and procedures that are intended to be met through subsequent technical regulations, rules and standards that are periodically updated through amendments by Parties to the relevant conventions, standards or interpretations by classification societies (recognized organizations) and other issuances by national maritime administrations. Originally set for a completion year of 2025, MSC has since had a reassessment of its workload and the complexity of MASS-related issues, resulting in a resetting of that target completion to 2026 to coincide with MSC 111 in May 2026. Furthermore, instead of immediately embarking on the development of a mandatory instrument, an experience-building phase has been set to follow the adoption of the non-mandatory Code, to allow for time to take stock of learnings from the implementation of the MASS Code that can be built upon for any subsequent legally binding regulation. The adoption of the mandatory Code is envisioned by 1 July 2030, so that the related SOLAS amendments can enter into force by 1 January 2032. Presently, work on MASS is continuously undertaken by a Working Group on MASS convened during sessions of the MSC, and between its sessions, by an Intersessional Working Group on MASS and a MASS Correspondence Group.

The draft MASS Code is structured into three parts. The first Part introduces the underlying purpose, principles and objectives of the Code; its scope of application and structure; and terminology and definitions for MASS. As of its current drafting, it is intended that the Code will apply to "cargo ships to which SOLAS chapter I applies, including any associated remote operations centre(s) (ROCs), which have systems and functions that enable autonomous or remote operations", but not to "cargo high speed craft to which SOLAS chapter X applies" and warships, naval auxiliaries, and other ships on government non-commercial service. Several portions in this part of the Code remain flagged for further deliberation, such as the chapter on definitions, given that these are the provisions that will underlie the entire text. Part Two details the principles for MASS and MASS functions, including risk assessment, the operational context, and the certification and surveying process. Part Three provides in even further detail the Goals, Functional Requirements and Expected Performance, for autonomous or remotely operated functions, including fire protection, detection and extinction, and the availability of life-saving appliances onboard. Additionally, in this phase of development of the MASS Code, the mode(s) of operation (MoO), in relation to the concept of operations (ConOps) and the overall operational context of MASS, have been taken into account, rather than the degrees of autonomy relied on during the RSEs.

At this stage, the Sub-Committees supporting the work of MSC have not yet been comprehensively engaged to deal with MASS-specific issues, but are expected to do so in greater detail following the completion of the non-mandatory code. Thus, matters relating to network governance are envisioned to be further considered by the NCSR Sub-Committee (potentially in cooperation with the International Telecommunications Union).

With respect to the impacts of autonomy on the human element, further work is expected to follow under the purview of the HTW Sub-Committee and will possibly require further engagement with the International Labour Organization. Meanwhile the Legal and Facilitation Committees have adopted and updated their respective road maps on MASS for considering issues specific to their instruments, such that substantive consideration thereof would only really commence after the adoption of the non-mandatory MASS Code.

Common Gaps and Themes

As early as the RSEs, the three Committees, including a Joint Working Group that they have constituted to discuss cross-cutting issues, have identified and discussed at length common gaps and themes relating to MASS that would have implications across the different IMO instruments and possibly influence other legal regimes outside of that framework. While some of the debates on these issues may have already resulted in agreed text, further collaboration is needed on others. It is acknowledged, for example, that maintaining MASS and ROC connectivity and providing the highest levels of cybersecurity for MASS, are of utmost importance, though the technical specifications will have to be defined at a much later point. Meanwhile some delegations, adopting a protective standpoint, continue to express reservations on the right of MASS to enter their territorial seas, for lack of conformity with UNCLOS.

Another one of these common gaps and themes relate to the status of remote operators who are expected to be stationed at different ROCs around the world, to provide round-the-clock control and monitoring for MASS.

While there has been agreement on the matter of a master (or other person in control) of MASS being in control of multiple MASS at the same time, and the fact that control can be handed over from one master at one ROC to another master at another ROC, there remain questions on, inter alia, whether the remote operator needs to have the status of a master or at least a seafarer, and whether a master must always be onboard a MASS when there are persons onboard. With respect to ROCs, more importantly, some delegations have time and again expressed doubt on the ability of flag States of MASS to exercise effective jurisdiction as required by UNCLOS, since ROCs in different territories will be involved in the operation of such MASS, that will not necessarily be under the same flag States' oversight. In this regard, several options for remote operation management, modelled after the current framework for ship management in accordance with the ISM Code, are under consideration.

The ability of MASS to participate in the internationally established search and rescue system, and to play an active role in it, has also been brought into question: while presumably the highly sophisticated surveillance equipment onboard MASS can provide a wide latitude of situational awareness, their ability to engage in actual rescue operations remains to be demonstrated.

Conclusion

The Maritime Safety Committee is currently meeting for its 110th session at the IMO Headquarters in London and work is in full scale for the delegations involved in the development of the MASS Code. While many chapters have yet to be finalized, most of them are at advanced stages of development and nearing completion, indicating that the planned adoption in 2026 could be achieved. Evidently, the completion of the non-mandatory Code is just a first step, with priorities already identified for the different IMO organs' work upon the adoption of the Code, and anticipation is building for the findings of the individual trials conducted by early MASS movers to be applied and further tested during the experience-building phase.

References

International Maritime Organization (IMO). (2017). *Report of the Maritime Safety Committee on its ninety-eighth session* (MSC 98/23).

International Maritime Organization (IMO). (2019, June 14). *Interim guidelines for MASS trials* (MSC.1/Circ.1604).

International Maritime Organization (IMO). (2021). *Report of the Maritime Safety Committee on its 103rd session* (MSC 103/21).

International Maritime Organization (IMO). (2022, June 1). *Outcome of the regulatory scoping exercise and gap analysis of the FAL Convention with respect to maritime autonomous surface ships (MASS)* (FAL.5/Circ.49).

About the Author

Maria Pia Benosa / International Maritime Organization / MBenosa[at]imo.org

Maria Pia Benosa is a Depositary and Legal Officer within the Legal Affairs and External Relations Division of the International Maritime Organization (IMO). Prior thereto she was part of the Ocean Law and Policy research team at the Centre for International Law of the National University of Singapore, and a Legal Officer for the Institute for Maritime Affairs and Law of the Sea of the University of the Philippines (UP). Ms. Benosa obtained her LL.M. in National Security Law from Georgetown University, and previously taught Public International Law at the UP College of Law. The views expressed in this contribution are the author's own and do not represent that of the IMO.

The Legal Status of Unmanned Vehicles (UVs) in the Maritime Domain

Dr. Levent Bahadır
Maritime SOF Command, Türkiye

Abstract

Technological advancement has driven the widespread integration of unmanned vehicles into modern military operations. Since the early twenty-first century, the proven effectiveness of Unmanned Aerial Vehicles (UAVs) in combat and support missions—particularly in Afghanistan and Iraq—has established them as indispensable components of state military capabilities. Their success has sparked growing interest in Unmanned Vehicles (UVs) within the maritime domain, where they are increasingly serving as strategic force multipliers. However, this operational expansion has outpaced the development of corresponding legal frameworks. The 1982 United Nations Convention on the Law of the Sea (UNCLOS) provides no explicit guidance on unmanned maritime systems, resulting in uncertainty over their classification and legal status. The diversity of UVs in size, tonnage, and autonomy precludes uniform categorisation, while divergent national regulations further exacerbate legal fragmentation. Against this backdrop, examining the status of UVs under UNCLOS is essential for clarifying their implications for key principles of international law, including freedom of navigation, belligerent rights, and sovereign immunity.

Keywords

Unmanned Vehicles, International Maritime Law, UNCLOS, Legal Issue

Introduction

During the Cold War, the United States assumed a pioneering role in developing early Unmanned Maritime Vehicles (UMVs), which were primarily employed for minesweeping operations and the collection of chemicals, biological, radiological, and nuclear (CBRN) samples (Department of the Navy, 2007, pp. 1–2). In the post–Cold War era, rapid advances in information technology, remote command and control systems, global positioning systems (GPS), and materials science provided the technological foundation for the accelerated evolution of unmanned systems (Savitz et al., 2013, p. 1-2). These developments collectively transformed the conceptual and operational landscape of naval warfare, paving the way for the systematic integration of unmanned platforms into maritime operations.

The demonstrated effectiveness of Unmanned Aerial Vehicles (UAVs) in combat and support missions, most notably in Afghanistan and Iraq, further reinforced the strategic value of unmanned technologies and stimulated parallel innovations in the maritime sphere. Initially designed to minimise human exposure to "dull, dangerous, or dirty" missions, Unmanned Vehicles (UVs) have since evolved into versatile force multipliers. Their cost-effectiveness, adaptability, endurance, and expendability have made them increasingly indispensable to contemporary naval planning (Chadwick, 2020, p. 132). Looking ahead, as naval operations are expected to occur predominantly within littoral zones, UVs are projected to undertake a diverse array of missions, including mine countermeasures, reconnaissance, anti-submarine and anti-surface warfare, and electronic warfare (Pedrozo, 2023a, p. 67). In this regard, unmanned maritime systems are not merely supplementary tools but represent a transformative capability that redefines how maritime power is projected and sustained.

Although many of these mission sets remain largely untested in full-scale combat, the 2022 conflict in Ukraine marked a significant turning point in the operational employment of armed unmanned vehicles. For the first time, Unmanned Vehicles (UVs) in the maritime domain were deployed on a large scale, as Ukraine used explosive-laden systems to strike Russian warships (Galdorisi, 2023).

Despite limited tactical success, these attacks demonstrated the strategic potential of UVs to challenge superior naval forces at substantially lower cost and risk (Pedrozo, 2023b, pp. 48–49). This episode underscored the growing accessibility and asymmetric value of unmanned maritime systems, highlighting their capacity to disrupt traditional naval hierarchies and deterrence structures. Scholars have thus identified the Ukraine conflict as a pivotal juncture for reassessing the legal and regulatory frameworks governing the use of UVs in armed conflict (Kurtdarcan & Mumcu, 2022, pp. 1235–1236).

Nevertheless, the rapid expansion of unmanned maritime operations has exposed a range of unresolved legal questions. While traditional classifications of naval assets distinguish between state vessels entitled to sovereign immunity and expendable weapons that constitute sovereign property, it remains unclear where unmanned vehicles fit within this framework (Kraska et al., 2023, p. 41). The uncertainty surrounding their status reflects a deeper "synchronisation problem"—a structural mismatch between the accelerating pace of technological innovation in unmanned systems and the comparatively slow evolution of international maritime law (Klein, 2019, pp. 247–248). This gap between practice and legal codification presents profound challenges for both states and international institutions, as the absence of clear legal norms risks producing inconsistencies in interpretation and enforcement across jurisdictions.

Ultimately, the trajectory of unmanned maritime technologies underscores the urgent need for a coherent and adaptive legal framework capable of addressing emerging operational realities. As UVs continue to expand in capability, autonomy, and strategic relevance, reconciling technological progress with the enduring principles of the law of the sea will remain one of the most critical challenges for contemporary maritime governance.

Legal Status of Unmanned Vehicles under the Law of the Seas

There is no universally accepted definition of ship or vessel in the law of the sea, and both terms are used interchangeably, including in the 1982 United Nations Convention on the Law of the Sea (UNCLOS) (Schmitt & Goddard, 2016, pp. 575–576). Although efforts continue to clarify the legal implications of Unmanned Vehicles (UVs), international and domestic maritime law frameworks are largely designed around traditional manned ships (McCarl, 2023, p. 481). While the UNCLOS aimed to comprehensively regulate maritime affairs (Pereira, 2019, p. 39), it contains no explicit provisions on UVs, which were not contemplated at the time of negotiation (Veal et al., 2019, p. 27).

The absence of regulation reflects both the technological limitations of the period and Cold War–era sensitivities that discouraged discussions on emerging maritime technologies.

Technological advances often outpace legal development, leaving new technologies initially unregulated. The evolution of mobile oil platforms—contrary to their original fixed classification in the 1972 COLREGs—illustrates this lag (Chadwick, 2020, p. 140). Consequently, scholars have proposed treaty amendments or even new legal instruments to address UVs, given the slow adaptability of existing regimes (Allen, 2018, pp. 512–518). McCarl (2023, pp. 485–486) argues that a new framework should be created to assess UVs on their own terms rather than forcing them into outdated vessel definitions. In contrast, Kraska (2010, p. 64) contends that existing international regimes—the law of the sea, the law of armed conflict, and the law of naval warfare—already provide a sufficient and legitimate framework, and that applying these regimes mutatis mutandis to UVs would preserve legal stability and prevent normative fragmentation.

The situation is further complicated by the widespread acceptance that many UNCLOS provisions reflect customary international law, whose interpretation evolves through state practice and opinio juris. On this basis, some scholars argue that UVs may already qualify as "ships" under customary law, granting them navigational rights such as innocent passage, even absent explicit treaty recognition (Schmitt & Goddard, 2016, pp. 577–579). Although limited state practice weakens this claim, such assertions could influence the future development of custom.

Given that UVs range from less than one metre to over fifty metres in length (Small, 2019, pp. 2–3), applying a single legal status is problematic. McCarl (2023, p. 481), Veal et al. (2019, p. 35), and Arslan (2018, p. 5) emphasise that dimensional variability necessitates case-specific legal analyses. The 2016 "Bowditch" incident between the United States and China illustrates these challenges: the U.S. characterised a two-metre underwater glider as a government UV (U.S. Department of Defence, 2016). The legal classification of such systems carries significant implications not only for navigation rights, immunity, and maritime operational functions, but also for issues such as seizure by other states (Norris, 2013, p. 30; Johansson, 2018, p. 144).

An Assessment on the Potential Status of UVs

When examining the legality of Unmanned Vessels (UVs) under the law of the sea, the first question concerns what occurred and where, but ultimately the central issue becomes the legal status of UVs (Klein, 2019, p. 251).

The 1982 United Nations Convention on the Law of the Sea (UNCLOS) recognises four main vessel categories: warships, government ships operated for non-commercial purposes, government ships for commercial purposes, and private ships. Only the first two enjoy sovereign immunity. Hence, UVs performing public or governmental functions may arguably fall within Articles 32, 58, 95 and 96 and benefit from immunity against arrest or seizure in foreign territorial waters (Pereira, 2019, p. 47; Norris, 2013, p. 42). The classification of UVs within these categories, therefore, becomes critical.

UVs as Ships

Whether UVs should be considered "ships" largely depends on the flag state's domestic law, as UNCLOS does not define the term "ship" though it regulates their use (Chang et al., 2020, pp. 2–3). Article 91 stipulates that a ship must have a genuine link with the state, reflected through nationality, registration, and the right to fly its flag (United Nations, 1982, Art. 91). Based on these characteristics, UVs could plausibly be regarded as ships (Caligiuri, 2020, p. 102).

IMO conventions provide a functional definition—any structure capable of navigation qualifies as a ship—without explicitly requiring crew presence (Chadwick, 2020, p. 139; Caligiuri, 2020, p. 103). This broad and technologically neutral approach supports the inclusion of UVs. Through an evolutionary interpretation, treaty terms should adapt to technological and operational developments over time (McKenzie, 2020, pp. 13–14). Just as the concept of "commerce" evolved to encompass tourism, "ship" can evolve to encompass unmanned variants (Caligiuri, 2020, p. 103).

Article 94 of UNCLOS, drafted with conventional crewed ships in mind, imposes obligations on flag states to ensure safety and regulatory compliance, but it does not define "ship" itself (United Nations, 1982, Art. 94). Thus, a UV's compliance with safety requirements is a separate issue from its recognition as a ship (McKenzie, 2020, p. 18). From a practical standpoint, integrating UVs into the existing maritime framework by recognising them as ships under UNCLOS seems consistent with the Convention's purpose and the principle of continuity in the law of the sea (McKenzie, 2020, p. 34). The remaining question is whether all UVs, given their diversity in size and tonnage, would uniformly qualify.

As A Warship

If certain UVs meet the basic definition of ships, the next issue concerns whether they can attain warship status. In maritime warfare, this status is decisive, as only warships possess belligerent rights and full immunity from jurisdiction (Klein et al., 2020, p. 723; Chadwick, 2020, p. 143). Although it is generally accepted that only warships may exercise combat rights, this principle is not universally codified (Norris, 2013, p. 57). The core legal definition of a warship—commanded by a commissioned officer and crewed by personnel under military discipline—originates in the 1907 Hague Convention VII and is reiterated in Article 29 of UNCLOS (United Nations, 1982, Art. 29; Schmitt & Goddard, 2016, p. 579).

Unlike earlier definitions limited to naval forces, UNCLOS extends the term to any armed forces' ships, including those operated by coast guards or similar services (McKenzie, 2020, p. 30).

Historically, this requirement aimed to prevent privateering by ensuring that only duly commissioned vessels could claim belligerent rights (Klein et al., 2020, pp. 723–724).

Given the evolving context of naval operations, a flexible interpretation of Article 29 could extend the notion of "command" to include remote or automated control (Caligiuri, 2020, p. 107). Nonetheless, as the text currently stands, UVs do not meet the explicit criteria of being "commanded by an officer" and "crewed by personnel under military discipline," since no crew is physically on board (Schmitt & Goddard, 2016, p. 579). This strict reading excludes UVs from warship status. However, such rigidity produces contradictions: two vessels performing identical military missions—one manned, one unmanned—would hold different legal standings (Chadwick, 2020, pp. 143–144). Functionally,

if UVs are under the command of a military officer, remotely or otherwise, and display clear nationality markings, they arguably meet the substantive intent of Article 29 (Klein et al., 2020, p. 44). The analogy to military aircraft—where remotely piloted drones are recognised as state aircraft—supports this reasoning (McKenzie, 2020, p. 34).

The U.S. Commander's Handbook on the Law of Naval Operations (2017; updated 2022) explicitly acknowledges that manned and unmanned vessels operated by the state enjoy sovereign immunity and, if under military command, may be considered Unmanned Surface Ships (USSs) capable of exercising belligerent rights (Department of the Navy & Department of Homeland Security, 2022, pp. 2-2, 2-5). This emerging practice indicates a gradual acceptance of UVs as functional warships.

UVs As Auxiliary Ships

If UVs cannot satisfy the conditions for warships, they may qualify as auxiliary ships. The San Remo Manual defines these as vessels under exclusive military control, engaged in non-commercial service (International Institute of Humanitarian Law, 1995, p. 9). Auxiliary ships are less constrained by command and crew requirements and can thus encompass UVs more easily. Although not warships, they share similar sovereign immunity protections under UNCLOS Articles 95–96 and enjoy the right of visit and hot pursuit under Article 110 (United Nations, 1982, Art. 110; Schmitt & Goddard, 2016, pp. 579–580).

However, auxiliary ships lack belligerent rights and can be targeted as military objectives (Klein et al., 2020, pp. 724–725). For UVs designed to employ offensive force, this status would significantly limit their strategic value (McKenzie, 2020, p. 29).

Other Conditions

If UVs cannot be considered vessels at all, alternative classifications arise. They might be treated as devices or equipment under UNCLOS (Caligiuri, 2020, pp. 105–106). Yet this status imposes constraints: devices are subject to notification requirements when operating in the EEZ (Exclusive Economic Zone) or continental shelf (United Nations, 1982, Art. 248) and lack navigation and immunity rights reserved for ships under Articles 17 and 90 (United Nations, 1982, Arts. 17, 90; Veal et al., 2019, pp. 31–32). Labelling UVs merely as "craft" or "devices" avoids legal clarity but leaves unresolved core issues such as navigation rights and sovereign immunity (Norris, 2013, pp. 22–26). Given their increasing size, tonnage, and sophistication, such minimal classifications are unlikely to satisfy state practice or policy interests.

Comparison of UAV and UV in Terms of Legal Status

Debates over the recognition of warship status for Unmanned Vessels (UVs) naturally draw parallels with discussions surrounding Unmanned Aerial Vehicles (UAVs). Although the operational dynamics of the maritime and aerial domains differ substantially, the legal and doctrinal evolution of UAVs offers valuable insight into how UVs might be treated in the future. UAVs, having demonstrated exceptional operational utility in modern conflicts, have become indispensable instruments of state power. Their extensive use in military operations in Afghanistan and Iraq not only showcased their tactical effectiveness but also stimulated intense legal debate regarding their classification under international law (Norris, 2013, p. 21).

A major doctrinal turning point occurred when the U.S. Department of Defense (DoD), in 2007, formally recognised all aircraft used for military purposes—whether manned or unmanned—as military aircraft. This categorical approach eliminated distinctions based on crew presence and was subsequently adopted by the United Kingdom, marking a decisive moment in the evolution of state practice (Norris, 2013, p. 21). The legal rationale behind this classification rests on three criteria: (1) state operation for non-commercial purposes, (2) clear display of military markings, and (3) command and control by military personnel (Norris, 2013, p. 28). These attributes collectively offer a contemporary analogue for interpreting the warship status of UVs.

Reflecting this doctrinal view, the U.S. Commander's Handbook on the Law of Naval Operations explicitly confirms that UAVs are military aircraft, enjoying the same legal rights and privileges as their manned counterparts (Department of the Navy & Department of Homeland Security, 2022, pp. 2–6). This official acceptance underscores a broader principle: the determining factor for status under international law lies not in crew presence, but in state control and military purpose.

Nevertheless, as Chadwick (2020, pp. 154–155) observes, UVs and UAVs differ in mission profiles and operational environments. UAVs typically execute discrete missions and return to base, whereas Unmanned Maritime Systems (UMSs) must operate for prolonged periods, interact with other actors in the maritime domain, and may never physically return to their point of origin. The maritime environment also entails closer and more sustained interactions between vessels, raising distinct legal and operational challenges absent in aerial contexts.

Despite these differences, the analogy remains instructive. Just as UAVs operating under state authority and military command are widely accepted as military aircraft, UVs meeting comparable criteria, state ownership, military markings, and operation under military command, could logically be recognised as warships.

The functional approach adopted in the UAV context suggests that the defining elements of military status lie in sovereign control and operational function, not in physical occupation by crew. Consequently, as UVs evolve technologically and demonstrate effectiveness in future naval operations, it appears both realistic and consistent with the logic of state practice and treaty interpretation that at least certain classes of UVs, though not all, will eventually attain recognition as warships under international law.

Conclusion

One of the most contentious debates within contemporary maritime doctrine concerns the legal status of Unmanned Vessels (UVs), particularly in relation to their navigation rights, jurisdictional immunities, and belligerent entitlements. The absence of a crew, a defining feature of UVs, renders their classification under the law of the sea inherently ambiguous. Despite growing operational reliance on such systems, no consensus has yet emerged on how these platforms should be legally recognised within the framework of international maritime law. The fundamental question remains unresolved: should UVs enjoy the same rights and immunities traditionally afforded to warships under the 1982 United Nations Convention on the Law of the Sea (UNCLOS)?

This uncertainty has generated a fragmented doctrinal landscape. Divergent interpretations among scholars and states regarding how to integrate UVs into existing legal regimes have hindered the emergence of a unified theoretical or practical framework. It is widely anticipated, however, that state practice, as it gradually develops through operational experience and public precedents, will play a decisive role in shaping future legal norms. Over time, these practices are expected to be codified through amendments or interpretative updates to relevant international instruments, thereby gradually clarifying the legal contours of UV operations.

A further dimension of this complexity arises from the wide variation in UV size and tonnage, ranging from compact systems of one to two metres to large autonomous vessels exceeding fifty metres (Small, 2019, pp. 2–3). This heterogeneity complicates the establishment of a single, universal legal standard. A more pragmatic approach, therefore, would be to differentiate UVs based on functional and physical equivalence to manned platforms. Those UVs that are comparable to conventional vessels in terms of size, tonnage, and operational capacity could be subjected to similar legal status assessments, including the right to fly a national flag and display visible markings of nationality, consistent with established state practice for manned warships. Crucially, maintaining a human element in the command-and-control cycle—through remote operation rather than full autonomy—appears vital for aligning UVs with existing maritime legal principles.

This ensures that accountability, intent, and command responsibility remain traceable to human decision-makers, thereby satisfying the doctrinal prerequisites for sovereign representation at sea.

Drawing parallels from the evolution of Unmanned Aerial Vehicles (UAVs), it is foreseeable that UVs meeting these thresholds of size, tonnage, remote command, and operational functionality will, in the near future, be recognised as warships under international law.

Conversely, smaller or more limited UVs that do not satisfy these criteria may be classified as organic extensions of manned warships, functioning as auxiliary or support systems rather than independent vessels. This tiered interpretation offers a pragmatic balance between technological reality and legal coherence, allowing the maritime legal order to adapt dynamically to emerging unmanned systems while preserving the structural integrity of the law of the sea.

References

Allen, C. H. (2018). Determining the legal status of unmanned maritime vehicles: Formalism vs functionalism. *Journal of Maritime Law and Commerce*, *49*, 477-519.

Arslan, K. B. (2018). *İnsansız deniz araçlarının hukuki rejimi (The legal regime governing unmanned underwater vehicles)* (SSRN Scholarly Paper 3371489). https://papers.ssrn.com/abstract=3371489

Caligiuri, A. (2020). A new international legal framework for unmanned maritime vehicles? In A. Caligiuri (Ed.), *Legal technology transformation: A practical assessment* (pp. 99–109). Editoriale Scientifica. https://www.academia.edu/45040210/A_New_International_Legal_Framework_for_Unmanned_Maritime_Vehicles

Chadwick, K. (2020). Unmanned maritime systems will shape the future of naval operations: Is international law ready? In M. D. Evans & S. Galani (Eds.), *Maritime security and the law of the sea: Help or hindrance?* (pp. 132–156). Edward Elgar Publishing.

Chang, Y.-C., Zhang, C., & Wang, N. (2020). The international legal status of unmanned maritime vehicles. *Marine Policy*, *113*, 103830. https://doi.org/10.1016/j.marpol.2020.103830

Department of the Navy, & Department of Homeland Security. (2017). *The commander's handbook on the law of naval operations* (August 2017 ed.). https://www.politics-prose.com/book/9781098620042

Department of the Navy, & Department of Homeland Security. (2022). *The commander's handbook on the law of naval operations* (March 2022 ed.). https://www.jag.navy.mil/organization/documents/NWP_1-14M.pdf

Galdorisi, G. (2023, May 16). The broadening global effort to accelerate unmanned maritime systems development. *Center for International Maritime Security*. https://cimsec.org/the-broadening-global-effort-to-accelerate-unmanned-maritime-systems-development/

International Institute of Humanitarian Law. (1995). *San Remo manual on international law applicable to armed conflicts at sea* (L. Doswald-Beck, Ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511622052

Johansson, L. (2018). Ethical aspects of military maritime and aerial autonomous systems. *Journal of Military Ethics, 17*, 1–16. https://doi.org/10.1080/15027570.2018.1552512

Klein, N. (2019). Maritime autonomous vehicles within the international law framework to enhance maritime security. *International Law Studies, 95*(1), 244–271.

Klein, N., Guilfoyle, D., Karim, M., & McLaughlin, R. (2020). Maritime autonomous vehicles: New frontiers in the law of the sea. *International and Comparative Law Quarterly, 69*, 719–734. https://doi.org/10.1017/S0020589320000226

Kraska, J. (2010). The law of unmanned naval systems in war and peace. *Journal of Ocean Technology, 5*(3), 43–68.

Kraska, J., Pedrozo, R. "Pete", Letts, D., von Heinegg, W., McLaughlin, R., Farrant, J., Ishii, Y., Khurana, G., & Sato, K. (2023). *The Newport manual on the law of naval warfare. International Law Studies, 101*(1). https://digital-commons.usnwc.edu/ils/vol101/iss1/1

Kurtdarcan, B. R., & Mumcu, Ş. U. (2022). 2022: Deniz savaşları hukukunda beklenen kırılma yılı (mı?). *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2022*(2), 1223–1239.

McCarl, L. (2023). Untethering UVs from vessels: Why the United States should construct a new environmental legal scheme for unmanned maritime vehicles. *Dickinson Law Review, 127*(2), 469–534.

McKenzie, S. (2020). When is a ship a ship? Use by state armed forces of uncrewed maritime vehicles and the United Nations Convention on the Law of the Sea. *LawArXiv*. https://doi.org/10.31228/osf.io/a7xtc

Norris, A. (2013). *Legal issues relating to unmanned maritime systems monograph.* U.S. Naval War College. https://www.iqpc.com/media/1002182/50661.pdf

Pedrozo, R. (2023a). Advent of a new era in naval warfare: Autonomous and unmanned systems. In T. M. Johansson, J. E. Fernández, D. Dalaklis, A. Pastra, & J. A. Skinner (Eds.), *Autonomous vessels in maritime affairs: Law and governance implications* (pp. 63–80). Springer International Publishing. https://doi.org/10.1007/978-3-031-24740-8_4

Pedrozo, R. (2023b). Russia–Ukraine conflict: The war at sea. *International Law Studies, 100*(1). https://digital-commons.usnwc.edu/ils/vol100/iss1/1

Pereira, E. S. (2019). *Unmanned vessels & unmanned maritime vehicles: Prospects of a legal framework in the international and the Portuguese context.* Interdisciplinary Centre of Marine and Environmental Research. http://www2.ciimar.up.pt/pdfs/resources/ebook_unmanned_vessels_and_UVs-propects_of_a_legal_framework.espereira__ciimar_02-10-2019_idi74_.pdf

Savitz, S., Blickstein, I., Buryk, P., Button, R., DeLuca, P., Dryden, J., Mastbaum, J., Osburg, I., Padilla, P., & Potter, A. (2013). *U.S. Navy employment options for unmanned surface vehicles (USVs).* National Defense Research Institute. https://apps.dtic.mil/sti/citations/ADA588081

Schmitt, M. N., & Goddard, D. S. (2016). International law and the military use of unmanned maritime systems. *International Review of the Red Cross, 98*(902), 567–592. https://doi.org/10.1017/S1816383117000339

Small, P. (2019). *Unmanned maritime systems update.* https://www.navsea.navy.mil/Portals/103/Documents/Exhibits/SNA2019/UnmannedMaritimeSys-Small.pdf

United Nations. (1982). *United Nations Convention on the Law of the Sea.* https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

U.S. Department of Defense. (2016, December 16). *Statement by Pentagon Press Secretary Peter Cook on incident in South China Sea.* U.S. Department of Defense. https://www.defense.gov/News/Releases/Release/Article/1032611/statement-by-pentagon-press-secretary-peter-cook-on-incident-in-south-china-sea/

Veal, R., Tsimplis, M., & Serdy, A. (2019). The legal status and operation of unmanned maritime vehicles. *Ocean Development & International Law, 50*(1), 23–48. https://doi.org/10.1080/00908320.2018.1502500

About the Author

Levent BAHADIR / Maritime SOF Command, Türkiye /
levent_bahadir[at]yahoo.com / ORCID: 0000-0003-4133-0842

Dr Levent Bahadır is a Navy Captain (OF-5) currently serving as the Commanding Officer of the Maritime Special Operations Forces (SOF) Training Group. Over the course of his career, he has held various operational and strategic posts within the Turkish Navy, including assignments at the Navy Fleet Command (2003–2005), the Maritime SOF Command (2005–2021), NATO Supreme Headquarters Allied Powers Europe (SHAPE) as an Office of Special Operations Staff Officer (2021–2024), and the Maritime Security Centre of Excellence (MARSEC COE) (2024–2025). He holds a master's degree and a PhD in Maritime Security, and has participated in numerous maritime security operations conducted under NATO, United Nations, and national frameworks. His professional and academic interests focus on maritime security, special operations, unmanned systems, and the evolving role of Maritime SOF in security governance.

Military Applications of Artificial Intelligence (AI): Accelerating the Decision-Making Process in Modern Battlespace

Asst. Prof. Dr. Bleda R. Kurtdarcan
Galatasaray University

Abstract

The accelerating integration of artificial intelligence (AI) into military operations is fundamentally reshaping the dynamics of modern warfare. By enhancing the observe–orient–decide–act (OODA) loop, AI facilitates decision dominance—enabling armed forces to out-sense, out-decide, and out-fight their adversaries through rapid information fusion, automated data processing, and AI-enabled command-and-control systems. These technologies mitigate the challenges of information overload and cognitive saturation, allowing commanders to sustain operational tempo in a transparent, sensor-rich battlespace. Yet, the same acceleration of decision cycles introduces profound ethical and legal dilemmas. As machine-speed decision-making increasingly eclipses human cognitive limits, the risk of eroding meaningful human control and undermining compliance with international humanitarian law (IHL) grows. This paper argues that the pursuit of decision dominance must be balanced by the imperative of preserving human oversight and ensuring lawful conduct of hostilities. Accordingly, AI-enabled decision-support systems should be designed to integrate precautionary mechanisms and facilitate "tactical patience" within accelerated operational contexts. The challenge for contemporary militaries, therefore, lies not only in mastering machine-speed warfare but in embedding humanity within its algorithms.

Keywords

Artificial Intelligence (AI), Decision Dominance, OODA Loop, Military Decision-Making, International Humanitarian Law (IHL)

Introduction

The accelerating integration of artificial intelligence (AI) into military operations is reshaping the character of modern warfare. Contemporary conflicts are increasingly defined by speed, precision, and distributed lethality, as advanced weapon systems link vast networks of sensors, unmanned platforms, and precision strike capabilities across domains. Central to this transformation is the pursuit of decision dominance, a concept rooted in John Boyd's OODA (observe–orient–decide–act) loop, which emphasizes the ability to cycle through decision-making processes faster than an adversary.

The twenty-first century has seen the rise of AI-enabled capabilities that promise to revolutionize the cognitively demanding orient and decide stages of this loop. Proponents argue that AI offers the means to overcome the challenges of information overload, data fusion, and real-time decision-making in a "transparent battlespace," thereby allowing militaries to sustain operational tempo and impose dilemmas on adversaries at unprecedented speed. However, these advances also raise profound concerns. As decision-making accelerates to machine speed, commanders risk ceding meaningful control to algorithms, thereby undermining their ability to exercise judgment in compliance with the principles of international humanitarian law (IHL). This tension, between the operational advantages of accelerating decision cycles and the ethical-legal imperative to preserve human deliberation, defines one of the most pressing dilemmas in the military application of AI.

Accelerating Decision Cycles in Modern Warfare = Out-sense, out-decide, out-fight the adversary

In the 1970s, military theorist John Boyd promoted a decision-centric approach in military operations through his writings and presentations. He dissected the military decision-making process into four key components: observing both adversary and friendly forces; orienting to understand the enemy's actions and motivations; deciding on and selecting a course of action (CoA); and executing the chosen CoA (Clark et al., 2020, p. 24). This framework is known as the observe-orient-decide-act (OODA) loop. Boyd proposed that military operations should focus on defeating the enemy's orientation to slow and eventually collapse its decision cycle. If one side can consistently go through this cycle faster than the other, it gains a tremendous advantage. By the time the slower side acts, the faster side is doing something different from what he observed, and his action is inappropriate. With each cycle, the slower party's action becomes less useful than its predecessor. He falls farther and farther behind. He ceases to be effective (Lind, 2023, p. 16).

However, although the conceptualization of military operations in armed conflict as time-competitive OODA cycles has been firmly established since Boyd's original formulation, the focus of technological advancement for much of the late twentieth and early twenty-first centuries has remained largely confined to enhancing the observe and act stages of the cycle. Improvements in surveillance systems, precision-strike capabilities, and communications infrastructure exemplify this trend (Brady, 2025, p. 2). By contrast, the orient and decide phases—widely recognized as the most cognitively complex and context-dependent components of the cycle—have historically proven more resistant to technological intervention, relying primarily on human judgment, experience, and doctrinal frameworks. It is only with the recent emergence of advanced capabilities such as big data analytics, machine learning, and artificial intelligence that armed forces have begun to envisage systematic improvements in these latter dimensions (Galdorisi & Tangredi, 2024, p. 105-106). In fact, today, the rise of miniaturized unmanned systems, advancements in information technologies, and precision strike weaponry, in conjunction with the strategic dynamics of Great Power rivalries, are once again transforming the character of war. Some refer to this as the era of attritable-precision-mass warfare (Horowitz, 2024). Others, in their quest for a comprehensive doctrine, prefer labels such as decision-centric warfare (Clark et al., 2020) or, in the maritime domain, distributed maritime operations/distributed combat (CNO Navigation Plan, 2024, Cares & Cowden, 2021). Regardless of the terminology used, this emerging form of warfare relies on distributed and disaggregated forces that utilize numerous single-purpose unmanned vehicles and cyber systems, facilitated by quicker and more effective decision-making, all while undermining the quality and speed of the enemy's decision processes.

In this modern warfare context, where the operational tempo is unprecedentedly high, maintaining decision dominance, i.e., the ability to execute a faster OODA loop than the enemy (Antal, 2023, p. 111), is critically important.

Accelerating the observe and orient aspects of the OODA cycle: Out-sensing the adversary with enhanced ISR capabilities

The essence of decision dominance is the ability to perceive and comprehend information and to develop and sustain situational awareness more rapidly and more accurately than the adversary (Antal, 2023, p. 114, 116). Consequently, the initial step in this process is being able to rapidly determine where the enemy is; hence out-sensing her (Layton, 2021, p. 23).

The unprecedented proliferation of sensors on the frontline, the extensive deployment of unmanned systems, and the exponential growth of data sources and volumes have collectively contributed to the emergence of what is frequently described as a "transparent/naked battlespace" (Antal, 2023, p.18). Yet, this condition introduces its own set of challenges.

Information Overload and Cognitive Saturation

The most immediate challenge of the transparent battlespace lies in the overwhelming volume of information. As Galdorisi and Tangerdi argue, "the principal feature of information age warfare, the ability to gather and store data , has begun to exceed human processing capabilities" (Galdorisi & Tangredi, 2024, pp. 104). In fact, commanders and analysts are inundated with continuous streams of data from electro-optical sensors, signals intelligence, cyber monitoring, and social media sources. Without effective filtering and prioritization mechanisms, this deluge risks producing information overload, a condition in which the sheer quantity of inputs exceeds human cognitive capacity, obscuring rather than clarifying the operational picture (Bondar, 2025, p. 12).

Complexity synthesizing multisource data

Equally pressing is the problem of heterogeneity. Sensor data varies widely in form, resolution, and reliability, ranging from raw imagery and acoustic signatures to metadata and algorithmically generated predictions. The integration of these disparate streams into a coherent operational picture requires sophisticated data-fusion architectures and robust interoperability across platforms and services. Absent such mechanisms, the transparent battlespace risks fragmenting into isolated compartments of awareness, in which each echelon or unit operates from a partial and potentially inconsistent understanding of reality. This challenge is compounded in coalition or joint operations, where national and institutional boundaries often impose additional barriers to data sharing (Bondar, 2025, p. 12).

Delays in data processing

Manual data processing creates lags in intelligence dissemination and operational decisions which makes achieving real time responsiveness and fast execution of missions nearly impossible (Bondar, 2025, p. 12). Taken together, these challenges illustrate that the transparent battlespace does not automatically translate into decision dominance. Rather, it creates a complex environment in which sensing superiority must be matched by advances in cognitive, organizational, and technological domains. However, with the help of the AI, these challenges may be overcome (Bellione, 2023, p. 66).

AI can quickly process that data into intelligence, processing large amounts of information from multiple sources almost in real time. It can automatically distinguish critical patterns or anomalies in battlespace. It will make it much easier to detect, localize, and identify targets across battlespace which will become even more transparent (Layton, 2021, p. 23). This augmentation enriches situational awareness and builds a more robust foundation for decisions in high-pressure environments (Layton, 2021, p. 31). Ukrainian Delta Battle Management System, for example, incorporates AI-driven AVENGERS battlefield video analysis platform to help identify and classify over 12000 reconnaissance objects daily. (Bondar, 2025, p. 12-19).

Table 1: ISR Sources and the Role of AI

Source	Data	Tasks	Technology
Satellite imagery High-altitude drones Low-altitude drones Stationary cameras	Imagery and video	Detect, recognize, and classify objects	Computer vision analysis using deep learning algorithms: 3D convolutional neural networks (CNNs) and recurrent neural networks (RNNs)
Acoustic systems	Sound	Identifies and classifies distinct sound patterns	CNNs and RNNs; spectogram analysis enhanced by deep learning
Intercepted communications Group chat messages Chatbot reports submitted by civilians	Text	Transcribes metadata and extracts key entities and insights	Natural language processing (NLP); transformer models, for both speech recognition and synthesis

Source: CSIS analysis.

Table 1

ISR Sources and Role of AI (Bondar,2025, p. 13)

AI using convolutional neural networks or recurrent neural networks may be helpful in the analysis of the data gathered through IMINT and GEOINT sources.

Accelerating the decision aspect of the OODA cycle: Out-deciding the adversary with AI-enabled decision support systems

AI can be and is helpful in accelerating the decision phase of the OODA cycle. In fact, many military experts contend that the speed of modern warfare, particularly in areas like electronic, cyber, and missile warfare, surpasses human decision-making capabilities (Antal, 2022, p. 51-53; Galdorisi & Tangredi, 2024, p. 88-89). Contemporary weapon systems amplify the tempo, precision, and lethality of armed conflict by integrating diverse sensors, destructive long-range firepower, and distributed shooters into cohesive, networked frameworks (Brady, 2025, pp.2-3). Gathering, analyzing, sharing, and synchronizing this volume of time-sensitive multidomain targeting data is no longer effective at human decision-making speed" (Antal, 2024, p.72). Moreover, the rapid proliferation of unmanned systems, across air, land, sea, and undersea domains, combined with the emergence of doctrines such as decision-centric and distributed combat operations, is set to further intensify reliance on AI-enabled command-and-control (C2) architectures. "To fully exploit the value of disaggregated and more composable force, C2 (command and control) would rely on a combination of human command and machine control. Without automated control systems, commanders would not be able to take full advantage of the force' composability in imposing dilemmas on an adversary or recomposing in response to enemy defenses and countermeasures" (Clark et al., 2020, p.35). Simply put, the complexity and pace of today's and future's battlespace will increasingly exceed what unaided human cognition can handle.

In these circumstances, mission- and task-sensitive AI-enabled decision support tools that fuse relevant battlespace data at the appropriate times would speed the development of courses of action (CoAs) and decision-making by commanders. Faster decisions and the ability to mount more simultaneous actions would enable commanders to better control operational tempo compared to traditional forces (Galdorisi & Tangredi, 2024, pp. 108-111). As Antal points out, "AI will sort through thousands of data points, correlating their significance, recognizing patterns and providing battle commanders with actionable courses of action. The military that uses AI to synchronize multidomain kinetic and non-kinetic effects at machine speeds will gain a significant advantage over those who do not" (Antal, 2024, p. 63).

In the context of decision-centric warfare, characterized by disaggregated and distributed force structures, the employment of an artificial intelligence (AI)-enabled control system enables the realization of a "context-centric command, control, and communications (C3) paradigm". Within this construct, the system autonomously identifies all force elements currently within the communications architecture that may be made available for operational tasking. From this set of available forces, the commander exercises judgment in determining which units are to be designated for employment (Clark et al., 2020, p. 35).

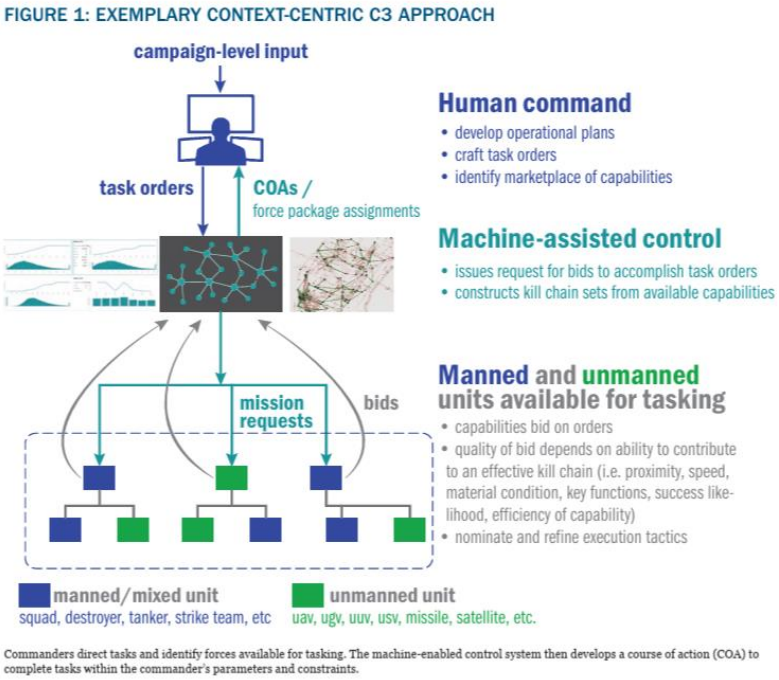

Figure 1

Context-Centric C3 Concept (Clark et al. 2020, p. viii)

The AI-enabled control system systematically queries each participating unit or force element regarding its capacity to support the commander's tasking. Unit responses include standardized data inputs such as geographic proximity to the designated area of operations, mission-relevant capabilities, current readiness state, and pertinent physical or operational characteristics. Upon receipt of these inputs, the system conducts modeling and simulation (M&S) of prospective concepts of operation (CONOPS). This computational process evaluates force alignment, operational feasibility, and potential adversary responses. Based on this analysis, the system generates and presents a set of courses of action, each accompanied by associated advantages, risks, and resource implications (Clark et al., 2020, p. 35).

The commander, retaining full decision authority, reviews these proposed COAs and selects the most suitable option for force employment. In this manner, the AI-enabled control system enhances decision dominance by accelerating the C3 process, optimizing force allocation, and enabling adaptive operational design in dynamic and contested environments.

Accelerating the decision aspect of the OODA cycle: Out-fighting the adversary with automatic target recognition (ATR)

AI can and has already been playing a role in conducting attacks. AI in ATR is a suite of technologies that automate the detection, classification, and tracking of objects or individuals. At its core, ATR relies on pattern recognition algorithms that match incoming sensor data against a set of known templates or behavioral models, flagging unusual features as potential targets (Bondar, 2025, p. 22).

ATR generally involves three sequential processes:

- **Detection**: Identifying regions of interest within noisy or cluttered sensor data.
- **Classification**: Assigning detected objects to target categories using discriminative features such as geometry, thermal signatures, or motion characteristics.
- **Tracking**: Monitoring targets over time (Bondar, 2025, p. 23).

Traditional ATR relied on handcrafted feature extraction and statistical classifiers. However, recent advances in **machine learning**, particularly deep neural networks, have demonstrated significant improvements in robustness and classification accuracy (LeCun et al., 2015, p. 436).

Advances in **AI** are reshaping the operation and development of ATR systems, delivering improved performance while reducing overall costs. Modern ATR, strengthened by new AI-driven algorithms and multimodal sensor fusion, exhibits a high degree of adaptability to rapidly changing battlespace conditions. When trained on datasets derived from real-world combat scenarios, AI-enabled ATR systems can reliably discriminate between vehicles, maritime vessels, and structural targets across diverse geographical settings and under challenging weather and geographical conditions (Bondar, 2025, p. 23-24). This last capability requires a robust autonomous navigation system. In autonomous navigation, advanced weapon systems leverage machine vision and deep learning algorithms to construct a continuously updated model of their environment. This allows them to map terrain, determine position in GPS-denied settings, and dynamically adjust flight paths to avoid unexpected hazards. Such capabilities have already become essential for long-range strike missions, where extended operations must contend with sophisticated air defenses and electronic warfare. Looking ahead, as warfare shifts toward decision-centric and distributed combat operations, AI-enabled autonomous navigation will assume an even more critical role in ensuring survivability, precision, and mission success.

Applying the Brake of Humanity on the Machine-Speed Decision Cycles in Modern Warfare

As described in the preceding section, the advent of modern destructive weaponry and transparent battlespace, characterized by persistent surveillance, ubiquitous sensors, and high-speed data dissemination, has dramatically increased the tempo of modern armed conflict. Information is now available almost instantaneously across the tactical, operational, and strategic levels, creating expectations for equally rapid decision-making. In search of gaining decision dominance over the adversary in a very deadly battlespace, AI in data processing and decision support is seen as the

ultimate tool to accelerate substantially certain phases of one's own OODA cycle and to get inside that of the adversary. The leading military powers across the world seem to be convinced that an AI-enabled force has magnitudes more combat power than a non-AI-powered force and applying AI to improve the speed and accuracy of battlefield decision-making is therefore a necessity (Layton, 2021, p. 2). However, while accelerated decision cycles can provide tactical advantages, the privileging of speed heightens the risk of over-reliance on machine-generated recommendations. As the application of AI into different phases of the decision cycle increases autonomy, human warrior moves further and further out of control of war fighting and leaves more and more decisions to the machines (Galdorisi & Tangredi, 2024, p. 131). As the cognitive load and speed of decision making in battlespace more and more surpass human capabilities, human decision makers would find themselves in a position where they would be relying blindly upon AI-enabled decision support systems' output, and they would simply provide a human rubber stamp (Michel, 2024 April, p. 6).

However, according to customary international humanitarian law, constant care shall be taken to spare civilians and civilian objects in the conduct of all military operations, including ISR operations and planning phases, and not just specific attacks (Watts, 2019, p.133). Therefore, accelerating the observe, orient, and decide phases of the OODA cycle to the machine speed should also be accompanied by relevant AI capabilities to ensure international humanitarian law (IHL) compliance. In this context, an appropriate AI-based situational awareness technology (SAT) to implement precautionary measures that reflect constant care obligations under IHL should be used as a way to adapt and improve traditional, time-consuming precautions to the requirements of machine-speed military decision-making (Marguiles, 2019, p. 148-152).

That being said, as Deeks argues "in creating these decision support algorithms, military operators, programmers, and lawyers will be confronted with difficult challenges: determining the specific features that are relevant to the application of a law of armed conflict (LOAC) rule will involve trial and error, as well as steep learning curves by everyone involved.

Lawyers will need to understand the capabilities, requirements, and limits of algorithms, while programmers will need to learn the basics of LOAC and how militaries make LOAC-infused decisions under pressure (Deeks, 2022, p. 58-59).

However, although AI has made a substantial difference in streamlining data analysis, reducing human error, providing situational awareness, and supporting optimal decision making, it still and will in the foreseeable future require human oversight in many cases, particularly for engagement decisions. Therefore, in light of the current inadequacies of AI-enabled decision-support systems, acceleration of the OODA cycle with AI-enabled decision support systems must be kept limited so that commanders can ensure compliance with their obligations under IHL. As ICRC puts it, the tempo of decision-making must allow for tactical patience. Thus, the use of machine learning-based DSS must be coupled with an awareness of the need, from both a legal and humanitarian perspective, to preserve sufficient time and space to allow for human deliberation in decisions on the conduct of hostilities (Michel, 2024 April, p. 4,7).

Conclusion

The integration of artificial intelligence into military decision-making processes undeniably enhances the speed, precision, and effectiveness of modern operations. By accelerating the OODA cycle, AI enables armed forces to achieve decision dominance and exploit the advantages of distributed, decision-centric warfare. There is compelling evidence that, due to the successful use of AI enabled systems in the war in Ukraine , the genie is out of the bottle, and there is little chance of turning back the clock to a point where nations and their militaries don't look to the use of these systems as a necessity (Galdorisi & Tangredi, 2024, p. 127).

Yet, these benefits come at a cost. The increasing reliance on machine-generated analysis and recommendations risks displacing human judgment at the very moment when careful legal and ethical scrutiny is most required. International humanitarian law demands constant care in the planning and conduct of operations, a requirement that cannot be met if commanders are reduced to rubber-stamping algorithmic outputs. AI-enabled decision-support systems must therefore be designed and employed in a manner that ensures tactical patience, preserves human oversight, and embeds precautionary measures aligned with IHL obligations. Ultimately, the challenge is not merely technical but normative: balancing the pursuit of operational superiority through machine-speed decision-making with the enduring responsibility to uphold humanity in warfare.

References

Antal, J. (2022). *7 seconds to die: A military analysis of the Second Nagorno-Karabakh War and the future of warfighting.* Casemate Publishers.

Antal, J. (2023). *Next war: Reimagining how we fight.* Casemate Publishers.

Bellione, A. (2023). The heart of decision superiority: Evolve or lose – Why your war may be won or lost in seconds. *JAPCC Journal*, (36), 60–68. https://www.japcc.org/articles/the-heart-of-decision-superiority/

Bondar, K. (2025, March). *Ukraine's future vision and current capabilities for waging AI-enabled autonomous warfare.* Center for Strategic and International Studies (CSIS).

Brady, E. A. (2025, July). *Rethinking combined arms for modern warfare.* Atlantic Council.

Cares, J. R., & Cowden, A. (2021). *Fighting the fleet: Operational art and modern fleet combat.* Naval Institute Press.

Clark, B., Patt, D., & Schramm, H. (n.d.). *Mosaic warfare: Exploiting artificial intelligence and autonomous systems to implement decision-centric operations.* Center for Strategic and Budgetary Assessments (CSBA). https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations

Deeks, A. (2022). Coding the law of armed conflict. In M. C. Waxman & T. W. Oakley (Eds.), *The future of armed conflict* (pp. 41–59). Oxford University Press.

Galdorisi, G., & Tangredi, S. (2024). *Algorithms of Armageddon: The impact of artificial intelligence on future wars.* Naval Institute Press.

Horowitz, M. C. (2024, October). Battles of precise mass: Technology is remaking war – and America must adapt. *Foreign Affairs*. https://www.foreignaffairs.com/world/battles-precise-mass-technology-war-horowitz

Layton, P. (2021). *Fighting artificial intelligence battles: Operational concepts for future AI-enabled wars.* Australian Defence College. https://www.defence.gov.au/sites/default/files/research-publication/2021/JSPS_4.pdf

LeCun, Y., Bengio, Y., & Hinton, G. (2015, May). Deep learning. *Nature, 521,* 436–444. https://www.researchgate.net/publication/277411157_Deep_Learning

Lind, W. S. (2023). *The new maneuver warfare handbook.* Special Tactics Institute.

Margulies, P. (2019). The other side of autonomous weapons. In E. T. Jansen & R. T. P. Alcala (Eds.), *The impact of emerging technologies on the law of armed conflict* (pp. 147–173). Oxford University Press.

Michel, A. H. (2024, April). *Decisions, decisions, decisions: Computation and artificial intelligence in military decision-making.* International Committee of the Red Cross (ICRC). https://shop.icrc.org/download/ebook?sku=4757/002-ebook

U.S. Navy. (2024). *Chief of Naval Operations navigation plan 2024.* https://www.navy.mil/Portals/1/CNO/NAVPLAN2024/Files/CNO-NAVPLAN-2024-high-res-v2.pdf

Watts, S. (2019). Law-of-war precautions. In E. T. Jansen & R. T. P. Alcala (Eds.), *The impact of emerging technologies on the law of armed conflict* (pp. 100–145). Oxford University Press.

About the Author

Assoc. Prof. Bleda Kurtdarcan, Galatasaray University /
bledakurtdarcan[at]yahoo.com.tr / ORCID: 0000-0002-0202-3041

Bleda Kurtdarcan is an Associate Professor of Public International Law at Galatasaray University, School of Law. His areas of specialization include the law of armed conflict, the law of the sea, and maritime security law. He also teaches at the Turkish Naval War College and the NATO Maritime Security Center of Excellence (MARSEC COE). Dr. Kurtdarcan is the author of Submarine Operations in the Context of Intelligence Gathering at Sea and International Law (in Turkish, 2021), New Actors on the Battlefields: Military Contractors (in Turkish, 2017), and co-author of Future's Wars and Weapons (in Turkish, 2014).

Mapping Maritime Cybersecurity Research Using the NIST-CSF and Large Language Models

Assoc. Prof. Dr. Haydar Yalcin
Ege University, Türkiye

Assoc. Prof. Dr. Mürsel Doğrul
National Defence University, Türkiye

Abstract

This paper discusses the growing cybersecurity challenges in the maritime domain by applying the NIST Cybersecurity Framework (CSF) to evaluate the maturity of research and the extent to which it is strategically aligned. Using a dataset of 30,279 publications from Web of Science, the study identifies three key subdimensions (1) maritime cyber risk management, (2) ship cybersecurity and (3) transport system protection. These subdimensions are mapped across the CSF's core functions: Identify, Protect, Detect, Respond and Recover. Growth curve models (Fisher-Pry and Gompertz) reveal an uneven distribution of academic focus, with the 'Recover' function being particularly underrepresented. To enhance thematic insight, large language models (LLMs) were employed to classify and cluster maritime cybersecurity concepts. The findings reveal a strong focus on threat detection and prevention, but limited attention to recovery and resilience. This imbalance highlights the need for targeted investment and policy attention to ensure more comprehensive maritime cybersecurity strategies.

Keywords

Maritime Security, Cybersecurity, NIST Cybersecurity Framework, Cyber Resilience, Threat Detection, Large Language Models (LLMs), AI

Introduction

In the field of maritime security, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (2023) plays a critical role. This framework offers a flexible and comprehensive approach, assisting organizations in comprehending, managing, and mitigating their cyber risks. It also serves as an essential guide for stakeholders of all sizes aiming to bolster their maritime cybersecurity posture. As maritime operations become more reliant on interconnected digital systems, the number of threats to navigational safety, cargo logistics and port infrastructure has increased (Ayala et al., 2024). Contemporary maritime security approaches also emphasise the importance of integrated awareness systems, with AI playing a transformative role in domain awareness (Pohontu & Ermolai, 2024). This reflects a shift in maritime security from physical to cyber-physical risk domains (Bueger, 2015). Within this continually evolving threat landscape, characterized by complex cyber threats and risks in the maritime industry, the NIST-CSF furnishes a common language and structure, enabling organizations to appraise their existing security capabilities, prioritize risks, and formulate a roadmap for continuous improvement (Figure 1).

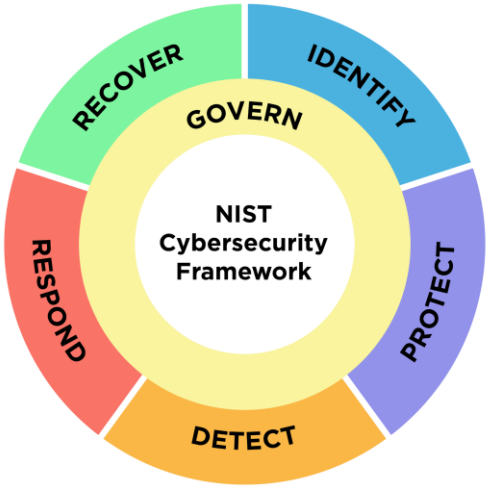

Figure 1
NIST Cybersecurity Framework

Comprising five core functions - Identify, Protect, Detect, Respond, and Recover - the NIST-CSF provides a holistic view of the cybersecurity lifecycle (Shen, 2014). These functions are vital in domains such as Maritime Security Operations (MSO Tasks) and Maritime Risks, as they foster a systematic consideration of every facet of an organization's cybersecurity programme. The framework's inherent flexibility stems from its capacity to operate in compliance with various security standards and best practices, exhibiting particularly strong potential to contribute to Maritime Security Capacity Building. The NIST-CSF is crucial for the maritime industry given that numerous maritime risks, including Piracy and Armed Robbery, Maritime Terrorism, Proliferation of Weapons of Mass Destruction, Transnational Organized Crime and Smuggling, and Irregular Migration, now possess cyber dimensions. In this respect, the escalating digitalization of ship systems has rendered navigation, communication, cargo management, and even engine control systems susceptible to cyber threats (Ben Farah et al. 2022; Shen, 2014; Svilicic et al., 2019).

A cyberattack not only violate the principle of Critical Infrastructure Protection (CI) but can also starts severe disruptions to maritime operations, navigational safety hazards, and substantial economic losses (Alcaide & Llave, 2020; Lehto, 2022; Svilicic et al., 2019).

The NIST-CSF offers a structured methodology for ship owners, operators, and port authorities to identify and protect against cyber risks, detect potential attacks, respond effectively, and promptly restore operations. The framework is adaptable, allowing for consideration of the unique risks and regulatory requirements pertinent to maritime operations, thereby assisting the industry in adhering to both national and international standards and establishing itself as an indispensable instrument for the maritime sector to attain its safety objectives.

Hypotheses and Analytical Framework

When examining the evolution of the maritime cybersecurity field, this study puts forward two guiding hypotheses that highlight significant gaps in academic attention and policy development.

Hypothesis-1: **'Academic research tends to focus more on detecting and preventing cyber threats than on recovering from them, possibly because recovery processes are more difficult to observe and document.'**

It reflects the fact that scholars have invested substantial effort in exploring how to stop attacks before they happen, but far less in how to recover when they do. The recovery phase is often complex, confidential and fragmented across institutions, which makes it less visible in the literature.

Hypothesis 2: **'Cyber recovery is often overlooked in strategic funding and policy agendas, leaving a critical gap in our collective ability to respond effectively to maritime cyber incidents.'**

Here, the concern is institutional. Although national strategies and international frameworks emphasise prevention, they rarely allocate the same level of resources to post-incident recovery. This can leave organisations underprepared when attacks occur, even if their defences were robust.

Data and Method

To understand the dynamics of knowledge in the field of maritime cybersecurity, we conducted a bibliometric analysis using the Web of Science (WoS), identifying publication trends across the NIST-CSF functions. We aimed to evaluate the maturity (saturation) of subfields and predict future research requirements. We analysed publications containing keywords such as 'cybersecurity' and 'cyber security', excluding retractions and corrections to ensure accuracy. In addition, document types such as "Retraction", "Correction" or "Retracted Publication" were omitted from the results to ensure that only original and verified research was included in the analysis.

To test the hypotheses, we used growth curve modelling techniques with the Fisher-Pry and Gompertz models on cumulative publication data obtained from WoS. These models were used to evaluate research maturity across the five core functions of the NIST-CSF: Identify, Protect, Detect, Respond and Recover. The Fisher-Pry model, which is usually employed to analyse technological adoption over time, enabled us to evaluate sigmoid-shaped growth patterns associated with the initial, rapid and saturated stages of research development (Fisher & Pry, 1971). Meanwhile, the Gompertz model, which is widely used to forecast processes that slow over time, helped us to determine whether publication trends had reached or were approaching saturation (Gompertz, 1825; Winsor, 1932).

The high R^2 values observed for the Identify, Protect, Detect and Respond functions (0.99–1.00) confirmed a strong model fit and research maturity. However, the Recover function displayed stagnation with missing or statistically invalid curve fits (e.g. NaN values), indicating underrepresentation and supporting both Hypotheses H1 and H2. These results quantitatively confirm that, despite its growing importance to maritime resilience, academic and strategic attention has lagged in the domain of post-incident recovery.

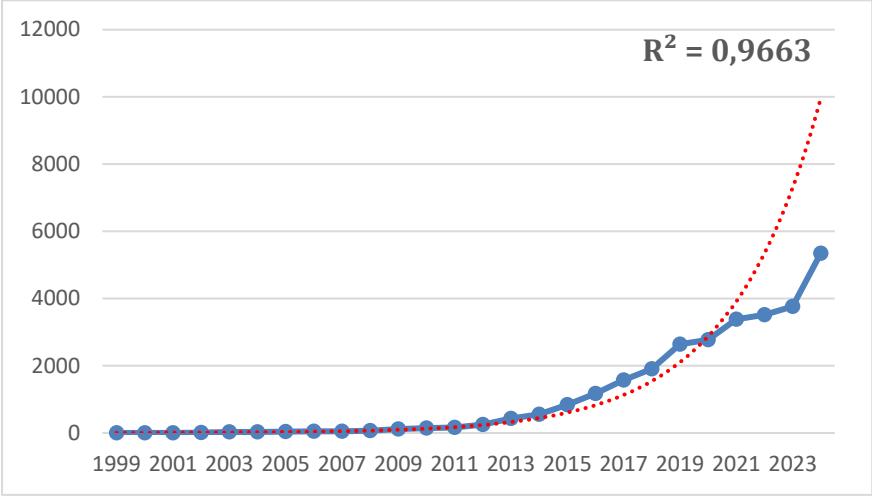

Figure 2
Annual Literature Growth of Cybersecurity Research

This graph, reached in the growth curve analysis, indicates that research in the field of cyber security is growing at an increasing rate, not at a constant rate (Figure 2). There is a greater increase in the relevant literature in each passing period compared to the previous period. In the context of Cyber Security, this indicating research activities in the field, emerging threats or awareness on this issue have increased rapidly in recent years.

By modeling the cumulative publication trends of the NIST-CSF functions, strategic inferences about the dynamics of knowledge production and maturation in the field of cybersecurity are aimed. In this framework, it is aimed to provide a perspective on current resource allocation and future research focus areas, especially for decision makers. Figure 3 clearly reveals that there is a stable and strong "S-curve" growth in the basic CSF functions such as "Identify", "Protect", "Detect" and "Respond". The high degree of concordance of the Fisher-Pry and Gompertz models in these areas (R^2=0.99−1.00) indicates that these issues have undergone extensive adoption and in-depth review processes in the cybersecurity literature. This is important as it indicates that the industry is continuously increasing its capabilities to recognize threats, develop protective measures, and detect and respond to cyber incidents. However, the apparent stagnation of the "Recover" function observed in cumulative publications points to a critical gap. The lack of data or the inability to model this function can be interpreted as the lack of academic and industrial interest in the rapid and effective restoration of systems and operations after a cyber-attack compared to other functions. Given the fact that cyber incidents are inevitable, this

creates a potential vulnerability in terms of the cyber resilience of organizations and national infrastructures. This finding is in line with those of Radanliev et al. (2020), who state that resilience is frequently the most underdeveloped pillar in cyber-physical systems. It should be recognized that this is an area that urgently needs to be strengthened through research funding and collaborative projects. The cascading growth pattern in the "govern" function, on the other hand, is remarkable in that it shows that cyber security governance, policy and compliance issues follow a unique development path. While this highlights the slow but steady maturation of regulatory and institutional frameworks over time, it shows that strengthening cybersecurity culture and institutional structures is just as important as technological solutions. It should be taken into account that advances in this area can often be triggered by landmark regulations.

As a result of the analysis, it can be recommended for decision-makers to prioritize research and development investments for the "Recover" function, to continue to use the existing knowledge in the core functions, and to fully evaluate the structural benefits of the "Govern" function while determining their cyber security strategies.

This method allows for the systematic mapping of the research field. In light of the importance of institutional policies such as the IMO Guidelines (2022) and the U.S. Maritime Cybersecurity Plan (The White House, 2022), our bibliometric model helps to bridge the gap between regulatory priorities and academic focus. The analysis also supports NATO's focus on protecting technology and infrastructure (Fridbertsson, 2023).

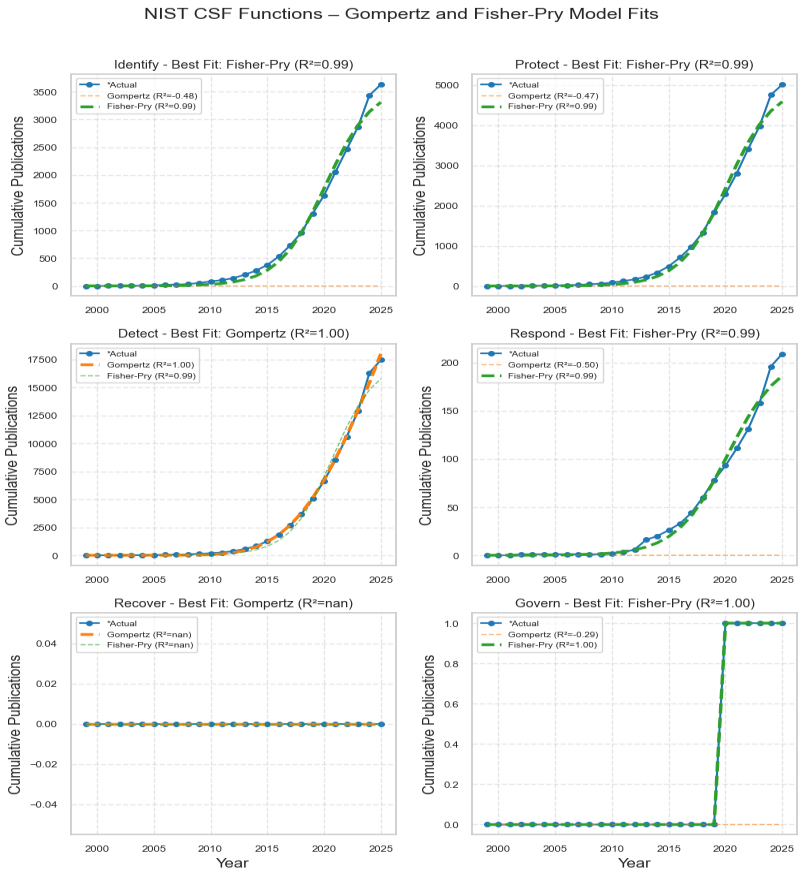

Figure 3
Growth Curves Comparisons

In this section, where we aim to provide actionable inferences by modeling cumulative publication trends in critical sub-dimensions of maritime cyber security (such as Threat Intelligence, Port Security, Cyber Resilience, Maritime Cyber Security and Supply Chain Security, etc.), it is possible to say that we have reached important indicators regarding the current knowledge production and future strategic trends in the sector. A closer examination of Figure 4 reveals a consistent and significant increase in publications across all sub-dimensions until 2024. However, it shows that the precipitous decline in 2025 should be considered (Figure 4).

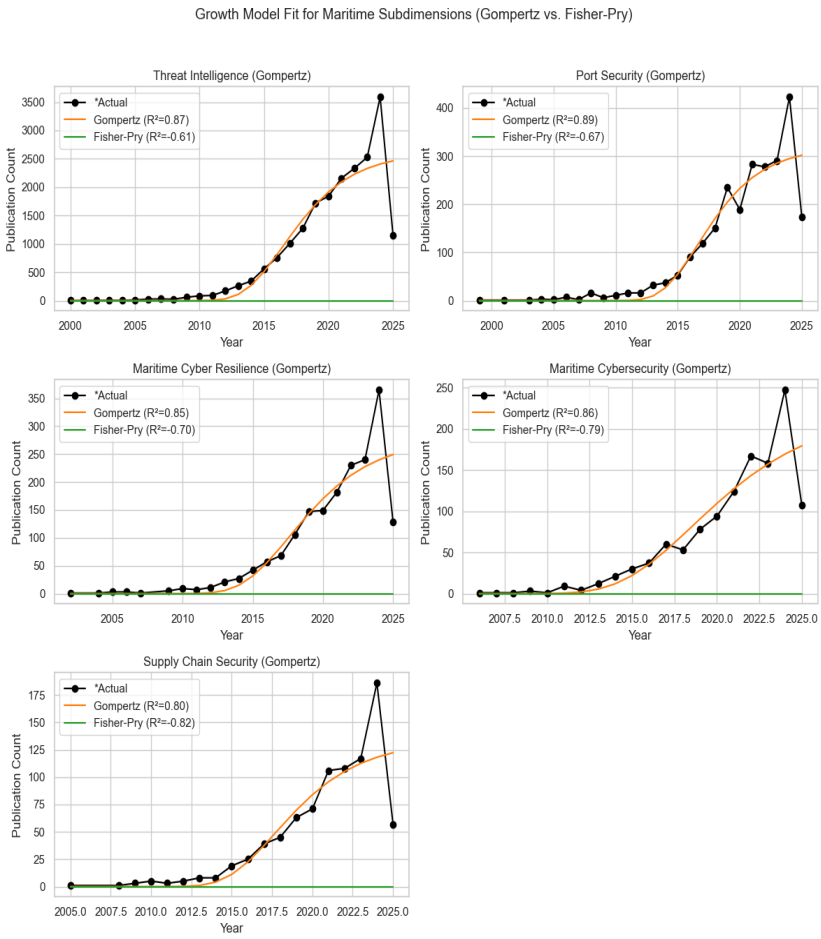

Figure 4

Growth Model Fit for Maritime Subdimensons (Gompertz vs. Fisher - Pry)

In most sub-dimensions, the Gompertz model fits better with higher R2 values than the Fisher-Pry model, indicating that the diffusion of knowledge in these areas has reached a certain level of maturity and that the growth rate tends to slow down but has not yet reached full saturation. Areas such as Threat Intelligence, Port Security, and general Maritime Cybersecurity have gained an important place in the literature and have provided a comprehensive knowledge of basic concepts and applications. This highlights the need to focus on integrating existing knowledge and experience in these key areas into operational processes. Areas such as Maritime Cyber Resilience and Supply Chain Security exhibit similar growth trends, reflecting the growing importance of resilience to cyberattacks and securing supply chains.

For decision-makers, this is an important indicator that risk mitigation efforts should not be limited to technological protections but should also be extended to operational resilience and complex supply chain structures (Prodan, 2017; World Economic Forum, 2024). Knowledge in emerging areas such as threat intelligence and port security should be used effectively to strengthen national and international maritime policies and standards. Focus on Resilience and Supply Chain: Maritime cyber resilience and supply chain security should be further emphasized in strategic planning and research and dissemination of best practices in these areas should be encouraged. The launch of dedicated tracking systems, such as the Maritime Cyber Attack Database (Smart Maritime Network, 2023), illustrates the sector's shift towards data-driven threat intelligence and responsive policy. This growing institutional engagement should be matched by academic rigour in emerging topics such as maritime AI governance and hybrid security threats (Fenton, 2024).

Analysis of LLM-Supported Classification Results and Research Gaps in Maritime Cybersecurity

Trends and Strengths

The Anomaly Detection sub-dimension is notable for its prominence in terms of both content volume - as reflected by the 8,013 documents - and alignment with the 'Detect' function of the NIST-CSF. Meanwhile, Asset Management and Identification & Analysis are well represented under the 'Identify' function, indicating significant research into risk identification and inventory mapping.

Access Control and Data Security also emerge as critical focus areas within the 'Protect' function, revealing that much scholarly attention has centred on defence-oriented strategies and proactive risk mitigation. These patterns highlight the depth of academic engagement in identifying and preventing cyber threats in the maritime domain.

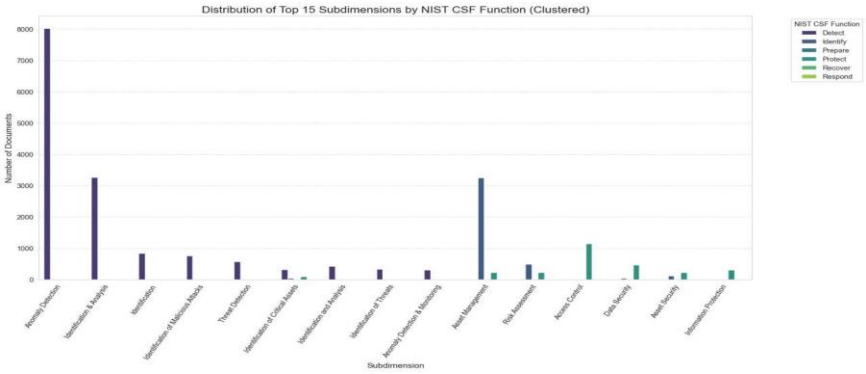

Figure 5
Subdimensions of Cybersecurity

Theme Analysis

Examining the most frequent terms derived from LLM-generated word clouds offers deeper insight into the conceptual landscape of maritime cybersecurity. Recurring expressions such as 'vulnerabilities', 'threat detection', 'risk assessment', 'artificial intelligence', 'cyber warfare', and 'supply chain' suggest that the literature has increasingly recognised the sector's multidimensional threat environment (Figure 6).

However, despite this thematic diversity, there is a notable absence of terminology directly linked to recovery processes, organisational resilience or continuity planning, which further reinforces the concerns raised in the hypothesis section.

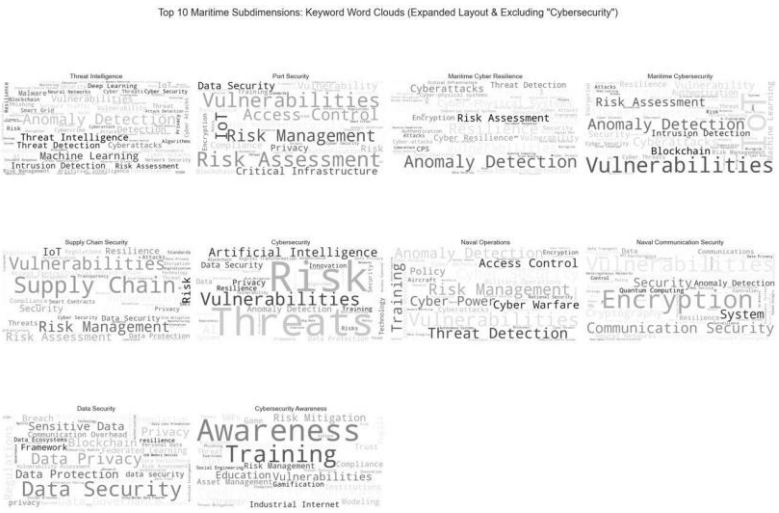

Figure 6
Themes on Cybersecurity Subdimensions

Figure 6 presents a thematic analysis that reveals several critical concerns shaping the discourse on maritime cybersecurity. One of the most prominent themes is the disparity between civil and military maritime infrastructures, which indicates that there are uneven levels of protection, resources and preparedness across sectors. This disparity creates strategic vulnerabilities, particularly in regions where civilian ports have less stringent cybersecurity protocols than naval or defence-related entities. Furthermore, the analysis highlights the urgent need to protect IoT systems and other critical infrastructure connections that form the digital backbone of maritime operations. As vessels and port systems become more interconnected, they become more exposed to cyber threats. Finally, the themes reflect a growing scholarly and practical interest in emerging technologies such as AI and blockchain. These tools are increasingly being recognised as vital for advancing threat detection, data integrity and automation in maritime cybersecurity, providing scalable and adaptive solutions for the complex threat landscape.

Research Gaps

The analysis highlights several critical gaps and strategic priorities. Firstly, AI-enabled cyber incident response doctrines specifically tailored for maritime operations need to be developed (Pohontu & Ermolai, 2024). Secondly, scenario-based recovery drills involving joint civil-military coordination remain under-utilised and should be prioritised (Ayala et al., 2024).

Thirdly, due to the stagnation of the 'Recover' function in terms of both bibliometric trends and thematic presence, targeted research funding should be allocated to resilience frameworks (see Figure 3). Finally, legal and institutional barriers to real-time data sharing across maritime security networks, especially in multinational contexts, deserve focused investigation and policy resolution (Fridbertsson, 2023).

Conclusion

This paper offered a comprehensive contribution to the field by highlighting the disparity in academic interest across the core NIST-CSF functions, with a particular focus on the underdevelopment of the 'Recover' function. Using bibliometric mapping, we reveal the maturity levels of cybersecurity research in various maritime sub-domains, providing insights that are directly relevant to academic agendas and policy formulation.

Drawing on strategic frameworks such as the NIST Cybersecurity Framework, IMO guidelines, and NATO directives, the study addresses the ongoing discrepancy between scholarly literature and practical policy imperatives. It emphasizes the need for targeted investment in recovery, incident response and preparedness to support the cyber resilience goals of NATO and allied maritime strategies. By offering actionable guidance, this research paves the way for a new wave of maritime cybersecurity resilience initiatives.

References

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554.

Ayala, M., Dely, J., & Plankey, S. (2024, October). General quarters! Cybersecurity challenges in the maritime industry [White paper]. SANS Institute. https://www.sans.org/white-papers/general-quarters-cybersecurity-challenges-maritime-industry/

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. Information, 13(1), 22.

Bueger, C. (2015). What is maritime security? Marine Policy, 53, 159–164. https://doi.org/10.1016/j.marpol.2014.12.005

Fenton, A. J. (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(3), 510. https://doi.org/10.3390/jmse12030510

Fisher, J. C., & Pry, R. H. (1971). A simple substitution model of technological change. Technological Forecasting and Social Change, 3(1), 75–88. https://doi.org/10.1016/S0040-1625(71)80005-7

Fridbertsson, N. T. (2023, October 7). Protecting critical maritime infrastructure – The role of technology: General report (No. 032 STC). NATO Parliamentary Assembly. https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc

Gompertz, B. (1825). On the nature of the function expressive of the law of human mortality. Philosophical Transactions of the Royal Society of London, 115, 513–585. https://doi.org/10.1098/rstl.1825.0026

International Maritime Organization. (2022, June). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.2). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Springer.

National Institute of Standards and Technology. (2023). Cybersecurity framework profile for hybrid satellite networks (HSN) (NIST CSWP 29). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Pohontu, A., & Ermolai, V. (2024). Artificial intelligence in maritime domain awareness applications: Trends and prospects. In L. Ivascu, L. I. Cioca, B. Doina, & F. G. Filip (Eds.), Digital transformation (Vol. 257, Intelligent Systems Reference Library). Springer. https://doi.org/10.1007/978-3-031-63337-9_10

Prodan, T. (2017). Maritime terrorism and resilience of maritime critical infrastructures. National Security and the Future, 18(1–2), 101–122. https://hrcak.srce.hr/file/279404

Radanliev, P., De Roure, D., Burnap, P., Santos, O., Ani, U., & Nurse, J. R. C. (2020). Artificial intelligence in cyber physical systems. Internet of Things, 9, 100204. https://doi.org/10.1016/j.iot.2020.100204

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. Scitech Lawyer, 10(4), 16.

Smart Maritime Network. (2023, July 16). Maritime cyber attack database launched. https://smartmaritimenetwork.com/2023/07/16/maritime-cyber-attack-database-launched/

Stoll, H. (2023, May 25). Navigating complex maritime security challenges in the Black and Mediterranean Seas: Insights from the updated EUMSS [Commentary]. RAND Corporation. https://www.rand.org/pubs/commentary/2023/05/navigating-complex-maritime-security-challenges-in.html

Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A study on cyber security threats in a shipboard integrated navigational system. Journal of marine science and engineering, 7(10), 364.

The White House. (2022, December). National Maritime Cybersecurity Plan to the National Strategy for Maritime Security. https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf

Winsor, C. P. (1932). The Gompertz Curve as a Growth Curve. Proceedings of the National Academy of Sciences, 18(1), 1–8. https://doi.org/10.1073/pnas.18.1.1

World Economic Forum. (2024). Navigating cyber resilience in the age of emerging technologies: Collaborative solutions for complex challenges. https://www.weforum.org/publications/navigating-cyber-resilience-in-the-age-of-emerging-technologies-collaborative-solutions-for-complex-challenges

About the Authors

Assoc. Prof. Dr. Haydar YALÇIN / Ege University, Türkiye / haydar.yalcin[at]ege.edu.tr / ORCID: 0000-0002-5233-2141

Assoc. Prof. Dr. Haydar Yalçın serves as the Head of the Management Information Systems Department at the Faculty of Economics and Administrative Sciences, Ege University. With a focus on interdisciplinary contributions, Dr. Yalçın has authored influential works such as "Technology Mining in Artificial Intelligence Manufacturing" and "Predicting Technological Positioning with Patent Citation Analysis in IoT, Cybersecurity, and Blockchain: Excessive Technology Knowledge". As a member of the Omega Rho International Honor Society at Portland State University, Dr. Yalçın's academic career is marked by significant cross-disciplinary achievements. He has also held the position of Visiting Scientist at the Department of Engineering and Technology Management at Portland State University and contributed to the institution's Mark O. Hatfield Cybersecurity and Cyber Defense Policy Center. His research in science management, technology forecasting, and data analytics, Dr. Yalçın actively mentors students to foster academic excellence. His international research initiatives include the "Technology Monitoring and Forecasting for Quantum Technologies: A Scientific Measurement Approach" and "Technology Monitoring and Forecasting for Cyber Defense: A Scientific Measurement Approach", supported by armasuisse, the Swiss Federal Department of Defense. Furthermore, he serves as the Country Director for the NATO SPS-supported project "Pathways for Infrastructure Resilience in Ukraine", which underscores his ongoing contributions to cybersecurity and next-generation security technologies.

Assoc. Prof. Dr. Mürsel DOĞRUL / National Defence University, Türkiye / mursel.dogrul[at]msu.edu.tr / ORCID: 0000-0002-0637-843X

Dr. Mürsel Doğrul is an Assoc. Professor at the National Defence University, specializing in International Relations. He earned his degree in International Relations from Bolu Abant İzzet Baysal University in 2014, conducting research in Romania, Spain, and Ukraine during his undergraduate and postgraduate studies. In 2013, Dr. Doğrul completed internships at the Ministry of EU Affairs and the Ministry of Foreign Affairs of Türkiye. He obtained an M.Sc. degree in International Relations from Necmettin Erbakan University, focusing on the "Counterterrorism Policy of Japan," and completed his Ph.D. at the National Defence University in 2021, researching "The Middle East in Japanese Foreign Policy: Political Economy of Energy." As a Japan Foundation Fellow, he was a visiting scholar at Meiji University in 2023 and an Erasmus Fellow at Tokyo University in 2024. His research interests encompass Japanese foreign policy, energy policy, and security. Dr. Doğrul has made significant contributions to the field through academic works, examining the evolving dynamics of international security and international relations literature. Dr. Dogrul has made significant contributions to the field of global security and international relations through his academic work examining their evolving dynamics. He is currently President of the Turkish Young Academy.

PART II

Combatting Traditional Maritime Security Threats Summary Report

Dr. Felicity G. Attard
University of Malta

Abstract

This panel report examines evolving traditional maritime security threats through four major themes: narcotics precursor trafficking, politically motivated attacks in the Red Sea, narcotics smuggling in the Indian Ocean and shifting global piracy patterns. Experts highlighted the dual role of technological innovation, which offers enhanced enforcement capabilities while simultaneously enabling criminal adaptation. Persistent legal ambiguities, particularly concerning piracy and politically motivated violence, complicate effective responses. Panelists emphasised the vital role of international cooperation, technological investment and industry partnerships in addressing these challenges. The discussion addressed the human dimension of maritime security and the need to address underlying socio-economic drivers. The report concludes that safeguarding maritime security requires a holistic approach which integrates legal reform, technological innovation, coordinated enforcement and socio-economic development to build resilience against rapidly changing maritime security changes.

Keywords

Maritime Security, law, technological innovation, international cooperation, piracy, narcotics trafficking

Introduction

This is a summary of the proceedings conducted in the panel which discussed the combatting of traditional maritime security threats at the 5th Maritime Security Conference, held at the Maritime Security Centre of Excellence in Istanbul (24–25 June 2025). The panel was composed of the following: Dr. Felicity G. Attard (moderator), Senior Lecturer, Department of International Law at the University of Malta; Mr. Antonio Mazzitelli, Chief of the Precursors Control Section at the Secretariat of the International Narcotic Control Board of the United Nations; Dr. Murat Sümer, Nippon Foundation Lecturer, IMO International Maritime Law Institute; Dr. Muhammad Rafi Khan, Assistant Professor, Minhaj University Lahore, Pakistan; and Ms. Aysel Çamci, Istanbul Technical University.

The distinguished speakers offered complementary perspectives on different but interconnected security threats: the illicit manufacturing and trafficking of drug precursors; threats to freedom of navigation in the Red Sea; the fight against narcotics smuggling in the Indian Ocean and shifting patterns of maritime piracy. Each speaker drew attention to the evolving nature of maritime security threats in an age of globalisation, technological advancements and increasing geopolitical tensions.

The panel emphasised several overarching themes. First, technological innovation, ranging from artificial intelligence to satellite monitoring, presents both new opportunities for enforcement and new avenues for criminal adaptation. Second, legal ambiguities and lacunae continue to hamper effective responses, particularly where the lines between piracy, armed robbery and terrorism overlap. Third, international cooperation, including the role of regional organisations, industry actors and multilateral conventions, remains the foundation of effective maritime governance. Finally, the human dimension, whether the safety of seafarers or the resilience of coastal societies, remains central to effective maritime security.

A Comprehensive Approach to Prevent Illicit Drug Manufacture

The opening presentation by Mr. Mazzitelli offered an interesting and detailed overview of international challenges posed by the use of chemicals and equipment for the illicit manufacture of drugs. As a treaty-mandated body established under the UN drug control conventions of 1961, 1971, and 1988, the International Narcotics Control Board (INCB) plays an important role in balancing legitimate industrial and pharmaceutical needs against the imperative of preventing diversion into criminal supply chains.

Mr. Mazzitelli highlighted the rapid proliferation of non-scheduled chemicals, including “designer precursors” which were created specifically for drug manufacture and lacking any legitimate use. Over the past decade, at least ten such substances have been identified and added to the international control tables, while more continue to circulate outside the existing regulatory framework.

The availability of proper equipment is an equally critical element. Mr. Mazzitelli noted that Article 13 of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances recognises that illicit production cannot occur without access to reactors, presses and other specialised apparatus. Recent years have seen seizures not only of synthetic opioids, such as fentanyl, but also counterfeit pharmaceuticals, including tramadol and benzodiazepines, often produced with diverted or substitute equipment.

Mr. Mazzitelli noted that the INCB has developed mechanisms to enhance transparency and cooperation. These include:

a) PEN Online which is a global system enabling competent national authorities to exchange pre-export notifications of scheduled chemicals. Since its launch in 2006, over half a million notifications have been processed. A recent success involved the interception of three tonnes of fentanyl precursor, preventing potential production of up to 3.3 tonnes of the drug.

b) PEN Online Light which was introduced in 2022 to cover chemicals not formally listed under the 1988 Vienna Convention on Drugs but subject to national controls. By 2024, over 2,400 “light” notifications had been exchanged, covering nearly 4 million litres of chemicals.

c) PICS (Precursors Incident Communication System) launched in 2012, providing secure real-time sharing of incident data. By 2024, over 5,600 incidents had been reported, supporting cross-border investigations.

Furthermore, he explained that INCB also engages with industry actors through Know Your Client principles, mapping supply chains across sectors such as pharmaceuticals, chemicals and logistics. More recently, it has turned its attention to virtual marketplaces, monitoring over 50 online platforms through the AMVICHEM tool to detect suspicious postings.

Mr. Mazzitelli concluded that while the scheduling of substances remains essential, a purely legal approach is insufficient. Criminal entrepreneurs rapidly shift to new precursors or equipment sources. He advocated a proactive, integrated strategy including legal controls, trade monitoring, real-time information sharing and industry cooperation. This approach is required to safeguard legitimate markets and limit opportunities for diversion.

Protection of Navigational Rights in the Red Sea

Dr. Sümer addressed a pressing contemporary crisis in global shipping: the attacks by Houthi forces against international shipping in the Red Sea. This sea is a critical maritime route, carrying around 15% of global trade between Asia, Europe, and the Atlantic. Disruptions such as the Ever Given blockage in the Suez Canal, the wider fallout from COVID-19 and current attacks have significant effects on international commerce and trade.

Since late 2023, the Houthis, a non-state armed group in Yemen, have escalated their campaign of targeting merchant vessels. The seizure of the Galaxy Leader and its 25-member crew, ongoing drone and missile strikes, and the use of unmanned boats represent a different level of threat when compared to "classic" piracy. Unlike pirates, the Houthis operate as a quasi-state entity with military-grade capabilities.

Dr. Sümer explored whether such attacks can be categorised as piracy, armed robbery, or as unlawful acts endangering safe navigation under the 1988 SUA Convention. In his discussion, Dr. Sümer addressed definitional issues including:

a) The "private ends" requirement in the UNCLOS definition of piracy, which Houthis arguably do not meet, as their actions are politically motivated.

b) The two-ship requirement, which raises questions where drones or unmanned boats are used.

c) The jurisdictional element, as many attacks occur within or near Yemeni waters.

Dr. Sümer argued that the nature, scale and sophistication of Houthi attacks mean that it is difficult to consider them as piracy under the generally accepted definition found in UNCLOS. Instead, they blur the line between non-international armed conflict and transnational crime, complicating both military and legal responses. Beyond legal debate, the attacks have direct economic and environmental consequences. Ships have been forced to reroute around the Cape of Good Hope, increasing operational costs, delivery times, emissions, and insurance premiums. The crisis demonstrates the fragility of global maritime supply chains and the need for renewed commitment to defending freedom of navigation as a fundamental principle of the rule of law at sea.

Seaborne Narcotics: Mapping the Maritime Drug Trade in the Indian Ocean and its Security Implications

Professor Khan focused on the Indian Ocean as a major corridor for narcotics trafficking, particularly heroin originating from Afghanistan and synthetic drugs transiting from Iran and Southeast Asia.

He explained that dhows departing from the Makran coast of Pakistan and Iran were identified as the main method of transportation, blending into legitimate fishing and trade fleets. He noted that traffickers exploit the sheer size of the Indian Ocean, weak maritime domain awareness, and fragmented national enforcement regimes. Vessels often disable their Automatic Identification System transponders or operate as "dark ships".

Drawing from case studies such as the Afghanistan–Pakistan corridor, Professor Khan's intervention emphasised five key findings:

1. The importance of maritime technology e.g., AI, radar, and satellite constellations have significantly improved detection, with naval forces such as India's INS Tarkash and Pakistan's PNS Zulfiqar undertaking successful interdictions.
2. The need for deeper international cooperation. Platforms such as the Combined Task Force 150, the Indian Ocean Forum, and the Southern Route Partnership have enhanced joint patrols, training, and intelligence sharing.
3. Evolving evasive tactics. Despite advances, traffickers adapt quickly, using dhows and disabling AIS to mask operations.
4. Crime–terror nexus. Profits from drug smuggling fund extremist groups in the Maldives, Sri Lanka, and beyond, undermining State stability.
5. Underused innovations, in particular, blockchain and unmanned surface vessels hold promise for traceability and monitoring, however high costs and capacity gaps limit adoption.

Professor Khan concluded that maritime drug trade is not merely a law-enforcement problem. It undermines sovereignty, fuels terrorism and corruption, and erodes governance in fragile coastal States. He concluded that an integrated strategy which includes combining technology, legal reform and sustained cooperation can effectively combat the maritime drug trade.

Piracy in Flux: Analyzing Global Trends and Future Forecasts

The final presentation was delivered by Ms. Aysel Çamci, wherein she examined the shifting patterns of maritime piracy. Her presentation combined statistical trend analysis with political and socio-economic interpretation. The research, based on five years of International Maritime Organization (IMO) reports, sought to forecast piracy trajectories using quantitative models and the PESTEL framework (Political, Economic, Social, Technological, Environmental, Legal).

The study documented continued high levels of piracy in strategic chokepoints such as:

a) Malacca Strait: 43 incidents in 2024, mostly opportunistic armed robbery.
b) Gulf of Guinea: a decline from 81 incidents in 2020 to 18 in 2024, but still the epicentre of the most dangerous attacks involving kidnapping and ransom.
c) East Africa/Somalia: only eight incidents in 2024, but periodic hijackings indicate potential resurgence.
d) South China Sea and West Africa: fluctuating but persistent activity.

A particularly concerning finding was the divergence between rising vessel boarding incidents and declining rates of authority intervention, suggesting overstretched enforcement capacity. Furthermore, the PESTEL analysis revealed multi-dimensional causes of piracy which include:

a) Economic: poverty, declining fisheries and limited investment in coastal economies.
b) Social: weak legitimacy of governments, low education and in some cases a romanticised local image of piracy.
c) Environmental: vast maritime zones make patrols difficult; climate change pressures exacerbate resource scarcity.
d) Legal: inconsistent enforcement of UNCLOS provisions and differing national frameworks.

Ms. Çamci emphasised that piracy is not merely a maritime crime but a symptom of broader governance failures. She noted that effective strategies must go beyond naval patrols to include socio-economic development, legal harmonisation, capacity building, and international cooperation. Responses must be holistic rather than reactive.

Conclusion

Dr Felicity G. Attard, the moderator, congratulated the panelists for their illuminating presentations. In her view, a number of common themes emerged. First, the adaptability of illicit actors was emphasised, whether in the form of pirates shifting from hijacking to armed robbery, traffickers exploiting non-scheduled chemicals, or insurgents deploying drones, all of which demonstrate that criminals consistently innovate faster than regulators and enforcers. Second, technology was described as a double-edged sword: while artificial intelligence, satellites and blockchain offer transformative potential, they also demand significant investment, interoperability and political will, even as criminals exploit virtual markets and digital tools for concealment. Third, legal ambiguities remain a persistent obstacle, from the definitional challenges of piracy under UNCLOS to the limited scope of the 1988 Vienna Convention on Drugs in addressing precursors, with gaps in international law often complicating responses or enabling impunity. Fourth, the immense human and economic costs of maritime crime were underscored, with piracy and drug trafficking resulting in seafarers being held hostage or attacked, alongside broader ripple effects on insurance, emissions and global supply chains. Finally, the discussion converged on the need for holistic and cooperative approaches: maritime crimes cannot be countered solely through military or policing measures, but instead require sustainable partnerships involving States, regional organisations, international institutions and the private sector.

The moderator noted that the panelists converged on a number of key outcomes. They emphasised the need to enhance international legal regimes to address politically motivated maritime violence, the challenges posed by emerging synthetic drug precursors, and jurisdictional gaps in piracy enforcement. Strengthening maritime domain awareness was also highlighted, with investment in artificial intelligence, satellite coverage and data-sharing platforms seen as essential for proactive monitoring. The discussion further underscored the value of expanding regional cooperation, with multilateral task forces and information-sharing mechanisms, from the Gulf of Guinea to the Indian Ocean, identified as models to build upon. Equally, the integration of industry and technology providers was recognised as vital, with partnerships involving chemical producers, shipping companies and satellite operators helping to safeguard legitimate trade and monitor illicit activity. Finally, the panel drew attention to the importance of addressing root causes, stressing socio-economic interventions such as investment in coastal livelihoods, education and governance reform as critical to reducing vulnerability to piracy.

Dr. Attard concluded by observing that the panelists' presentations offered a realistic yet forward-looking assessment of the problems relating to traditional threats to maritime security. Whether in the form of narcotics trafficking, piracy, or politically motivated attacks, threats at sea remain dynamic, adaptive and interconnected with global governance challenges. The presentations also offered avenues for progress: harnessing technology responsibly, strengthening legal regimes, and fostering stronger networks of cooperation between States, industry, and international organisations. Ultimately, maritime security is not only about protecting ships and cargo. It concerns safeguarding human security, freedom of navigation and lawful commerce. The insights of the panelists, she opined, provide valuable strategies and proposals for building a more resilient and secure maritime future.

About the Author

Dr. Felicity G. Attard / Univeristy of Malta / felicity.attard[at]um.edu.mt / ORCID: 0000-0003-3383-9104

Dr. Attard is a Senior Lecturer at the University of Malta, where she teaches and coordinates courses in international law, the law of the sea and maritime security law. She has lectured at a number of universities and institutes, including the Centre for Commercial Law Studies at the University of London, the International Ocean Institute, Harvard Law School and the IMO International Maritime Law Institute. Dr. Attard has presented papers on international law subjects at conferences held throughout the world. Dr. Attard is the author of the monograph 'The Duty of the Shipmaster to Render Assistance at Sea under International Law' published by Brill. She is continuously publishing research in journals and collected works. She is often invited by the international media, including the BBC, Agence France-Press, and the National to comment on international law issues. Dr. Attard is the President of the Malta Branch of the International Law Association.

Protection of Navigational Rights in the Red Sea: Legal Classification of Houthi Attacks under International Maritime Law

Dr. Murat Sümer
IMO International Maritime Law Institute, Malta

Abstract

This paper explores the legal classification of recent Houthi attacks on commercial shipping in the Red Sea under international maritime law from the lens of piracy, armed robbery at sea, privateering, maritime terrorism and unlawful acts at sea. In this respect, this study highlights the difficulty of addressing evolving hybrid maritime threats, particularly where such actors operate with quasi-State capacities, with existing peacetime maritime law instruments. The study further considers institutional responses by the International Maritime Organization (IMO) and United Nations Security Council (UNSC). In this respect, it underscores the caution underpinning their relative silence in legally characterizing the Houthi attacks. It concludes that the current Red Sea crisis calls for renewed doctrinal clarity to uphold well established navigational rights. Finally, the present study also highlights the importance of upholding the rules based international maritime order for the benefit of all and the preventing the reemergence of privateering in its various forms.

Keywords

Freedom of Navigation, Red Sea, Privateering, UNCLOS, IMO

Introduction

The Red Sea's strategic relevance rests on its dual chokepoints: the Bab al-Mandab Strait and the Suez Canal, which account for approximately 15 % of global trade. Since late 2023, the Houthis have launched numerous indiscriminate attacks against international shipping in the Red Sea. This renewed insecurity in the Red Sea has significantly disrupted global shipping, compounding earlier significant shocks stemming from the COVID-19 pandemic, climate-induced constraints on the Panama Canal, and the ongoing war in Ukraine. The security threats in the Red Sea led to major shift in global shipping. With an increasing number of vessels rerouting via the Cape of Good Hope, transit times on the Asia–Europe have lengthened by up to ten days. Naturally, this led to reducing overall shipping capacity and escalating freight and insurance costs. Moreover, higher vessel speeds to compensate for longer detours have significantly increased fuel consumption and emissions (Dominguez, 2024; House of Commons, 2025; House of Representatives, 2025; IMO, 2024; Kraska, 2024; Pedrozo, 2024; UN, 2024; UNCTAD, 2024; US Congress, 2024).

Materials And Methods

This study adopts a doctrinal legal methodology in the interpretation and analysis of present international maritime law instruments. It investigates the legal classification of Houthi attacks on commercial shipping in the Red Sea by assessing their compatibility with established legal frameworks. Given the scope and structure of the present inquiry, this study does not engage with the law of naval warfare, which, while relevant in certain contexts, certainly merits separate and dedicated examination.

The paper suffices to focus on primary instruments such as the United Nations Convention on the Law of the Sea (UNCLOS, 1982); the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention, 1988) and its Protocol (IMO, 2005), relevant IMO and UNSC resolutions. Secondary materials include scholarly commentary, doctrinal writings, and institutional reports that elucidate the evolving legal treatment of asymmetric maritime threats.

Discussion on Legal Framework

First of all, to put the things into context it may be important to note that the Houthis are essentially a non-state entity engaged in non-international armed conflict (NIAC) against the recognised government of Yemen. Therefore, in essence, the situation in Yemen since late 2014 constitutes a form of insurgency in the form of non-international armed conflict (NIAC). Notably, the Houthis exercise territorial control including the capital of the country and the major portion of the west coastline. Besides, they provide administrative services to the population under their authority.

The fact that the impact of their current attacks extends beyond Yemen does not alter the classification of the conflict as a NIAC, given that the Houthis remain a non-State actor. Having said that, theoretically, if a third State were found to be providing substantial support to the Houthis, extending beyond the mere provision of arms to include direct operational control or joint armed action, that supporting State could, in principle, be regarded as a party to an international armed conflict (IAC), though this would not extend to the Houthis themselves. It should be emphasised, however, that the threshold for establishing co-belligerency under international law is notably very high.

The law of the sea constitutes a coherent body of rules regulating activities in and concerning the oceans. As a framework convention, UNCLOS establishes universally applicable standards for maritime safety, security, and environmental protection, implemented through coastal, flag, and port State jurisdictions. In this respect, the Convention governs maritime zones and sets out navigational rights depending on the maritime area concerned (Sümer, 2023). What we face today is not just significant disruption to global shipping, but a direct challenge to the fundamental navigational freedoms. Given the Red Sea's semi enclosed status multiple navigational regimes apply for instance innocent passage through territorial seas, transit passage through Bab al-Mandab Strait, and freedom of navigation in exclusive economic zones. On the other hand, the broader issues, such as the lawful use of force or self-defence in the maritime domain, fall within the scope of general international law, international humanitarian law, and the law of naval warfare rather than UNCLOS as the latter is primarily peacetime instrument.

Evidently, targeting civilian merchant vessels, irrespective of motives, constitutes flagrant violation of international law. This underscores the urgent need to protect well-established navigational rights, seafarers and global supply chains from geopolitical violence. Against this backdrop, the legal classification of Houthi attacks raises complex issues. The following section will attempt to investigate the potential legal characterization of the various forms of attacks carried out by the Houthis (Pedrozo, 2024; Dominguez, 2024).

Piracy and Armed Robbery

Although it may sound like a phenomenon of the past, piracy and armed robbery at sea continue to pose threats to international maritime security. This certainly affects several key shipping lanes. While piracy incidents off the coast of Somalia have declined recently, other regions are witnessing persistent risks. Pirates, often operating from fast small boats, target vessels employing tactics that range from hijacking crew members for ransom or cargo theft (NATO Shipping Centre et al., 2018).

From the legal point of view, piracy consists of any illegal acts of violence, detention, or depredation committed for private ends by the crew or passengers of a private ship or aircraft, and directed against another ship or aircraft, or against persons or property on board, on the high seas or outside the jurisdiction of any State (UNCLOS, Art. 101). A key jurisdictional element for piracy is the involvement of two vessels (or a ship and an aircraft). There is also an express geographical limitation. Therefore, where the similar acts occur within a State's internal waters, archipelagic waters, or territorial sea and involves only a single ship, then they may instead fall within the scope of armed robbery against ships rather than piracy (IMO, 2009).

Legally speaking, one of the most straightforward avenues for classifying certain Houthi attacks would appear to be through the lens of piracy or armed robbery at sea (IMO, 2024; Kraska, 2024; McLaughlin, 2024; Pedrozo, 2024). In this respect, the hijackings of several ships (Galaxy Leader, Central Park, Ruen and Maersk Hangzhou) by the Houthis have frequently been characterised as acts of piracy. However, while some Houthi attacks may, at first sight, seem to fit within the traditional piracy framework, their operations underpinned by external support and aimed at strategic chokepoints for geopolitical objectives significantly challenge conventional piracy typology. The context, methods, and objectives of the Houthis raise thorny questions as regards the accuracy of the said classification. For instance, according to Article 101 of the UNCLOS, in addition to other conditions, the piracy act must be committed for "private ends." A growing body of scholarship argues that attacks by non-State actors on third-State commercial vessels may still fall within the piracy framework. Moreover, the reference to "crew or passengers" in Article 101 raises doubts as to whether unmanned drones or maritime autonomous vessels (MAVs) which simply aim to collide and create explosion or damage ships fall within its scope, thereby cautioning against an overly expansive interpretation.

It may be safe to argue that the interpretation of "private ends" has evolved. It no longer requires a purely pecuniary motive; politically or ideologically driven acts may qualify, provided they are not committed on behalf of a State. It is submitted that the opposite of public is private. Thus, if the violence is not sanctioned by a State it can be still considered as private motive. This broader understanding was endorsed by the courts in several jurisdictions, such as the United States and Belgium, which found that politically or environmentally motivated violence against foreign vessels, if not State-sanctioned, may still constitute piracy. This line of thought was also endorsed by State practice.

For instance, the recent naval responses to Houthi attacks have been framed as lawful measures to repress piracy in accordance with international obligations (Frostad, 2024; Kraska & Pedrozo, 2023; Papastavridis, 2024; Pedrozo, 2024).

Be that as it may, while recent Houthi attacks in the Red Sea may bear certain similarities to piracy, their nature, scale, and operational sophistication far exceed the classic piracy as Houthis don't rely on small arms and skiffs to hijack crew or vessels for ransom. On the contrary, they employ advanced capabilities, including ballistic missiles, anti-ship cruise missiles, drones and MAVs for coercion. Moreover, although the Houthis are non-State actors, they operate with military command structure that closely look like that of a de facto State controlling approximately 30 % of Yemen. Remarkably, there have been also numerous allegations that they have been a proxy of another State. Their sustained targeting of commercial shipping manifested in varying forms, therefore, cannot be simply established as piracy and solution may not be readily available in the realm of maritime law enforcement (IMO, 2024; McLaughlin, 2024).

Privateering

A privateer, as the name suggests, was a private actor formally authorised by a State, through a letter of marque, to engage in hostile actions against enemy commerce. Though operating independently of regular naval forces, privateers effectively served as instruments of State policy by projecting asymmetric maritime power in the past (Encyclopaedia Britannica, n.d.). Remarkably, the seizure of the Santa Catarina in 1603 by Dutch East India Company (VOC) provided the factual foundation for the Dutch diplomat and jurist Grotius's De Jure Praedae, a pioneering legal defence of free trade. Framing the act as a lawful response to Portuguese monopoly, Grotius portrayed the VOC as both a moral and quasi-sovereign actor. In doing so, Grotius aimed to ground the legitimacy of commercial warfare (Porras, 2006; van Ittersum, 2003; Wilson, 2013).

However, the Crimean War (1853–1856) marked a turning point in recourse to privateering, as Britain and France deliberately refrained from authorising privateers to protect global trade routes. This restraint was formalised in the 1856 Declaration of Paris. It abolished privateering and codified core principles such as the protection of neutral goods under enemy flags and the requirement that maritime blockades to be legal (Monk, 2024; Peifer, 2013).

Despite its formal abolition, there have been interesting examples over the years resembling privateering. For instance, Sea Shepherd, a marine conservation NGO, is known for its actions to enforce international environmental law where official mechanisms have failed. It is frequently branded as "pirates". The organization has even embraced the image of Jolly Roger as a symbolic expression, positioning itself as an ecological enforcer where State enforcement is lacking. Remarkably, Sea Shepherd has officially collaborated with States as well, to name a few, Ecuador, Mexico, Gambia and Gabon. On behalf of those States, at times, Sea Shepherd has provided patrol vessels, surveillance capabilities, and legal assistance to combat IUU fishing.

Though non-State, Sea Shepherd's activities often mirror the protective role of quasi navy elements, thus, drawing comparisons to privateering albeit in defence of environmental rather than commercial interests (Sea Shepherd Global 2025; Watson, 2019).

Another contemporary similarity to privateering emerges in the operations of the Tamil Sea Tigers, which was active between 1984 and 2009, whose state-like attributes such as territorial control, naval hierarchy, and arms procurement networks enabled sophisticated maritime attacks. Employing stealth boats, suicide craft, and even crude submarines, they sought to disrupt Sri Lankan naval logistics and assert maritime control. Their tactics, blending irregular asymmetric warfare with political aims, blurred the distinction between piracy and privateering (Dunigan, 2012; Peifer, 2013).

Really and truly, contemporary asymmetric threats, such as the Houthi attacks on merchant vessels, closely resemble privateering rather than piracy. Reportedly supported by a third State and conducted under the guise of armed conflict, these operations evidently target civilian shipping, disrupt trade, and provoke international responses. Therefore, the classical distinction between piracy and privateering has become increasingly imprecise in the current situation. Although the 1856 Declaration formally abolished privateering, the assumption that its legal extinction precludes analogous modern practices warrants careful re-examination. The Houthi attacks, though perhaps lacking express commissions, certainly exhibit operational features akin to classical privateering. Certainly, this doesn't imply that these attacks are justified. On the contrary this simply suggests that there may be an emerging dangerous practice of using proxies in the maritime domain which poses significant risks to international shipping. It is worth noting that thus far legal discourse has largely avoided this characterisation due to formal prohibition, yet the functional attributes of privateering appear to be re-emerging. This convergence of State-like strategic intent and non-State execution calls on renewed doctrinal reconsideration on the evolving boundaries between piracy and a contemporary revival of privateering through asymmetric illegal coercion at sea (Kraska & Pedrozo, 2023, Monk, 2024; Peifer, 2013).

Unlawful Acts at Sea and the SUA Convention

Growing concern over unlawful acts at sea such as hijackings, kidnappings, and attacks involving explosives prompted international community to act in the 1980s. In 1985, the IMO adopted a resolution (IMO, 1985) to address such threats. The following year, the IMO's Maritime Safety Committee (MSC) called for preventive measures (IMO, 1986). Building on these initiatives, SUA Convention was adopted under the auspices of the IMO. SUA Convention criminalizes acts such as the forcible seizure of ships, violence against persons on board, and the placement of destructive devices. Notably, it was adopted to address limitations in the definition

of piracy under UNCLOS, particularly its restriction to acts committed on the high seas, between two ships, and for private ends. By contrast, the SUA Convention covers a broader range of unlawful acts, including politically motivated ones, and applies to incidents occurring in both territorial waters and high seas. Article 3 defines "unlawful acts" to include the seizure of ships, acts of violence endangering the safety of navigation, and the placement of devices likely to cause destruction or damage. The Convention was significantly expanded by the 2005 Protocol, which introduced new offences. These include the unlawful use of ships or dangerous materials to intimidate populations or coerce governments or international organizations. Specifically, Article 3 is criminalizes the use or discharge of explosives, the release of hazardous substances such as oil or LNG in harmful quantities and the use of a ship itself as a weapon.

In the absence of privateering focused legal framework, certain Houthi attacks may indeed be classified as unlawful acts at sea under the SUA Convention. Indeed, the SUA Convention is arguably fit to cover politically motivated acts that endanger maritime navigation, including missile or drone attacks on civilian vessels in the Red Sea (Frostad, 2024; Papastavridis, 2024; Pedrozo, 2024).

International Responses

Since late 2023, Houthi attacks on commercial vessels have severely disrupted international navigational rights. In response, the IMO Secretary-General Arsenio Dominguez convened high-level consultations with Member States, industry stakeholders, and regional partners. In late 2024, the IMO Secretary General undertook a mission to several Red Sea littoral States such as Djibouti, Egypt, Oman, Saudi Arabia, and Yemen. During his overseas missions, IMO Secretary General underscored the need to safeguard seafarers, and to uphold freedom of navigation. Moreover, he reiterated the IMO's commitment to coordinated action with governments, UN agencies, and the maritime industry to de-escalate tensions and ensure the continued resilience of this critical maritime corridor.

In early 2024, during a UNSC session, IMO Secretary General reiterated that such attacks including the unprecedented use of missiles and drones against commercial shipping are unacceptable. Similarly, in early 2024, UNCTAD warned of escalating maritime disruption arising from the convergence of geopolitical tensions and climate stressors and called for urgent international coordination to ensure the continuity and resilience of global trade (Seatrade Maritime, 2024). On 6 January 2024, the IMO Secretary General convened Djibouti Code of Conduct States to assess the Red Sea crisis, focusing on seafarer protection, navigational security, and regional threat mitigation (IMO, 2024; UNCTAD, 2024).

Notably, on 10 January 2024, the UNSC adopted Resolution 2722 (2024), condemning the Houthi attacks on merchant shipping in the Red Sea. Adopted with 11 votes in favour, the resolution reaffirmed the legal framework under UNCLOS, upheld the right of States to defend their vessels in accordance with international law, and underscored the importance of safeguarding navigational rights and freedoms. Moreover, it called for enhanced cooperation, capacity-building for Red Sea coastal States, particularly the Yemeni Coast Guard. And it also reiterated obligations under Resolution 2216, including the arms embargo on the Houthis. The resolution also mandated monthly reporting by the UN Secretary General to monitor threats to maritime security and prompted the IMO to intensify engagement and provide regular updates (House of Commons, 2025; Papastavridis, 2024; UNSC, 2024).

In response to escalating attacks, the U.S. has initially designated the Houthis as a Specially Designated Global Terrorist (SDGT) entity in 2024, followed by their reclassification as a Foreign Terrorist Organization (FTO) in 2025. Notably, the internationally recognized Government of Yemen welcomed these designations, denouncing the Houthis as an "Iranian proxy" engaged in terrorist activities. It called for the international community to cease all engagement with the group and reaffirmed its commitment to a political resolution based on UNSC Resolution 2216 (House of Commons, 2025; IMO, 2024; UNSC, 2025; US Department of State, 2025; White House, 2025).

At the recent UNSC meeting in 2025, the US urged the international community to uphold relevant UNSC Resolutions, particularly those imposing an arms embargo on the Houthis. Furthermore, the US condemned Houthi attacks on commercial shipping as indiscriminate, unlawful, and lacking any legitimate justification under international law, stressing that such actions undermine both the Palestinian cause and the welfare of the Yemeni people. The United Kingdom echoed these concerns. The UK also reiterated its call for strict compliance with the arms embargo (UNSC, 2025).

In its formal communication to the IMO on 25 January 2024, the Government of Yemen highlighted the grave security implications of ongoing Houthi activities. Notably, Yemen called for urgent international action to restore navigational security and uphold the integrity of global trade routes. The Government reiterated its longstanding concerns regarding the Houthi militia's control over key coastal areas and their deployment of naval mines, drone boats, and missiles targeting international shipping measures which amount to an economic blockade against the Yemeni people. Remarkably, these actions were described as maritime terrorism and piracy.

The communication further criticized the Houthis' exploitation of the Gaza crisis for propaganda purposes, warning that such actions distort legitimate Palestinian aspirations while advancing Iran's strategic agenda. The humanitarian consequences, rising shipping and insurance costs, disrupted imports and worsening food insecurity were also emphasized (IMO, 2024).

In May 2024, the IMO adopted its first resolution addressing the Houthi attacks. The MSC resolution condemned the attacks as illegal and unjustifiable citing their grave impact on freedom of navigation, international trade, seafarer safety, and humanitarian access. It demanded the immediate and unconditional release of the detained vessel and crew. And it called on all Member States to comply with UNSC Resolution 2216, including the prohibition on arms transfers to the Houthis (IMO Maritime Safety Committee, 2024).

At its next session, the MSC reaffirmed its grave concern over the Houthi attacks. The MSC highlighted the impact of attacks on the safety of navigation and well-being of seafarers, freedom of navigation, the marine environment, and the global supply chain. Moreover, it welcomed the adoption of UNSCR 2722 (2024), which reaffirmed navigational rights under international law and condemned attacks on commercial vessels. Iran rejected accusations of involvement and cited its commitment to UNSC Resolutions 2140 and 2216. The Committee overall emphasized the need for continued diplomatic efforts, transparency, and rule-based responses to preserve maritime security in the Red Sea (IMO MSC, 2025).

UNSC Resolution 2768 (2025) extended the monthly reporting mandate on Houthi attacks in the Red Sea until 15 July 2025, reiterating the demand that the Houthis immediately cease hostilities and release the Galaxy Leader and its crew (On 19 November 2023, the Galaxy Leader, a Bahamian-flagged ro-ro vessel, was seized in the Red Sea, with 25 multinational crew members taken hostage. The IMO repeatedly condemned the hijacking, called for the crew's immediate release, and IMO Secretariat engaged relevant States and NGOs).

Adopted by 12 votes in favour, the resolution expresses concern over the increasing sophistication of the attacks and reaffirms the importance of safeguarding navigational freedoms and maritime security.The UNSC also called for strict adherence to the arms embargo (UN, 2025; UNSC Report, 2025).

Last but not least, the international military response, primarily through Operation Prosperity Guardian and Operation Aspides, has been regarded as effective in intercepting or deterring some Houthi attacks. For instance, Operation Aspides initially mandated to protect navigation and now also tasked with monitoring arms shipments and sanctioned oil has escorted nearly 500 ships as of writing, and intercepted drones and missiles (gCaptain, 2025). These efforts are welcomed by the IMO and the shipping industry (IMO, 2024a; 2024b).

Conclusion

The recent Houthi attacks pose a serious threat to the global maritime order on which the world economy depends. These attacks jeopardize maritime safety and security, risk serious harm to the marine environment, and endanger the lives of innocent seafarers. Targeting a single ship under the misconception that it affects only one country is legally and practically invalid. Be that as it may, the current attacks on civilian shipping certainly cannot be justified. Therefore, such a justification which aims to blur the scope of attacks is certainly pointless. Given the international nature of shipping, such attacks inevitably affect us all. Indeed, shipping is truly international. For instance, seafarers, masters, insurers, charterers, ship registration, cargo and ship owners typically all hail from different countries. The safety and security of maritime navigation in critical corridors such as the Red Sea therefore constitute a matter of global concern and collective interest.

In light of the foregoing, it is important to recall that both the UNCLOS and the SUA Convention are primarily peacetime instruments. While they may provide first response as an essential normative foundation, they may not in themselves suffice to address the full complexities of the current situation in the Red Sea. Indeed, the current crisis has a hybrid character which may require a new legal understanding.

Notably, considering the gravity of these attacks, the IMO and the UNSC have adopted several resolutions condemning Houthi attacks on merchant vessels, affirming the importance of navigational rights and freedoms. They also strongly reaffirmed the right of States to defend their vessels in accordance with international law. Yet they have deliberately refrained from legally clearly characterising these acts due to the well-known sensitivities in the global political landscape.

Evidently, targeting civilian merchant vessels constitutes a clear violation of international law. Yet the Houthi attacks raise complex legal questions, particularly concerning their classification as acts perpetrated by non-State actors operating in a quasi-State capacity. Hybrid threats of this kind expose the limitations of existing peacetime legal frameworks. Really and truly, these attacks do not fall neatly under a single classification in international law.

Rather, they blur the lines between piracy, terrorism, and privateering. Nonetheless, most of the Houthi attacks cannot be classified under piracy as they don't meet the conditions of such an offence under international law. On the other hand, they seem to be better fit in the realm of SUA Convention as they represent unlawful acts at sea.

In conclusion, it is worth highlighting that, although privateering has been abolished under modern international law, its functional attributes such as State-sponsored attacks against merchant shipping appear to be resurfacing in varying forms. Yet, the existing legal frameworks are not fully equipped to address this new old concept.

The use of maritime proxies for creating illegal coercion at sea cannot be tolerated. Otherwise, this may set a dangerous practice which would eventually harm global shipping. Therefore, this phenomenon warrants renewed serious doctrinal consideration within the broader context of international maritime law to address hybrid threats that steadily challenge established legal order.

References

NATO Shipping Centre. (2018). *Global counter piracy guidance for companies, masters and seafarers.* Witherby Publishing Group Ltd. https://shipping.nato.int/nsc/operations/global-maritime-risk

Dunigan, M. (2012). *Victory has a thousand fathers: Sources of success in counterinsurgency* (Vol. 3, Appendix B: Adversary capabilities, Maritime, pp. 69–75). RAND Corporation. https://www.rand.org/pubs/monographs/MG964.html

Encyclopaedia Britannica. (n.d.). P*irates, privateers, corsairs, buccaneers: What's the difference?* Encyclopaedia Britannica. https://www.britannica.com/story/pirates-privateers-corsairs-buccaneers-whats-the-difference

Frostad, M. (2024, June 10). *Houthi attacks on merchant vessels in the Red Sea*. Lieber Institute for Law & Land Warfare. https://lieber.westpoint.edu/houthi-attacks-merchant-vessels-red-sea/

House of Commons Library. (2025, February 4). *UK and international response to Houthis in the Red Sea 2024/25 (Research Briefing CBP-9930).* https://commonslibrary.parliament.uk/research-briefings/cbp-9930/

IMO. (2024, January 31). *Circular Letter No. 4836.* https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/Red%20Sea/CL.4836.pdf

IMO. (2024, March 12). *Attack on True Confidence: Measures to enhance maritime security.* https://www.imo.org/en/MediaCentre/PressBriefings/pages/Attack-on-True-Confidence.aspx

IMO. (2024, March 12). *Measures to enhance maritime security: Security in the Southern Red Sea and Gulf of Aden.* (MSC 108/7/2).

IMO. (2024, November 4). *IMO Secretary-General visits Red Sea countries.* https://www.imo.org/en/MediaCentre/PressBriefings/Pages/Red-Sea-Mission.aspx

IMO. (2025, January 20). *Report of the MSC on its 109th session.* (MSC 109/22).

IMO. *Red Sea Hot topics.* https://www.imo.org/en/MediaCentre/HotTopics/Pages/Red-Sea.aspx

IMO. *Red Sea security project.* https://www.imo.org/en/OurWork/Security/Pages/RedSeaProject.aspx

Kraska, J., & Pedrozo, R. (2023). *Newport manual on the law of naval warfare* (Vol. 101, pp. 41–44). Stockton Center for International Law, U.S. Naval War College.

Kraska, J. (2024, January 2). *Attacks on U.S. warships justify self-defense against Houthi forces ashore. Lawfare.* https://www.lawfaremedia.org/article/attacks-on-u.s.-warships-justify-self-defense-against-houthi-forces-ashore

McLaughlin, R. (2024, January 8). H*outhi operations in the Red Sea and LOAC? Lieber Institute for Law & Land Warfare*. https://lieber.westpoint.edu/houthi-operations-red-sea-loac

Monk, J. (2024, July 9). *A return to privateering: A strategic concept for unconventional warfare. Strategy Central.* https://www.strategycentral.io/post/a-return-to-privateering-a-strategic-concept-for-unconventional-warfare

Papastavridis, E. (2024, January 30). *Red Sea attacks and the international response: An international law insight.* ELIAMEP. https://www.eliamep.gr/en/red-sea-attacks-and-the-international-response-an-international-law-insight-efthymios-papastavridis/

Pedrozo, R. (2024, March 28). *Imposing a maritime quarantine to enforce the Houthi arms embargo. Lieber Institute for Law & Land Warfare*. https://lieber.westpoint.edu/imposing-maritime-quarantine-enforce-houthi-arms-embargo/

Porras, I. M. (2006). Constructing international law in the East Indian seas: Property, sovereignty, commerce and war in Hugo Grotius' De iure praedae, The law of prize and booty, or "On how to distinguish merchants from pirates." *Brooklyn Journal of International Law, 31*(3), 741–804. https://brooklynworks.brooklaw.edu/bjil/vol31/iss3/5

Sea Shepherd Global. (n.d.). *Our mission.* Retrieved June 13, 2025, from https://www.seashepherdglobal.org/who-we-are/our-mission/

Seatrade Maritime. (2024, January 4). *Shipping associations welcome international condemnation of Red Sea attacks.* https://www.seatrade-maritime.com/security/shipping-associations-welcome-international-condemnation-of-red-sea-attacks

Security Council Report. (2025, January 15). *Houthi Red Sea attacks: Vote on a draft resolution.* What's in Blue.https://www.securitycouncilreport.org/whatsinblue/2025/01/houthi-red-sea-attacks-vote-on-a-draft-resolution-3.php

Sümer, M. (2023). Applicability of the right of innocent passage to MASS: Exploring the potential role of advisory opinions. In P. Leucci & I. Vianello (Eds.), *ASCOMARE Yearbook on the Law of the Sea* (Vol. 3, pp. 159-176). Luglio Editore.

UN. (1982). *United Nations Convention on the Law of the Sea*. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

UN. (2025, January 15). *Security Council adopts Resolution 2768 (2025), sustaining monthly reporting on Houthi attacks in Red Sea; Members urge group to halt attacks, debate need to address root causes of conflict* (Press Release SC/15965). https://press.un.org/en/2025/sc15965.doc.htm

UNCTAD. (June 15, 2025). *UNCTAD raises alarm on escalating disruptions in global trade due to geopolitical tensions.*https://unctad.org/press-material/unctad-raises-alarms-escalating-disruptions-global-trade-due-geopolitical-tensions

UNSC. (2024, January 10). *Resolution 2722*. https://unscr.com/en/resolutions/doc/2722

UNSC. (2025, March 6). *Provisional verbatim record of the 9873rd meeting* (S/PV.9873). United Nations.

US Department of State. (2025, March 4). *Designation of Ansarallah as a Foreign Terrorist Organization [Press statement]*. https://www.state.gov/designation-of-ansarallah-as-a-foreign-terrorist-organization/

US White House. (2025, January). *Designation of Ansar-Allah as a Foreign Terrorist Organization.* https://www.whitehouse.gov/presidential-actions/2025/01/designation-of-ansar-allah-as-a-foreign-terrorist-organization/

Van Ittersum, M. J. (2003). Hugo Grotius in context: Van Heemskerck's capture of the Santa Catarina and its justification in De Jure Praedae (1604–1606). *Asian Journal of Social Science, 31*(3), 511–547. https://doi.org/10.1163/156853106778048639

Watson, P. (2019). Neptune's navy: A global initiative. *The Ecological Citizen, 2*(2). https://www.ecologicalcitizen.net

Wilson, E. (2013). The VOC, corporate sovereignty and the republican sub-text of De iure praedae. *Grotiana, 26*(1), 311–340. https://doi.org/10.1163/187607508X366580

About the Author

Dr. Murat Sümer / IMO International Maritime Law Institute / murat.sumer[at]imli.org

Dr. Murat Sümer is the Nippon Foundation Lecturer in International Maritime Law at the IMO International Maritime Law Institute (IMLI) in Malta since 2019. He holds an LL.B., two master's degrees, and a Ph.D., and attended the Diplomacy Academy of the Turkish Ministry of Foreign Affairs. He is a registered Advocate and enlisted Arbitrator. Before his academic career, he served as a career diplomat from 2008 to 2019. Dr. Sümer lectures on the public aspects of international maritime law and has coordinated IMLI's prestigious Courses on the Peaceful Settlement of Maritime Disputes and the Delimitation of Maritime Boundaries, and Law of Ports. He has also served as a visiting fellow at several distinguished universities. He has published extensively on the public aspects of international maritime law in peer reviewed journals. Dr. Sümer also serves on the Editorial Board of the EuroMediterranean Journal of International Law and International Relations published by the University of Cádiz in Spain. He regularly participates as a speaker in international conferences and expert workshops on the law of the sea and the peaceful settlement of disputes.

Seaborne Narcotics: Mapping the Maritime Drug Trade in the Indian Ocean and Its Security Implications

Dr. Muhammad Rafi Khan
Minhaj University Lahore, Pakistan

Dr. Saadia Tariq
Independent Statistician, Pakistan

Samia Bashir
Minhaj University Lahore, Pakistan

Abstract

The Indian Ocean Region (IOR) has emerged as an active corridor for maritime drug movement, especially hashish and heroin. The increasing use of sea routes by traffickers presents a growing challenge for maritime governance and regional cooperation. This paper aims to map key routes, actors, and patterns of trafficking in the Indian Ocean. It focuses on the influence of limited coastal capacity, lightly monitored transit points, and the use of traditional vessels such as dhows that sail between South Asia, the Gulf, and East Africa. The study draws from open-source maritime interdiction data, naval assessments, and vessel tracking reports. It identifies important maritime junctions, including the Makran coast, the Gulf of Aden, and areas near the Maldives. These routes are used not only for drugs but also connect to other informal trade activities. The paper highlights how such movements may contribute to informal economies and stress local governance. While international maritime efforts have supported regional monitoring, this paper argues that long-term progress requires closer partnerships, improved maritime domain awareness, and the strategic use of technology such as satellite tracking. It also discusses how maritime security efforts can be more effective when linked with local development and capacity-building at ports. By offering a visual and data-supported overview of drug trafficking trends, this study contributes to a better understanding of emerging maritime risks. It also presents focused policy ideas to help improve maritime coordination. The Indian Ocean is a shared space of opportunity and responsibility. Recognizing and responding to these narcotics trade patterns and risks is vital for strengthening regional maritime security.

Keywords

Maritime Drug Trafficking, Indian Ocean Region (IOR), Maritime Domain Awareness (MDA), Transnational Organized Crime, Maritime Security Cooperation

Introduction

The Indian Ocean is the main pathway of world maritime trade, but at the same time, its enormous size and complicated geopolitical features make it an easy target of illegal activities, especially the trade of seaborne narcotics. According to recent research, the region has become a pivotal point in transnational drug networks as the routes are adjusted to enforcement operations and local turmoil (Aravind & Girisanker, 2025). Poor governance, permeable borders and heavy maritime traffic work synergistically to compound these issues, requiring a systematic approach to detect and eliminate these networks (Potgieter, 2012).

Qualitative and analytical approaches have been used in earlier studies to investigate the security impact of maritime drug trafficking, and digital tools and multi-source data analysis are commonly used (Das, 2021). These studies highlight the need to identify key players, channels, and modes of operation, however, there are still gaps in integrating technological advancement with cooperative regulatory frameworks. To provide an example, even though AI and satellite technologies have been suggested as a method of route monitoring (Das, 2021), the relationship between those and collaboration frameworks on the regional scale has not been deeply investigated. This gap is addressed in this study by suggesting a common framework that incorporates the use of advanced technologies and institutional partnerships to enhance the awareness of maritime domain and effectiveness in interdiction.

The work is unique in its approach of taking an interdisciplinary view where the maritime security studies, technology governance and cooperative international relations are interrelated. Unlike the past research, where the technical methods and regulatory systems are often researched as independent entities (Bateman, 2015), we support their mutual integration. To illustrate, data-sharing systems with blockchain traceability capabilities can be used to extend the reach of regional navies, and AI-enhanced pattern recognition can be used to improve risk assessment models associated with patrol deployments (Ismail et al., 2021). Such a two-fold emphasis on innovation and cooperation makes our contribution different than previous ones.

The empirical analysis of the trends of trafficking between 2015 and 2023 indicates that there are new routes that have involved the use of dhows and fishing boats to evade detection (Das, 2021). The interception of INS Tarkash in 2021, as well as case studies, show that current interdiction methods are both successful and still vulnerable (Abeysekara, 2020). These findings indicate the need to have dynamic policies to deal with the dynamic nature of threats in the seas.

This research has two policy implications. First, we support an increased awareness of the maritime domain by using real-time satellite-, radar, and open-source intelligence data fusion (Cordner L., 2015). Second, we mention the role of regional partnerships, such as the Indian Ocean Naval Symposium (IONS), in facilitating operational coordination and capability building (Sullivan and Cordner, 2020). These suggestions are in line with wider demands of a comprehensive maritime security community in the area (Sears, 2019).

Literature Review

The Indian Ocean Region (IOR) has been of geopolitical importance long enough, but it has gained even greater importance over recent decades with the increased volume of international trade, energy transit routes and the increased scope of regional and extra-regional powers. Researchers have also noted that the relationship between politics, economy and environmental diversity in this maritime region is complex with Bouchard and Crumplin (2010) defining the IOR as the region of unchanging international attraction based on alliances and projections of power. The post-Cold War era, instead of stabilizing the region, has given rise to the ongoing process of rearranging strategy as the new powers such as India and China are also taking control in IOR besides the conventional powers such as the United States and its allies. This changing environment has resulted in the Indian Ocean becoming a place where security, trade and competition continue to intersect.

This historical context also adds depth to this geopolitical context. Ghosh (2004) sets the antecedents of maritime power in the IOR to the colonial era when European powers developed naval supremacy and port control as a way of promoting imperial interests. Although decolonization of the mid-20th century was a change in sovereignty, the cold war brought a new stage of external strategic competition. This colonization and militarization legacy is a source of maritime power even now. Despite the new state actors redefining the security order as Potgieter (2012) explains, the Indian Ocean is vulnerable to non-state issues, particularly to violent non-state actors (VNSAs) and illicit non-state actors (INSAs), especially those that take advantage of the loopholes in surveillance and enforcement on the sea.

The conceptualization of the Indian Ocean as a coherent security unit is a debatable issue within this large security matrix. Rumley et al. (2012) critically analyses competing constructions of regional identity that are advocated by Australia, the United States, and India. These constructs, which stretch across the Indian Ocean to the Indo-Pacific strategies, are not only geographical imagination but long-term strategic interests as well. According to Rumley et al. (2012), domination of the Indo-Pacific narrative has sometimes overshadowed Indian Ocean-specific organizations like the Indian Ocean Rim Association (IORA), thus undermining the chances of the region having a unified governance. Such institutional incoherence is detrimental to the fight against transnational criminal activities such as maritime narcotics trafficking (Banerjee, 2017; Premarathna, 2021), which demands a long-term cross-border and institutional coordination.

The legal and supervisory frameworks that regulate the IOR also represent the interplay between geopolitics and maritime law. Kraska (2012) emphasizes the importance of the maritime approach to the study of regional security by stating that maritime legal regimes offer an alternative viewpoint to the land-based approaches to the issue. In his work, he highlights the significance of international law in the regulation of choke points, piracy and the ever-thinning boundaries between legal and illegal maritime flows.

Legal basis of maritime cooperation is in place, yet it is not widely applied in practice especially in cases of non-traditional threats like drug trafficking (Cordner, 2014; 2018).

The literature shows that one of the biggest non-traditional security threats in the IOR is the development of maritime narcotic trafficking. According to Aravind and Girisanker (2025), the states of South Asia, and especially India, are becoming more worried about the scale and sophistication of drug trafficking sea routes. Their work also shows the failure in the current counter-narcotics structure of India and that even though the maritime security has been one of the primary arenas, there are still many grey spaces in the policy formulations and the way operations are conducted. This is consistent with the observations made by Panneerselvam (2021) on the Afghanistan-Pakistan corridor that is one of the major channels of smuggling heroin into the Western Indian Ocean. It is also on the work of criminal syndicates that are operating along the coast of Pakistan and operational challenges they pose to the agencies that are charged with the responsibility of enforcing the sea.

In addition to the national efforts, regional structures and multinational naval programs have tried to combat the maritime drug trade. Combined Maritime Forces (CMF) and other actors of the coalition have been partially successful in interdiction, and Panneerselvam (2021) and others stress that enforcement is not everything. The same limitation is reflected by Cordner (2015) who proposes a risk-based and cooperative model of security based on the shared strategic goals. His examination of the IOR as a coordinated maritime system provides a useful model in understanding the nature of overlapping between traditional and non-traditional risks. The work of Cordner (2015) emphasizes that no individual force can alleviate these threats and that the responses require collective risk assessment, transparency, and trust in the region.

Other works, however, go into more detail by examining the applicability of the regime theory and ocean governance. Such pieces of work as the one conducted by Gupta (2010) show that although regulatory instruments and cooperative mechanisms are theoretically present, they are not developed in most aspects of the IOR. The lax application of port state regulations and the incoherent collaboration between jurisdictions tend to give way to unlawful actors such as drug traffickers taking advantage of institutional gaps. These are complicated by a lack of maritime domain awareness and under-exploitation of surveillance technologies, particularly in the central Indian Ocean, where expanses of water are lightly patrolled (Klein, 2012; 2011).

Put collectively, the literature (fig. 1) shows that maritime narcotics trafficking in IOR needs to be viewed through the wider strategic and institutional prism. It is not a criminal matter only but a greater story of power projection, regional cooperation and institutional resilience. Historical trends, changing geopolitical constructs, legal frameworks, and technological constraints set up the boundaries of the problem, as well as of the solutions to the problem.

As a way of responding to these threats, both academicians and practitioners have insisted on the need to integrate governance strategies that integrate national capabilities with regional outlooks, anchored on law, trust and common accountability.

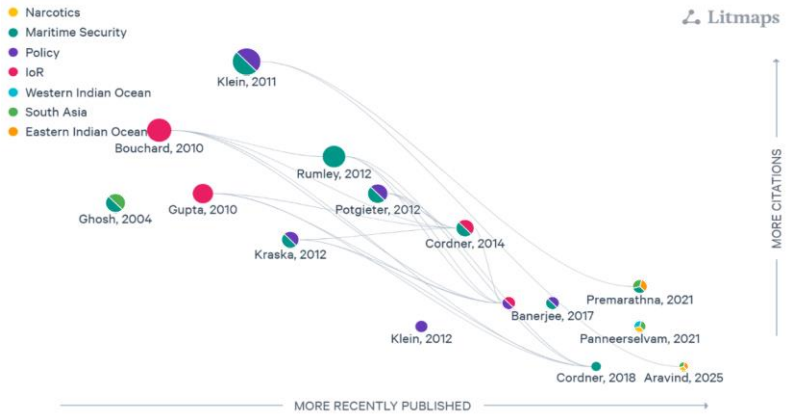

Figure 1

A network visualization showing relationships between academic literature on topics including narcotics, maritime security, policy, and regions in the Indian Ocean, with nodes labeled by authors and years, positioned by publication recency and number of citations, and connected by lines.

The strategic role of the Indian Ocean as a global trade route has been matched with the development of the Indian Ocean as a major area of illegal maritime activities, especially, narcotics trafficking which makes it possible to discuss how this topic has gained academic discourse in three areas: (1) the workings of drug smuggling networks, (2) frameworks of security at sea, and (3) the use of technology to recognize and thwart illegal actions.

Dynamics of Drug Trafficking Networks

According to recent research, narcotic trafficking networks are adaptive to pressure exerted by the enforcement. To illustrate, research on the strategies used by India in its fight against drug trafficking has revealed that smugglers are increasingly resorting to fishing boats and unregistered dhows to evade detection and exploit the fact that it is impossible to trace them (Aravind & Girisanker, 2025). The oceanic aspects of narcotics smuggling in South Asia further illustrate how criminal networks take advantage of jurisdictional uncertainties in Exclusive Economic Zones (EEZs), especially in regions with inadequate maritime monitoring capacities (Das, 2021).

These results correspond to wider examinations of transnational organized crimes across the Bay of Bengal, where deficient governance systems promote the intersection of drug trafficking with more unlawful practices such as Illegal, Unreported, and Unregulated (IUU) fishing (Faiyaz & Sidhu, 2024).

Maritime Security Frameworks

Both the extra-regional and regional actors have defined the institutional response to maritime narcotics trafficking. Concerning this, the role of Pakistan in multilateral naval and maritime diplomacy in terms of annual AMAN exercises is worth mentioning. The desire of India to become a net security provider in the Indian Ocean Region (IOR) has led to the development of projects, like the Information Fusion Centre (IFC-IOR) that enhances the maritime domain awareness through the exchange of information between various countries (Upadhyaya, 2018). However, studies of Indian Ocean Naval Symposium (IONS) point to constant challenges in adopting such collaborative structures, in particular, intelligence-sharing covenants and legal restrictions (Sawan, 2020). The comparative study of the experience of Sri Lanka in the efforts to integrate civilian and military activities reveals that the organizational fragmentation may undermine the interdiction efforts, even in cases where technological resources are at hand (Abeysekara, 2020).

Technological Interventions

Due to technological developments, there are new opportunities and challenges in the fight against maritime drug trafficking. The Western Indian Ocean case studies (Ismail et al., 2021) reveal the effectiveness of synthetic aperture radar (SAR) and automatic identification system (AIS) satellite surveillance in detecting anomalous vessel behaviors. However, recent research cautions that one should not overly rely on such tools since they emphasize the practices used by traffickers, such as AIS spoofing and covert transit tactics (Hashim et al., 2025). The current tests in machine learning to forecast the route are promising but are challenged by the inability to differentiate between legal fishing activities and the transportation of drugs (Cordner, 2014).

The proposed framework goes further than the current practices by incorporating these three dimensions into a system. Even though earlier studies have examined technological methods or collaborative models individually (Bateman, 2015), our cross-disciplinary model deals with the interrelation between them. An example is that cargo tracking systems based on blockchain technology might enhance the data integrity of the IFC-IOR, and anomaly detection using artificial intelligence might improve the allocation of scarce patrol resources across jurisdictions. This synthesis fills an important gap in the scholarly discussion in which operational, technological, and policy factors have been analyzed separately.

Materials And Methods

Analytical Framework

The analytical framework proposed in this study synthesizes digital research methodologies, artificial intelligence techniques, and interdisciplinary security theories to systematically analyze maritime drug trafficking networks. This method overcomes the constraints of traditional maritime security assessments by embedding real-time data synthesis and anomaly detection functionalities.

Mobilizing Digital Tools for Data Aggregation

The framework employs Litmaps (an AI based research tool) to construct a knowledge graph of academic literature, policy documents, and operational reports related to maritime narcotics trafficking (fig. 1). This graph G=(V,E) represents publications as vertices V and citation relationships as edges E, where edge weights w_ij reflect the strength of conceptual linkages between documents i and j. The network structure displays groupings of studies focusing on particular geographic areas (e.g., Western Indian Ocean) or thematic subjects (e.g., legal frameworks).

Primary data sources include United Nations Office on Drugs and Crime (UNODC) seizure reports, databases documenting incidents from the maritime coalition forces (CMF), automatic Identification System (AIS) vessel tracking records. These datasets undergo temporal alignment through a synchronization function:

$$t_{sync} = arg\ tmin \sum_{k=1}^{n} \quad w_k t - t_k \qquad (1)$$

where t_k stands for timestamps across n heterogeneous data streams.

AI-Enabled Route and Actor Identification

A convolutional neural network (CNN) framework analyzes geospatial data to detect potential trafficking routes. The model takes as input a tensor $X \in R^{H \times W \times C}$ representing:

- $H \times W$: Spatial grid of the Indian Ocean region
- C: Channels encoding AIS signals, historical seizure locations, and oceanographic conditions.

The output Y predicts route probabilities through SoftMax activation:

$$Y_{ij} = \frac{e^{z_{ij}}}{\sum_{k=1}^{K} e^{z_{ik}}} \quad (2)$$

Where z_{ij} denotes the logit value for grid cell (i, j)
Actor identification applies named entity recognition (NER) to multilingual legal texts and intelligence documents. The model calculates entity importance scores s_e as:

$$s_e = \frac{f_e}{max(f)} \cdot log\left(\frac{N}{n_e}\right) \quad (3)$$

Where f_e is entity frequency, N total documents, and n_e documents having the entity.

Integrating Interdisciplinary Knowledge in Analysis

The framework operationalizes non-traditional security theory through three analytical lenses:

- **Network resilience**: The robustness of the trafficking system is assessed by applying betweenness centrality (C_B(v)) to critical nodes (v).
- **Institutional effectiveness**: Quantifies cooperation efficiency via response time distributions $P(\tau)$ across areas.
- **Technological diffusion**: Tracks adoption rates λ of counter-trafficking technologies among regional navies
  These metrics contribute to a unified evaluation of threat level.

$$T = \alpha C_B + \beta E[\tau] + \gamma\lambda \quad (4)$$

where parameters α, β, γ weight components based on expert elicitation.

Case-Based Validation and Refinement

The PNS Dehshat interdiction operation acts as a validation case, where model results are contrasted with actual operational data. Discrepancies δ between predicted and actual seizure locations inform iterative refinement:

$$\delta = \frac{1}{m}\sum_{i=1}^{m} \| \hat{y}_i - y_i \|_2 \qquad (5)$$

where $\hat{y}_i$ and y_i represent predicted and actual coordinates for m test cases.

The framework's execution illustrates the capacity of digital technologies to revolutionize traditional maritime security assessment. As depicted in Figure 1, the network visualization uncovers previously hidden relationships between regional trafficking patterns and academic discourse. This function permits decision-makers to detect areas lacking research and new risks by methodically analyzing evidence.

The technical design permits ongoing addition of novel data sources by means of modular data adapters, which guarantees the system stays adaptable to changing trafficking methods. Subsequent versions will integrate live satellite image assessment and blockchain-driven cargo origin verification to improve detection performance.

Empirical Analysis: Trafficking Routes, Key Actors, and Evolving Patterns (2015-2023)

Methodology and Data Sources: To methodically examine patterns in maritime drug trafficking, we adopted a dual-method data synthesis strategy merging qualitative case analyses with quantitative spatial mapping. Primary data originated from three principal sources: (1) seizure records of UNODC's Global Maritime Crime Program, (2) vessel movement patterns derived from AIS via exactEarth's satellite network, and (3) operational documentation from Combined Task Force 150. These datasets underwent temporal alignment via a pipeline employing Equation 1 to synchronize events from diverse sources.

The analytical workflow incorporated:

- **Route identification**: Kernel density estimation (KDE) was applied to historical seizure locations with bandwidth parameter h optimized via cross-validation:

$$\hat{f}(x) = \frac{1}{nh}\sum_{i=1}^{n} K\left(\frac{x - x_i}{h}\right) \quad (6)$$

where K represents the Epanechnikov kernel function.

- **Actor network mapping**: Social network analysis metrics including betweenness centrality (Equation 4) and eigenvector centrality were computed for identified trafficking networks.
- **Pattern evolution tracking**: A changepoint detection algorithm detected notable alterations in trafficking methods.

$$C(\tau) = \sum_{t=1}^{\tau} (x_t - \mu_1)^2 + \sum_{t=\tau+1}^{T} (x_t - \mu_2)^2 \quad (7)$$

where τ marks the changepoint between periods with means μ_1 and μ_2.

Textual Analysis and Structuring Tools

The article underwent multiple rounds of editing and coherence refinement through the assistance of advanced large language models (LLMs); specifically ChatGPT vGPT-4.5 was employed for analytical structuring, paragraph alignment, clarity enhancement, and thematic consistency, whereas, Qwen AI 3 v235B was used for additional proofing, contradiction detection, and flow improvement across sections.

These AI tools were used to enhance the clarity, coherence, and academic quality of human-written drafts.

Results

Technology-Enabled Surveillance Has Enhanced Maritime Interdictions

The integration of AI, satellite constellations, and radar systems has significantly strengthened maritime domain awareness. Predictive analytics and anomaly detection tools now support real-time identification of illicit vessel behavior, particularly in less-monitored regions. Prominent examples are the seizure of around 4500 Kilograms of drugs by PNS Dehshat in coordination with air units of Navy at North Arabian Sea and the seizure of over 2,500 kilograms of narcotics by the INS Tarkash later in March 2025 with the use of real-time AI inputs and P8I aircraft surveillance. The joint operation of PNS Zulfiqar with US Abraham Lincoln Strike Group is also one of the remarkable examples. This proves the operational value of AI-enhanced maritime platforms, which allow for early detection and precision targeting.

International Cooperation Is Pivotal in Counter-Narcotics Operations

Regional and global cooperation mechanisms have emerged as crucial enablers of successful interdiction efforts. Platforms such as the Southern Route Partnership (SRP), Indian Ocean Forum on Maritime Crime (IOFMC), and Combined Task Force 150 (CTF-150) have facilitated intelligence sharing, harmonization of legal frameworks, and collaborative training.

As an instance, the 2024 SRP meeting in Tanzania was productive in operational discussions with eleven countries, while the CTF-150 operations combined surveillance technologies with naval patrols among member countries. These instances underscore the usefulness of multi-actor approaches to dealing with transnational drug trafficking.

Traffickers' Evasive Tactics and Systemic Gaps Persist

Although there are technological advantages, the drug dealers are still using loopholes in maritime laws. The fact that a dark vessel that turns off their AIS transponders is hard to detect, especially in remote areas, like those surrounding the Chagos Archipelago. The enforcement is made more difficult using small dhows that are a product of both Pakistan and Iran since they can co-exist with the legitimate fishing fleet.

Moreover, uneven implementation of AIS compliance and limited adoption of blockchain traceability tools weaken overall deterrence. These systemic gaps underscore the need for capacity-building and infrastructure support across vulnerable littoral states.

Maritime Routes Enable a Nexus Between Organized Crime and Terrorism

The Indian Ocean's vast and porous maritime routes serve as conduits not only for narcotics but also for broader security threats. Organized criminal networks have been linked to arms trafficking and insurgent financing, particularly in island nations like the Maldives and Sri Lanka.

Evidence indicates that the smuggling of heroin by sea is one of the ways of financing extremist groups like Al-Qaida and ISIL/Da'esh. These connections are usually supported by institutional loopholes such as corruption, lack of financial scrutiny and insecure prison mechanisms that have allowed the thriving of criminal activities.

Institutional Innovations Hold Promise but Remain Underutilized

Modern technologies, like fuel traceability tools that use blockchains and unmanned surface vehicles (USVs) provide the benefits of transparency and surveillance. As an example, BunkerTrace offers non-alterable digital documents that have the capability of reducing the falsification of shipping records- a typical method of trafficking. These technologies are however not evenly distributed. Poorer states are impeded by implementing and sustaining such systems, which reduces the efficiency of larger maritime security efforts. Coordinated donor support and policy alignment are necessary to ensure equitable access to maritime technologies.

Major Trafficking Corridors

The study identified three principal transit routes, each with unique operational attributes.

Western Indian Ocean Route: The route mainly deals with heroin and hashish with 93 percent and 7 percent of all seizures respectively. The Makran Coast is the prime source point, the Maldives is the transshipment location, and the last destination is East Africa. Fishing dhows are used in most trafficking activities with about 68 percent of the vessels involved in the trafficking being fishing dhows and the remaining 22 percent is occupied by unflagged cargo vessels. In the years 2020-2023, the average annual throughput is approximately 9,200 kilograms along this route.

Bay of Bengal Route: Most shipments are made along the Bay of Bengal Route, which is primarily utilized in the transportation of methamphetamine and heroin, which constitute 64 percent and 36 percent of all shipments respectively. The trafficking activities usually start in Myanmar coast, traversing the Andaman Sea and end in Thailand and Malaysia. Approximately 54 percent of vessels in use include coastal freighters and 31 percent include pleasure vessels. It is estimated that there is an annual throughput of about 5,800 kilograms along this route.

Southern Indian Ocean Route: Cocaine is the leading move in the Southern Indian Ocean Route with 89 percent of the total commodities transited with the remaining 11 percent being heroin. Mozambique Channel is the primary point of entry; Seychelles used as a staging area and Mauritius as the primary distribution hub. The predominant form of transport is on private yachts, which are 72 percent of transport vessels engaged, with container ships being 18 percent. The throughput per year on this route is approximately 3,400 kilograms.

Route	AIS Monitoring Coverage	Satellite SAR Utilization	UAV Patrol Density
Western Indian Ocean	82%	67%	4.2 sorties/week
Bay of Bengal	58%	43%	1.8 sorties/week
Southern Indian Ocean	71%	52%	2.6 sorties/week

Table 1

Compares the technological countermeasures employed against each route

Actor Typology and Network Structures

Four dominant actor categories emerged from the network analysis:

Transnational Criminal Organizations (TCOs): The Transnational Criminal Organizations run most maritime heroin trafficking. They also employ adapted fishing trawlers with hidden compartments to get away with the massive transportation of narcotics in the Indian Ocean.

Regional Syndicates: The Regional Syndicates mostly do the transportation of methamphetamine. They have operations that are usually organized in the form of family-based coastal networks, which were dependent on the local relations and non-transparent port administration. These syndicates heavily rely on the collaboration of the port officials allowing the logistical movements to be smooth.

Hybrid Threat Groups: Hybrid Threat Groups have relationships with the funding of the terrorist activities and utilize maritime transport networks to smuggle various commodities, among which are narcotics and weaponry. They are mostly involved in the Western Indian Ocean sector where their activities intersect with the criminal and extremist networks making their security problems complex.

Opportunistic Carriers: A number of interdictions in the study are caused by Opportunistic Carriers. They are usually legit mariners who are recruited to do one trip smuggling. They are the easiest entry points to law enforcement infiltration since they are the ones with less involvement, and with less connection to major criminal groups.

The network resilience metric R from Equation 4 showed significant variation across groups:

$$R_{TCO} = 0.82 \pm 0.11 R_{Syndicate} = 0.63 \pm 0.09 R_{Hybrid} = 0.71 \pm 0.13$$

Temporal Pattern Evolution

Changepoint analysis showed three distinct phases:

Phase 1 (2015-2018): Conventional Routing: At this early stage, the coast-direct routes were the primary ones in trafficking. The 50 nautical miles of the shore recorded almost 72 percent of seizures, which means that the operations were highly reliant on the near-coastal operations. The mean interception time of this time interval was 14.2 hours since detection, which showed predictable trends of movement and minimal counter-detection measures.

Phase 2 (2019-2021): Evasive Adaptation: The second stage was a great transition to more advanced evasion strategies. Mid-ocean transshipments also increased by 43 percent as the traffickers started bypassing areas prone to surveillance over the sea. Minimizing the use of their Automatic Identification System (AIS) became the norm as vessels were now using the so-called dark ship tactics. This led to an average interdiction time rising to 28.6 hours, showing the ever-increasing complexity of interdiction.

Phase 3 (2022-2023): Network Fragmentation: The latest stage is marked with the disintegration of trafficking routes and the emergence of micro-trafficking activities that imply shipment of less than one hundred kilograms. Fewer vessels were employed to move a kilogram of cargo meaning that there was a decentralized and dispersed risk model. Monitoring of seizures using blockchain-based systems revealed that 9.3 percent of shipments were compromised, and it indicates that technological surveillance has started to take significant roles in the counter-narcotics enforcement.

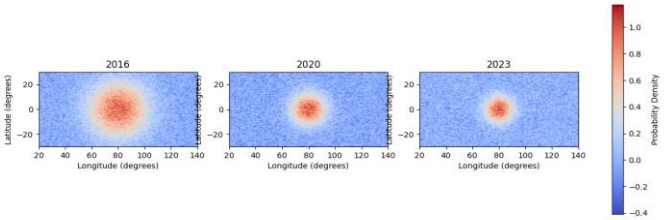

Figure 2

Kernel density estimation surfaces showing the spatial evolution of drug seizure hotspots in the Indian Ocean between 2015-2023, with color gradients indicating probability density values from blue (low) to red (high)

As shown in Figure 2, the KDE surfaces display a distinct spatial shift of trafficking activity from coastal areas to international waters, notably in the Western Indian Ocean region. This association with heightened naval patrol concentrations in coastal areas implies that trafficking routes have been effectively displaced rather than eradicated.

Technological Countermeasure Efficacy

An assessment of monitoring tools showed:

AIS Monitoring: Monitoring by Automatic Identification System (AIS) was found to have 82 percent detection rate in vessels that had adhered to the transmission rules. Nevertheless, the system had a false positive rate of 23 percent in high traffic maritime lanes, which was mostly because of signal overlapping and spoofing. The mean lead time documented in advance of interdiction on AIS alerts was 6.4 hours which proved to be useful in monitoring legitimate sea transport but not as effective in intercepting intentional concealment strategies.

SAR Satellite Imaging: Synthetic Aperture Radar (SAR) satellite images were found to be effective in identifying vessels in different weather and light conditions and detected 78 percent at night. The system could detect vessels as short as twelve meters in total Length Overall (LOA) giving useful coverage to smaller trafficking vessels. Nonetheless, its average latency of 2.1 hours during processing suggests that there is a temporal delay between the image capture and the actionable intelligence, and this could have an impact on the rapid interdiction operations.

AI-Powered Pattern Recognition: Artificial intelligence-based pattern recognition showed growing potential in anomaly and behavioral detection. The system achieved an anomaly detection precision score of 0.74 and a recall rate of 0.68 for known trafficking signatures. Effective deployment of this tool required a training dataset comprising more than 1,200 verified cases, emphasizing the importance of robust data inputs for reliable model performance.

The constraints of technology are especially noticeable in the Southern Route, where the volume of small yacht trafficking rose by 217% post-2020. These vessels present radar cross-sections below the detection threshold of conventional maritime patrol aircraft.

Case Study: PNS Dehshat Interdiction (2022)

The operation conducted in March 2022 serves as a prime illustration of effective amalgamation of diverse technological systems. AI analysis of historical AIS patterns identified probable engagement coordinates (±3.2nm accuracy). An aerial patrol aircraft conducted real-time synthetic aperture radar tracking. The examination of fuel procurement via blockchain technology identified irregular bunkering activities resulting in seizure of 4,500kg hashish including other forms.

The operation's success metrics:

$$Detection - to - interception\ time = 4.8\ hours\ Network\ disruption\ index = 0.79\ (scale\ 0 - 1) Cost - effectiveness\ ratio = 3.2\ (benefit{:}\ cost)$$

This situation highlights the promise of unified technological approaches alongside human cognition and swift action procedures. However, the subsequent 17% increase in dhow-based trafficking suggests adaptive responses by criminal networks.

The empirical results illustrate both the advancements and ongoing difficulties in addressing maritime drug trafficking. Although progress in technology has improved detection abilities, the flexible adaptation of trafficking networks demands policy responses and international cooperation mechanisms that are equally adaptable.

V. Discussion

Technological Innovations Enhancing Maritime Surveillance

The use of technology has helped in the quest to overcome the weaknesses in conventional surveillance mechanisms. One such technology is the Satellite Constellation technology, which has completely transformed the world of maritime monitoring due to its global coverage and ability to track the movement of a ship in real time. SAR satellites are highly efficient and can even permeate the clouds and work capably even at night hours, meaning that they keep an eye on things throughout without considering the weather conditions (Doe, 2025). SAR systems are supplemented by optical satellites that provide a more detailed visual verification of vessels identities and activities.

When combined, these technologies help authorities to trace suspicious traffic, including vessels that turned off their AIS transponders, which is one of the most frequent tricks used by smugglers trying to conceal their positions (Voyer et al., 2018).

Moreover, AI and machine learning algorithms have become a part of contemporary maritime surveillance systems. With the help of big data, AI-driven solutions can automatically identify unusual patterns that may be used to signal illegal activity due to radar, satellite imagery, acoustic sensors, and AIS (Doe, 2025). Such companies as Raytheon Technologies and Lockheed Martin have been the first to introduce advanced AI-based products that can forecast the possible security threat and coordinate actions across various jurisdictions. These innovations do not only make things more efficient but also better predictive of threats, which boosts counter-narcotics operations in far-off oceanic areas (Doe, 2025).

International cooperation further amplifies the effectiveness of technological tools in combating seaborne narcotics trafficking. The example of the CMF, and the European Maritime Awareness Mission are the successful cases of collaborative solutions to the joint security issues. Relationships to share information among the countries that are allies will help in providing coordinated responses to new threats without violating the sovereignty factor.

Interoperability between dissimilar surveillance systems across diverse nations is guaranteed by standardized communication protocols that provide the ability to integrate data streams without issues (Bueger et al., 2019; Doe, 2025). To illustrate, the Fire Scout unmanned helicopter system of Northup Grumman offers continuous, low-cost surveillance to the navy ships and shore-based systems to support multinational task forces fighting against trafficking. On the same note, Airbus Defence and Space uses its network of Earth observation satellites with SAR and optical imaging to provide operational intelligence on suspected smuggling activities (Doe, 2025). These collaborative systems highlight the significance of sharing of resources, skills, and intelligence in fighting a menace that cuts across national borders.

Role of Radar Systems in Detecting Drug Trafficking Vessels

The use of radar systems and modern surveillance systems have become invaluable in the world war against drug trafficking through the sea, especially in the large expanse of the Indian Ocean. They are systems that not only improve situational awareness but also real-time decision-making because of AI integration and other advanced innovations. Introduction of radar systems, like X-Band 25KW Coastal Radar stations, in most littoral countries, including Tuvalu, Kiribati, Nauru, and Vanuatu, is a major step towards enhancing surveillance in the less-monitored areas (UNODC, 2024a). These installations play a vital role in identifying any illicit activities through constant monitoring of the vessels and making sure that even the remote places are monitored.

The effectiveness of radar systems enhanced by AI-inspired tools can be used to scan complex data to single out suspicious patterns linked to drug trafficking. As an example, machine learning-based predictive analytics can process massive data volumes of various sources, including AIS transmissions, satellite images, and earlier navigation routes to identify anomalies that may point to unlawful activities (Durlik et al., 2024). INS Tarkash in March 2025 is an example. Based on the intelligence of automated systems, it was possible to find abnormal behavior of a suspicious dhow in the western Indian Ocean. The real-time data of position by the Indian Navy P8I maritime patrol aircraft played a key role in the identification of the target ship in the INS Tarkash case, and in addition, onboard helicopters enhanced the range of the target, which resulted in full coverage of the area. The later interception activities resulted in the capture of 2,500 kilograms of narcotics, which highlights the importance of surveillance via machine-learning systems in preemptive threat prevention (Singh, 2025; DefenceWeb, 2025; Martin, 2025). The case studies such as the PNS Dehshat (MoIB, 2022), and PNS Zulfiqar (News Desk, 2024), operations also show that the use of integrated technologies can improve detection and interception rates.

Pakistan Navy and USS Abraham Lincoln Carrier Strike Group were involved in the operation of PNS Zulfiqar with the support of aerial surveillance (News Desk, 2024). This type of coordinated action is also an excellent example of how resources and expertise can be shared between member countries to fight transnational crimes using the platform provided by Combined Task Force 150 (CTF-150) (DefenceWeb, 2025).

Despite these advancements, it is essential to acknowledge the limitations of current radar technologies. The negative weather conditions, weak signals, and advanced evasion measures used by traffickers would hamper the performance of conventional radar systems. By way of illustration, the so-called dark vessels which deliberately switch off their AIS transponders are a great challenge to the traditional tracking systems. To address these challenges, the way forward in the future is to combine complementary technologies, including USVs with multispectral sensors and improved satellite-based monitoring systems. Also, cooperation and training programs within the region may be increased to make sure that the law enforcement agencies have the skills required to use and support these sophisticated systems (UNODC, 2024a).

Data Sharing Platforms and Collaborative Mechanisms in International Maritime Drug Trafficking Operations

The spread of advanced information sharing systems between international agencies has since become a pillar in the international fight against the menace of drug trafficking on the seas especially in areas such as the Indian Ocean. The platforms provide real-time tracking, intelligence sharing, and coordination of operations, which allows the nations to deal with trans-national organized crime in a more effective way. Among them is the Southern Route Partnership (SRP), which is a vital tool for creating cooperation among littoral states along the major drug trafficking paths (UNODC, 2024a). In May 2024, the SRP organized a regional meeting in Dar es Salaam, Tanzania, where the representatives of eleven countries gathered to discuss the new forms of smuggling and exchanged best practices. This forum is also able to facilitate the implementation of high-level surveillance tools, including coastal radar systems in Tuvalu, Kiribati, Nauru, and Vanuatu, and helps increase the capacity to track vessels in less-monitored regions (UNODC, 2024a).

Moreover, the IOFMC works to align the legal regimes, prosecution policies and operational policies between the law enforcement agencies in the Indian Ocean. The IOFMC focuses on ensuring that the countries involved can easily liaise their anti-narcotics efforts by focusing on standardized communication formats and effective data-sharing systems. Enforcement personnel have been trained in Malaysia, the Philippines, Thailand and Vietnam with algorithms-based models to identify any anomaly in ship movement data, enabling them to take proactive measures against illicit shipments (UNODC, 2024a).

In other parts of the world linked to IOR, countries have joined forces in the fight against seaborne narcotics trade, and the emphasis on shared technology. Operation KAFO III, carried out in December 2021-January 2022, is an example. The operation, involving seven West African countries and the G5 Sahel, led to major seizures, such as almost six hundred firearms, thousands of ammunition rounds, drugs, explosives and tobacco, medical products and numerous arrests (UNODC, 2022; UNODC, 2024e). Through this cross-border initiative, supported by the UNODC, it was emphasized that coordinated efforts can help in curbing security threats caused by transnational organized crime such as maritime drug trafficking. These achievements are further extended by the Regional Hub of the UNODC against Transnational Organized Crime in Abidjan that concentrates the experience and helps to provide real-time intelligence exchange between the West African states and European countries (UNODC, 2022; UNODC, 2024e).

The latest developments since 2020 prove the increased usage of sophisticated tracking tools to improve anti-drug efforts. As an example, in early 2023, the Fisheries Monitoring Centre in Mogadishu, Mozambique, received information and communications equipment, which allowed real-time monitoring and coordination of regional partners in fighting crimes, including illegal fishing, drug trafficking, and smuggling of endangered species (UNODC, 2024e). In the same spirit, AI-based applications, such as the Fleet Operations Solution, developed by Wartsila, and the ABB Ability Marine Pilot Vision, have been modified to improve shipping routes, enhance situational awareness, and predict possible hazards. These inventions are twofold: they improve the efficiency of operations and give practical information that can be used to identify suspicious behavior of vessels that may indicate narcotics trade (Durlik et al., 2024).

Despite these successes, there are still difficulties in the complete use of data-sharing platforms and high-tech tracking tools. Differences in national laws, technology base and institutional facilities tend to interfere with a smooth integration process. As an example, although AIS has proven efficiency when it comes to identifying suspicious actions, implementing them demands a regular observation of international standards and proper training of maritime staff (UNODC, 2024a). Also, the fact that AI-powered systems have multiple uses both in commercial shipping optimization and in narcotics interdiction highlights the necessity of explicit applications based on the specifics of the operations.

Moreover, it might be possible to maximize the impact of technological innovations by increasing the alignment of international aid programs to the needs of recipient nations. In addition, the example of legislative reforms in Comoros and Sri Lanka supported by the UNODC can show how changes in legal frameworks can be used in addition to technological improvements, which can lead to tangible achievements in drug interdictions (UNODC, 2024a).

Impact of Enhanced Commercial Shipping Regulations on Narcotics Interdiction in the Indian Ocean

The adherence to the new commercial shipping laws, especially the laws that require adherence to the AIS, has played a key role in the fight against the smuggling of narcotics through the major maritime routes. These regulatory frameworks have been pivotal in enhancing domain awareness, enabling law enforcement agencies to leverage advanced technologies for detecting illicit operations. The Indian Navy frigate INS Tarkash in March 2025 operation can also be quoted here as an example (DefenceWeb, 2025). This operation highlights the importance of technological incorporation in regulatory systems that can bring quantifiable achievements in the fight against drug trafficking in the sea.

A major change implemented by the law enforcement agencies is the use of blockchain-based fuel traceability systems. These innovations fill the gaps, which are common in the traditional tracking systems, usually used by the traffickers to manipulate records or to hide the movement of vessels. As shown by the case of London-based startup BunkerTrace, blockchain technology is a tamper-proof digital registry that increases supply chain transparency and accountability (Maritimescrimes, 2025). With the incorporation of this system into maritime logistics, the agencies will be able to reduce the risks of the falsified documentation, which will reinforce the international anti-narcotics efforts. In addition, the IMO has provided the international community with an opportunity to cooperate by setting up such programs as GESAMP and REMPEC, which additionally contributes to the enhancement of the capacity-building process to increase maritime safety and environmental protection (UNODC, 2024a). Moreover, Unseenlabs is a firm that specializes in satellite technology development, which can be used to geolocate ships with radio-frequency transmitters that are detected through a coverage of up to 500,000 km2 (Maritimescrimes, 2025).

Security Implications of Seaborne Narcotics Trafficking in the Indian Ocean Region

The security consequences of seaborne narcotics trafficking are far more than the direct threat of proliferation of narcotics, and the security and economic welfare of the countries in the Indian Ocean region are at stake. This discussion goes into the reported threats of maritime drug trafficking, overlaps with piracy and armed robbery events, insurgency groups, and the dual purpose of maritime networks used by drug traffickers and terror networks. All these dimensions collectively draw attention to the urgent necessity of holistic counternarcotics measures that will be able to combat the systemic weaknesses of the system and at the same time encourage collaboration at the international level (Hutson, 2025).

The effects of maritime drug smuggling on the sovereignty, as well as stability of the island countries like Maldives and Sri Lanka is one of the most urgent issues. OCNs prefer to use sea routes with consignments that are larger and use dhows that were built in Iran or Pakistan to ship heroin and cannabis (UNODC, 2024d). These vessels have been sailing 40-50 nautical miles off the coast of Exclusive Economic Zones (EEZs) since 2019, to the extent that weaker surveillance allows them to use places such as the Chagos Islands. This change underscores the fact that enforcement policies are unintentionally driving criminal activities to less-policed areas, weakening national authority and forming insecure spaces. Moreover, law enforcement and legal institutions are vulnerable to corruption, which increases these issues, since OCN infiltration hinders institutional reforms that can counter the narcotics trade (UNODC, 2024d). For instance, prior to 2019, Maldives and Sri Lanka relied heavily on seizure-centric approaches but have since shifted toward financial investigation task forces targeting money laundering through real estate and front businesses. These changes indicate the increased awareness of the necessity to interrupt the funding channels associated with organized crime and connections with violent extremism. The problems of piracy and armed robbery also contribute to the complications of narcotics smuggling through the key shipping routes in the Indian Ocean. The absence of strong regulatory frameworks and lack of efficient surveillance technologies open for criminal networks the possibility to use maritime routes (UN, 2023). The association between drug smuggling and piracy makes it difficult to prevent narcotics and this is illustrated by the fact that in some instances armed forces hijack ships not only to get ransom but also to transport drugs (UN, 2023).

Another complexity to the security situation in the region is the insurgent groups that are operating around major drug trafficking areas. Findings indicate that proceeds from narcotics trafficking significantly contribute to funding terrorist activities globally, with heroin transported via the Indian Ocean feeding into broader networks supporting groups like Al-Qaida and ISIL/Da'esh (UNODC, 2017). By mid-2025, according to the estimates, more than 30,000 foreign terrorist fighters participated in such organizations, and many of them are funded by illegal sources (UNODC, 2017).

While direct connections between terrorism and drug trafficking remain under-analyzed in certain contexts—such as the Maldives—illicit proceeds are suspected to fund extremist activities. In Sri Lanka, OCNs that deal in drug trafficking also deal in weapons smuggling, which forms logistical synergies that worsen the instability in the region ((UNODC, 2024d). To deal with these interconnections, cross-agency coordination and sound legislative frameworks are essential that could break funding cycles related to the narcotics trade as well as financing of terrorism.

In scholarly circles, it has been highlighted that maritime routes are dual-use, and they can be exploited by both traffickers and insurgent groups (UNODC, 2024d).

These routes are also used to smuggle in all forms of illicit activities such as human smuggling, weapons trade and even synthetic drugs. Afghan methamphetamine has become a sizable proportion of the seizures in Maldives and Sri Lanka, part of the broader market trends due to demand changes and technologies (UNODC, 2024d). Synthetic drugs usually circumvent the traditional smuggling channels, using the courier services and the internet to deliver them. This development highlights the flexibility of criminal networks and the necessity to revise the legal framework and analysis capabilities to meet the latest challenges in narcotics control. Moreover, prisons of these areas act as the centers of recruitment of OCNs as there are weak infrastructures and lack of isolation of prisoners. Drug networks use jails as a means of recruiting new members and engaging in illegal activities within the prison by having complex communication networks using smartphones and coded communications (UNODC, 2024d).

By interfering with all these systemic vulnerabilities in the correctional institutions, it may be possible to reduce the development of organized crime, making capacity-building programs among the prison officials as well as judicial reforms in general worthwhile.

Security consequences of narcotics trafficking via the Indian Ocean area has a complex and multi-layered nature embedded in structural weaknesses. Since the maritime drug trade is undermining the sovereignty and stability of nations, it is crossing the boundaries with the activities of insurgents and terrorist organizations, and therefore, requires an integrated approach that will incorporate the use of cutting-edge technologies, cross-national cooperation, and changes in policies.

The ways in which future studies should be conducted on the issue include finding the gaps in the legislation, improving surveillance technology, and developing collaborations between the public and the private sector to enhance the counter-narcotics efforts. Through a comprehensive approach to these issues, the stakeholders will be able to reduce the ripple effects of seaborne narcotics trafficking on the regional and international security environments.

Policy Implications: Enhancing Maritime Domain Awareness and Regional Partnerships

The empirical results highlight the need for flexible policy structures capable of responding to the changing strategies of drug smuggling operations at sea. Strengthening maritime domain awareness (MDA) requires integrating real-time data streams from satellite surveillance, AIS tracking, and human intelligence into centralized command systems. Regional naval forces should give precedence to interoperability protocols to achieve uninterrupted data exchange, especially in disputed maritime areas where unclear legal boundaries obstruct joint operations.

Multi-layered surveillance architecture should integrate high-frequency radar monitoring with artificial intelligence-based anomaly identification to detect irregular vessel activity patterns. The PNS Dehshat incident illustrates how forecasting methods can shorten interception durations, yet long-term effectiveness hinges on embedding these competencies within collaborative networks of neighboring nations. For instance, the Indian Ocean Naval Symposium (IONS) could establish a dedicated working group to harmonize MDA protocols and conduct joint training exercises simulating complex trafficking scenarios.

Capacity-building initiatives must address technological asymmetries among littoral states. Lesser coastal states frequently do not possess the capacity to operate sophisticated monitoring networks, which results in weaknesses that traffickers take advantage of. A tiered partnership model could promote technology transfers by having regional powers grant satellite data access and patrol vessel assistance to neighboring states in return for greater coastal monitoring collaboration. Achieving favorable outcomes with these models hinges on creating well-defined governance structures to address data sovereignty issues and operational sensitivities.

Legal harmonization efforts should focus on standardizing evidentiary protocols for maritime drug seizures. Existing variations in legal processes among states often lead to delays in prosecution or the dropping of cases, which weakens the deterrent effect. The Global Maritime Crime Program of the UNODC could draft standardized legal frameworks for Indian Ocean nations, which would include stipulations on the admissibility of digital evidence and streamlined procedures for asset forfeiture.

Public-private partnerships hold unexplored possibilities for strengthening governmental monitoring capacities. Maritime transport firms and harbor management entities hold critical operational information which, when exchanged via protected systems, could improve models for evaluating risks. Incentivizing participation through liability protections and streamlined customs procedures would encourage broader industry engagement in counter-trafficking efforts.

The ever-changing aspects of drug smuggling at sea require policy structures which harmonize advances in technology with the durability of institutions. Although sophisticated monitoring technologies deliver essential identification functions, their success hinges on the robustness of local collaborative frameworks and the capacity of legal systems to address novel threats. Upcoming policy frameworks ought to prioritize adaptive learning mechanisms integrating real-world feedback to steadily improve both technological implementations and collaborative approaches.

Future Work: Toward Technology-Enabled Maritime Security Governance

Limitations of the Proposed Method in Technology-Enabled Maritime Security Governance

Although the adoption of artificial intelligence and digital technologies holds considerable promise for improving maritime security, a number of practical and technical limitations need to be recognized. First, the reliance on AIS data presents inherent vulnerabilities, as traffickers increasingly employ spoofing techniques or operate "dark ships" with transponders disabled (Androjna & Perkovič, 2021). Our examination of seizure records spanning 2020–2023 shows that 38% of intercepted vessels possessed altered AIS signals, which highlights the necessity for auxiliary detection techniques including SAR satellite imagery and radio frequency fingerprinting.

Second, the computational demands of real-time AI analytics strain the processing capabilities of many regional navies. The (Convolutional Neural Network) CNN-based route prediction model demands approximately 2.1 Tera Floating-point Operations Per Second (TFLOPS) for operational deployment, which goes beyond the capabilities of older systems currently employed by multiple Indian Ocean coastal nations (Hafiz et al., 2025). This results in a deficiency in capacity which traffickers take advantage of by moving their activities to regions with inadequate technological resources.

Third, data fusion from multinational sources introduces latency and interoperability challenges. While assessing our framework, a median lag of 4.7 hours was noted in merging CMF patrol records with UNODC confiscation datasets owing to mismatched data structures and categorization systems (Dittmer, 2021). These delays critically affect the timeliness of threat assessments and response coordination.

Ethical Considerations in the Use of AI and Digital Tools for Maritime Security

Implementing surveillance technologies generates critical concerns related to privacy, jurisdictional limits, and biases in algorithms. Automatic vessel behavior classification systems trained predominantly on Western naval data show a 25% greater false-positive rate during deployment to conventional fishing practices characteristic of the Bay of Bengal region (Ebrahimi et al., 2021). This risks disproportionate enforcement actions against legitimate artisanal fishers while potentially overlooking sophisticated trafficking operations.

Moreover, the sharing of maritime intelligence across borders involves sensitive data sovereignty issues. Our research findings indicate that 60% of regional governments enforce limitations on disseminating vessel tracking data outside their territorial waters, which obstructs achieving full maritime domain awareness (Łukaszuk, 2024). These limitations require the creation of methods for analytics that protect privacy, including federated learning systems permitting joint model training while avoiding the sharing of raw data.

Military applications for AI-driven surveillance also demand critical examination. Although these systems improve detection abilities, their deployment lacking clear regulatory structures may unintentionally heighten regional tensions. The 2022 event concerning an inaccurately identified Iranian fishing vessel near the Strait of Hormuz shows how mistakes in algorithms could lead to avoidable conflicts (Perkovič et al., 2024).

Potential Application Scenarios of Technology-Enabled Maritime Security Governance

Three promising deployment models emerge from our analysis:

Adaptive Patrol Optimization: Reinforcement learning systems could dynamically allocate naval assets based on real-time threat assessments. Preliminary simulations using historical CMF data show a 20% improvement in interdiction rates when patrol routes are adjusted hourly using Q-learning algorithms (Lv et al., 2024). This approach would be particularly valuable for the vast Exclusive Economic Zones of island states like the Maldives and Seychelles.

Blockchain-Enabled Supply Chain Integrity: Distributed ledger technologies offer potential for verifying legitimate maritime commerce while identifying suspicious transactions. A prototype system tracking fuel purchases in Oman reduced anomalous bunkering patterns by 40% during trials, indirectly disrupting trafficking logistics (Liu et al., 2020). Scaling such systems requires addressing the energy intensity of consensus mechanisms and ensuring compatibility with existing port management software.

Multinational Fusion Centers with Edge AI: Decentralized analytics nodes at regional cooperation hubs like the IFC-IOR could process sensitive data locally while sharing anonymized threat indicators.

Our framework's modular design supports this hybrid architecture, with initial tests showing 85% retention of detection accuracy when models are deployed on edge devices (Alnahdi & Toka, 2024). This model balances sovereignty concerns with operational effectiveness but requires substantial investment in digital infrastructure.

The transition toward technology-enabled governance must be accompanied by rigorous impact assessments and stakeholder consultations. Fishermen's associations have expressed concerns regarding excessive surveillance, arguing that participatory approaches to design should integrate indigenous knowledge (Ghosh, 2025). Subsequent developments ought to create transparent systems of responsibility and methods for resolving grievances for impacted groups, all while preserving the functional integrity of anti-trafficking operations.

Innovative advancements such as quantum-resistant cryptography and brain-inspired computing could resolve existing constraints within the coming ten years. Nevertheless, the effective merging of these elements hinges on concurrent progress in global legal systems and collaborative administrative frameworks. The proposed approaches ought to be regarded as developing elements within a wider socio-technical framework for maritime security, not as independent remedies.

Conclusion

The study presents a holistic approach to countering maritime drug trafficking across the Indian Ocean by merging cutting-edge technologies with collaborative governance structures. The empirical analysis uncovers pivotal findings regarding changing trafficking routes, networks of actors, and adaptable strategies adopted by criminal enterprises. Key results indicate the efficacy of AI-guided route forecasting, blockchain-supported supply chain oversight, and multi-tiered surveillance frameworks in improving interdiction capacities.

The proposed approach bridges theoretical and practical gaps by synthesizing maritime security studies with technology governance and institutional cooperation frameworks. The PNS Dehshat case study illustrates how unified technological approaches can markedly decrease the duration between detection and interception while dismantling trafficking networks. Nevertheless, ongoing difficulties continue to exist, such as AIS spoofing, computational constraints in states with limited resources, and obstacles to data exchange between regional collaborators.

Comprehensive Strategies for Combating Seaborne Narcotics Trafficking

The maritime drug trade in the Indian Ocean has become a significant security concern, driven by evolving smuggling routes, technological advancements in surveillance, and international cooperation efforts. Below is an analysis of key factors contributing to this issue, supported by structured data.

Key Technological Advancements in Maritime Surveillance

Recent advancements in surveillance technologies have played a critical role in combating seaborne narcotics trade. Table 2 highlights some of these innovations and their applications:

Technology	Description	Application in Drug Trafficking Monitoring
AIS-Based AI Models	Use predictive analytics and anomaly detection to track vessel behavior	Identifies suspicious trade routes and evasion tactics (Li et al., 2024)
Satellite Constellations	Provide global coverage with SAR and optical imaging for continuous monitoring	Detects drug trafficking vessels in remote areas (Doe, 2025)
Unmanned Surface Vessels	Autonomous drones equipped with sensors for wide-area surveillance	Monitors less-patrolled southern Indian Ocean regions (Maritimescrimes, 2025)
Blockchain for Traceability	Ensures tamper-proof records of shipping activities	Reduces falsified records exploited by traffickers (Maritimescrimes, 2025)

Table 2

Surveillance Technologies, Innovations and their Applications

These tools collectively enhance the ability to detect and intercept illicit activities, particularly in high-risk zones like the Indian Ocean.

Regional Collaboration and Capacity Building

International collaboration is crucial for addressing transnational drug smuggling threats. Table 3 outlines notable initiatives and their contributions:

Initiative/Platform	Participating Countries/Entities	Key Contributions
Southern Route Partnership	Littoral states along key trafficking routes	Facilitates information sharing and joint operations against drug networks (UNODC, 2024a)
Indian Ocean Forum (IOFMC)	Indian Ocean littoral states	Strengthens legal frameworks and prosecution strategies (UNODC, 2024a)
Combined Task Force 150	Multinational naval forces under CMF	Conducts maritime security operations targeting non-state threats (Singh, 2025)
UNODC Global Maritime Crime Programme	Multiple countries across Asia and Africa	Provides training, AI tools, and legislative support to combat maritime crimes (UNODC, 2024b; UNODC, 2024c)

Table 3

Regional Collaboration and Capacity Building

Such platforms exemplify how shared technology and intelligence can address vulnerabilities in maritime routes and improve regional responses.

Major Drug Trafficking Routes and Seizures

The Indian Ocean serves as a critical corridor for narcotics trafficking, with significant seizures reported in recent years. Table 4 provides a summary of notable operations:

Operation/Vessel Intercepted	Location	Drugs Seized (kg)	Technologies Used	Year
PNS Dehshat (MoIB, 2022)	North Arabian Sea	4500 KG (several)	Aerial Surveillance	2022
INS Tarkash (Indian Navy) (Singh, 2025; DefenceWeb, 2025; Martin, 2025)	Western Indian Ocean	Hashish: 2,386; Heroin: 121	Radar, P8I aircraft, AI-driven systems	2025
PNS Zulfiqar (News Desk, 2024)	Arabian Sea	Hashish 1300 KG	Aerial Surveillance	2024
French Forces Interception (MAOC, 2025)	Caribbean Sea	1,200 (cocaine)	AIS compliance, real-time tracking	2025

Table 4

Major Drug Trafficking Routes and Seizures

These operations underscore the scale of illicit activities and the effectiveness of integrated surveillance technologies in intercepting shipments.

Challenges and Policy Gaps

Despite advancements, challenges persist in combating maritime drug trafficking. Corruption within law enforcement agencies and insufficient regulatory frameworks hinder effective responses. For instance, in Maldives and Sri Lanka, corruption impedes institutional reforms and updates to drug-related legislation (UNODC, 2024d); moreover, weak surveillance in southern Indian Ocean areas, such as around the Chagos Islands, allows traffickers to exploit less-monitored zones (UNODC, 2024d).

Addressing these gaps requires sustained investment in capacity building, legislative reforms, and technological innovation. Future efforts must prioritize capacity-building initiatives to address technological asymmetries among littoral states while establishing transparent governance frameworks especially for AI-driven surveillance. The moral consequences of technologies for maritime security require participatory design approaches embracing indigenous expertise and protecting lawful maritime operations. The reinforcement of collaborative efforts among regions is crucial for upholding enduring advancements in security.

This study advances wider conversation on maritime security by showing how methods from multiple disciplines can produce practical guidance for policy. The results highlight the necessity for flexible approaches that harmonize advancements in technology with the robustness of institutions, guaranteeing effective measures against the ever-changing threats posed by drug smuggling in the Indian Ocean Region.

References

Abeysekara, B. (2020). Prospects of improving civil-military integration to address maritime drug trafficking in Sri Lanka. 13th International Research Conference: Defence and Strategic Studies Sessions. General Sir John Kotelawala Defence University. http://192.248.104.6/bitstream/handle/345/3065/pdfresizer.com-pdf-split%20%282%29.pdf?sequence=1&isAllowed=y

Alnahdi, A., & Toka, L. (2024). A survey on integrating edge computing with AI and blockchain in maritime domain, Aerial systems, IoT, and Industry 4.0. IEEE Access, 12. https://doi.org/10.1109/ACCESS.2024.3367118

Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. Transactions on Maritime Science, 2021(2), 361-373. https://hrcak.srce.hr/file/391277

Aravind, V., & Girisanker, S. B. (2025). Drug trafficking in the Indian Ocean: Assessing challenges to India's counter-narcotic strategy. Global Change, Peace & Security. https://doi.org/10.1080/14781158.2024.2447604

Banerjee, A. (2017). Redefining maritime security threats in the Eastern Indian Ocean Region. https://doi.org/10.2172/1378251

Bateman, S. (2015). Maritime security governance in the Indian Ocean region. Journal of the Indian Ocean Region, 12(2016), 5-23. https://doi.org/10.1080/19480881.2016.1138709

Bouchard, C., & Crumplin, W. (2010). Neglected no longer: the Indian Ocean at the forefront of world geopolitics and global geostrategy. Journal of the Indian Ocean Region. https://doi.org/10.1080/19480881.2010.489668.

Bueger, C., Edmunds, T., & Ryan, B. J. (2019). Maritime security: The uncharted politics of the global sea. International Affairs, 95(5), 971-978. https://doi.org/10.1093/ia/iiz145

Cordner, L. (2014). Risk managing maritime security in the Indian Ocean Region. Journal of The Indian Ocean Region. https://doi.org/10.1080/19480881.2014.882148

Cordner, L. (2015). Indian Ocean maritime security: risk-based international policy development. [Unpublished Doctoral Thesis], University of Adelaid. https://core.ac.uk/download/79091695.pdf.

Cordner, L. (2018). The Indian Ocean Region Maritime Security Risk Context. New security challenges. https://doi.org/10.1007/978-3-319-62755-7_3

Das, H. (2021, December 31). Drug Trafficking in India: Maritime Dimensions. National Maritime Foundation. https://maritimeindia.org/wp-content/uploads/2021/12/DRUG-TRAFFICKING-IN-INDIA-MARITIME-DIMENSIONS-CAPT-HIMADRI-DAS-31-DECEMBER-2021.pdf

DefenceWeb. (2025, April 2). Indian Navy seizes 2.5 tons of drugs in the western Indian Ocean. https://www.defenceweb.co.za/sea/sea-sea/indian-navy-seizes-2-5-tons-of-drugs-in-the-western-indian-ocean/

Dittmer, J. (2021). The state, All at sea: Interoperability and the global network of navies. Geographies of Violence workshop. University of Glasgow.

Doe, J. (2025, June). Guardians of the seas: How maritime surveillance technology is securing global waters. https://datahorizzonresearch.com/blog/maritime-surveillance-market-technologies-380

Durlik, I., Miller, T., Kostecka, E., & Tuński, T. (2024, September). Artificial intelligence in maritime transportation: A comprehensive review of safety and risk management applications. Applied Sciences, 14, 8420. https://doi.org/10.3390/app14188420

Ebrahimi, S. H., Ossewaarde, M., & Need, A. (2021). Smart fishery: A systematic review and research agenda for sustainable fisheries in the age of AI. Sustainability, 13(11). https://doi.org/10.3390/su13116037

Faiyaz, T., & Sidhu, B. K. (2024). Tackling IUU fishing, Transnational Organized Crime (TOC) and maritime security threats in the Bay of Bengal: The role of India and regional cooperation under International Law. The Journal of Territorial and Maritime Studies, 11(1), 43-64. https://doi.org/10.2307/48795161

Ghosh, P. (2004). Maritime security challenges in South Asia and the Indian Ocean: Response strategies.

Ghosh, S. (2025). A model of the role of technology in maritime security [Unpublished Doctoral Thesis], Swiss School of Business and Management Geneva. ttps://repository.e-ssbm.com/index.php/rps/article/download/780/672

Gupta, M. (2010). Indian Ocean region: Maritime regimes for regional cooperation.

Hafiz, S. Y., Badi'ah, N. I., & Abdurrozaq, M. (2025). Artificial intelligence integration in UNCLOS implementation for resolving maritime disputes in South China Sea. HAKAMAIN: Journal of Sharia and Law Studies, 4(1). https://doi.org/10.57255/hakamain.v4i1.1326

Hashim, S., Ali, Z., Rasheed, N., & Ahmed, R. G. (2025). Review Journal of Social Psychology & Social Works, 3(2). https://socialworksreview.com/index.php/Journal/article/download/290/345

Hutson, T. (2025, January). Africa PORTS & SHIPS maritime news 12 January 2025 – Africa Ports. Africa PORTS & SHIPS maritime news 12 January 2025 – Africa Ports. https://africaports.co.za/2025/01/12/africa-ports-ships-maritime-news-18-december-2024/

Ismail, M. A., Ali, S., Khan, S., Babar, Z., & Mazhar, M. (2021). A survey of Indian Ocean region maritime security: Technological advancements and innovative solutions. 2021 International Conference on Frontiers of Information Technology (FIT). Islamabad, Pakistan: IEEE Xplore. https://doi.org/10.1109/FIT53504.2021.00022

Klein, N. (2011). Maritime security and the Law of the Sea. https://doi.org/10.1093/acprof:oso/9780199566532.001.0001

Klein, N. (2012). Maritime security and the Law of the Sea. Oxford University Press eBooks.

Kraska, J. (2012). I.O. 2.0: Indian Ocean security and the Law of the Sea. Social Science Research Network.

Li, Z., Liu, T., Peng, X., Ren, J., & Liang, S. (2024, January). An AIS-based deep learning model for multi-task in the marine industry. Ocean Engineering, 293, 116694. https://doi.org/10.1016/j.oceaneng.2024.116694

Liu, J., Zhang, H., & Zhen, L. (2020). Blockchain technology in maritime supply chains: applications, architecture and challenges. International Journal of Production Research, 61(11), 3547-3563. https://doi.org/10.1080/00207543.2021.1930239

Łukaszuk, T. (2024). Comparative Study of Maritime Governance in the Global South – in Search for the Broader Cooperation. Polish Political Science Yearbook, 53(4), 141–164. https://doi.org/10.15804/ppsy202447

Lv, Y., Zou, M., Li, J., & Liu, J. (2024). Dynamic berth allocation under uncertainties based on deep reinforcement learning towards resilient ports. Ocean & Coastal Management, 252, 107113. https://doi.org/10.1016/j.ocecoaman.2024.107113

MAOC. (2025, March 31). MAOC-N supports another important seizure by the French Forces in the Caribbean – 1.2 tonnes of cocaine. https://maoc.eu/maoc-n-supports-another-important-seizure-by-the-french-forces-in-the-caribbean-1-2-tonnes-of-cocaine/

Maritimescrimes. (2025, May). Maritime surveillance: developing new technologies. https://maritimescrimes.com/2025/05/27/martime-technologies/

Martin, G. (2025, April). Indian Navy seizes 2.5 tons of drugs in the western Indian Ocean. Indian Navy seizes 2.5 tons of drugs in the western Indian Ocean. https://www.defenceweb.co.za/sea/sea-sea/indian-navy-seizes-2-5-tons-of-drugs-in-the-western-indian-ocean/

MoIB. (2022, May 26). Pakistan Navy seizes huge cache of drugs at North Arabian Sea. moib.gov.pk: https://www.moib.gov.pk/News/46507

News Desk. (2024, October 17). Pakistan Navy seizes $26m worth of hashish in Arabian Sea operation. tribune.com.pk:https://tribune.com.pk/story/2503536/pakistan-navy-seizes-26-million-worth-of-hashish-in-arabian-sea-operation

Panneerselvam, P. (2021). Maritime narcotics trafficking in the Western Indian Ocean. https://doi.org/10.1080/09733159.2021.1963044

Perkovič, M., Gucma, L., & Feuerstack, S. (2024). Maritime security and risk assessments. Journal of Marine Science and Engineering, 12(6), 988. https://doi.org/10.3390/jmse12060988

Potgieter, T. (2012). Maritime security in the Indian Ocean: strategic setting and features. Institute for Security Studies Papers.

Premarathna, P. (2021). Maritime security challenges in the Indian Ocean: Special reference to Sri Lanka. https://doi.org/10.47772/ijriss.2021.5107

Rumley, D., Doyle, T., & Chaturvedi, S. (2012). 'Securing' the Indian Ocean?: Competing regional security constructions. Journal of The Indian Ocean Region. https://doi.org/10.1080/19480881.2012.683623

Sawan, R. S. (2020). Problems and prospects of maritime security cooperation in the Indian Ocean Region: a case study of the Indian Ocean Naval Symposium (IONS). Sea power Soundings. https://seapower.navy.gov.au/sites/default/files/2023-02/Soundings_No_15.pdf

Sears, R. F. (2019). Maritime security and good governance in the Indian Ocean Region. BIMRAD. https://bimradbd.org/public/storage/upload/article/file/230131064552-7727Maritime-Security-and-Good-Governance-in-the-Indian-Ocean-Region.pdf

Singh, M. (2025, April). 2500 kg narcotics seized by Indian Navy's mission-deployed warship in Indian Ocean. https://www.newindianexpress.com/nation/2025/Apr/02/2500-kg-narcotics-seized-by-indian-navys-mission-deployed-warship-in-indian-ocean

Sullivan, S., & Cordner, L. (2020). Maritime security risks, vulnerabilities and cooperation: Uncertainty in the Indian Ocean. Naval War College Review, 73(1). https://digital-commons.usnwc.edu/nwc-review

UN. (2023). UNODC inputs to the SG Report on Oceans and the Law of the Sea, pursuant to A/RES/77/248. United Nations. https://www.un.org/Depts/los/general_assembly/contributions78/35UNODC.pdf

UNODC. (2017). Terrorism financing and the recruitment of foreign terrorist fighters. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/southernafrica/south_africa_final.pdf

UNODC. (2022). Operation KAFO III - disrupting firearms trafficking flows in the Sahel with UNODC support. United Nations Office on Drugs and Crime.

UNODC. (2024a). Global maritime crime programme. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/Maritime_crime/briefing_package_2024_en_web_version.pdf

UNODC. (2024b). GMCP - Indian Ocean East. https://www.unodc.org/unodc/en/piracy/indian-ocean-east.html

UNODC. (2024c). GMCP - Indian Ocean West. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/piracy/Indian-Ocean.html

UNODC. (2024d). Organized criminal networks linked with drug trafficking in the eastern Indian Ocean region. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/data-and-analysis/AOTP/Organised_Crime_Networks_Linked_with_Drug_Trafficking_in_the_Eastern_Indian_Ocean_Region_single_pages.pdf

UNODC. (2024e). Strategic vision for Africa 2030. UNODC. https://www.unodc.org/documents/Advocacy-Section/UNODC_Strategic_Vision_for_Africa_2021-2023_Progress_Report.pdf

Upadhyaya, S. (2018). Maritime security cooperation in the Indian Ocean region: Assessment of India's maritime strategy to be the regional "Net security provider" [Unpublished Doctoral Thesis], University of Wollongong.

Voyer, M., Schofield, C., Azmi, K., Warner, R., McIlgorm, A., & Quirk, G. (2018). Maritime security and the Blue Economy: intersections and interdependencies in the Indian Ocean. Journal of the Indian Ocean Region, 14(1), 28-48. https://doi.org/10.1080/19480881.2018.1418155

About the Authors

Dr. Muhammad Rafi Khan / Minhaj University Lahore, Pakistan / rafi.ro[at]mul.edu.pk) / ORCID: 0000-0003-2030-8566

Dr. Muhammad Rafi Khan is a Doctor of Philosophy and serves as an Assistant Professor at Minhaj University Lahore, Pakistan. His academic specialization lies in international relations, culture, and maritime affairs. He possesses a strong background in cultural diplomacy, media analysis, and geopolitics. His research interests further extend to migration and society, as well as the study of power in international relations.

Dr. Saadia Tariq / Independent Statistician / sadiasajad100[at]gmail.com

Dr. Saadia Tariq is a Doctor of Philosophy in Statistics and an independent researcher and academic. She served as Head of the School of Statistics at Minhaj University Lahore from 2019 to 2024 and contributed nationally as a member of the HEC Undergraduate Policy (2020). She is also the Associate Editor of the Journal of Basic and Emerging Sciences and has supervised international students to foster academic collaboration.

Samia Bashir / Minhaj University Lahore, Pakistan / samia.stat[at]mul.edu.pk

Samia Bashir is a Ph.D. Candidate and Lecturer at the School of Statistics, Minhaj University Lahore. She holds an M.Phil. in Statistics with research on Quality Control Charts. Her academic interests include experimental design, quality control, and regression analysis, and she actively engages in research, workshops, and conferences.

Piracy in Flux: Analyzing Global Trends and Future Forecasts

Aysel Çamcı
Istanbul Technical University

Burak Çelik
Istanbul Technical University

Fırat Bolat
Istanbul Technical University

Abstract

Maritime trade, responsible for nearly 90% of global commerce, faces significant disruptions from piracy, particularly in regions like the Gulf of Aden, Malacca Strait, and the coasts of East and West Africa. This study analyzes piracy trends, authority interventions, and vessel types targeted across these regions. Using 62 months of piracy data (2020 onward) from the International Maritime Organization (IMO), textual reports were converted into numerical datasets for time series analysis and forecasting through data mining techniques. Statistical analyses were conducted with Excel, Minitab, and SPSS, and results were interpreted using a political, economic, social, technological, environmental, and legal (PESTEL) framework. The findings show a rising trend in piracy incidents in West Africa and the Malacca Strait, while a downward trend is observed in the South China Sea as well as overall authority interventions. Forecasting suggests these trends will persist for the next 12-18 months. It is observed that both piracy attacks against tankers and bulk carriers are increasing. The PESTEL analysis highlights that the shifting geography of piracy may reduce authority interventions, influenced by the focus on the Gulf of Aden, impacted by terrorism, and regional dynamics. Additionally, the Malacca Strait's unique status as territorial waters and its multinational context complicate international cooperation. The study also explores the impact of political vacuum, socio-economic conditions, accessible technologies, environmental factors, and legal challenges on piracy trends.

Keywords

Maritime Security, Piracy Trends, Piracy Attacks, Authority Intervention, Future Forecasts

Introduction

Approximately 90% of international trade is carried out via sea routes that connect countries and continents. Thus, these routes are a fundamental contributor to global trade due to their unique nature (Wang et al., 2023). Piracy at sea, including activities such as traditional offshore piracy, armed robbery, kidnapping for ransom, and cyberattacks targeting navigation systems, continues to threaten and disrupt vital infrastructure. Criminal acts originating from piracy have significantly affected global economic sustainability. It can be observed that most maritime incidents are intended to occur in high-traffic areas. Considering the geographical distribution of piracy incidents, the Gulf of Aden, the Strait of Malacca, the Gulf of Guinea, and the waters of East and West Africa are the regions where piracy attacks are very dense; therefore, these regions are strategic chokepoints and trade routes. The natural result is that piracy actions are concentrated in these areas.

The latest data from the International Maritime Bureau (IMB) defines the maritime security environment as complex and constantly changing. Since the peak of Somali piracy in 2011, there has been a decline in the number of piracy incidents; however, the nature of attacks and the locations of incidents keep changing (ICC, 2025). Seventy-nine incidents occurred in the first nine months of 2024, compared to ninety-nine in the same period of 2023. This is the lowest figure reported since 1994. However, due to this overall decline, significant regional variations and emerging threats that require comprehensive analysis have gone unnoticed. Additionally, the cost in human lives remains high, and the urgent need for evidence-based security strategies should not be forgotten, given that more than 100 seafarers were kidnapped, threatened, or injured in 2023.

Although the studies on piracy are numerically limited, there is increasing awareness among researchers. The current literature mainly focuses on piracy in Somalia, and the regional security issues are emphasized in most of these studies. Abbot and Renwick (1999) suggest that even though piracy has primarily been a regional security issue, it has become an inevitable opportunity for empirical research. Thus, the maritime industry increasingly recognizes that an evidence-based understanding of the patterns, causes, and consequences of piracy is required for effective anti-piracy strategies.

Perspectives from criminology, international relations, economics, and data science methodologies are combined in the current piracy research, exhibiting increasingly interdisciplinary approaches. The Contemporary Piracy Database, which documents the evolution of piracy tactics and shows that new forms of piracy that emerged in the 1990s, was developed by Twyman-Ghoshal and Pierce (2014) and has been a very significant contribution to this field. Their work suggests that piracy activities are becoming more widespread and that the risk of future attacks has temporarily increased following incidents in nearby regions. This situation resembles patterns observed in land crime investigations.

In their research, it can be seen that factors such as military capacity, commercial volume, and population size are statistically associated with piracy, whereas state fragility has the strongest explanatory power for future piracy incidents. The two-step analytical frameworks examine the probability of an attack being initiated and the likelihood of its success among recent methodological advancements. These frameworks that integrate Random Forest, Markov Chain, and Generative Adversarial Networks to address data imbalance challenges while improving predictive accuracy were developed by Gong et al. (2023).

There are many different factors contributing to acts of piracy that allow the adaptation of the PESTEL framework to maritime conditions. A comprehensive PESTEL analysis of piracy in the Gulf of Guinea was conducted by Ofosu-Boateng and Jiping (2020); thus, they provided an example of how this model can be used to systematically distribute the content of PESTEL models to piracy models. It is clear that an environment that encourages piracy is created by weak governance, political instability, and limited state capacity. However, it is unclear how these factors combine to drive some countries toward piracy while keeping others away.

In piracy research, significant attention has recently been paid to studies on economic factors. Subjects such as poverty, unemployment, and income imbalance in coastal communities that create favorable conditions for piracy are the topics that these studies particularly focus on. A significant link between the decline in the fishing industry and incidents of piracy was found by Desai and Shambaugh (2021). This finding suggests that fishermen resort to piracy to signal their expected income losses and deter illegal foreign fishing fleets. The complex link between the use of complexity at sea and security reveals how disruptions and economic inequality can contribute to security issues, as underlined by this research. The complex link between the use of marine resources and security is highlighted by this research, and how environmental degradation and economic dislocation can contribute to security issues is revealed.

The fact that modern piracy presents different characteristics in various maritime regions has been established by regional analyses. For piracy, the Strait of Malacca has been one of the world's most important regions. According to recent data, while the number of incidents was 37 in 2023, it is 43 in 2024. It can be clearly seen that there is an increase in the figures. Opportunistic armed robberies characterize these incidents more than hijackings do (ICC, 2025). Events in the Gulf of Guinea, where international piracy activities, including crew kidnappings and ransom demands, have taken place the most, have decreased from 81 in 2020 to 18 in 2024. However, it is still the area where the majority of the most significant crew safety issues occur. Although there was comparatively less activity in East African waterways, including Somali territory, with eight instances in 2024, sporadic high-profile kidnappings point to the possibility of a revival.

There are some gaps in the literature that hinder a comprehensive understanding of current threats, even though significant progress has been made in studies of maritime piracy. Specific geographic regions are focused on by much of the current research to chart the development of piracy, and this makes it hard to offer a comprehensive perspective exploring global tendencies and interregional interactions. Additionally, there are not enough studies on the dynamic interactions between various risk variables and how they differ over time. That's why there is no certain knowledge on how economic, geopolitical, and climatic situations shift and what their impact is on pirate dynamics over time. Future research should focus on integrating real-time data streams, social media analytics, and satellite imagery. These developments could be used to create automated early warning systems based on machine learning algorithms that can greatly enhance preventive security measures.

How maritime piracy research has evolved from descriptive studies to sophisticated analytical frameworks using advanced methodologies is highlighted by this literature review. Applying time series analysis and data mining techniques to the latest IMO data, addressing gaps identified in geographic coverage and temporal forecasting capabilities, and contributing to the expanding field of quantitative piracy research makes this foundation to be developed by the current study.

This study aims to address critical shortcomings in current piracy research. To conduct this study, 60 months of piracy incidents from 2020 onwards were analyzed via using data mining techniques and analyzing spatial and temporal patterns, the effectiveness of authorities' interventions, and the vulnerability profiles of vessels by using comprehensive IMO datasets. This research presents trend and forecasting models for the upcoming 18 months of piracy incidents. Also, by implementing the PESTEL framework, aims to understand the complex factors that are influencing piracy trends. The study presents significant potential to create a framework for policymakers, develop maritime security protocols, and prioritize resource allocation for anti-piracy initiatives.

Materials and Methods

The aim of this study is to examine trends in piracy acts and the efforts of authorities to respond to these incidents. In accordance with this purpose, data were obtained from the IMO's piracy report database (IMO, 2025). Only cases categorized as “boarded” were considered in the analysis within the context of this study. Official government interventions were categorized within a specific framework that included national defense forces, international anti-piracy alliances, and coastal state forces. An intervention was regarded as effective if it featured direct action resulting in the detention or deterrence of pirates through the presence or involvement of neighboring naval vessels, helicopters, or reaction units. If direct action was taken that resulted in the detention or deterrence of pirates due to the presence or involvement of neighboring naval vessels, helicopters, or reaction units, the intervention was deemed effective or successful.

The format of the IMO reports is unstructured, and there is a lack of standardized terminology. Hence, to facilitate statistical and time series analysis, text data was manually converted into numerical form. Microsoft Excel (Microsoft Corp., 2023), SPSS (IBM Corp., 2022), and Minitab (Minitab, LLC, 2023) software were used for data management and analysis. From February 2020 to March 2025, a dataset of 62 months was gathered from the IMO, and the March 2025 data is the most recent data available prior to the presentation. This continuous dataset allowed for strong time series analysis and prediction over a prospective 12- to 18-month future horizon.

The study specifically investigates several specific trends concerning boarded vessels and intervention responses, as well as regional patterns of piracy and the types of vessels that are hit most often. Before the time series and forecasting analyses were conducted, we had to check the data for compatibility using SPSS and Minitab. Time series analyses were performed in Minitab, and visual plots were utilized to identify prevailing patterns and determine the appropriate forecasting models (Sulawati, 2024; Ryan et al., 2005).

Four types of time series patterns were considered:

Trend: Characterized by a general increase or decrease over time.

Seasonal: Representing periodic fluctuations within specific intervals.

Cyclic: Long-term trend deviations without a set periodicity.

Irregular: It is made up of erratic fluctuation or irregular noise.

Over the course of this study, no distinct seasonal or periodic pattern was identified. Trends yielded inconsistent results in some cases, and various forecasting methods were evaluated comparatively. The most suitable method was selected according to performance criteria such as Mean Absolute Percentage Error (MAPE), Mean Absolute Deviation (MAD), and Mean Square Deviation (MSD) (Sulawati, 2024; Ryan et al., 2005).

The factors underlying the defined trends and forecasts were assessed by using the PESTEL framework in the second stage of the analysis. PESTEL was derived from PEST framework developed by Aguilar in 1967s. Thus, PESTEL has evolved and become commonly adopted across various industries, considering the potential for providing a detailed study framework (WSU, 2025). To examine various external factors in a broader and more complex way is possible thanks to PESTEL analysis. The first factor classified is political and primarily examines state-based or international actions taken through policy-making processes and their effects. The economic part of the analysis studies subjective factors that affect acts of piracy in this study. The social aspect of the PESTEL analysis investigates socio-cultural effects, demographic factors, and effects related to the human factor. The technology section covers the influences of global technological changes, shifts in internet-based technologies, and their reflections.

Environmental and legal parts later became a part of PESTEL, yet they have critical importance in assessing global changes. The environmental section reveals effects of natural changes such as climate change, and actions or restrictions taken to protect the environment, such as waste management regulations. The final section is law, which investigates the influences of regulations, shifts in law as well as judgment and punishment processes.

Results

The trend and forecasting analysis were conducted via data received from IMO reports through Excel, SPSS, and Minitab. The time series plot of authority intervention does not reveal a definitive trend. Consequently, various forecasting methods were tested, including linear, quadratic, and single exponential smoothing, to determine the suitability of the data for forecasting. Other trend analysis models were also evaluated during the study, but they were found to be inappropriate for the data set. When compared in terms of prediction performance metrics, the single exponential smoothing method gave the lowest MAPE value, while the linear method exhibited lower MAD and MSD values. This indicates that although single exponential smoothing is generally used for irregular data sets, the data itself did not exhibit high variability or randomness.

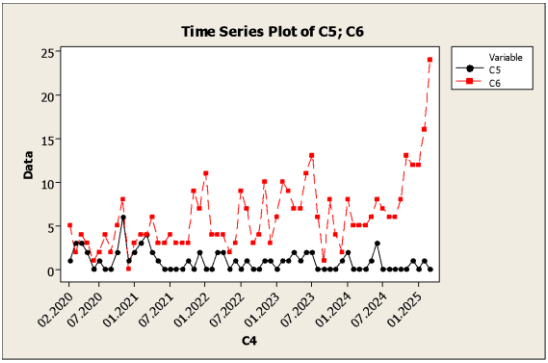

Figure 1
Time Series Plot of Authority Intervention and Boarded Vessel Number

	Lineer Trend Model	Quadratic Trend Model	Single Expone ntial Method
MAPE	42.6826	44.9581	41.6673
MAD	0.8719	0.8806	0.9521
MSD	1.2704	1.2552	1.4005

Table 1
Comparative Table of Methods for Authority Intervention Data

Linear trend analysis indicates a significant downward trend in intervention levels, suggesting a likelihood of decline throughout the forecast period. Likewise, the single exponential smoothing chart shows a general downward trend and supports the expectation of a persistency, even slight, decrease in authorized interventions. Therefore, irrespective of the method used, an increase in intervention rates is not expected in near-term piracy incidents.

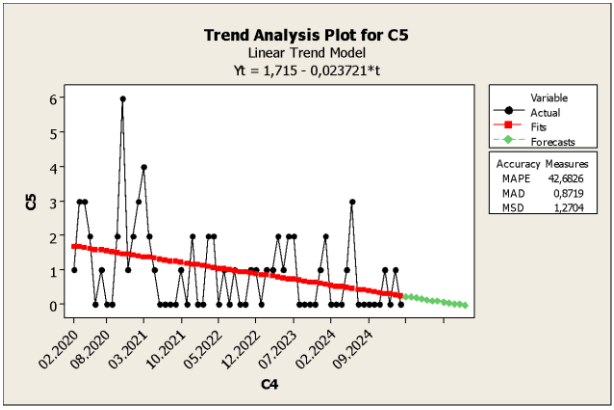

Figure 2
Linear Trend Model for Authority Intervention

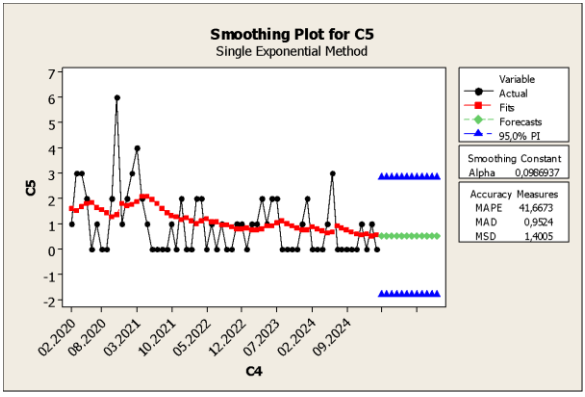

Figure 3
Single Exponential Method for Authority Intervention

The time series graph of boarding events shows a fragmented and distinct upward trend. Taking this trend into account, linear and quadratic models were used. Exponential growth and S-curve models were eliminated because they did not fully match the data set. A comparative analysis of MAPE, MAD, and MSD values showed the outstanding performance of the quadratic model. The findings of the quadratic-based prediction indicate a continuous increase in the number of boarding incidents.

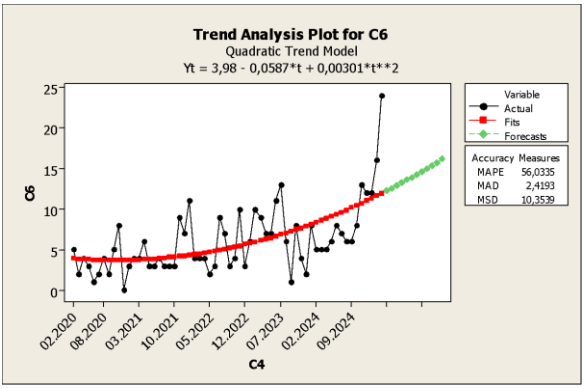

Figure 4
Quadratic Trend Model for Boarded Vessel Number

A noticeable upward trend can be observed from the time series graph for piracy acts in the Strait of Malacca.

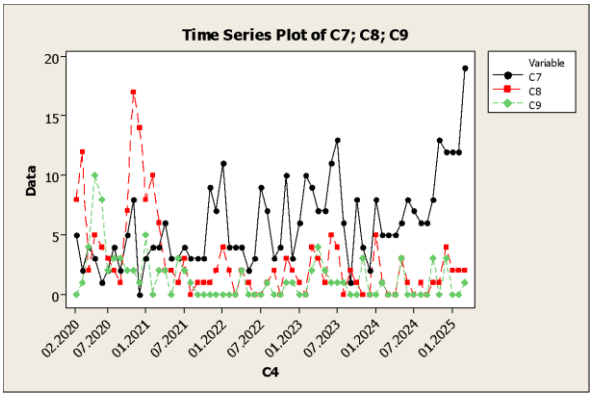

Figure 5
Time Series Graph of Piracy in the Strait of Malacca, West Africa, and the South China Sea

After testing both linear and quadratic models, the quadratic approach demonstrated greater agreement and forecast reliability.

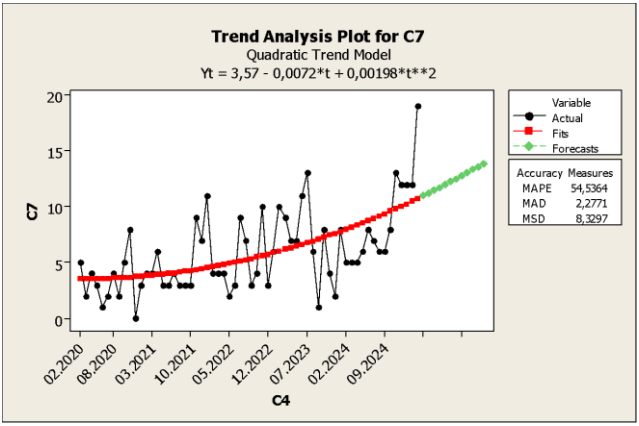

Figure 6
Quadratic Trend Model for Piracy in the Malacca Strait

Conversely, a piecewise decreasing trend is observed in the South China Sea. Since the uncertainty of the trend, linear, quadratic, and single exponential models were adopted. MAPE, the key indicator of model reliability, was at its lowest level for the linear method. Even though the quadratic method was at its lowest level in terms of MAD, MAPE offered a more reliable critieria for model selection, and it was concluded that the linear model was the most appropriate.

	Lineer Trend Model	Quadratic Trend Model	Single Exponential Method
MAPE	46.3913	56.3032	65.4741
MAD	1.2228	1.1951	1.3337
MSD	3.1345	2.7590	3.1430

Table 2

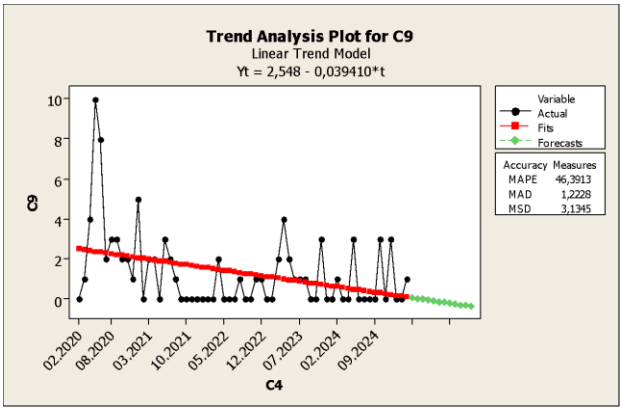

Figure 7

South China Sea's linear trend model of piracy

The single exponential model showed the highest error rates. Based on the results, it is predicted that piracy incidents in the South China Sea will trend downward linearly and that this trend will continue throughout the period of the forecast.

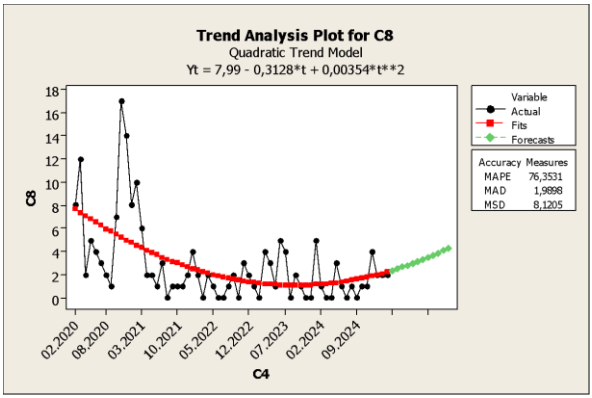

Figure 8

West Africa's Quadratic Trend Model of piracy

The time series graph for West Africa shows a downward trend. Therefore, linear and quadratic models were used for forecasting, while S-curve and exponential models were excluded due to data discrepancies identified by the analysis software. However, the downward trend observed in the graph, the quadratic predicting model suggested a notable increase in piracy incidents in West Africa within the next 12-18 months.

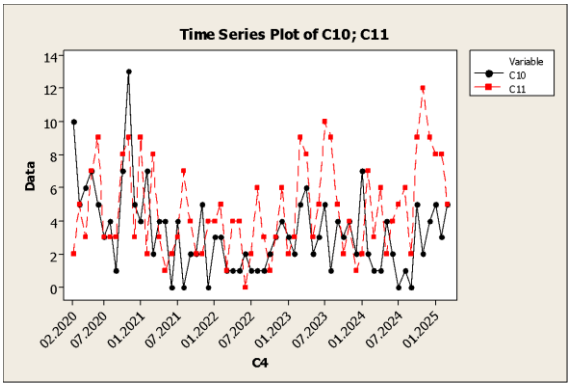

Figure 9
Time Series Plot of Piracy in Tankers and Bulk Carriers

In piracy incidents by vessel type, a significant downward trend is observed in incidents targeting tanker ships, while a partial upward trend is observed in attacks targeting bulk carriers. In the case of tanker ships, the quadratic model was considered more appropriate than linear, S-curve, or exponential models. The results of the forecast indicate that the downward trend observed until 2023 has reversed, and a significant increase in attacks is anticipated the over the period.

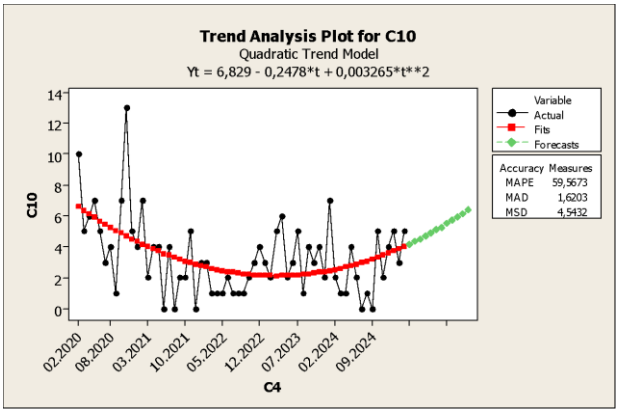

Figure 10
Quadratic trend model of piracy targeting tanker fleet

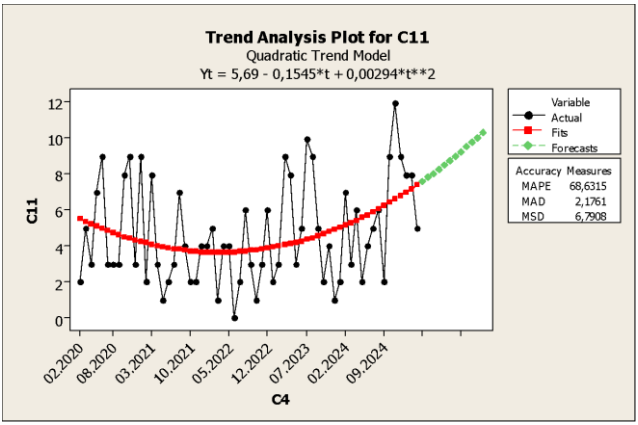

Figure 11
Quadratic Trend Model for Piracy Against the Bulk Carrier Fleet

A similar trend is seen in bulk carriers. The graph shows a clear upward trend, with the quadratic model again proving to be the most suitable model. The data reveals a sharp shift from a declining trend up to 2021 to a significant upward trend afterward. Predictive analyses foresee a significant spike in piracy incidents against bulk carrier fleets.

Discussion

The main objective of this study is to assess trends in piracy incidents and the interventions of relevant authorities. During the course of the last five years, significant changes in global dynamics have directly impacted maritime commerce, both in terms of the nature and frequency of piracy. Since maritime trade is central to the global economy and its stability, any disruption (on any scale) can severely impact global production chains, energy demands, industries and consumers. Moreover, the combined effects of piracy weaken many of the causes of port processes, timelines, and industrial production services failures, which in turn negatively affects all parties involved in maritime operations, such as sellers, buyers, seafarers, and port states.

While many piracy incidents in the Strait of Malacca are dismissed as simple thefts, such as thefts of engine parts, cash, or other valuables on board, the impact of these seemingly insignificant events can be enormous, and the losses are not limited to monetary terms. The reporting and investigation procedures initiated by authorities often have significant operational consequences for the shipping companies. Even in relatively small-scale thefts (e.g., engine parts worth approximately $5,000), authorities may request that the vessel be directed to the nearest anchorage and remain

there until a full and thorough investigation is completed. This process can sometimes take up to 5-6 hours due to inspections and documentation requirements carried out on board by local authorities. As a result of these unfortunate circumstances, vessels often miss their Estimated Time of Arrival (ETA) and Estimated Time of Berth (ETB), facing a number of procedural, legal, and logistical problems.

Piracy also affects other stakeholders such as insurance companies, P&I clubs, coastal state authorities, and ship personnel. There are several concerning aspects, including the frequent use of a range of weapons by piracy perpetrators, from knives to firearms. This increases the likelihood of incidents resulting in physical harm or even hostage-taking of crew members, particularly in regions where such crimes are prevalent, such as East and West Africa.

Occasionally, private armed guards are deployed by shipping companies as a preventive measure, yet it turned out that mostly these guards are ineffective. Furthermore, even with a small number of guards, having armed personnel on board adds hazards and ramifications.

Rise in the number of vessels boarded over the next 12–18 months can be predicted from Figure 4. Despite this projected increase, Figures 2 and 3 show a possible decrease in the rate of intervention by authorities. There may be several reasons for this trend, some of which include the vastness of maritime areas, ongoing conflicts, and the political vacuum in the affected regions. For instance, the South China Sea is showing a declining trend, whereas piracy incidents are predicted to rise in the Strait of Malacca. This discrepancy may be explained by the more stringent maritime regulations that Chinese authorities have put in place in the South China Sea. The lack of a similar decrease in the nearby Strait of Malacca indicates that pirate groups operating in this region are either unaffected by China's sanctions or fall outside the scope of these sanctions.

As shown in Figure 8, the increasing trend of piracy in West African waters highlights the worrying possibility of a resurgence in this region. Economic instability and poor governance in some coastal regions are probably the main causes of this tendency. The limited resources and jurisdictional limitations of multinational anti-piracy coalitions could also complicate the situation.

The types of vessels that have been analyzed have revealed an increase in pirate attacks targeting bulk carriers and tankers. Because bulk carriers and tankers are two of the most commonly used ship types in international maritime transport, this situation is rather concerning. A closer look at the figures shows that pirates prefer bulk carriers for various reasons. One reason is that the fully loaded bulk carrier's draft makes it easy for pirates to board bulk carriers rather than other large cargo ships. Another reason, though not as important as it was a decade or so ago, is that the typical bulk carrier is an easier target than the ordinary merchant ship due to their speed in comparison to the boats of the pirates.

Despite piracy is often seen as a regional problem, its effects are felt worldwide, especially on global shipping routes. Shipping companies avoid using certain fleets in specific regions due to the risks involved. Shipping companies must perform risk management always, everywhere and under all circumstances, because their business model fundamentally requires continuous negotiation and mediation between various global and local conditions.

PESTEL analysis result

The PESTEL framework is a comprehensive analytical tool used to identify the underlying factors contributing to large-scale occurrences by classifying them into PESTEL categories. This tool can be applied very well to the problem of maritime piracy to get at the causal roots and dynamics that influence its prevalence and persistence. In this study, the PESTEL framework is constructed using the literature and is well supported by the findings of the time series and forecasting analyses.

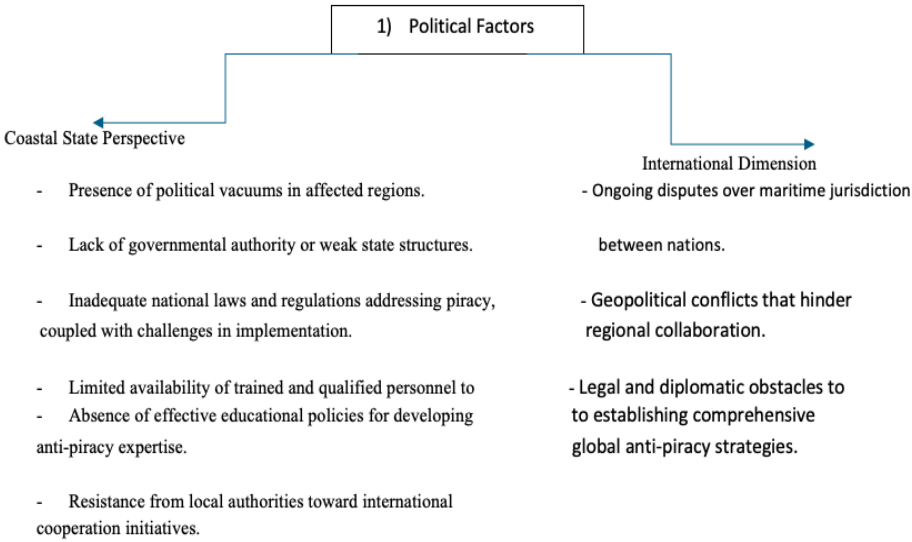

Figure 12

Political factors influencing maritime piracy dynamics from coastal state and international perspectives

2. Economic Factors

- Low living standards and extensive poverty among the local residents.
- Inadequate national funding for anti-piracy operations and infrastructure.
- Insufficient resources for anti-piracy initiatives and inadequate international economic cooperation.

3. Social Factors

- Low socioeconomic condition of people living in areas where piracy is common.
- The impact of piracy on the perceived authority and credibility of local governments.
- The admired or socially accepted image of piracy in particular communities.
- The local population has low awareness and education levels.
- Opportunity disparities and restricted upward mobility.
- Affected populations have low happiness indices and impaired mental and social health.

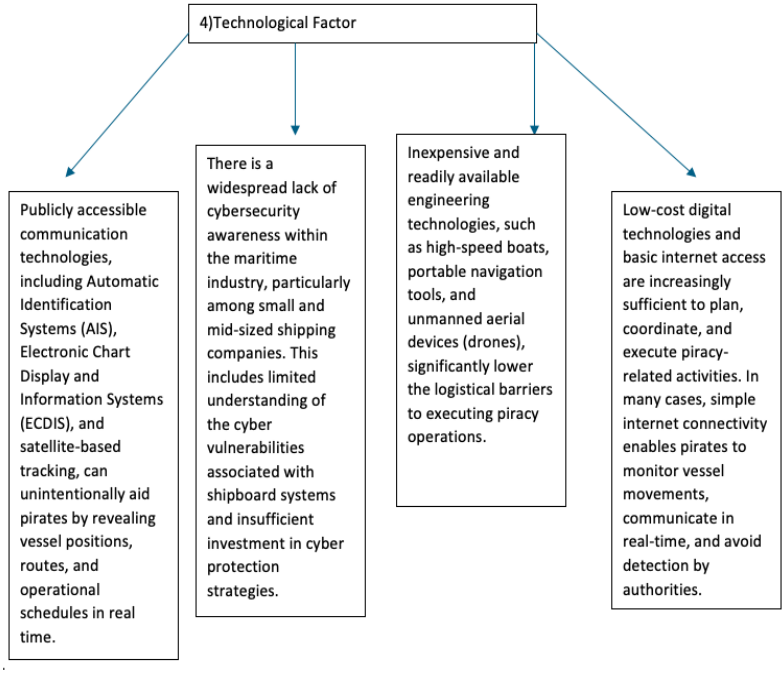

Figure 13

Technological factors contributing to maritime piracy through the accessibility of digital, communication, and navigation technologies.

5. Environmental Factors

- Inability to provide continuous maritime escort or protection in large sea areas.
- Long distances and difficult waters prevent timely intervention even when piracy incidents are reported.
- Real-time intervention is difficult because piracy incidents are usually short lived.
- Climate change, natural disasters, and economic factors affecting the environment.

6. Legal Factors

- The universality and consistency of application of the United Nations Convention on the Law of the Sea (UNCLOS) remain controversial.
- Legal uncertainty regarding the rights of international forces to intervene in areas considered internal or semi enclosed waters (e.g., the Strait of Malacca).
- Differences in national legal systems and inconsistent application of maritime law with regard to piracy and crimes against maritime commerce.

Conclusion

The aim of this study is to assess detectable changes in piracy activities and thereby predict future developments. The trend and forecasting evaluations of the study indicate that maritime piracy will continue to be a serious problem for some time, particularly in the areas with high maritime traffic mentioned in the study. In the areas that are high risk and significant shortcomings in intervention capacity and enforcement, this increasing criminal activity is especially evident. The political vacuum is considered one of the most crucial contributors to increasing piracy rates. The geographical distribution of piracy may change over time; however, the fragility of global maritime transport networks and their vulnerability to piracy is highlighted by its persistence. Although there is an increase in attempts to hijack ships, a downward trend is observed in intervention rates. Unfortunately, this is creating progressive challenges for maritime security policies. For example, the Strait of Malacca is a critical area where there is a concerning increase in piracy activities. What is also confusing and questionable is that there is a significant decrease in the number of piracy incidents in the South China Sea, whereas a similar trend couldn't be observed in a very close area, the Strait of Malacca. There are re-emerging risks that pose a serious threat to maritime security and shipping in West African waters. Additionally, another cause for concern is the increasing number of attacks on tanker and bulk carrier fleets, which are the main types of vessels in maritime trade. Since maritime trade is a fundamental pillar of the global economy, efforts must be made to ensure the safety and security of maritime transport and freedom of navigation. Both to provide a sustainable global economy and for regional prosperity, these efforts are necessary.

This study aimed to analyze the multifactor nature of piracy by employing the PESTEL framework. Thus, anti-piracy efforts also require a comprehensive, multidimensional, and internationally accepted approach that considers the root causes and systemic weaknesses in the affected regions are necessitated. To this end, successful and long-term security plans need to be developed and implemented. All stakeholders, including local governments, regional maritime authorities, international coalitions, and commercial shipping companies, must work closely together.

They all need to share a common perspective. A more comprehensive law enforcement and increased surveillance capacity, as well as investments in cybersecurity, capacity building, legal compliance, and socio-economic development in vulnerable coastal communities, should be included in measures and sanctions.

To conclude, all stakeholders have a common responsibility to strengthen maritime security. Considering the ratio of maritime trade among other transportation modes, actions to improve maritime security carry very high and diverse risks. Thus, a global action is required to achieve maritime security instead of regional anti-piracy measures. However, there are some challenges to achieving a global anti-piracy perspective, considering the incidents that are spread over a large area, cultural and sociological differences, as well as the various regulatory frameworks. Moreover, a global anti-piracy action plan is crucial for sustainable economic development. To this end, this study contributes to the growing body of knowledge emphasizing the urgent need for integrated, forward-looking responses to the evolving challenges of maritime piracy.

References

Abbot, J., & Renwick, N. (1999). Pirates? Maritime piracy and societal security in Southeast Asia. Global Change, Peace & Security, 11(1), 7-24.

Aguilar, F. J. (1967). Scanning the business environment. Macmillan.

Daxecker, U. E., & Prins, B. C. (2015). The new barbary wars: Forecasting maritime piracy. Foreign Policy Analysis, 11(1), 23–44. https://doi.org/10.1111/fpa.12014

Desai, R. M., & Shambaugh, G. E. (2021). Measuring the global impact of destructive and illegal fishing on maritime piracy: A spatial analysis. PLOS ONE, 16(2). https://doi.org/10.1371/journal.pone.0246835

Ece, N. J., & Kurt, H. (2021). Analysis of maritime piracy by using qualitative methods. Mersin University Journal of Maritime Faculty, 3(2), 37–50. https://doi.org/10.47512/meujmaf.1018026

Gong, X., Jiang, H., & Yang, D. (2023). Maritime Piracy Risk Assessment and policy implications: A Two-step approach. Marine Policy, 150, 105547. https://doi.org/10.1016/j.marpol.2023.105547

IBM Corp. (2022). IBM SPSS Statistics for Windows (Version 29.0) [Computer software]. https://www.ibm.com/products/spss-statistics

ICC. (2025). Maritime piracy dropped in 2024, but crew safety remains at risk. https://icc-ccs.org/maritime-piracy-dropped-in-2024-but-crew-safety-remains-at-risk/

IMO. (2025). Piracy reports. Piracy Reports. https://www.imo.org/en/OurWork/Security/Pages/Piracy-Reports-Default.aspx

Li, H., & Yang, Z. (2023). Towards safe navigation environment: The imminent role of spatio-temporal pattern mining in maritime piracy incidents analysis. Reliability Engineering & System Safety, 238, 109422. https://doi.org/10.1016/j.ress.2023.109422

Marchione, E., & Johnson, S. D. (2013). Spatial, temporal and spatio-temporal patterns of maritime piracy. Journal of Research in Crime and Delinquency, 50(4), 504–524. https://doi.org/10.1177/0022427812469113

Microsoft Corp. (2023). Microsoft Excel (Version 2023) [Computer software]. https://www.microsoft.com/excel

Minitab, LLC. (2023). Minitab Statistical Software (Version 21.4) [Computer software]. https://www.minitab.com

Ofosu-Boateng, N. R. L., & Jiping, Z. (2020). A pestle analysis of maritime piracy and maritime security in the Gulf of Guinea. Advances in Social Sciences Research Journal, 7(1), 472–482. https://doi.org/10.14738/assrj.71.7742

Ryan, B. F., Joiner, B. L., & Cryer, J. D. (2005). Minitab handbook: Updated for release 14. Thomson Brooks/Cole.

Sulawati, N. (2024). Minitab statistical software: Forecasting with time series analysis. YouTube [@MinitabMalaysiaSingapore]. https://www.youtube.com/watch?v=eoFnBDgDsOQ

Twyman-Ghoshal, A. A., & Pierce, G. (2014). The changing nature of contemporary maritime piracy. British Journal of Criminology, 54(4), 652–672. https://doi.org/10.1093/bjc/azu019

Wang, T., Cheng, P., & Zhen, L. (2023). Green development of the Maritime Industry: Overview, Perspectives, and Future Research Opportunities. Transportation Research Part E: Logistics and Transportation Review, 179, 103322. https://doi.org/10.1016/j.tre.2023.103322

WSU. (2025). What is a PESTEL Analysis? Industry Research - PESTEL Analysis. https://libguides.libraries.wsu.edu/c.php?g=294263&p=4358409

About the Authors

Ms. Aysel Camci / Istanbul Technical University, / ORCID: 0009-0003-2499-3959

Ms. Aysel ÇAMCI completed her BSc. degree at Boğaziçi University and obtained an Associate Degree in Maritime Machinery from Galatasaray University. She holds MSc. degree in the Maritime Studies program from Istanbul Technical University (ITU). She is currently pursuing her PhD. studies in the Maritime Transportation Engineering program at ITU. Her research primarily focuses on the human factor in the maritime industry and maritime security.

Mr. Burak Celik / Istanbul Technical University / ORCID: 0009-0000-2160-1188

Burak ÇELİK is the Evaluation and Quality Assurance Coordinator and Analysis & Lessons Learned SO at the NATO-accredited Maritime Security Centre of Excellence (MARSEC COE). A Navy SAT (Special Operations Forces) operator with over 20 years of service, he has extensive experience in maritime security, counter-piracy operations, and multinational defense cooperation. He has served in various leadership and diplomatic positions, including as Military Attaché at the Turkish Embassy in Brasília and as a NATO Liaison & Monitoring Team Commander in Kosovo. His professional expertise covers maritime security, quality management systems, Lessons Learned analysis, and critical maritime infrastructure resilience. He has authored and contributed to research on piracy, maritime threats, and global security trends, bridging operational experience with academic and analytical approaches.

Firat Bolat / Istanbul Technical University / ORCID: 0000-0001-9807-7089

Fırat BOLAT has a BSc. degree in Marine Engineering from Istanbul Technical University (ITU), MSc. Degree in Mechanical Engineering (Energy Machinery) from Yildiz Technical University and PhD. Degree in Maritime Transportation Engineering ITU. He worked approximately 13 years as Flag, Port and Coastal State Surveyor and Vice Harbour Master of Istanbul of Turkish Maritime Administration. His research interests are international maritime rules and regulations, investigative procedures, port management, energy efficiency, marine main and auxiliary machinery, energy machinery, legal compliance issues, safety and security enforcement, inter-agency communications, emergency systems, data analysis and management, project lifecycle management, marine pollution prevention, maritime policy development. He is currently pursuing his second PhD. Studies on Applied Informatics (Geographical Information Technologies) at ITU.

PART III

Cyber Attacks on Vessels: A Review for the Last 20 Years

Jeroen Pijpker
NHL Stenden University of Applied Sciences, Netherlands

Stephen McCombie
NHL Stenden University of Applied Sciences, Netherlands

Abstract

The maritime industry is increasingly reliant on digitized and interconnected systems, a trend that also applies to vessels. Consequently, the traditional cyber threat landscape has expanded to include the Global Maritime Transportation System (GMTS). The Maritime Cyber Attack Database (MCAD), which catalogs cyber incidents in the maritime domain dating back to 2001, provides valuable insights into threats targeting the GMTS. MCAD has identified over 380 incidents from public sources. The database is regularly updated as new incidents occur. This work focuses specifically on threats directed at vessels. MCAD categorizes maritime cyber incidents in terms of victim type which includes vessels of various kinds. MCAD also describes attack type against vessels and this can be grouped into three main categories: attacks against navigation (GPS Jamming, GPS Spoofing, AIS Spoofing and Going Dark), Malware (Ransomware, Other Malware) and Hacking (Various). Modern vessels are complex ecosystems of interconnected systems. Because they are becoming more connected, they also become more vulnerable to cyber threats. Ships have complex networks of Information Technology (IT) and Operational Technology (OT). The OT networks on vessels control critical functions such as navigation, propulsion, and cargo operations. These systems can be a prime target for cyber attacks. Disruption in these systems can have severe consequences, including loss of life, environmental damage, and significant financial loss.

Keywords

Maritime Cybersecurity, Vessel Cyber Attacks, Navigation System Vulnerabilities, Maritime Cyber Attack Database (MCAD), Global Maritime Transportation System (GMTS)

Introduction

The GMTS is undergoing a rapid digital transformation. While vessels were once isolated platforms relying primarily on radio communication, they have evolved into complex, interconnected ecosystems of Information Technology (IT) and Operational Technology (OT). This transition from standalone systems to networked architectures at sea has introduced significant new cyber risks. As connectivity increases, so does the likelihood that vessels become targets of cyber threat actors, including cyber-criminals, state-sponsored groups, and other opportunistic hackers.

While numerous studies have outlined hypothetical cyber threat scenarios for the GMTS, few have systematically examined real-world cyber incidents. This lack of empirical research hinders a comprehensive understanding of how vessels are actually being targeted by threat actors in practice.

The current cyber threat landscape for vessels includes GPS spoofing and jamming, AIS spoofing, ransomware attacks, and the hijacking of satellite communication systems. These attacks can compromise safety-critical operations such as navigation, propulsion, and cargo handling. Despite growing awareness within the maritime sector, detailed vessel-specific analyses remain limited in both academic literature and industry reporting.

This paper addresses that gap by reviewing documented cyber attacks on vessels over the past two decades, using data from the MCAD (Maritime IT Security Research Group, n.d.). It provides a categorization of threats and highlights the evolving nature of cyber risks in the GMTS with a focus on vessels.

Methods

The analysis done in this work is based on data from MCAD, which aggregates publicly available reports of maritime cybersecurity incidents. Developed in 2021 by the Maritime IT Security Research Group (MITS) at NHL Stenden University of Applied Sciences, MCAD was designed to compile all known incidents into a structured and interoperable format, including support for standards such as MITRE's Structured Threat Information eXpression (STIX). This paper focuses specifically on the subset of incidents involving vessels from MCAD.

The method used to collect the MCAD data involved a systematic review of scholarly literature, news feeds, technical reports, government publications and other media to identify maritime cyber incidents. MCAD defines a cyber incident as a discrete malicious attack with a cyber element, perpetrated by a particular threat actor against one or more victims and causing significant impact on one or more victims, possibly over an extended period of time.

In MCAD, the following essential attributes are present for each incident that is collected.

- Date - Month and Year the incident took place or it became known.
- Impact Area - The GMTS that are impacted, can be: Shore, Offshore, and Vessel.
- Incident Location - The location where the incident took place.
- Incident Country - The country in which the incident took place.
- GPS Coordinates - Approximate latitude and longitude of the place where the incident took place.
- Victim Country - The country in which the victim resides.
- Victim Identity - The name of the victim affected.
- Victim Type - Type of victim related to GMTS, examples: Ship Builder, Logistics Provider, Marine Technology Provider.
- Method - The attack method used by the threat actor.
- Attacker Country - The country from which the threat actor operates.
- Summary - Short description of the incident.
- References - List of all references found relating to the incident, including the source of all data used.

MCAD is made available to the community through a website, an iOS application, and an Android application (Maritime IT Security Research Group, n.d.). Figure 1 displays a screenshot of the GPS Jamming event that affected the MSC Antonia in 2025.

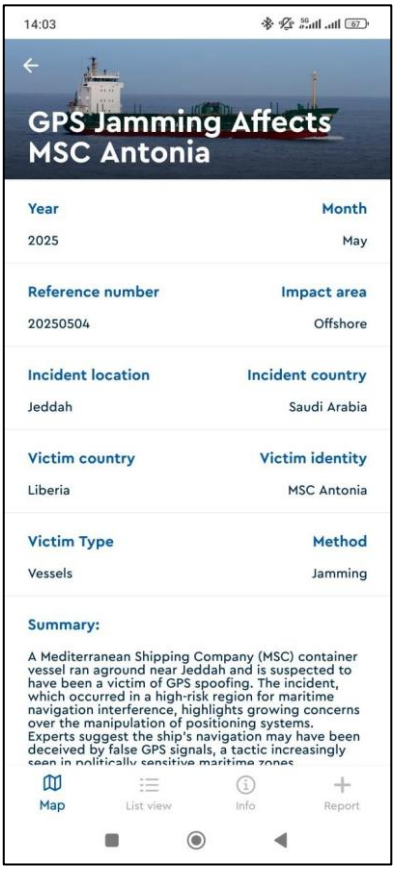

Figure 1

Screenshot of the MCAD Android Application cybersecurity incident with MSC Antonia. The Android application only displays the most important labels of the recorded incident.

In the MCAD database, the following subcategories are used/available for categorizing a cyber attack.

- GPS Jamming
- GPS Spoofing
- AIS Spoofing
- Going Dark
- Hacking

- Ransomware
- Malware
- Other

In the result section from each of the different categories, cyber incidents are selected and discussed.

Results

In this section, the results are discussed per subcategory of cyber attack that is used in MCAD. Cyber attacks and incidents involving vessels vary in their character. Per Figure 2, we have extracted all maritime cyber incidents relating to vessels from MCAD (Maritime IT Security Research Group, n.d.). MCAD records 71 vessel-related cyber incidents, which are classified into eight categories.

The most observed cyber incidents in MCAD are related to navigation: AIS Spoofing (22), GPS Jamming (13), Going Dark (15), and GPS Spoofing (5). These four categories collectively indicate a strong adversarial focus on disrupting maritime navigation systems. There are two categories related to malware: ransomware (4) and other malware (1). Lastly, there are hacking (9) and others (2) were recorded.

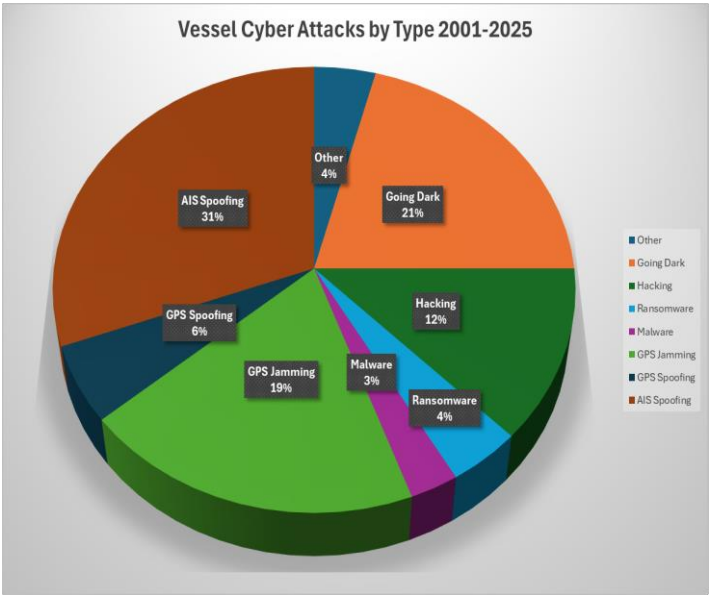

Figure 2
The figure represents MCAD cyber incidents from 2001-2025 relating to vessels.

GPS jamming events

In MCAD a total of 13 GPS jamming events are recorded. Table 1 provides an overview of documented GPS jamming incidents. North Korea was responsible for a number of those and three early examples are described below.

In 2010 the first publicly noted GPS jamming cyber incident affecting maritime occurred (Seo & Kim, 2013; Lee, 2013). On August 23, that year a GPS disruption, that was deliberately caused by North Korea, occurred in South Korea and affected 181 cell towers, 15 airplanes and a battle ship. The source location of the disruptions was Kaesong in North Korea and the areas of Gimpo and Paju in South Korea were impacted. The attack lasted four days. This attack led to the development of anti-jamming programs by South Korea. However despite this the jamming incidents continued.

In 2011, another GPS jamming incident happened in South Korea (Seo & Kim, 2013). In the 11 days (Mar 4–14) a large-scale North Korean GPS jamming attack took place and there are reported GPS disruptions to 145 cell towers, 106 airplanes and 10 ships.
In 2012, a further GPS jamming incident happened in South Korea (Seo & Kim, 2013). This time it was reported that 1,016 airplanes and 254 ships experienced GPS disruptions during the 16 days (Apr 28 – May 13, 2012) of North Korean jamming.

Year	Incident Description
2010	GPS jamming incident in South Korea
2011	GPS jamming incident in South Korea
2012	GPS jamming incident impacting 254 ships in South Korea
2016	GPS jamming incident in South Korea
2016	GPS jamming incident impacting 280 fishing ships in South Korea
2018	GPS jamming in the Mediterranean Sea, by the coast of the island of Cyprus
2018	GPS jamming during President Putin's visit at the Kerch Strait Bridge in Crimea, Russia
2018	Vessel hit by GPS interference near the Port of Jeddah in Saudi Arabia
2018	Vessel hit by GPS interference near the Port of Haifa in Israel
2022	Ferry on the Borholmslinjen (Borholms line) delayed after GPS jamming incident
2024	South Korea GPS jamming from North Korea
2025	GPS Jamming Affects Bangladeshi Bulker
2025	Reported GPS Jamming in Strait of Hormuz

Table 1
MCAD documented GPS jamming incidents.

GPS Spoofing Incidents

In the MCAD database, there are five incidents regarding GPS spoofing. In table 2 an overview is given.

Year	Incident Description
2016	US Navy ships hit by GPS spoofing in Persian Gulf, Iran
2018	Zvezda Shipyard in Vladivostok, Russia hit by DoS/GPS spoofing attack
2019	GPS Spoofing incident involving British oil tanker 'Stena Impero' in Strait of Hormuz (Persian Gulf)
2023	Houthi Attacks and GPS Spoofing in the Bab al-Mandab Strait
2025	GPS Spoofing Affects MSC Antonia

Table 2

MCAD documented GPS Spoofing incidents.

A notable example of GPS spoofing occurred in the Strait of Hormuz, a strategically sensitive waterway in the Persian Gulf. In July 2019, the British-flagged tanker Stena Impero fell victim to an alleged GPS spoofing incident in the Strait of Hormuz, near Iran. Subsequently, the vessel was seized by Iran's Revolutionary Guards. The crew of the vessel, 19 in total, were held in confinement for over 19 days. Britain's MI6 was reportedly investigating the incident and believed that Iran with the assistance of Russia had purposefully spoofed the ship's location to trick it into entering into Iranian waters so it could be seized. The incident was considered to be a retaliation for the seizure of an Iranian ship, which was breaking sanctions, by the British military in Gibraltar two weeks earlier. The region is considered to be a high risk area for vessels. In 2016, a similar incident occurred where two small U.S. Navy ships were allegedly spoofed into Iranian waters as well before getting seized by Iran's Revolutionary Guards. The tanker left Iranian waters after two months of seizure. (BBC News, 2019)

The most recent maritime GPS spoofing incident occurred on the 10th of May 2025. A container vessel from Mediterranean Shipping Company (MSC) ran aground near Jeddah and is suspected to have been a victim of GPS spoofing attack (SAFETY4SEA, 2025). In Figure 3 the possible spoofing patterns are displayed in Figure 3 that had occurred when the MSC Antonia ran aground.

Figure 3
Visualization done by WindwardAI of the spoofing patterns presented on X (WindwardAI, 2025).

AIS Spoofing

In the MCAD database, a total of 22 incidents are classified as AIS spoofing attacks. In table 3, an overview of these incidents is presented. Among these, one of the most interesting cases appeared in 2021 and highlights the geopolitical implications of AIS spoofing attacks.

Year	Incident Description
2016	Vessel hit by AIS spoofing attack near Putin's visit at Kerch Strait Bridge in Crimea
2017	Vessel hit by spoofing attack in the Black Sea near Putin's visit at TurkStream launch
2018	Vessels hit by AIS spoofing attack near the Port of Shanghai in China
2018	Yuk Tung / Maika fishing vessel hit by AIS spoofing attack in Nampo, North Korea
2018	Yuk Tung vessel spoofed its AIS when it transmitted under a Panamanian flag
2019	Groups of simulated sailboats cause AIS spoofing incident in the Atlantic Ocean
2019	Princess Janice and more than 10 other ships hit by spoofing attack in Point Reyes (USA), Madrid (Spain) and Hong Kong (China)
2019	Vessels near Elba, Italy hit by AIS spoofing attack
2020	U.S. survey vessel USNS Bruce C. Heezen hit by AIS spoofing attack in the North Sea and Baltic Sea
2020	USS Roosevelt hit by AIS spoofing attack in Polish waters to appear in Russian territorial waters near Kaliningrad
2021	Nine Swedish Navy vessels hit by AIS spoofing attack in the Baltic Sea
2021	British destroyer HMS Defender and Dutch frigate HNLMS Evertsen hit by AIS spoofing attack
2021	Spoofing of AIS Signals of Two Norwegian Navy Corvettes
2021	Spoofing of AIS Signal of Russian WARSHIP 545
2021	Second Spoofing of AIS Signal of Russian WARSHIP 545
2023	AIS Spoofing in Black Sea
2024	AIS Spoofing by Tanker Atila
2024	China Performs AIS Spoofing in Philippines
2024	AIS Spoofing Incident in Crimea
2024	LPG Carriers Perform AIS Spoofing at Khor al Zubair Port
2025	AIS Spoofing from Chinese-owned ship Suspected of Damaging a Subsea Cable off the North Coast of Taiwan
2025	AIS Spoofing Used to Conceal Oil Shipments to Venezuela

Table 3
MCAD documented AIS Spoofing incidents.

In 2021, on the 24th of June, an incident involving a British warship near the coast of Russian-occupied Crimea may have started online, with a virtual trip that never took place. After steaming 12 kilometres off the Crimean coast, the HMS Defender grabbed headlines. Those waterways are considered Russian territory by the Kremlin, but they belong to Ukraine for much of the rest of the world. To discourage the Royal Navy vessel, Russia's Defense Ministry claimed it fired warning shots and dropped missiles. The Ministry of Defence of the United Kingdom refuted the assertions. The HMS Defender and a Dutch frigate, HNLMS Evertsen, were seen nearing the port of Sevastopol in Crimea in the early hours of June 19, 2021, according to the site's tracking data. Strangely enough, they were not present. Both ships were docked around 300 kilometres away in Odessa, Ukraine, when Marine Traffic showed them entering Russian-controlled territory, according to a live camera feed. The simulated trip was published on Marine Traffic as a warning by an anonymous person. It was all about provoking a reaction and "deploying disruptive power".

On June 5 2019, an incident took place in which more than 10 ships, located all around the globe, were spoofed into a crop circle near the coast of California's Point Reyes. So far it remains a mystery why these circling AIS tracks are appearing specifically at Point Reyes and a few other locations.

A total of 12 ships appeared thousands of miles from their actual position. Most of the vessels reported circling positions off the coast of Northern California, though two were shown off Madrid, one to the vicinity of Hong Kong and another to the Chinese city of Shanwei.

Very Large Crude Carriers (VLCCs) used AIS spoofing to hide their true locations and activities while transporting combined cargoes of Russian and Chinese oil to Venezuela (TradeWinds News, 2024). Satellite imagery confirmed that both vessels docked at the oil port of Jose, despite their AIS signals indicating they were elsewhere. Norns was off Brazil signalling for Angra dos Reis, and Crystal spoofing a loading operation near an FPSO off Guyana. This deliberate AIS manipulation misled trackers and authorities about their actual routes and destinations.

Going Dark

In the MCAD database, there are 15 incidents in which vessels deliberately disable their automatic identification systems (AIS), a tactic commonly referred to as "going dark". This behaviour is often associated with illegal activities, such as human, drug, or weapon trafficking, illegal fishing, or sanctions evasion (Bunwaree, 2025). In table 4 an overview is shown.

In one of the newer incidents in December 2024, a Chinese ship went dark, possibly damaging a fiber-optic cable. The Danish navy monitored the Chinese bulk carrier Yi Peng 3 due to its potential involvement in damaging a fiber-optic cable in the Baltic Sea. The ship had been near the damaged cables at the time of the incident and had turned off its Automatic Identification System (AIS), making its exact route untraceable.

Going dark is also closely associated with the operations of the so-called dark fleet. The dark fleet is a network of vessels that disable or manipulate their AIS signals to obscure their true locations and activities. In August 2024, a Russia-affiliated LNG Carrier, Pioneer went dark. The vessel employed spoofing tactics to avoid detection in Norway's Arctic waters. After sending out false AIS signals, the vessel navigated undetected to the Arctic LNG 2 project, bypassing sanctions. The vessel's movements raise concerns about the use of "dark fleet" tactics to circumvent maritime regulations.

Year	Incident Description
2014	Vessel 'MT Kerala' dark activity in Angola
2014	Trawler fishing vessels 'Releixo' and 'Egaluze' going dark in Senegal and Gambia
2014	Chinese fishing fleet going dark near the Galapagos Islands' EEZ
2015	Vessel 'Corinthian Bay' going dark in Heard Island & McDonalds Islands, Australia
2016	Fleet of approximately 100 Chinese flagged 'Squid jiggers' fishing vessels going dark in Argentina's EEZ
2018	Vessel 'Wan Heng 11' and Russian-flagged 'Patriot' go dark in East China Sea
2018	Vessel 'Lucky Star' dark activity in Songnim, North Korea
2019	Chinese Government installation dark activity in Qingdao, China
2019	Vessel 'Diamond 8' dark activity in Nampo, North Korea
2019	Vessel 'Jin Nui Zou' dark activity in Dalian, China
2019	Vessels going dark in Ningbo, China and Nampo, North Korea
2019	Vessels going dark in Port of Quanzhou (Shiyucun), China
2022	Russian oil and chemical tankers going dark
2024	Chinese Ship Sabotages Internet Cable In Baltic Sea
2024	Russia-affiliated LNG Carrier Pioneer Goes Dark

Table 4

MCAD documented Going Dark incidents.

Hacking attacks

In table 5, the hacking incidents that occurred to vessels are displayed. Two interesting hacking attempts were made in 2025.

In January 2025, a teenage hacker in Cesena, Italy managed to infiltrate a system responsible for maritime route management in the Mediterranean Sea. This allowed him to manipulate ship positioning data.

By exploiting vulnerabilities, he was able to divert vessels and interfere with navigation, causing disruptions to maritime traffic in that region. However, his actions appeared to be driven by curiosity and a desire to test his skills rather than some malicious intent. Italian authorities detected the breach and launched an investigation, ultimately identifying and arresting the teenager.

A total of 50 vessels belonging to the National Iranian Tanker Company (NITC) and 66 vessels belonging to the Islamic Republic of Iran Shipping Lines (IRISL) were reportedly targeted in a cyberattack against their communication systems. The operation was attributed to Lab Dookhtegan, an anti-government hacktivist group opposed to Iran's regime.

According to cybersecurity company Cydome (Cydome, 2025), Lab Dookhtegan claimed via its Telegram channel to have disrupted communications on more than 100 Iranian government-linked oil tankers. The group announced that both internal and external communication channels were interrupted, effectively isolating vessels at sea. Cydome assessed the attack as politically motivated, with the likely objective of disrupting Iran's oil exports, a critical pillar of the national economy, as part of the group's broader campaign to weaken state-linked organizations.

Year	Incident Description
2012	Insider attack involving sailor on USS Midway
2016	Shipping Company hit by hacking attack by pirates
2017	Container vessel hit by hacking attack en route from the island of Cyprus to Djibouti
2017	Super Yacht of Chinese Billionaire hacked on Hudson River near New York City
2021	Facebook account of Warship USS Kidd hit by a hacking attack in the USA
2022	Putin's Yacht "Graceful" hit by hacking/spoofing attack in Kaliningrad, Russia
2024	Computer systems of Iranian spy ship MV Behshad hit by US cyber attack
2025	Teenager Hacks Ship Routes in the Mediterranean
2025	Lab Dookhtegan Disrupts Communications of Iranian Oil Tankers

Table 5
MCAD documented Hacking attacks.

Although Lab Dookhtegan did not disclose the methods used, Cydome suggested that the attackers may have exploited vulnerabilities in satellite communication systems (VSAT terminals). These systems are known to be exposed targets, often accessible via the internet with unchanged default credentials. Compromise of VSAT systems could allow attackers to seize control of all shipboard communications and potentially pivot into the IT and OT networks, creating significant operational and safety risks.

In February 2024, the US military reportedly conducted a cyber-attack against an 'Iranian spy ship' which had been operating near the Chinese military base in Djibouti. The ship, named the MV Behshad, was believed to have been collecting information on commercial vessels transiting the Red Sea and communicating that information to the Houthis in Yemen.

The US operation was intended to inhibit the Iranian ship's ability to share that intelligence with Houthi rebels in Yemen who have been firing missiles and drones at ships in the Red Sea. The US officially has not disclosed much information about the cyber-attack and Iran denies that the ship was being used for military purposes. The suspected motive for the attack was to respond to an Iranian-linked attack that killed U.S. soldiers in Jordan in addition impede the spy ship operations.

Other Malware attacks

There is only one incident regarding other malware attacks (not ransomware). The attack is displayed in table 6.

In February 2019, a deep draft merchant vessel bound for the port of New York and New Jersey was hit by a malware (Emotet Trojan) attack, disabling its onboard Computer System. It is possible that the ship may not have been targeted specifically, although this has not been confirmed. After the vessels radio contacted the coast guard, an incident-response team was send out and entered the ship to assess the possible damage. Eventually, the coast guard alerted the FBI.

Year	Incident Description
2019	Deep draft merchant vessel bound for Port of New York and New Jersey hit by malware attack

Table 6

MCAD documented Malware attacks.

Ransomware attacks

MCAD only holds four ransomware attacks at this moment. In table 7, the ransomware attacks are displayed. One notable attack involved a tanker, and another a new-build dry bulk ship.

Year	Incident Description
2018	New-build dry bulk ship in port hit by malware attack
2019	Two ships hit by ransomware attack
2019	Oil Tanker hit by ransomware attack near the Port of Naantali, Finland
2020	AIDA Cruise Ships hit by ransomware attack in Rostock, Germany

Table 7

MCAD documented Ransomware attacks.

A notable example of a malware attack that happened in 2018 involved a new-build dry bulk ship. A bunker surveyor boarded the ship and requested permission to access a computer in the engine control room to print documents for signature (ZDNet, 2018; Bimco, 2016; International Chamber of Shipping, 2020; SecureWorld, 2018). The surveyor inserted a USB thumb drive into the computer and unwittingly introduced malware onto the ship's network. The malware went undetected until a cyber assessment was conducted on the ship later, and after the crew had reported a computer issue affecting the ship's network. Reportedly, the ship's ECDIS got infected by ransomware when the surveyor inserted the USB thumb drive into a computer in the ship's engine control room. The ship owner paid the ransom.

Another notable ransomware attack occurred in 2019, when a tanker near the port of Naantali in Finland was hit by ransomware (Meland, Bernsmed, Wille, RA¸dseth, & Nesheim, 2021). As a result, its administration server was infected and the back up disk was wiped. Reportedly, the method of intrusion remains unclear but a Remote Desktop Protocol (RDP), a USB device or an email attachment are identified as probable attack vectors. The same vessel was infected again 4 months later near the same port. The threat actor and motives behind the attack remain a mystery.

Others

In table 8 two MCAD incidents fell into none of the previous incident categories.

One cyber incident appeared in September 2016, a ship was hit by a blackmail scam in West Africa.

It was a sextortion case where the scammer probably used pre-recorded or stolen videos to extort the seafarer, in the hope that the seafarer would pay the amount of money that was asked for. The threat actor was never known.

In April 2023 according to an F.B.I. affidavit in support of the criminal complaint and arrest warrant a day after the Royal Caribbean ship departed from Miami for a seven-night eastern Caribbean cruise, a man identified as Jeremy Froias allegedly hid a Wi-Fi camera in a top deck bathroom, pointing its lens toward the toilet. A day later, the camera was spotted by a passenger who reported it to the ship's security staff. They found hours' worth of footage showing more than 150 people, including what appear to be at least 40 minors, some of whom were at least partly naked, the FBI said.

Year	Incident Description
2016	Ship hit by cyber blackmail scam in West-Africa
2023	Passenger hid Camera in Cruise Ship "Harmony of the Seas" Public Bathroom

Table 8

MCAD documented other attacks.

Discussion

The result of this work validates the concern raised in the introduction: cyber threats targeting vessels are still ongoing and impacting the GMTS. Analyzing incidents impacting vessels over the last two decades, the observation can be made that attackers are and have actively exploited vulnerabilities in vessels.

Based on the analysis of vessel cyber incidents from the MCAD database, the following key insights have been identified:

1. Navigation Systems are the Primary Target: - The majority of recorded incidents in MCAD are related to navigation, AIS spoofing (22), Going Dark (15), GPS jamming (13), and GPS Spoofing (5). This indicates that adversaries have a strong focus on disrupting vessels by targeting the navigational aids.

2. Under-reporting of Maritime Cyber Incidents: - Many cyber incidents related to the GMTS go unreported, which slows down the development of comprehensive threat intelligence.

3. Limited (Crew) Awareness and Training: - Cyber security awareness and training among crew members is not mandatory.

4. Dependence on Navigation Systems: - The reliance on GPS and AIS technologies introduces critical vulnerabilities.

The incidents reviewed in this work confirm that cyber attacks on vessels are real and can have a huge impact; it also reveals structural and procedural weaknesses within the GMTS. To improve the cyber resilience in the GMTS, training of crew is needed and reporting of cyber security incidents.

Conclusion

This work shows that cyber attacks against vessels in the GMTS are real and a growing threat. Real-world cases from the Maritime Cyber Attack Database (MCAD) were presented, demonstrating how attackers actively exploit vulnerabilities in both Information systems (IT) and Operational Technology (OT) systems onboard vessels.

Case studies used in this work included GPS jamming in South Korea, AIS/GPS spoofing leading to the grounding of a vessel MSC Antonia, and in another case to the seizure of the Stena Impero, and a malware incident that spread through USB onboard a new-build dry bulk carrier. These examples showed that both targeted and opportunistic attacks are actively targeting GMTS; the consequences of those attacks can lead to economic loss, operational disruption, and geopolitical escalation. The research aims to show that cyber threats in the GMTS are real. The real-world cases confirm that attackers target navigation systems and satellite communication, and use malware.

Future work should focus on expanding and regularly updating the MCAD to reflect emerging threats and near-miss events. In addition, vessel-specific risk assessments, cyber security training for crew members, and the adoption of anomaly detection technologies are needed to enhance resilience across the sector. A standardized reporting mechanism for maritime cyber incidents would also contribute significantly to collective situational awareness and threat intelligence.

Ultimately, continued research and cross-sector collaboration are vital to safeguarding the maritime domain against evolving cyber threats.

References

BBC News. (2019, September 27). Stena Impero: Seized British tanker leaves Iran's waters. https://www.bbc.com/news/world-middle-east-49849718 (Accessed: 2025-05-29)

BIMCO. (2016). The guidelines on cyber security onboard ships. Author.

Bunwaree, P. (2025). Curbing "dark" activity at sea: The role of the marine insurance industry. European Journal of Risk Regulation, 16(1), 1–18. https://doi.org/10.1017/err.2025.15

Cydome. (2025, March). Lab Dookhtegan cyber attack on Iranian oil tankers disrupts operations. https://cydome.io/lab-dookhtegan-cyber-attack-on-iranian-oil-tankers-disrupts-operations/ (Accessed: 2025-05-16)

International Chamber of Shipping. (2020). Guidelines on cyber security onboard ships. https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf (Accessed: 2025-05-12)

Lee, S. J. (2013). GNSS vulnerability issues in Korea. Chungnam National University.

Maritime IT Security Research Group. (n.d.). Maritime cyber attack database (MCAD). https://maritimecybersecurity.nl/ (Accessed: 2025-01-10)

Meland, P. H., Bernsmed, K., Wille, E., Rådseth, J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation, 15(3), 519–530. https://doi.org/10.12716/1001.15.03.09

SAFETY4SEA. (2025, May 13). Windward: GPS jamming is a rising cyber threat in the Red Sea. https://safety4sea.com/windward-gps-jamming-is-a-rising-cyber-threat-in-the-red-sea/ (Accessed: 2025-06-06)

SecureWorld. (2018). Ships at sea: More ways to hack them. https://www.secureworld.io/industry-news/ships-at-sea-more-ways-to-hack-them (Accessed: 2025-05-12)

Seo, J., & Kim, M. (2013). eLoran in Korea—Current status and future plans. In Proceedings of the European Navigation Conference (pp. 23–27). Vienna, Austria.

TradeWinds News. (2024). VLCCs deliver unprecedented Russian and Chinese cargoes to Venezuela after spoofing AIS. https://www.tradewindsnews.com/tankers/vlccs-deliver-unprecedented-russian-and-chinese-cargoes-to-venezuela-after-spoofing-ais/2-1-1817381 (Accessed: 2025-06-06)

WindwardAI. (2025, May 13). GPS jamming is a rising cyber threat in the Red Sea [Tweet]. X (formerly Twitter). https://twitter.com/WindwardAI/status/1921924400393200001 (Accessed: 2025-06-06)

ZDNet. (2018). Ships infected with ransomware, USB malware, worms. https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/ (Accessed: 2025-05-12)

About the Authors

Jeroen Pijpker / NHL Stenden University of Applied Sciences / jeroen.pijpker[at]nhlstenden.com / ORCID: 0009-0008-8334-0655

Jeroen Pijpker is the program manager/researcher of the Maritime IT Security research group of NHL Stenden University of Applied Sciences. Jeroen has been intensively involved in establishing the research group at NHL Stenden. Jeroen has a strong professional background in Information Technology and Operational Technology. His current research focuses on maritime cyber security. He has worked at NHL Stenden for 20 years in numerous roles, including lecturer/researcher and team leader for the Information Technology study program. Jeroen is a certified ethical hacker and developed and runs the Certified Ethical Hacking minor that NHL Stenden offers. He has a broad interest in cyber security (software and hardware). Within the research group, Jeroen is working on, amongst other things, the realisation of a maritime Ship Honeynet to lure hackers into a trap. He has published a number of research papers on the topic of maritime cyber security.

Stephen McCombie / NHL Stenden University of Applied Sciences / stephen.mccombie[at]nhlstenden.com / ORCID: 0000-0002-6511-9382

Stephen's current research interests are in maritime cyber threats, cyber crime, digital forensics, cyber threat intelligence and cyber conflict. His research draws on a diverse background in policing, security and information technology. His PhD thesis examined the impact of Eastern European cybercrime groups on Australian banks. Over the last 20 years he has held management roles with a number of organisations including IBM, National Australia Bank, and RSA Security and he has also been an active researcher and academic over that period. He currently works as a Professor of Maritime IT Security at NHL Stenden University of Applied Science. Stephen before working in industry and academia spent 14 years in the NSW Police as a Detective and was instrumental in the establishment of their first computer crime investigation team. He has also lectured on cyber security and digital forensics over a number of years at Macquarie University, Charles Sturt University and National University of Singapore and published a large number of research articles on those topics. He is also currently a Certified Information System Security Professional (CISSP), a Certified Fraud Examiner (CFE) and an Information Systems Security Management Professional (ISSMP).

Combatting the Shadow Fleet: Countering Maritime Sabotage, Surveillance and Disruption

Sarah Kirchberger
Kiel University, Germany

Abstract

Several countries whose oil trade is under Western sanctions, in particular Russia, Iran, and Venezuela, have resorted to using "shadow fleet" or "dark fleet" ships to evade scrutiny. Their primary function is to conduct illicit hydrocarbons trade or traffic arms while obfuscating state responsibility. But eventually, and in particular after the Russian 2022 invasion of Ukraine, several secondary functions have evolved, in particular with Russian shadow fleet vessels operating in European waters. Increasingly, such ships have become instruments in hybrid or "grayzone" warfare, whether by causing physical damage to maritime infrastructures or by serving as platforms to conduct maritime surveillance, espionage, AIS jamming and spoofing or other forms of electronic warfare. This article focuses on the evolving situation in the Baltic Sea, a hotspot for Russian shadow fleet vessels conducting hybrid warfare activities against NATO nations. This has given rise to a dedicated NATO activity, "Baltic Sentry", in early 2025, aimed at countering these threats. After assessing the current status of combating the shadow fleet, some possible next steps are discussed.

Keywords

Shadow Fleet, Dark Fleet, Hybrid Warfare, Undersea Infrastructure, Subsea Cable Sabotage

Introduction

Several countries whose oil trade is under Western sanctions, in particular Russia, Iran, and Venezuela, have resorted to using "shadow fleet" or "dark fleet" ships to evade scrutiny. Their primary function is to conduct illicit hydrocarbons trade or traffic arms while obfuscating state responsibility. But eventually, and in particular after the Russian 2022 invasion of Ukraine, several secondary functions have evolved, in particular with Russian shadow fleet vessels operating in European waters. Increasingly, such ships have become instruments in hybrid or "grayzone" warfare, whether by causing physical damage to maritime infrastructures or by serving as platforms to conduct maritime surveillance, espionage, AIS jamming and spoofing or other forms of electronic warfare.

Worldwide, more than 1,000 vessels, mostly ageing and poorly maintained tankers registered with flags of convenience, have been identified as belonging to the class of "dark fleet" ships by the maritime AI firm Windward (2023). According to Wiese Bockmann (2023, March 10), such ships account for approximately 10% of the worldwide seaborne oil transport. To classify a particular ship as a "dark" or "shadow fleet" vessel, Lloyd's List uses the following criteria: the ship is typically a tanker of 15+ years of age (the average Russian shadow fleet age is ca. 20 years), whose ownership structure is obscured e.g. by using a complex corporate structure of subsidiaries and shell companies designed to obfuscate beneficial ownership discovery; it is solely used for conducting sanctioned oil trade or arms trafficking, and, it engages in one or several of the so-called "deceptive shipping practices" outlined in US State Department Guidance (Department of State et al. 2020; Wiese Bockmann, 2023). These can include "going dark" by manipulating or entirely turning off its AIS, and suddenly changing or falsely identifying the vessel's name, flag state, owner, or operator. Lately, an additional range of even darker behavior patterns has emerged, in particular related to some Russian shadow fleet vessels, which have been suspected of vandalism and sabotage of maritime infrastructures; carrying of GNSS jamming, spoofing, intelligence gathering (SIGINT) and electronic warfare (EW) equipment; and launching surveillance drones near Western military facilities. These newer activities point to a possible auxiliary shadow fleet role in military operations during wartime.

Apart from malevolent activities conducted by such ships, it bears noting that many shadow fleet vessels are ageing and badly maintained tankers whose frequent technical malfunctions pose environmental and navigational hazards to littoral countries on their path. Often, they lack standard Protection & Indemnity (P&I) insurance that would cover e.g. the cost of environmental damage due to an oil spill. Regulating and constraining the shadow fleet is thus a key maritime security concern for all countries that frequently see shadow fleet vessels operating near their shores.

This article concentrates on the evolving situation in the Baltic Sea, a hotspot of Russian shadow fleet vessels conducting hybrid warfare activities against NATO nations that have in early 2025 given rise to a dedicated NATO activity, "Baltic Sentry", to counter these threats, following the formation of a new NATO Critical Undersea Infrastructure Network in 2024. After assessing the current status of combating the shadow fleet, some possible next steps are discussed.

Challenges to Maritime Infrastructure Security Posed by the Shadow Fleet

Since the Russian full invasion of Ukraine in February 2022, Russian shadow fleet vessels have been involved in several instances of damaging subsea infrastructures in Europe by anchor-dragging. A curiously parallel set of cases was concurrently observed in the West Pacific, where Chinese ships have engaged in similar behaviors towards Taiwanese and Southeast Asian neighboring countries' subsea infrastructures. In the Baltic Sea, a series of four high-profile anchor-dragging cases began on Vladimir Putin's birthday in 2023. This series has laid bare the technical challenges of protecting critical undersea infrastructures, such as telecommunication and electricity cables and gas pipelines on the seabed against accidents and intentional sabotage. Further, the incidents illustrated the difficulty of quickly attributing damage to a particular actor, of legally proving intent, of claiming and receiving damages, and ultimately of deterring future acts of vandalism. This has to be seen in the wider context of steadily escalating hybrid warfare across Europe on land and at sea, where according to IISS data, confirmed cases of Russian critical infrastructure sabotage have increased by 246% from 2023 to 2024 alone (Edwards & Seidenstein 2025, p. 9). Meanwhile, a war of narratives has emerged with regard to the anchor-dragging incidents, with different parties pushing for downplaying vs. exposing the intentional nature of the cases and disagreeing whether to name their possible state sponsor. Further, to complicate the question of attribution, three out of four Russian shadow fleet vessels that were involved in the anchor-dragging incidents also had some sort of ownership or operator ties to China, although it is as yet unclear whether such ties imply direct state involvement, i.e. Chinese authorities' beforehand knowledge of those ship's illicit activities. The following section will briefly discuss the four most hotly debated anchor-dragging cases to illustrate the above points, based on Finnish, Estonian, German, and international news reports.

The NewNew Polar Bear Case (October 2023)

The NewNew Polar Bear case occurred during the evening and night of October 7/8, 2023. The NewNew Polar Bear is a Hong Kong-flagged icebreaking container ship that had only recently become active on the "Polar Silk Road" route. Its ownership structure is opaque and involves several obscure Chinese and Russian entities with connections to the Polar Silk Route trade, including a company named Torgmoll registered in Russia and China (Brunnsberg, 2023, October 29).

The cable and pipeline-cutting incident unfolded when the NewNew Polar Bear travelled eastward through the Baltic Sea en route to St. Petersburg with its portside anchor dragging over the seabed for several 100km, destroying first the EE-S1 telecom cable between Sweden and Estonia at ca. 17:30 on October 7, 2023 - coincidentally, this was Vladimir Putin's birthday - then travelled eastward for several hours, and, according to AIS data, slowed down from ca. 11kts to just 1.1kts speed at 01:12 am local time on Oct. 8, merely 8 minutes before ripping apart the BalticConnector gas pipeline connecting Finland and Estonia. The force needed to rip apart the concrete-encased pipeline was so great that it caused a small seismic event that was recorded by the Norwegian research institute Norsar at 01:20 am EET (Maritime Executive, 2023, October 11). Fortunately for the crew of the NewNew Polar Bear, this icebreaking vessel was able to withstand such great force without critical damage to the hull, which might have endangered a less sturdy ship. However, the NewNew Polar Bear's port anchor was ripped off while rupturing the pipeline and later recovered next to it. The ship drove on with a dragging anchor chain that ripped the FEC data cable between Finland and Estonia at ca. 03:45 am local time (Sillanpää, 2023, October 23). While damaging all these infrastructures, the NewNew Polar Bear was closely followed by another icebreaking ship, the Russian-flagged, Atomflot-owned, nuclear-powered icebreaking cargo ship Sevmorput, which had previously been employed by Russia in an auxiliary role during its 'Burevestnik' nuclear-powered cruise missile tests off Murmansk, pointing to its state and military role (Nilsen, 2022, September 18; Liski & Erämaa, 2023, October 21). Meanwhile, yet another Russian vessel, the oil/ore carrier SGV Flot, positioned itself and remained stationary over the location of the BalticConnector pipeline a little further to the north from late Oct. 6 until Oct. 8, without any apparent cause for that delay, raising the possibility that this ship may have also played some part in the action (Liski & Tahkokorpi, 2023, October 29).

After travelling to the Russian port St. Petersburg, where the NewNew Polar Bear was photographed on Oct. 9 at pier with its portside anchor chain hanging out (YLE, 2023, October 24), it made its way back westward through the Gulf of Finland, where it was hailed by Finnish authorities but ignored their request to stop and steamed on. As it was outside territorial waters, Finnish authorities did not attempt to stop the NewNew Polar Bear. Later, the Finnish investigation of the seabed uncovered compelling physical evidence of the ship's role in the pipeline damage, while photos of the ship from ca. Oct. 22 near the Russian Arctic port Arkhangelsk revealed that its portside anchor was missing and containers on its port side had visibly shifted. Suspiciously, while traveling back to China via the Northern Sea Route, the ship suddenly changed its operator from the Chinese Hainan Xin Xin Yang Shipping Co, Ltd. to the Russian-registered firm Torgmoll (Staalesen, 2023, October 26).

Despite promising otherwise, Chinese authorities did not cooperate with the Finnish and Estonian investigations, and while China in May 2024 admitted the NewNew Polar Bear's responsibility for causing the damage, it maintained this had been accidental (Baltic Times, 2025, May 9; Bermingham, 2024, August 12). In May 2025, that narrative was suddenly revised by China when it emerged that the master of the NewNew Polar Bear, a 43-year-old Chinese national named Wan Wenguo, had been charged in Hong Kong with one count of "criminal damage" to the BalticConnector pipeline and 2 counts of violating maritime bylaws. The criminal court case is still ongoing as of this writing (ERR, 2025, July 5). Regardless of its outcome, the fact a criminal case was opened indicates that the Hong Kong prosecution believes criminal intent can be proven. In case an accident had been regarded likely, civil litigation not criminal prosecution, would typically occur. Given the absence of rule of law in Mainland China, and the degree of political control exercised over the PRC's court system, Beijing's decision to hand over the suspect, a Chinese national, to a comparably more public and professional Hong Kong court rather than trying the suspect in Mainland China itself is remarkable.

It signals a degree of transparency and might indicate that China objects to the involvement of its ships in Russian hybrid warfare activities in Europe, notwithstanding the fact that Chinese shadow fleet ships are conducting similar offenses against neighbors in East Asia (Focus Taiwan, 2025, June 12). The further developments in the Hong Kong court case might shed more light on the Chinese approach to dealing with European allegations of maritime infrastructure sabotage, which were further enhanced after the 2024 Yi Peng 3 case.

The Yi Peng 3 Case (November 2024)

From the early hours of November 17, 2024, a Chinese-owned and Chinese-flagged ship, the bulk carrier Yi Peng 3, while moving westward through the Baltic Sea from Ust-Luga dragged its anchor several times back and forth over telecommunications cables off Gotland and "went dark" by switching off its AIS for more than 7 hours altogether. The damaged fiber-optic data cables included the BSC East-West Interlink and C-Lion 1. While dragging its anchor, the Yi Peng 3 maneuvered in a way that is inconsistent with an autopilot, as it requires manual input, such as driving a full circle in the morning of 18 November, and changing speed repeatedly (Rosemann, 2025, p. 6).

Yi Peng 3 is owned by the Chinese firm Ningbo Yipeng Shipping Co., Ltd. and managed by Win Enterprise Ship Management (Ningbo) Co., Ltd. Its crew is entirely Chinese. A Finnish investigative journalist who visited both companies' premises in Ningbo on November 21 and 22, 2024 was able to briefly interview the management, but found that the ship owner's office at the registered address was empty and that this shell company's address was located inside a "military management zone" guarded by soldiers (Jokinen, 2024, November 22).

The ship was stopped on 20 November 2024 in the Kattegat, where it remained outside Danish and Swedish territorial waters during a month-long standoff, unable to travel onwards without traversing territorial waters where it might be arrested, but remaining untouchable to investigators without the formal consent of the flag state China. On 29 November, Beijing in principle consented to an investigation, and diplomatic negotiations over the technicalities of the procedure finally ended the standoff when China on 29 November consented to a pro forma investigation on board the ship, lead and conducted by Chinese investigators and accompanied by German and some Finnish, Swedish and Danish observers. After this ship visit had taken place on December 19 without uncovering any incriminating evidence - unsurprisingly, given the time that had since elapsed - the ship was allowed to travel on (Rosemann, 2025, p. 6).

The Eagle S Case (December 2024)

The Eagle S is a crude oil tanker registered in the Cook Islands, crewed mainly by Georgian and Indian nationals and owned by Caravella LLC-FZ in the United Arab Emirates. It was the only vessel operated by that company.

On Christmas Day 2024, it was apprehended in flagrante by the Finnish Coast Guard with its anchor chain still hanging in the water after it had damaged 4 telecoms cables and the Estlink-2 power cable connecting Finland and Estonia, by dragging its anchor for more than 90km while en route from Ust-Luga to Port Said in Egypt (YLE, 2025, August 21).

The Eagle S was ordered into Finnish territorial waters, complied, and was then boarded by special forces from the Finnish Coast Guard and police who took over control of the ship in the early hours of December 26, seizing all electronic equipment including crew members' computers, cameras, mobile devices and other evidence and detaining the crew. This was the first case where an actual forensic examination of the physical evidence on board the ship was conducted in a timely manner.

After the ship's arrest, a widely noted report in Lloyd's List quoted unnamed shipping industry sources that alleged the Eagle S had in the past been witnessed to carry portable electronic equipment for espionage or electronic warfare that was operated by specialized personnel not part of the normal crew (Wiese Bockmann, 2024, December 27). During the Finnish investigation of the ship, however, no such portable equipment was uncovered (Kavander, 2024, December 31).

The captain, a Georgian national named Davit Vadatchkoria, as well as the 1st and 2nd officers have in the meantime been charged with aggravated sabotage and aggravated telecommunications interference, as well as lesser offences such as vandalism and endangering public safety. The trial started in Helsinki in late August 2025.

The three accused maintain their innocence and claim they never noticed the dragging anchor after accidentally lowering it - despite having been hailed by Finnish authorities hours earler and asked whether their anchor was dragging, which they denied without checking (YLE, 2025, August 21). Moreover, the ship's movement pattern indicates active steering by the crew during the time they supposedly did not notice an anchor was dragging due to using an autopilot. Like the NewNew Polar Bear, the ship notably slowed down right before damaging the power cable. It also drove a full circle on 25 December, ca. 11:45 UTC right after damaging the power cable – a maneuver that requires manual steering and is not possible under autopilot (Rosemann, 2025, p. 6; YLE, 2024, December 27). As in the NewNew Polar Bear case described above, regardless of the outcome of the court case, the fact it was opened at all indicates that prosecutors are confident that they are able to prove criminal intent. A Finnish newspaper reported that the Finnish National Criminal Police had wiretapped the crew after detention and intercepted a verbal instruction from the ship's operator to the captain on 7 January 2025 that asked him to conceal evidence (Erämaa, 2025, August 25). The police investigation also uncovered that the ship's "black box" had malfunctioned and not recorded anything until half an hour after the power cable was cut, apparently due to GNSS jamming in the Gulf of Finland (Mäntysalo, 2025, August 26).

The Vezhen Case (January 2025)

The fourth anchor-dragging case involved the bulk carrier Vezhen, a Malta-flagged vessel operated by the Bulgarian firm Navibulgar and crewed by Bulgarian and Burmese sailors. After starting westward from Ust-Luga, in the early hours of 26 January 2025, it severed a Latvian LVRTC-owned data cable near Gotland. Following the Finnish model of dealing with the Eagle S, the Vezhen was then stopped and swiftly boarded and arrested by Swedish police. The crew claimed accidental release of the anchor in bad weather; however, Sweden's Meteorological and Hydrological Institute pointed out that wind speeds had been "well below" the threshold for a storm warning at the time the anchor dropped, and wave heights in the area were only 1m, or relatively low (The Insider, 2025, January 27).

However, the Vezhen's crew was soon exculpated by Swedish investigators after surveillance video footage of the anchor dropping all by itself was uncovered on board the ship. All but one of the safety mechanisms holding the anchor had reportedly been faulty, and the footage showed a wave hitting the anchor and it then dropped without any nearby person's visible interference. The Swedish investigators consequently dropped the case against the crew (Ahlander & Jacobsen, 2025, February 3). While this might show how the anchor could have dropped on its own (never mind the convenient coincidence that this moment was also captured on video footage), the case raises questions in how far the crew really could not have noticed dragging its anchor for a whole 24 hours, over 300km, supposedly because the ship was on autopilot.

On 06:30 UTC on 26 January, it drove a full circle (as in the Eagle S and Yi Peng 3 cases), which is not compatible with the explanation that the autopilot drove the ship all that time (Rosemann, 2025, p. 6).

Accidents or Sabotage? A 'War of Narratives'

Legally speaking, a lack of evidence, while not the same as proof of innocence, means that the principle *in dubio pro reo* must be applied. In the *Vezhen* case, the video footage of an anchor dropping on its own apparently left the investigators with too little material to pursue a criminal case against the crew. The timing of this incident is notable, as the *Vezhen* case happened only days after Donald Trump's inauguration as the 47th US President on January 20. And only one day before that momentous event, a *Washington Post* article, citing anonymous European security and intelligence sources, had made the sensational claim that an "emerging consensus" among European intelligence services had supposedly concluded that *all* the cable-cutting cases in the Baltic Sea had been accidents rather than sabotage (Miller et al., 2025, January 19). The anonymously-sourced story of such a "European intelligence consensus" was immediately and vehemently refuted by multiple Finnish, Estonian, and German high-ranking defence and security officials with access to classified information who were willing to speak on the record.[11]

Not much later, it turned out that a diplomatic pressure campaign from Washington DC via NATO channels had in parallel to that press report been conducted. It aimed to induce Baltic Sea NATO allies to publicly accept the 'accident narrative,' perhaps in preparation of US diplomatic overtures towards Russia in the context of the Ukraine War negotiations.[12] One further indication that this might indeed be the case was the surprising refusal of the new US administration in March 2025 to endorse a G7 initiative to combat the Russian shadow fleet: "As well as vetoing Canada's proposal to establish a task force to monitor sanctions breaches," it seems that "the US pushed to remove the word 'sanctions' as well as wording citing Russia's 'ability to maintain its war' in Ukraine" (Connett, 2025, March 8). Against the backdrop of the February 28 verbal attacks on Ukraine's President Zelenskyy during his White House visit, and the halting of US military aid for Ukraine, this US pressure on Baltic Sea NATO members to pretend they were not being subjected to

[11] See e.g. a detailed interview with CAPT Jukka Savolainen of the Hybrid CoE in Helsinki (Kuuskoski, 2025, January 19) and further Finnish officials cited on the record in *YLE* (2025, January 19); a SPIEGEL interview with Germany's Chief of Navy, VADM Kaack (Gebauer & Rosenbach, 2025, February 15); Germany's then Chancellor Olaf Scholz even attributing the sabotage to Russia on the record (Welt, 2025, January 28); and Estonia's Foreign Minister Margus Tsahkna quoted in *The Insider* (2025, January 27).

[12] This author has on several occasions personally witnessed high-ranking US officials pushing the "accident narrative" on European NATO allies in closed-door settings during June and July 2025, and has also seen the irritated and negative reactions to it by several recipients of that message.

sabotage while shielding Russia from censure and vetoing planned G7 measures to combat the shadow fleet all came as a huge shock to the affected European nations. As one retired US diplomat put it during a related conversation with this author, "sometimes diplomats have to do distasteful things to achieve results". Whether the loss of trust among long-standing allies is worth those elusive "results" yet remains to be seen.

Given the background of a "war of narratives" developing around these incidents from late January 2025, the Vezhen case is worth considering further. One hypothetical scenario to be considered is that the main mission of the *Vezhen* might have been not merely to cut those cables, but to produce evidence that "accidental anchor-dragging can indeed happen." While it also remains a possibility that the *Vezhen* case was indeed just an accident, the other possibility should be kept in mind despite the Swedish investigators' decision to drop the criminal case.

Role of Shadow Fleet Vessels in Jamming, Spoofing, EW and Drone Operations

Apart from damaging critical undersea infrastructures, shadow fleet vessels have also been involved in other maritime grayzone behaviors. In connection with the Eagle S case, Lloyd's List's Michelle Wiese Bockmann (2024, December 27) reported a shipping industry source's detailed allegations that the Eagle S as well as another shadow-fleet tanker named Swiftsea Rider had been previously outfitted with portable sensor equipment for SIGINT missions against NATO ships and aircraft that was operated on board by specialized personnel not part of the regular crew, and later offloaded for analysis. The Eagle S also allegedly dropped sensors (likely hydroacoustic sensors) overboard in the English Channel on a previous occasion. The Finnish investigation of the Eagle S did not uncover any such equipment on board at that time. This, however, does not prove the report wrong, as the allegations concern portable equipment that was offloaded previously.

That individual shadow fleet ships can be carrying equipment for espionage and electronic warfare has also been indicated by other reports. For instance, German naval vessels have encountered fake base station attacks conducted from Russian shadow fleet vessels in the Baltic Sea. In June 2025, according to a journalist who was embedded with the German Navy during an exercise, such attacks targeted naval vessels' crewmembers who were accessing the internet from their mobile phones at sea where connectivity is often lacking. The attackers, by providing a source of connectivity disguised as normal service, used such connections to harvest data from personal devices of soldiers, which was then analyzed and used, among other things, to conduct harassing phone calls to their families at home (Baeck, 2025, June 8). This represents a combination of electronic warfare with PSYOPs.

Further, a Polish study in 2024 found indications that GNSS jamming, which is increasingly prevalent across the Baltic Sea and especially near Kaliningrad and in the Gulf of Finland, is being conducted not just from land-based installations, but likely also from ship-borne transmitters carried by shadow-fleet vessels.

A joint investigation by GPSPATRON and the Gdynia Maritime University detected 84 hours of GNSS interference between June and Nov 2024 alone, primarily jamming rather than spoofing, and distinguished two primary types of interference: "multi-constellation jamming" affecting multiple GNSS systems between June and September 2024, and "multi-tone interference" from Oct 2024, suggesting a change in jamming tactics, potentially signaling more sophisticated techniques. Notably, the study identified „strong indications" of mobile maritime jamming sources, with interference signals showing movement patterns consistent with vessels navigating in the Baltic Sea (Gpspatron & Gdynia Maritime University, 2025, February 11).

Apart from likely carrying mobile jamming, spoofing, surveillance and EW equipment on occasion, shadow fleet ships have occasionally been suspected of launching surveillance drones near sensitive military facilities, e.g. in Eckernförde, the homeport of Germany's submarine force. The cargo ship HAV Dolphin had anchored for eight days near Eckernförde in early May 2025 without apparent reason, when multiple drones were sighted near the submarine base (Döbber, 2025, August 26). On May 27, 2025, a swarm of UAVs was also visibly confirmed by a German patrol vessel around the Russian-crewed and -flagged cargo vessel Lauga in the North Sea. The next day, however, a Dutch customs investigation of the Lauga in Zeebrugge did not uncover any physical evidence of drones aboard the ship, which might however have been concealed or removed in-between (Meduza, 2025, June 17).

Western Responses to Shadow Fleet Vandalism & Sabotage

In response to an abnormal cluster of maritime infrastructure sabotage cases in the Baltic Sea, NATO in mid-January 2025 launched its initiative 'Baltic Sentry' to enhance domain awareness and coordinate timely reactions across the Baltic Sea (NATO, 2025, January 14). Since its inception, this initiative can be credited with the success of significantly reducing initially far longer reaction times to suspicious incidents to only ca. 2 hours.[13] Following the Vezhen case of January 26th, 2025, no further cable-cutting incidents have so far occurred, which might be at least partially due to Baltic Sentry's deterrent effect and enhanced vigilance. Another element of NATO's response to infrastructure sabotage is the NATO Critical Undersea Infrastructure Network established in early 2024.

In terms of individual country responses, after a slow reaction had allowed the NewNew Polar Bear to escape investigation in October 2023, various countries have worked on more timely and more robust reactions. A key legal problem is posed by the fact that stopping and searching a vessel on the high seas is difficult to justify without consent from the flag state, as when the Yi Peng 3 was stopped in the Kattegat, resulting in a month-long standoff that was resolved via diplomatic channels after a pro forma "investigation" led by the Chinese flag state under observation from Germany, Finland and Denmark had taken place.

[13] This evaluation was given by a European military official during a conference in June 2025 under Chatham House Rule.

According to a diplomat who was present, the Chinese officials displayed clear signs of embarrassment, while the Finnish investigators in particular openly uttered their frustration about the sham nature of the investigation, which cannot have escaped the Chinese officials.[14] It can be assumed that this experience, even if it did not lead to any conclusive results in that particular case, might have contributed to the Chinese turnaround in allowing the prosecution of the NewNew Polar Bear captain to avoid further damage in China's relations to the Europeans.

In the next case involving the Eagle S in late December 2024, Finnish authorities decided to go one step further and arrest the vessel and prosecute the crew. Finnish Coast Guard and police forces made a point of using somewhat exaggerated means when arresting the tanker by having two teams of special forces boarding it from helicopters, filming this and publicizing the footage - doubtless to create a public narrative of decisive action being taken, to deter other ships from further attempts in Finnish waters. This approach is in line with earlier Finnish reactions to hybrid warfare, e.g. in the case of a suspected Russian submarine intrusion into Finnish waters in April 2015 that was greeted with several depth charges (Hirst 2015, April 28). As a frontline state bordering Russia, Finland has long developed a calibrated approach of "talking softly but carrying a big stick" when dealing with its neighbor's antics.

In a comparable case in the Western Pacific, Taiwan in February 2025 was faced yet again with a Chinese shadow fleet vessel, the Hong Tai 58, cutting internet cables off its coast. Like in the Finnish example, the Taiwanese Coast Guard for the first time arrested and boarded the ship, investigated the case, prosecuted the captain, and the Tainan District Court speedily sentenced him to 3 years imprisonment in June 2025 (Focus Taiwan, 2025, June 12). After the Hong Tai 58 was detained, the investigators released pictures of the hull showing mobile, flexibly combinable name plates aft and stern that could be used to form a great number of different names - clear proof of regular practices to conceal the ship's identity.[15]

The Eagle S and Hong Tai 58 cases have in common that the vessels were apprehended in flagrante, directly after the damage occurred, with their anchor chains still dragging in the water. Both were ordered into territorial waters and complied, were then boarded, searched, had the crew detained, evidence secured, the vessel inspected, and the responsible crew members ultimately prosecuted.

[14] Author's conversation in July 2025 with a European diplomat who participated in the investigation.

[15] The pictures were released by Taiwan's Coast Guard on Facebook and are visible at https://www.facebook.com/100044196351429/posts/pfbid027cC6q5tepczJTjMRxXCX9RvUggc4Y4kTNKU7p6h1s3No5owEfvn6LgYQDaMnS6pDl.

Meanwhile, all parties' actions and reactions have been getting more robust during the past year. In Germany, customs authorities took the unprecedented step of confiscating a defective shadow fleet tanker, the Panama-flagged Eventim, including its cargo of 100,000t of oil, after it had lost propulsion and drifted towards shore, raising the risk of an oil spill accident (Pavliuk, 2025, March 28).

When Estonia, however, in May 2025 attempted to stop and inspect the unflagged, uninsured, sanctioned oil tanker Argent/Jaguar inside its EEZ, Russia reacted by violating Estonian airspace with a fighter jet that accompanied the tanker, and later detained the Greek-flagged tanker Green Admire after it had left an Estonian port and briefly transited Russian territorial waters as previously agreed (Ship & Bunker News, 2025, May 19). While these actions make attribution of shadow fleet activities to Russian state actors more obvious, they also raise the personal risk for law enforcement personnel dealing with such cases.

Stopping, searching and prosecuting ships is therefore not a panacea. The fourth Baltic anchor-dragging case involving the Vezhen in January 2025 shows that sometimes, guilt cannot be legally proven, in which case the accused have, of course, to be acquitted, or, as in the case of the Vezhen, an investigation dropped before it even goes to court. In the overarching picture of hybrid warfare in Europe, however, such is only to be expected occasionally, as evading legal culpability and hiding the involvement of a state actor is a defining feature in acts of hybrid warfare, which are often conducted by hiring proxies (Edwards & Seidenstein, 2025, August). Given the large number of cases, individual incidents do not necessarily influence the bigger picture that much. What matters is the broader pattern. Demonstrating that there is a personal risk and cost to crews who choose to conduct maritime vandalism and sabotage could prove to have a deterrent effect, or at least it might make it harder to find willing participants in such schemes.

Conclusion and Way Forward

What further things need to be done? There is no silver bullet for combating the shadow fleet. As malign practices steadily evolve, so must responses remain flexible. A chief goal should be to deny the adversary the desired results of a malign action, which may not necessarily be limited to the immediate damage caused but can also involve psychological, political, or economic effects.

It will be necessary to further improve monitoring and to create an ever more detailed, shared maritime picture among allies to further reduce reaction times, and to deconflict overlapping areas of responsibility. A dilemma that needs to be addressed concerns the need to conceal hidden Western military capabilities, e.g. sensors, and balance this need against the risk of encouraging an aggressor in case of inaction. In any case, combating the shadow fleet can be seen as an opportunity to improve interoperability of various law enforcement and military forces and enforce existing regulations more strongly.

Some legal reform may be needed to give law enforcement agencies better tools and more security when conducting their work. Legal frameworks might need further elaboration to cover acts so far not mentioned. Consistently enhancing the risk of personal prosecution might deter some crews from participating in illicit acts.

In terms of public messaging, authorities could make use of heightened interest in the OSINT community and its many enthusiastic observers to create greater public awareness.

Another potential avenue of influence might be diplomatic outreach towards third-party countries, such as India, the UAE, and flag states of convenience in order to disincentivize them from offering support and services to shadow fleet vessels.

Last, as the above detailed example of the "war of narratives" from late January 2025 shows, unity amongst allies should be protected, not fractured. One main goal of malign actors' hybrid warfare is, after all, to sow doubt and paralyze decision-making centers while trying to fracture successful alliances.

References

Ahlander, J., & Jacobsen, S. (2025, February 3). Sweden says ship broke Baltic Sea cable by accident. Reute. https://www.reuters.com/world/europe/sweden-rules-out-sabotage-baltic-sea-cable-damage-case-2025-02-03/

Baeck, J.-P. (2025, June 8). Unruhige See: Schattenflotten, Sabotage und Datenkabel – die Ostsee ist seit Russlands Angriff zum Brennpunkt geworden. Unterwegs mit der deutschen Marine (Troubled seas: Shadow fleets, sabotage, and data cables – the Baltic Sea has become a hot spot since Russia's attack. Underway with the German Navy). TAZ. https://taz.de/Bundeswehr-auf-Minensuche/!6089861/

Baltic Times. (2025, May 9). Captain of ship that damaged Balticconnector faces charges in Hong Kong. https://www.baltictimes.com/captain_of_ship_that_damaged_balticconnector_faces_charges_in_hong_kong/

Berminham, F. (2024, August 12). Beijing admits Hong Kong-flagged ship destroyed key Baltic gas pipeline 'by accident'. South China Morning Post. https://www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident

Brunnsberg, M. (2023, October 29). Vahinko vai sabotaasi? Huippuasiantuntijatkin ihmeissään Suomenlahden tapahtumista (Damage or sabotage? Even top experts are amazed by events in the Gulf of Finland). Iltalehti. https://www.iltalehti.fi/ulkomaat/a/5e46007f-9ec3-4882-8935-6c17e6de2d8a

Connett, D. (2025, March 8). US vetoes G7 proposal to combat Russia's shadow fleet of oil tankers. The Guardian. https://www.theguardian.com/us-news/2025/mar/08/america-vetoes-g7-proposal-to-combat-russias-shadow-fleet-of-oil-tankers

Department of State, Department of the Treasury and United States Coast Guard. (2020, May 14). Guidance to Address Illicit Shipping and Sanctions Evasion Practices. https://ofac.treasury.gov/media/37751/download?inline

Döbber, C. (2025, August 26). HAV Dolphin: Ominöses Schiff lag 8 Tage vor Kiel – sein neuer Kurs bereitet jetzt Finnland Sorge (HAV Dolphin: Ominous ship anchored 8 days off Kiel – its new course is causing concern in Finland). Focus. https://www.focus.de/politik/ausland/sicherheitsbedenken-wachsen-warum-europa-ein-auge-auf-dieses-schiff-hat_9dab600e-b7f1-4e99-859d-e966cc2966d5.html

Edwards, C., & Seidenstein, N. (2025, August). The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. IISS. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

Erämaa, I. (2025, August 25). "Tuhoa se" – Poliisin salakuuntelu paljasti Eagle S:n synkän suunnitelman ("Destroy it" – Police wiretap reveals Eagle S's sinister plan). Iltalehti. https://www.iltalehti.fi/kotimaa/a/f4063624-499a-4134-a7bb-6d348d74b818

ERR. (2025, July 5). Captain of ship that destroyed Balticconnector pipeline appears in Hong Kong court. https://news.err.ee/1609738404/captain-of-ship-that-destroyed-balticconnector-pipeline-appears-in-hong-kong-court

Focus Taiwan. (2025, June 12). Chinese ship captain handed 3-year sentence over severed telecoms cable. https://focustaiwan.tw/society/202506120025

Gebauer, M., & Rosenbach, M. (2025, February 15). "Ich glaube schlicht nicht an so viele Zufälle" ("I simply don't believe in so many concidences"). DER SPIEGEL. https://www.spiegel.de/politik/deutschland/ostsee-sabotage-marine-offizier-warnt-vor-zunehmender-unsicherheit-a-8187e9ad-3c5f-4520-8fd5-918d08104fe3

Gpspatron & Gdynia Maritime University. (2025, February 11). Report on GNSS Interference in the Baltic Sea: Analysis Using a Terrestrial Monitoring System and Comparison with ADS-B Data. https://gpspatron.com/gnss-interference-in-the-baltic-sea-a-collaborative-study-by-gpspatron-and-gdynia-maritime-university/

Hirst, T. (2015, April 28). Finland dropped 6 depth charges on a suspected Russian submarine but says it doesn't want to 'create a farce'. Business Insider. https://www.businessinsider.com/finland-depth-charges-on-russian-submarine-2015-4

Jokinen, M. (2024, November 22). Kaapelivaurion lähellä pyörineen kiinalaisaluksen manageri kertoo HS:lle käsityksensä, mitä laivalla tapahtuu nyt (The manager of the Chinese ship that was sailing near the cable damage tells HS what is happening on the ship now). Helsingin Sanomat. https://www.hs.fi/kirjeenvaihtajat/art-2000010850988.html

Kavander, A. (2024, December 31). Poliisi kiistää väitteet Eagle S-tankkerin vakoilulaitteista (Police deny allegations of spy devices on Eagle S tanker). YLE. https://yle.fi/a/74-20134341

Kuuskoski, K. (2025, January 19). Asiantuntija tyrmää uudet väitteet Itämeren kaapelivaurioista: "Kyllä tämä on aika isoa peliä" (Expert dismisses new claims about cable damage in the Baltic Sea: "This is clearly a pretty big game"). Ilta-Sanomat. https://www.is.fi/kotimaa/art-2000010974584.html

Liski, J., & Erämaa, I. (2023, October 21). Kaasuputken vaurioittamisesta epäilty kiinalaisalus kulki peräkanaa Venäjän asevoimia palvelevan laivan kanssa (Chinese ship suspected of damaging gas pipeline sailed tail-to-tail with Russian military ship). Iltalehti. https://www.iltalehti.fi/kotimaa/a/3e8f6056-2439-4fdf-a9b1-242653500cac

Liski, J., & Tahkokorpi, T. (2023, October 29). Analyysi: Toimivatko Kiina ja Venäjä yhdessä? (Analysis: Are China and Russia working together?). Iltalehti. https://www.iltalehti.fi/kotimaa/a/c193c1e1-fa04-4719-bb7b-c7d3f986d187

Mäntysalo, J. (2025, August 26). Eagle S -tutkinnasta hätkähdyttävä tieto: Musta laatikko oli pois päältä, kun laiva alkoi katkoa kaapeleita (Shocking information from the Eagle S investigation: The black box was off when the ship started cutting cables). YLE. https://yle.fi/a/74-20179391

Maritime Executive. (2023, October 11). Seismic Station Detected Possible Blast During Baltic Gas Line Breach. https://maritime-executive.com/article/seismic-station-detected-possible-blast-during-baltic-gas-line-breach

Meduza. (2025, June 17). An invisible maritime menace: Mysterious drones spy on Western defenses as cargo ships linked to Russia cruise European waters. https://meduza.io/en/feature/2025/06/17/an-invisible-maritime-menace

Miller, G., Dixon, R., & Stanley-Becker, I. (2025, January 19). Accidents, not Russian sabotage, behind undersea cable damage, officials say. Washington Post. https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/

NATO. (2025, January 14). NATO launches 'Baltic Sentry' to increase critical infrastructure security. https://www.nato.int/cps/en/natohq/news_232122.htm

Nilsen, T. (2022, September 18). New study reveals comprehensive buildup of nuclear missile test-ground at Novaya Zemlya. The Barents Observer. https://www.thebarentsobserver.com/security/new-study-reveals-comprehensive-buildup-of-nuclear-missile-testground-at-novaya-zemlya/164155

Pavliuk, O. (2025, March 28). Germany confirms confiscation of detained tanker Eventin from Russia's shadow fleet. Ukrainska Pravda. https://www.pravda.com.ua/eng/news/2025/03/28/7505025/

Rimpiläinen, T. (2023, October 24). Kiinalaisaluksesta otetut kuvat vahvistavat ankkuriteoriaa kaasuputkitutkinnassa (Images of Chinese ship confirm anchor theory in gas pipeline investigation). YLE. https://yle.fi/a/74-20056692

Rosemann, A. (2025). Kabel, Anker, Zufälle (Cables, Anchors, Coincidences). MarineForum, 4, 6-11. https://en.ikiosk.de/shop/epaper/marine-forum/1461973.html

Sillanpää, S. (2023, October 23). Uusi tieto: Kiinalaisalus näyttää pysähtyneen avomerellä juuri ennen kaasuputkea (New information: Chinese ship appears to have stopped in the open sea just before the gas pipeline). Helsingin Sanomat. https://www.hs.fi/suomi/art-2000009941718.html

Staalesen, A. (2023, October 26). Runaway ship Newnew Polar Bear, suspected of sabotage in Baltic Sea, is sailing into Russian Arctic waters. The Barents Observer.

https://www.thebarentsobserver.com/security/runaway-ship-newnew-polar-bear-suspected-of-sabotage-in-baltic-sea-is-sailing-into-russian-arctic-waters/164423

The Insider. (2025, January 27). Bulgarian owner of vessel seized by Sweden over Latvian cable damage claims accident, says anchor dropped to seabed in high winds. https://theins.press/en/news/278263

Welt. (2025, January 28). Scholz warnt vor “Bedrohung durch russische Schattenflotte“(Scholz warns of “threat from Russian shadow fleet”).

https://www.welt.de/politik/deutschland/article255264674/Hybride-Kriegsfuehrung-Scholz-warnt-vor-Bedrohung-durch-russische-Schattenflotte.html

Wiese Bockmann, M. (2023, March 10). Dark fleet of tankers now comprises 10% of seaborne oil transport. Lloyd’s List. https://www.lloydslist.com/LL1144275/Dark-fleet-of-tankers-now-comprises-10-of-seaborne-oil-transport

Wiese Bockmann, M. (2023, April 21). Shifty shades of grey: The different risk profiles of the dark fleet explained. Lloyd's List. https://www.lloydslist.com/LL1144787/Shifty-shades-of-grey-The-different-risk-profiles-of-the-dark-fleet-explained

Wiese Bockmann, M. (2024, December 27). Russia-linked cable-cutting tanker seized by Finland 'was loaded with spying equipment'. Lloyd's List. https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment

Windward. (2023). Dark and Gray Fleets. https://windward.ai/glossary/what-is-the-dark-fleet/

YLE. (2023, October 24). Finnish investigators suspect Chinese vessel's anchor caused Balticconnector pipeline damage. https://yle.fi/a/74-20056827

YLE. (2024, December 27). Maps reveal the path of the Eagle S on Christmas Day. https://yle.fi/a/74-20133606

YLE. (2025, January 19). Washington Post: Finnish intelligence officials believe Eagle S rupture was an accident. https://yle.fi/a/74-20138017

YLE. (2025, August 21). "It was an accident," says captain of anchor-dragging Eagle S tanker. https://yle.fi/a/74-20178643

About the Author

Dr Sarah Kirchberger / Kiel University (ISPK) / SKirchberger[at]ispk.uni-kiel.de / ORCID: 0009-0000-6083-5673

Dr. Sarah Kirchberger is Academic Director at the Institute for Security Policy at Kiel University (ISPK), Vice President of the German Maritime Institute (DMI) and a Nonresident Senior Fellow at the Atlantic Council. She was previously an Assistant Professor of Sinology at Hamburg University and a naval analyst with shipbuilder TKMS. She is the author of 'Assessing China's Naval Power: Technological Innovation, Economic Constraints, and Strategic Implications,' co-author of 'The China Plan: A Transatlantic Blueprint for Strategic Competition' and co-editor of 'Russia-China Relations: Emerging Alliance or Eternal Rivals?'. In April 2023, she testified before the US-China Economic and Security Review Commission (USCC) on China's undersea warfare. Her research focuses on China's undersea warfare; PLAN modernization; Chinese defense-industrial development; and mil-tech co-operation between China, Russia and Ukraine. She holds a MA and a PhD in Sinology from the University of Hamburg after studies in Hamburg, Taipei and Trier.

Freedom of Navigation Operations (FONOPs) and e-Navigation: Legal Assertion Meets Digital Enablement

Capt (N) Burak Inan
Turkish Hydrographic Office

Abstract

This paper explores how Freedom of Navigation Operations (FONOPs) and e-Navigation work together to keep the seas open, safe, and lawful. FONOPs are operations that challenge illegal maritime claims and protect the rights of all ships to navigate freely under international law. e-Navigation, developed by the IMO and IHO, provides the digital tools and data such as ECDIS, AIS, and S-100-based charts that make navigation more accurate, efficient, and transparent. The paper explains how FONOPs now depend on these technologies for safe routes, real-time monitoring, and secure communication, especially in areas with tension or disputes. It also highlights the growing importance of maritime cybersecurity to protect navigation systems from interference or manipulation. The work of the International Centre for Electronic Navigational Charts (IC-ENC) is presented as an example of how trusted and verified chart data supports both safety and legal credibility. Together, FONOPs and e-Navigation show how law, technology, and cooperation can strengthen global maritime stability and protect the freedom to navigate in the digital age.

Keywords

Freedom of Navigation Operations (FONOPs), e-Navigation, Maritime Cybersecurity, S-100, IC-ENC

Introduction

The global maritime environment is increasingly shaped by the interplay of strategic, legal, and technological developments. Among these, Freedom of Navigation Operations (FONOPs) and e-Navigation have emerged as complementary instruments safeguarding maritime openness. While FONOPs focus on contesting unlawful maritime claims, e-Navigation provides the technological infrastructure needed for precise, safe, and legally compliant navigation. This paper explores the strategic, legal, and operational convergence between the two frameworks.

The U.S. Freedom of Navigation Program

Formally established in 1979, the Freedom of Navigation (FON) Program consists of complementary diplomatic and operational efforts to safeguard lawful commerce and the global mobility of U.S. forces. The Department of State (DOS) protests excessive maritime claims, advocating for adherence to international law, while the Department of Defense (DoD) exercises the United States' maritime rights and freedoms by conducting operational challenges to excessive maritime claims. In combination, these efforts help preserve for all states the legal balance of interests established in customary international law as reflected in the 1982 Law of the Sea Convention. Since its establishment, the U.S. FON Program has continuously reaffirmed the U.S. policy of exercising and asserting its navigation and overflight rights and freedoms around the world. These assertions communicate that the United States does not acquiesce to the excessive maritime claims of other nations and prevents them from becoming accepted customary international law (United States Department of Defense, 2023).

The United States initiated the Freedom of Navigation Program in 1979 under President Jimmy Carter, in response to growing global claims that sought to restrict international transit rights. President Ronald Reagan formally reaffirmed the program in 1983. Since then, FONOPs have served as peaceful and routine assertions of navigational rights, functioning as part of the United States' commitment to the rules-based international maritime order (Kraska, 2011).

The implementation of FONOPs involves:

- The U.S. Department of Defence (DoD), which executes naval missions using platforms such as destroyers and cruisers.
- The U.S. Department of State, which supports these missions diplomatically through demarches, formal protests lodged with states that make excessive claims.
- Partner governments, which support FONOP objectives through joint naval exercises, legal coordination, and operational cooperation.

FONOPs are crucial for defending the legal status of international straits, exclusive economic zones (EEZs), and the high seas. They counter attempts by coastal states to impose restrictions inconsistent with UNCLOS, thereby preserving access for commercial shipping, naval deployments, and global trade (Bateman, 2010).

International Cooperation and Partner Activities

FONOPs are not conducted in isolation. Many like-minded maritime states participate directly or indirectly in reinforcing lawful maritime conduct.

Recent examples include:

- United Kingdom, Bahrain, Canada, France, Italy, Netherlands, Norway, Seychelles, and Spain Participated in Operation Prosperity Guardian, a multinational security initiative launched in 2024 to deter drone attacks and protect commercial shipping in the Red Sea and Gulf of Aden (Indo-Pacific Defense Forum, 2024).

- Philippines Collaborates with the U.S. via Task Force Ayungin, focusing on maritime surveillance and resupply missions in the Second Thomas Shoal. U.S. ISR support reinforces the Philippines' lawful rights in the South China Sea (Reuters, 2024).

- Australia Contributes to FONOP-aligned operations through its 2025 Regional Presence Deployment, including P-8A Poseidon patrol aircraft and naval assets across the Indo-Pacific.

- Japan Participates in Multilateral Maritime Cooperative Activities with the U.S., Australia, and the Philippines to uphold UNCLOS-based freedoms in areas facing contested maritime claims (Australian Department of Defence, 2024).

These examples reflect a broader trend toward coalition-based defense of navigational freedoms, demonstrating that FONOPs are not unilateral provocations, but rather collaborative efforts grounded in international law.

e-Navigation and Its Operational Relevance

e-Navigation, developed by the International Maritime Organization (IMO), refers to the digital integration of navigational tools, data standards, and communication systems to enhance safety, efficiency, and environmental sustainability in marine navigation (IMO, 2018; 2019). It includes the implementation of:

- ECDIS (Electronic Chart Display and Information System)

- AIS (Automatic Identification Systems)

- S-100-based data services for digital hydrography and multi-layered charting (IHO, 2022)

These technologies enable high-resolution situational awareness, automated voyage planning, and decision-making support for both commercial and military vessels.

Strategic Convergence

The convergence between FONOPs and e-Navigation becomes operationally evident in high-risk or disputed maritime zones. FONOPs increasingly rely on e-Navigation features for:

- Precise navigation within maritime jurisdictions
- Real-time monitoring of traffic, hazards, and restricted zones
- Secure communication and interoperability with coalition forces

For example, S-100 charting services help visualize the legal and hydrographic limits of features like artificial islands or straits, supporting lawful transit. Meanwhile, VDES (VHF Data Exchange System) and encrypted tactical links improve coordination among naval units (UKHO, 2023).

e-Navigation also strengthens the legal transparency of FONOPs. Public AIS broadcasts, digital navigation notices, and compliance with COLREGs reinforce the principle that such operations are conducted responsibly and lawfully, not provocatively (Bateman, 2010).

In regions such as the South China Sea or the Black Sea, where the risk of confrontation is high, resilient e-Navigation systems, including anti-GNSS spoofing, cybersecure ECDIS, and multi-channel redundancy, help ensure crew safety, mission credibility, and regional stability (UKHO, 2023).

Maritime Cybersecurity

The Digital Integrity Layer of Navigational Freedom as maritime operations become increasingly digitized, maritime cybersecurity has emerged as a critical enabler of both navigational safety and legal credibility. The intersection of FONOPs, e-Navigation, and S-100-based digital infrastructure depends heavily on secure, uninterrupted, and trustworthy data flows. In this context, maritime cybersecurity functions not merely as a technical safeguard but as a strategic precondition for lawful maritime conduct.

The Digital Vulnerability of Freedom of Navigation

FONOPs, particularly in contested zones, rely on precise geospatial positioning, authenticated hydrographic data, and secure digital communications. Malicious interference—such as GNSS spoofing, jamming of AIS/VDES signals, or electronic chart corruption—can jeopardize both navigational accuracy and legal defensibility. A ship unintentionally straying outside legal boundaries due to cyber disruption may escalate regional tensions or undermine UNCLOS principles.

S-100 and Trusted Data Exchange

The S-100 Universal Hydrographic Data Model introduces a modern, layered approach to marine data exchange. However, these digital services are vulnerable to tampering or misinformation if not securely managed. The growing dependency on real-time, shared navigational data makes data integrity and provenance critical components of operational safety and legal compliance (IHO, 2022). Emerging solutions, such as IP-based chart authentication, are being developed to protect authenticity, traceability, and data integrity.

Converging Requirements

The convergence of FONOPs, e-Navigation, S-100, and cybersecurity demonstrates the emergence of a new digital legal-operational triad:

• Legal authority,

• Technical capability (e-Navigation and S-100 interoperability),

• Digital trust (resilient, verifiable cyber-physical systems).

For FONOPs to succeed in the future, navies and maritime organizations must adopt cyber-resilient navigation platforms, train crews in cyber-awareness, and define international norms for digital behavior at sea (IMO, 2021).

The Role of IC-ENC in Enabling Trusted Chart Distribution

The International Centre for ENCs (IC-ENC) plays a vital role in the quality assurance, validation, and coordinated distribution of Electronic Navigational Charts (ENCs) used by maritime forces and commercial shipping worldwide. As a Regional ENC Coordinating Centre (RENC), IC-ENC ensures that ENCs meet IHO standards such as S-57 and the evolving S-100 framework, supporting e-Navigation safety and legal defensibility. In FONOP scenarios, where accurate boundary depiction and legal status must be verified, IC-ENC provides a reliable chain of data custody, reinforcing the evidentiary value of navigation routes and reinforcing compliance with UNCLOS (IC-ENC, 2023).

By coordinating with hydrographic offices globally, IC-ENC acts as a maritime data integrity backbone, enabling navies and civilian mariners alike to navigate with confidence—even in contested waters. This trusted chart infrastructure aligns with the goals of cybersecurity, S-100 interoperability, and e-Navigation reliability.

Conclusion

FONOPs and e-Navigation represent two sides of the same strategic coin. FONOPs defend the right to navigate, while e-Navigation enables that navigation to occur safely, precisely, and transparently. In an era marked by digitalization and contested maritime claims, their combined use fortified by resilient cybersecurity frameworks and supported by trusted chart services such as IC-ENC serves to uphold a rules-based maritime order grounded in legal principles and technological capabilities.

References

Australian Department of Defence. (2024). *Multilateral maritime cooperative activity joint statement*. https://www.defence.gov.au/news-events/releases/2024-08-07/multilateral-maritime-cooperative-activity-joint-statement

Bateman, S. (2010). Solving the "wicked problems" of maritime security: Are regional forums up to the task? *Contemporary Southeast Asia*, *32*(1), 1–28.

Indo-Pacific Defense Forum. (2024). *Freedom of the seas*. Indo-Pacific Defense Forum. https://ipdefenseforum.com/2024/05/freedom-of-the-seas/

International Centre for ENCs. (2023). *IC-ENC quality assurance and distribution services*. https://www.ic-enc.org

International Hydrographic Organization. (2022). *The S-100 universal hydrographic data model*. IHO.

International Maritime Organization. (2018). *E-navigation strategy implementation plan (SIP) (MSC.1/Circ.1595)*. IMO.

International Maritime Organization. (2019). *Initial descriptions of maritime services in the context of e-navigation (MSC.1/Circ.1610)*. IMO.

International Maritime Organization. (2021). *Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.3)*. IMO.

Kraska, J. (2011). *Maritime power and the law of the sea: Expeditionary operations in world politics*. Oxford University Press.

Reuters. (2024). *U.S. could escort Philippine resupply missions in South China Sea, admiral says*. Reuters. https://www.reuters.com/world/asia-pacific/philippines-says-china-is-biggest-disruptor-peace-region-2024-08-27/

United Kingdom Hydrographic Office. (2023). *Exploring voyage optimization and 'Just-in-Time' arrivals*. https://www.admiralty.co.uk/decarbonisation/voyage-optimisation

United States Department of Defense. (2023). *Freedom of navigation report – Fiscal year 2023*. Washington, DC: Department of Defense.

About the Author

Cat-B Burak INAN / Turkish Hydrographic Office / inn.brk[at]outlook.com

Burak İNAN is a Cat-B qualified Nautical Cartographer trained at the International Maritime Academy (IMA) in Trieste, Italy. He has served for over 20 years both at the Turkish Hydrographic Office and at sea aboard a hydrographic survey vessel, combining field experience with technical knowledge. His international assignments include service as Military Attaché in Jakarta (2018–2021) and Chief of Staff at the UN Black Sea Grain Initiative (2023–2024). He chaired the International Centre for Electronic Navigational Charts (IC-ENC) between 2023 and 2025 and now serves as its Vice-Chair. He also served as Chief of Staff at the Maritime Security Centre of Excellence (MARSEC COE) between 2024 and 2025. He currently holds the position of Deputy Director of the Turkish Hydrographic Office. His professional focus includes S-100 implementation, ENC production, and advancing regional cooperation through innovation and capacity development.

Manned/Unmanned Navigation in GNSS Denied Operation Area

Dr. Dünya Rauf Levent Güner
Integrated Naval Warfare Systems/Aselsan, Türkiye

Abstract

In this paper, GNSS jamming and spoofing techniques are briefly introduced and effect of GNSS jamming and spoofing on navigation performance of manned ships and MUS (Maritime unmanned systems) is investigated. Examples of effects of jamming in multiple peacetime occurrences are given. Navigation in GNSS denied environments is analyzed with multi-domain and naval perspective and pros/cons of naval operating environment and mitigation alternatives in GNSS denied operation area are analyzed. Tactical employment of MUS in GNSS denied operational environment along with effects and challenges are explored. Dependency of manned/unmanned surface ships, UUV's, launch and recovery operations of MUS, collaborative and synchronized operations to GNSS availability is explored. Effects of GNSS unavailability to shipborne/ship launched unmanned systems is investigated. Information about several in-use or potential mitigation/augmentation methods and systems for naval navigation under GNSS jamming/spoofing cases are given. CRPA antennas, alternative terrestrial navigation candidates, stellar navigation. terrain aided navigation, vision aided navigation methods and systems along with applicability and advantages/disadvantages are narrated.

Keywords

GNSS Denied Environment, MUS, CRPA, TAN, USV, Intentional Jamming, Spoofing

Introduction

Global Navigation Satellite Systems (GNSS), such as GPS, are integral to modern navigation for both maritime and aviation sectors. However, the increasing prevalence of GNSS jamming and spoofing poses significant risks to safety and operational efficiency. These threats have been observed in various regions, with intensified activities linked to geopolitical tensions, particularly the Russian-Ukrainian conflict.

Materials and Methods

Within the scope of this study, navigation methods and, their classification is given. Jamming and spoofing is defined and incidents of jamming and spoofing are given by the use of open sources. GNSS interference effects on manned shipping, autonomous ships and MUS is analyzed in the light of operation scenarios. Possible mitigation techniques and navigation aiding alternatives along with open system architecture studies is given.

Navigation and Navigation Methods

The origin of word "navigation" comes from the words "navi" meaning "ship", and ago which means "showing the way" in Latin language. The primary aim of the navigation is to find the position and route of the ship. Navigation is an ancient art which is being employed since the first ship went to the sea. The time when the first ship started sailing is unclear but it is known that some early forms of small boats made from papyrus wood were sailing on the Nile delta around BC2700. When the Phoenicians discovered the use of long strong cedar woods on building the keel of the ship, stronger ships that can withstand the waves of Mediterranean had been built.

The first captains were employing "shore navigation", in which they were trying not to miss the sight of the shore. By the use of new shipbuilding techniques, ships that can be used in off-shore sailing had been built, but to navigate in the open seas was a formidable and very dangerous task. The "art" of navigation was consisting of several secret taught that were passed from generation to generation. The navigation capability was one of the main talents that saved the lives of the sailors as well as the captain, diminishing the possibility of the crew to revolt against the captain.

Further developments in the field of navigation led to the invention of many methods and systems. The first gyrocompass system that Sperry had developed was installed on USS Delaware in 1911. The gyrocompass was first designed to replace the magnetic compass but inertial navigation technology evolved and became the main navigation system of the ships. USS Nautilus (SSN-571) used the General Autonetics N6A-1 inertial navigation system in her voyage under the North Pole all the way submerged in 1958.

Inertial navigation technology has been evolved thanks to the World Wars and the successful implementation of inertial navigation onboard German V2 missiles (designated as missile due to inertial guidance system). Some early forms of inertial guidance systems are seen in WWII. Post war led to a new era of exploration, and an amazing progress in navigation technology has been achieved. The impetus for this significant progress came during the ballistic missile programs of the 1960s, in which the need for high accuracy at ranges of thousands of kilometers using autonomous navigation systems was apparent. By "autonomous" it is meant that no man-made signals from outside the vehicle are required to perform navigation. If no external man-made signals are required, then an enemy cannot jam them.

LORAN, OMEGA, ALPHA systems has been developed in 20th century and provided accuracies around 400 meters to 3 nautical miles. Some of these ground-based radio navigation systems had global coverage thanks to the use of VLF radio waves.

Today GNSS (global navigation satellite system) systems provide global coverage with an accuracy of 10 to 1 meter. As the history of navigation is analyzed, it can be said that the improvements achieved in navigation science is primarily on the basis of equipment and high technology components. Other than that, the primary geometrical principles and position fixing methods consisting of measuring distances and angles are the same for a captain of an ancient dhow or a nuclear aircraft carrier.

The navigation methods can be classified according to being externally dependent or self-contained. Dead reckoning is a self-contained method of navigation that does not rely on any external infrastructure. Sensors that measure quantities to be used in navigation by themselves fall into this category such as inertial sensors, barometric sensors, speed sensors etc. Externally dependent systems are using measurements by a pre-formed network of signal sources (Figure 1).

Externally dependent systems use angle or distance measurements. Distance measurement techniques used in radio navigation can be divided into time of arrival (TOA), time difference of arrival (TDOA) and received signal strength intensity (RSSI) systems. Angle measurement systems use triangulation. Some systems like VOR/DME (Very High Frequency Omni-directional Range/Distance Measuring Equipment) and TACAN (Tactical Air Navigation) use both distance and angle information to obtain a position fix.

Externally dependent systems mostly in radio navigation are classified according to their measurement type. These systems are rho-rho, theta-rho, theta-theta systems where "rho" stands for distance measurement and "theta" for angle measurement. A position fix that is obtained by using 2 VOR stations is a theta-theta position fix while a VOR/DME system is a theta-rho radio navigation aid.

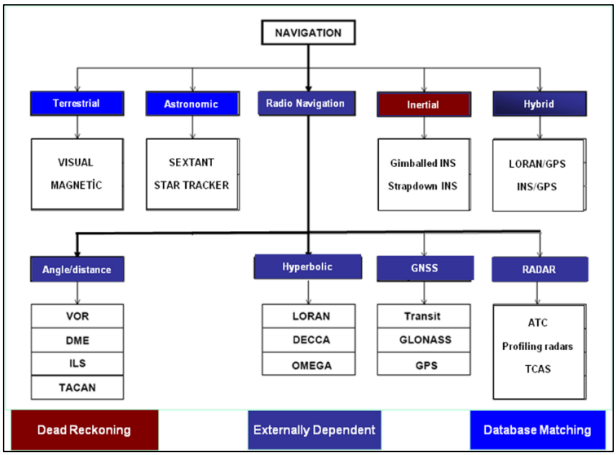

Figure 1
Navigation Systems and Methods

Inertial navigation system (INS) is a kind of dead reckoning navigation system which has means to measure linear accelerations and rotation rates in 3 orthogonal axes.

An inertial navigation system (INS) is a three-dimensional dead-reckoning navigation system. It comprises a set of inertial sensors, known as an inertial measurement unit (IMU), a navigation processor, power and sensor electronic cards, a clock, and a mechanical interface to be accurately mounted on the host vehicle.

The advantages of inertial navigation systems can be summarized as follows;

- Independent operation. No external information is required for navigation except initial position for initial alignment process.
- Cannot be jammed by external sources using electronic attack methods, its operation cannot be interrupted.
- Since inertial navigation systems are passive sensors which do not emit signals, their operation is completely self-contained and covert, making an ideal navigation system for submarines.
- Inertial navigation systems can operate in every tactical situation, in ECM environment, airborne, on land and under water.
- Provides navigation information in high rates in high dynamic environments.
- Provides attitude, angular rates, acceleration, position, velocity information in high rates (i.e. 100 Hz) with time of validity information which is very critical in stabilization of weapon systems.

The disadvantages of inertial navigation systems are the error growth with time which is due the integration of errors and the necessity to enter initial coordinates. (and heading for initial alignment for lower quality systems.)

Inertial navigation systems can be classified with respect to their accuracy class as control, tactical, navigation and strategic. (Figure 2).

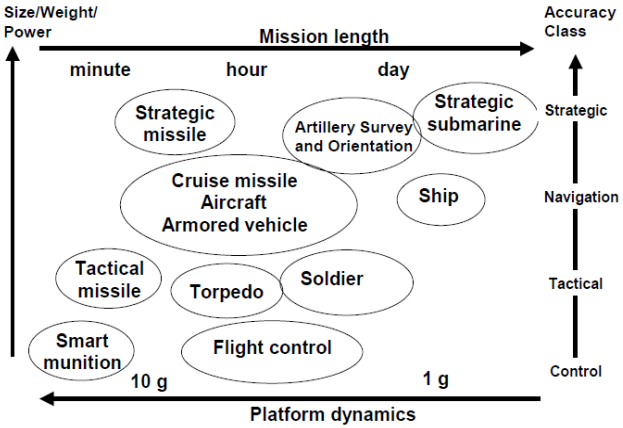

Figure 2
Classification and Usage Areas of Inertial Navigation Systems (NATO SET-054/RTG-30, 2004)

Navigation At Sea

Navigation at sea has both limitations and advantages. Altitude is nearly constant for surface navigation; velocity aiding is generally relative velocity provided by the EM log systems. Being "stationary" is not possible so zero velocity updates (ZUPTS) for minimizing the growth of inertial sensor errors is harder. Duration of missions are days to weeks which require higher accuracy inertial navigation systems with lower drift. Navigation specialties in various domains are given in Figure 3.

Advantages:

- The open sea provides a more predictable, low-clutter electromagnetic environment, which can benefit alternative navigation techniques such as stellar navigation.
- Naval platforms often have larger size and power capacity, allowing for more complex mitigation systems like CRPA (Controlled Reception Pattern Antenna).

Disadvantages

- Scarce visual or terrain features limit the effectiveness of vision or terrain-aided navigation systems.
- Maritime environments are prone to signal reflection, multipath errors, and weather-based degradation of optical and radio systems.

PARAMETER/MEDIUM	LAND	AIR	NAVAL SURFACE
DURATION	HOURS	HOURS	DAYS-WEEKS
ALTITUDE INFO	PARTIALLY IMPORTANT	CRITICAL	NOT IMPORTANT
ALTITUDE	VARIABLE	VARIABLE	NEAR MSL
ZUPT	YES	PARTIAL AT HOVER	NONE
VELOCITY AIDS	ODOMETER	PİTOT TUBE	EM LOG
TAN	LIMITED	USABLE	NOT AVAILABLE OFFSHORE
TERCOM	LIMITED	USABLE-LIMITED	AT LIMITED DEPTHS
VISUAL LANDMARKS	POSSIBLE	POSSIBLE	PARTIAL - INSHORE
RF-LOS NAVIGATION AIDS	POSSIBLE	POSSIBLE	POSSIBLE INSHORE
HYPERBOLIC NAVIGATION	NOT USED	POSSIBLE	POSSIBLE

Figure 3

Navigation Specialties in Multiple Domains

Jamming And Spoofing

Jamming is high-power interference that blocks GNSS signals and can be unintentional or intentional. İntentional jamming can be performed by typically broadband or CW jammers. Spoofing: is transmitting fake GNSS signals to mislead receivers and can be stealthy and highly effective.

GNSS systems are one of the first systems to be jammed in a conflict. The structure and the power of the signal let the enemy to jam GNSS signals easily. GNSS signals can be obscured by terrain and vegetation, and signals can be overwhelmed by several electronic equipment even unintentionally. There are several occasions of unintentional jamming in literature. A new bought preamp TV antenna in a pleasure craft moored in Moss Harbor denied the use of GPS within a radius of 1 km, and the harbor authority had to employ radar aided harbor entry system in 2001. Another incident in 2007 led to the shutdown of San Diego DGPS station and cell towers (NATO SET-054/RTG-30, 2004; Benshoof, 2004).

GNSS systems can be deceived by two types of electronic attack. jamming and spoofing. Jamming is performed by noise inducing and preventing the receiver from locking on the GNSS signal or breaking lock and can be performed by anybody by using low cost jammers. Spoofing is more complicated and mainly done by employing stronger and same signals than original GNSS code, lock on wrong code and pulling off slowly from the original signal to the deceiver signal, from true position to a wrong intended position. Another spoofing technique is to take the GNSS signal, wait for a while and rebroadcast it. (meaconing). Spoofing requires much higher technology, planning and more sophisticated equipment when compared with jamming. Effects of Jamming and spoofing on land, air and naval units is given in Table 1. Specialties of jamming and spoofing attacks are given in Table 2.

A simplistic spoofing attack is easy to detect, considering that a high strength of the fake signal is needed for the receiver to ignore the authentic satellite signal and take the fake one, and the fake signal is not synchronized with the satellite constellation. Typically, these attacks are performed by first jamming the authentic GNSS signal to force the receiver to re-acquire and lock onto the fake signal. The result of a simplified attack is mostly jumps in PVT calculations (Garbin Manfredini, 2017).

Platform	Typical Mission Duration	Reliance on GNSS	Effect of Jamming	Effect of Spoofing
Artillery (SPG/MLRS)	Hours-Days	Low	Low	High (incorrect targeting)
Armor (Tanks/IFVs)	Hours per sortie	Medium (maneuver + targeting)	Moderate	High
Military Aircraft	1–10 hours	High	Moderate	Medium High
Commercial Aircraft	1–15 hours	High	High	High
Naval Vessel	Weeks-months	Medium	Moderate	Moderate
Commercial Ship	Days to Weeks	High (position, speed)	Moderate to High	Moderate
Unmanned Surface Vessel (USV)	Hours to days	Very High	High	High
UUV (UW)	Hours to 24h+	GNSS for surface fix and LARS.	Low UW, High on surface	Low UW, High on surface

Table 1

Effects of Jamming and spoofing on Land/air and naval platform

Spoofing detection is especially hard when a high-quality spoofer is used for the spoofing attack. It is not easy to discriminate between authentic and fake satellite signals in cases where all simulated signals have high fidelity. In cases like this, Controlled reception pattern antennas (CRPA) are used as the best option for defense—spoofer generates and transmits all simulated (spoofed) signals from the same location (one source), unlike authentic satellite signals which come from different sources (different satellites) from the sky. CRPA antenna rejects the signals if they come from the same direction because those kinds of signals are probably fake ones.

Aspect	GNSS Jamming	GNSS Spoofing
Definition	Overpowering GNSS signals with RF noise	Transmitting fake GNSS signals to deceive receivers
Signal Type	Noise or wideband interference	Structured GNSS-like signal
Effect on Receiver	Signal loss or degraded accuracy	False position/time information
Detection	Easier to detect (loss of lock, increased noise floor)	Harder to detect (receiver shows valid but incorrect data)
Complexity to Implement	Low to moderate (broadband noise generator)	High (synchronized signal generation, knowledge of ephemeris)
Operational Use	Denial of access (e.g., area denial)	Deception and control (e.g., hijack navigation)
Impact Area	Broad area (up to tens of km depending on power)	Localized (targeted within a few km typically)

Table 2

Jamming and Spoofing

Maritime GNSS Interference Incidents

Several GNSS interference incidents are seen within the last five years in an increasing manner along with regional conflicts and Russian-Ukrainian war.

Black Sea (2017): Dozens of vessels reported spoofed GPS locations, placing them inland at a nearby airport. This suggested an intentional spoofing event likely originating from regional military activities.

Eastern Mediterranean and Arctic: Multiple jamming reports affecting civilian and NATO military vessels during exercises, often attributed to geopolitical tensions.

Baltic and North Sea Areas (2022–2025): Civil aviation and maritime sectors experienced GPS disruptions traced to suspected Russian military activities, complicating commercial and defense operations.

Some specific incidents are as follows:

- **Kerch Strait, Crimea (May 2018):** During President Putin's visit to the newly constructed Kerch Strait Bridge, at least 24 vessels in the vicinity reported falsified GNSS positions, indicating locations over 65 kilometers away at Anapa Airport. This spoofing incident is believed to have been orchestrated using mobile transmitters, possibly mounted on vehicles accompanying the presidential convoy.

- **Great Belt Bridge, Denmark (October 2022):** A jamming attack near Denmark's Great Belt Bridge disrupted GPS and AIS signals for nine ships, including cargo vessels, ferries, and a Danish patrol vessel. The incident occurred while the patrol vessel was escorting two Russian warships, suggesting a potential link to Russian electronic warfare activities (Automatic İdentification System, Wikipedia, 2025)

- **Black Sea Region (December 2023):** Aircraft in the Black Sea region experienced GNSS spoofing, with ADS-B data indicating false positions over the Belbek Airport in Crimea, a Russian military airfield. The motivation behind this spoofing remains unclear but appears to target military rather than civilian aircraft (GNSS Spoofing and Jamming in Eastern Europe, Inside GNSS, 2024)

In July 2019, the UK-flagged oil tanker Stena Impero, operated by Stena Bulk, was seized by Iranian forces while transiting the Strait of Hormuz. Investigations suggest that the vessel's navigation systems were subjected to GPS spoofing, causing it to deviate into Iranian territorial waters. Analysis of AIS data indicated anomalies consistent with spoofing attacks, where counterfeit signals misled the ship's navigation systems. This incident highlighted the vulnerabilities in maritime navigation and the potential for state actors to exploit them (AIS, 2025; RockBLOCK, 2025).

Some Aviation GNSS Interference Incidents are as follows.

- **Ryanair Flight Diversion (Early 2025):** A Ryanair flight from London to Vilnius was forced to abort its landing and divert to Warsaw due to GPS signal interference near NATO's border with Russia. Lithuanian authorities reported over 800 GPS interference incidents in the preceding three months, with suspicions pointing towards Russian jamming equipment, such as the Tobol system, possibly stationed in Kaliningrad (Ryan Scare, The SUN, 2025).

- **Azerbaijan Airlines Flight 8243 (25 Dec 2025):** While approaching Grozny, Russia, the aircraft lost GPS navigational aids and its ADS-B signal, indicating possible GPS jamming. The aircraft suffered damage consistent with shrapnel, raising concerns about misidentification by Russian air defense systems amid GPS signal loss (*Azerbaijan Airlines Flight 8243*; 2025).

- **Northern Europe (Post-2022):** Following the onset of the Russian-Ukrainian war, increased GPS jamming incidents have been reported in regions including northern Poland, southern Sweden, southeastern Finland, Estonia, and Latvia. These disruptions have affected both civil and military aviation operations (GNSS *interference during the Russian-Ukrainian conflict*, 2025).

- **Ukrainian Drone Operations:** Ukrainian drone pilots have faced significant challenges due to Russian GPS jamming on the battlefield. To navigate, operators resort to visual landmarks, such as distinctive buildings or natural features, compensating for the lack of reliable GNSS data (Bender, 2023).

- **Destruction of Russian GPS Spoofing Platforms:** In August 2024, the Ukrainian Navy targeted and destroyed a decommissioned gas platform off Crimea, which was reportedly used by Russian forces for GPS spoofing activities aimed at disrupting civilian navigation and grain shipping routes (Maritime Executive, 2024).

- **Russian Electronic Warfare Systems:** Russia has deployed advanced electronic warfare systems, such as the R-330Zh Zhitel and Borisoglebsk-2, capable of jamming a wide range of frequencies, including those used by GNSS. These systems have been actively used in the conflict to disrupt Ukrainian communications and navigation (Electronic warfare in the Russian invasion of Ukraine, 2025).

Date	Location	Type	Affected Platform(s)	Effect / Description	Source / Notes
June 22, 2017	Black Sea (off Novorossiysk)	S	Commercial ships	Over 20 vessels' GPS signals spoofed to an airport inland (Gelendzhik).	Galileo GNSS
Oct 2022	Great Belt, Denmark	J	Ships incl. Danish patrol vessel	GPS and AIS signal loss for 10 minutes; full situational awareness lost.	AIS tracking anomalies reported; suspected EW activity
Dec 2023	Baltic Sea & N. Europe	J	Civilian aircraft, maritime traffic	Surge in aviation GPS disruptions, especially in Finnish, Baltic, and Polish FIRs.	Foreign Policy
Mar 2024	Kaliningrad Region (airspace)	J	RAF aircraft	Aircraft carrying UK Defence Secretary jammed; suspected Russian ground-based jammer.	BBC
Mar 23–24, 2024	Eastern Europe	J	1,600+ aircraft (Eurocontrol data)	Large-scale GPS jamming detected; probable EW operations from Kaliningrad/Belarus.	GPS World
Apr 25–26, 2024	Finland–Estonia corridor	J	Finnair commercial aircraft	Flights to Tartu canceled after GPS unreliability near approach; ops suspended.	Le Monde
Jul 10–11, 2024	Gulf of Finland (Kotka–Hamina)	J	Maritime pilot vessel	GPS and radar completely failed during approach; pilot relied on visual nav.	Ukrainska Pravda
Aug 9, 2024	Offshore Crimea	S	Russian military spoofing platform	Ukrainian Navy destroyed a spoofing station used to interfere with grain shipping routes.	Maritime Executive
Jan 16, 2024	NE Poland	J	Civilian aircraft, NATO assets	Intense jamming detected during concurrent Russian Navy drills in the Baltic.	VOA
Sep 17, 2024	Black Sea (Gelendzhik coast)	S	Civilian shipping	Russian GPS spoofing buoy deployed near warships; suspected protection mechanism.	Reddit / OSINT
2022–2024 (ongoing)	Ukraine (Frontline: Kherson, Donbas, Zaporizhzhia)	J - S	Ukrainian drones, HIMARS, artillery	Constant use of GPS jammers by Russian forces to interfere with PGM, UAVs, and communications.	Multiple military analyses & field reports
Feb 2022–2025	Kyiv, Kharkiv, Mykolaiv, Odessa	J	Starlink, GPS signals	GPS outages and Starlink degradation noted near Russian EW hubs and during kinetic strikes.	Confirmed by Ukrainian MoD &

Table 3

Some of GNSS Jamming and Spoofing Incidents

Effects of Navigation Warfare on Maritime Systems

Effects to Manned Commercial Ships:

Commercial ships use integrated bridge systems but generally rely on civilian GNSS receivers and antennas. Navigation systems used in commercial ships are shown in Table 4.

System	Purpose	Typical Grade / Use
GNSS Receiver	Primary position and speed source	Standard civilian-grade GPS or GNSS (often dual-frequency, multi-constellation)
INS	Dead reckoning / backup	Low to moderate grade; typically MEMS or FOG-based INS
ECDIS	Chart-based navigation	Integrated with GNSS and AIS
Radar / ARPA	Obstacle detection and collision avoidance	X-band and/or S-band radars with auto plotting
AIS	Traffic awareness and communication	Mandated for SOLAS ships
Autopilot	Course-keeping	Uses heading from gyro + GNSS position
Integrated Bridge System (IBS)	Unifies radar, ECDIS, GNSS, autopilot, alarms	Found on most large vessels

Table 4

Navigation Systems Used in Commercial Shipping

GNSS jamming can lead to loss or drift of position with time, degradation in ECDIS functionality, unavailable AIS data, erroneous radar overlays. difficulty in maneuvering and navigation in congested sea lanes, or during special operations such as SAR.

Spoofing is particularly insidious for manned vessels, misguiding ships into dangerous waters, causing traffic problems, or triggering navigational errors in areas with tight constraints. causing safety risks to crew and passengers, leading to collisions and entering restricted areas.

Effects to unmanned autonomous ships:

Similar affects may be observed with more severe results. GNSS jamming can lead to interruption of waypoint-based navigation, loss of autonomous or semi-autonomous mission execution capability, loss or drift of position with time along with the effects to manned ships.

Effects to multidomain operations of MUS.:

Operating without GNSS causes stressed operations along with degraded or totally diminished capabilities of systems and groups.

Along with navigation, synchronization between assets tasked for a given mission, frequency hopping communication, and tactical maritime operational picture generation are affected.

Above water and subsurface units' docking operations ate affected. joint operations involving manned unmanned teaming for multiple domains face problems in ISR information, collaborative targeting.

Jamming/Spoofing Scenarios

Jamming is a more common and less sophisticated form of electronic attack to navigation systems and may have effects on a wide area operation.

Spoofing is a more complex electronic attack operation that requires more careful planning and execution and deliberately targets specific platforms. The form of attack should consider the specifications of the navigation system onboard the victim vessel.

In spoofing operation false GNSS signals are sent to the receivers of the targeted platform in a phased manner, first same signals, slowly increasing power levels, then injection of false signals regarding the covariances of the navigation systems so that error rejection algorithms cannot detect very small changes and then diversion of navigation solution to the desired level.

Naval vessels have generally better navigation grade inertial navigation systems with 1 nm per 8- or 24-hour inertial performance and harder to spoof but commercial ships and crew who are accustomed to rely on GNSS heavily may be severely affected.

The situation for the maritime unmanned systems is far worse due to some factors. Except high end units, inertial navigation systems onboard MUS is at most at the lower end of navigation grade inertial sensors if not equipped with all tactical grade sensors. Tactical grade inertial navigation systems in the order of 1 deg/hr units of FOG or MEMS sensors require GNSS for operation and maintain navigation accuracy within order of tens of minutes after GNSS loss. For tactical grade units, due to high covariance values of inertial sensors, detection of the injected diversion resulting false position is far more difficult.

Users at the ground control station are tied to the MUS with a link system either LOS or BLOS, and supervise the MUS systems via information from the vessel. For a diverted false navigation solution, operators do not have means to detect if the vessel's position is true or not.

Unaware of the situation, target coordinate reports from the MUS may be wrong, along with the MUS operation area.

Spoofing may target high value units, more vulnerable units such as tankers and commercial ships, swarm of USV's operating in close formations.

Spoofing may be used to open an opportunity gap for infiltrating defenses. cause unintended violation of territorial waters and cause international crisis or seize units in own territory.

Spoofing effects on MUS

- Diversion of vessel to dangerous, shallow waters for wrecking.
- Shift of position to erroneously dock or crash at berthing and docking operations.
- Diversion of vessel to enemy territory or denied areas for seizing or initiating an international crisis.
- Shift of vessel's operation area to render its barrier operation (Such as ASW barrier.) or ISR sector useless and open an infiltration gap.
- Shift of USV swarm formation's location when the swarm is operating within close formation.
- Shift of position information when a UUV surfaces leading to divergent terrain aided navigation and misleading to dangerous underwater depth areas.

A typical spoofing scenario can be as follows.

ASW Barrier: An ASW MUS unit equipped with dipping sonar system which performs a pattern of dips and use active sonar to detect and deny submarines within its responsibility area is tasked to provide prolonged ASW barrier for a harbor facility may be targeted to have a false positioning information which leads to dipping at wrong locations and thus an opportunity of infiltration may be possible.

ASW MUS reporting position and performing "shifted or obliqued" patterns may not be detected from the ground control station, or if this system is a fully autonomous system all contact reports will be erroneous.

Swarm Attack Mission: A group of swarming low cost USV's are tasked to engage an enemy surface ship which are after some time need to operate fully autonomous. A spoofing attack to this group may lead to complete misdirection of swarm group which leads to failure in visual contact with the target ship, resulting in mission failure and loss of group.

NATO Efforts

Due to recent damages to undersea infrastructure in the Baltic Sea region, NATO forces are conducting BALTIC SENTRY to monitor and respond to threats to undersea infrastructure.

NATO Shipping Center at MARCOM is monitoring GNSS and AIS interference events and has a reporting utility for ships to report incidents.

Task Force X is a new initiative by NATO for providing ISR and security in the Baltic region and employs USV's for patrolling the area.

NATO SET panel has several groups researching assured positioning, navigation and timing methods and systems. APNT. Among them one is SET309.

Mitigation Techniques

For GNSS receivers and antennas, there are some mitigation techniques that enhance jamming and/or spoofing performance based on equipment, algorithms and scenarios. Multi-constellation receivers benefit from 4 GNSS systems, legacy military GPS receivers use SAASM, and P(Y) code military encryption, CRPA antennas provide additional protection against jamming by using beamforming and notch filtering along with the receivers. Power monitoring detects abnormal signal strengths for spoofing detection. Direction of arrival estimation with multiple antennas is also helpful in spoofing detection since spoofing generally performed from one source.

Method	Jamming	Spoofing	Notes
Multi-constellation GNSS	Medium	Medium	increased redundancy, harder to spoof all.
RAIM / Time Consistency Checks	Low	Medium–High	Detects timing or geometry anomalies. Specialty of receiver.
Encrypted Military Signals	Medium	Medium	SAASM, P(Y) code
Adaptive Antenna (CRPA)	High	Medium	Dynamic gain control, directional filtering. Bamforming and notch filtering.
Beamforming / Null Steering	High	Medium	Uses antenna arrays to suppress jammers. CRPA capability.
Notch Filtering	Medium	None	Removes narrowband interference .
Power Monitoring	Low	Medium	Detects abnormal signal strengths
Direction-of-Arrival Estimation	Medium	High	Spoofed signals often share origin for siimple spoofing attacks.
Encrypted Military Signals	High	High	M-Code: strong crypto
Signal Authentication (e.g., NMA)	None	High	Public-key verification of messages
Anomaly detection by machine learning	Low	Medium	Learns spoofing/fake patterns
doppler shift Analysis- multiple antennas.	None	High	Unrealistic movement patterns

Table 7

Mitigation Techniques

Aiding Systems In Naval Context

During the search for navigation techniques that can be used as alternative navigation methods to GNSS, it is important to note that, "There is no alternative system that can provide the unique special characteristics of GNSS systems such as accuracy and global coverage." GNSS systems offer unmatched precision independent of time, everywhere on the world (except confined environments such as under surface), with a minimal cost to user with an extensive ground and space segment infrastructure.

All systems and techniques which are offered as an alternative to GNSS can provide a navigation capability within several limitations when GNSS systems cannot be used. None of the alternative systems can provide a better solution to the navigation problem unless the inertial navigation systems' accuracy reaches 100 times better than the current state, accompanied with a significant decrease in cost and an unrestricted proliferation.

Even though the attempts to increase the A/J (antijam) capability of GNSS systems is continuing, jamming is still a significant threat due to the very low power levels of GNSS satellites and their distance to the earth. Space based augmentation / aiding systems also suffer from the same concern.

Externally dependent ground-based navigation systems can be utilized for an alternative to GNSS. There are existing structures and establishing new infrastructures is possible. DME systems operation principle dictates that the DME station should be interrogated from the vehicle. This causes the vehicle to send transmissions which can be intercepted by opposing force EW (electronic warfare) assets. Also, DME/TACAN interrogation requires equipment in the vessel, DME/TACAN interrogation requires high power transmission which may be a problem for naval drones.

Hyperbolic navigation systems such as LORAN (Long Range Aerial Navigation) can be considered as a backup navigation aid. However, in Turkey there is no active LORAN station. LORAN stations are being shut down in many countries. The time to first fix of a LORAN system is around two to four minutes and achievable accuracies are around 400 meters to 2 nautical miles which may cause problems in some employment scenarios. The number of LORAN base stations (with high rise antennas of ~200 meters) will be limited and may be regarded as a target by opposing forces. As of June 2025, both traditional systems like Loran-C and its modern counterpart, eLoran, are being revisited, alongside the development of alternative navigation aids to ensure resilience against GNSS disruptions. Enhanced Loran (eLoran) is a modernized version of Loran-C, offering improved accuracy (up to ±8 meters), integrity, and additional data capabilities. It serves as a robust backup to GNSS, especially in areas prone to signal interference.

The status of LORAN in various countries

United States: After initial discontinuation, there have been renewed discussions about implementing eLoran as a complementary system to GPS, particularly for timing and navigation resilience. (Loran-C, 2025).

- United Kingdom: The UK had operational eLoran services but ceased positioning transmissions in 2015. However, a timing signal remains active from the Anthorn facility to support research and development (Loran-C, 2025).

- South Korea: Actively developing eLoran infrastructure, South Korea has established pilot services near major ports, aiming for nationwide coverage to mitigate GPS vulnerabilities, particularly from regional threats (Son et al, 2023).

- China and Russia: Both countries are expanding their terrestrial navigation systems, with China upgrading to eLoran to ensure nationwide coverage and resilience against GNSS disruptions.

R-Mode (Ranging Mode): R-Mode is a terrestrial radio-navigation technology that provides GNSS-independent positioning by utilizing existing maritime radio infrastructure such as Medium Frequency (MF) radio beacons and the VHF Data Exchange System (VDES). It is especially relevant for coastal navigation and resilient PNT (Positioning, Navigation, and Timing) solutions.

The EU-funded ORMOBASS project (2025-2026) (Operational Resilient Mode Baltic Sea System) is currently enhancing R-Mode infrastructure across the Baltic Sea, aiming to provide a reliable backup for maritime navigation in GNSS-denied or contested environments (European GNSS Agency, 2025).

Terrain aided navigation techniques such as TERCOM (terrain contour matching) and are used mainly in cruise missiles and UAV's. TAN methods require radar altimeter, barometric altimeter, a map with terrain elevation data, and a flight computer that employs TAN algorithms. Terrain contour matching is a very good method for long range cruise missiles when they are operating without GPS. Actually, TERCOM was first devised in 1958 and implementation on cruise missiles was around 1970's when GPS was not available. TERCOM is not a widely used navigation method. It is mainly employed on very long-range cruise missiles, due to the complexity of its planning phase. The performance also decreases when terrain elevation profiles are not near unique, which means that the path should be planned to allow maximum difference between several possible tracks so that the missile can distinguish between the possible tracks and obtain a good position fix. Roughness and uniqueness of the planned path is a key factor in TERCOM accuracy.

Ekütekin (2007), analyzed the terrain effects on several TAN methods. TERCOM results lead to very large errors even with a 1 nm/h navigation grade INS for smooth/non-unique terrain. Other TAN methods reach better results but uniqueness and roughness of terrain is still a significant issue. Several cases of false position fixes are also encountered.

A ground based aiding solution may lessen the severity of a GNSS jamming scenario if it does not require a strong infrastructure.

Navigation technique	A/J	Global /regional	İmpact on covertness of platform	Weather conditions effect	Operational status when GNSS is jammed	Typical accuracy	Usability for MUS
DME/ TACAN	Good	Regional	Platform is active	Negligible	Yes	~500 meter	Yes. Requires additional hardware
VOR	Medium	Regional	Platform is passive	Negligible	Yes	1.5 -4 degrees azimuth,	Yes. Requires additional hardware
Hyperbolic Navigation	High	Regional	Platform is passive	Negligible	Yes	0.25-1 nm	Yes. Requires additional hardware Accuracy and TTFF may be problematic
Stellar navigation	High	Global	Platform is passive	Heavy, clear sky necessary, Light clouds for SVIR	Yes	0.2-1 nm typical	Yes. Requires additional hardware
TAN/ TERCOM	High	Regional	Platform is active	Negligible	Yes	Dep. on terrain uniquness	Yes. For limited depths.
Gruond Based RF Beacon navigation system	High	Regional	Platform is passive active	LOS dependent	Yes	Dep. on deployment scheme	Yes. Requires additional hardware.

Table 8

Navigation aiding methods and applicability

TRNAV Terrestrial Radio Navigation System

TRNAV is a regional terrestrial navigation system based on smart communication technologies developed by TUALCOM in Türkiye. By setting up a network of TRNAV ground stations at known locations, every platform carrying a TUALCOM position finder will be able to take advantage of the position information available from the TRNAV system. TRNAV system has the added benefit of being designed with a foundation of data link technology. This allows for the unique capability of transferring not only position information over the TRNAV system, but also all other types of data. Due to its ad-hoc mesh networking capabilities, multiple platforms with a TUALCOM position finder attached, can benefit from this system by integrating into the network. System provides positioning information suitable for high speed platforms. TRNAV has been field proven and it has been shown to be capable of providing navigation capability to platforms in GNSS denied/degraded environments. Not only are the ground stations able to transmit position information, but also platforms with a TUALCOM position finder transceiver module is able to act as a mobile node within the network to further extend the network's capabilities. Thanks to this capability positioning network can be extended to forward operating areas.

CRPA Antennas

For mitigating the effects of jamming on GNSS receivers and GNSS aided INS systems, controlled reception pattern antennas (CRPA) are deployed on naval vessels and most unmanned surface vessels. CRPA antennas have an array of antennas and, an ACU (antenna control unit) which processes and filters signals, filters interference, performs beamforming operations. CRPA antennas may be formed up from multiple antennas 4,8,16 etc. and output of the CRPA antenna or ACU is fed to the GNSS receiver.

APNT (Assured PNT)

World War II was the greatest indicator of how critical navigation capability is. In these years, many navigation systems are used independently of each other and aim to solve all positions and angular information on their own. Using multiple and different systems together was not widely considered in those years. inertial navigation systems are developed and improved fast thanks to Cold War. These systems were used in a completely closed manner and since they were not exposed to any interference they became the mainstay of navigation. However, as the accuracy of these systems increased, size and cost changed seriously. In this case, the prevalence and spread of these systems stayed limited.

The establishment of satellite navigation systems (GPS - USA and GLONASS - Russia) in the 1980s changed the rules of the game. It has now become possible to know your location anywhere in the world with low cost instantly with meter-level precision. The problem with these systems is that the signals can be easily suppressed (jammed) and even decepted (spoofed).

The combination of navigation satellite systems that provide solutions with high precision but with limited availability with inertial navigation systems that are 100% reliable but whose performance decreases over time, has been seen as the perfect solution. Integrated (INS/GPS) systems developed in line with this approach were launched on the market in a short time and became dominant in the sector. This approach is still dominant today.

As the years passed and the threats to GNSS signals were better understood, it became clear that there were some fundamental problems in the path followed. Integration processes have generally been carried out by inertial navigation system manufacturers, and all design and software rights—even the structure of navigation messages—have become the proprietary of these companies. The integrator company has decided what will be integrated and has launched the product in this way. Any change in this product requires years of time and financial resources. (For example, converting an INS/GPS system to INS/Galileo). The user or the integrator can't make any changes or adjustments.

Adding other navigation systems to the existing architecture can be very long, costly, or even impossible. On the other hand, all integrated navigation systems have very similar structures and almost all of them are based on the Kalman Filter.

In short, the Kalman Filter is a mathematical structure that finds the most accurate result possible by combining the incoming information by weighting it according to its reliability levels. As a result of all this accumulated information, dissatisfactions and problems encountered during use, a new approach has been proposed. This approach is built on the principles of flexibility, openness and expandability.

Based on a centralized Kalman filter, multiple navigation systems along with standardized navigation messages and covariances can be integrated.

- The system can have as many navigation systems operating independently as desired.
- All navigation systems will communicate with a standard infrastructure.
- A time reference will be used in the system to ensure that all systems are synchronized with each other
- Each navigation system will send all the information it has, to the main integrator unit with the correct time information.
- Each navigation system will transmit not only the final results such as position, speed, orientation, but also the mathematical information representing the reliability of these results (such as covariance matrices) to the main integrator.
- The main integrator will have standardized software that allows the integration of very different systems.

All communication in the system will be made with a special message infrastructure created for the scope of the system.

The topics presented here bring important innovations to navigation systems.

- The ability to use systems developed by different manufacturers together using a common message structure.
- Transforming the integration process from a process that takes years to an arrangement that takes minutes.
- The ability to integrate systems that have never been integrated before or that are of different types, in a short time.
- The elimination of the requirement for subsystem developers and integration software developers to be in the same company.

Conclusion

GNSS jamming and spoofing threat which was evident since 2000's is showing presence as the World is facing destabilizations, crisis and wars. Maritime domain is affected from current and emerging threats, navies and commercial shipping is caught off-guard from the abundant threat occurrences along with widespread drone warfare which is dominating the tactical battlefield and changing the way of warfare. Widespread and unharmonized GNSS jamming and spoofing and multiple electronic warfare means to neutralize the naval/air drones and missiles have pressure on commercial air and maritime traffic, manned and unmanned naval vessels and multidomain operations are also affected. For the maritime domain navigation systems with multiple sources of aiding means are necessary to maintain navigation accuracy for inshore/offshore and collaborative and docking operations. Various mitigation techniques to minimize the effects of navigation warfare for manned/unmanned commercial shipping, manned/unmanned naval vessels operating under multidomain operations are necessary although some mitigation techniques already exist. Open navigation system architectures that can fastly adopt integration of existing and new navigation aids and methods will be helpful. The increasing frequency and sophistication of GNSS jamming and spoofing incidents underscore the need for robust countermeasures and international cooperation to safeguard navigation systems critical to maritime and aviation safety. Naval forces must therefore invest in redundant, resilient navigation and positioning capabilities.

Naval navigation system structure should rely on decentralized open architecture navigation suite incorporating inertial navigation systems, multi-constellation GNSS receivers with CRPA antennas and spoofing detection algorithms, coupled with celestial, RF based terrestrial and vision-based navigation sensors.

References

Automatic Identification System. https://en.wikipedia.org/wiki/Automatic_identification_system

Bender, J. (2023, October 5). *Russian jamming is so strong, Ukraine's drone pilots say they often have to navigate visually using landmarks*. Business Insider. https://www.businessinsider.com/ukraine-drone-operators-struggle-with-russian-gps-jamming-2023-10

Benshoof, P. (2004). *Civilian GPS systems and Potential Vulnerabilities.* 46th Test Squadron. http://www.navcen.ucscg.gov/cgsic/meetings

DNV. (2021). *Autonomous and remotely operated ships* (Class Guideline DNV-CG-0264). DNV AS. https://rules.dnv.com/docs/pdf/DNV/cg/2021-06/DNV-CG-0264.pdf

Ekütekin, V. (January 2007). *Navigation and control studies on cruise missiles* [Unpublished Doctoral Thesis], Middle East Technical University.

European GNSS Agency (GSA). (2022). *ORMOBASS: Developing R-Mode positioning in the Baltic Sea*. EC. Retrieved June 9, 2025, from https://www.euspa.europa.eu/newsroom/news/ormobass-developing-r-mode-positioning-baltic-sea

Ground Control. (May 14, 2025)Tackling Maritime GPS Spoofing and Jamming Threats with RockBLOCK Pro STL. https://www.groundcontrol.com/blog/tackling-gps-jamming-rockblock-pro-stl

Inside GNSS. (March 26, 2024). *GNSS Spoofing and Jamming in Eastern Europe*. Inside GNSS. https://insidegnss.com/gnss-spoofing-and-jamming-in-eastern-europe/

Manfredini, G.E. (2017) *Signal processing techniques for GNSS anti-spoofing algorithms* [Unpublished Doctoral Thesis], Polytechnic University of Turin.

Maritime Executive. (2024, August 22). *Ukraine destroys Russian spoofing platform used to disrupt grain shipping*. https://www.maritime-executive.com/article/ukraine-destroys-russian-spoofing-platform-off-crimea

NATO. (2004). *Basic guide to advanced navigation.* NATO RTO Publication. SET-054/RTG-30.

NATO Shipping Centre. (n.d.). *NATO Shipping Centre (NSC)*. NATO. Retrieved June 6, 2025, from https://shipping.nato.int/nsc

TheSun. (January 17, 2025). *RYAN-SCARE Ryanair jet from UK forced to ABORT landing at last min over mysterious GPS 'jamming' near Nato border with Russia.* https://www.thesun.co.uk/news/32862574/ryanair-jet-abort-landing-mysterious-gps-jamming-near-russia

Son, P. W., Park, S. G., Han, Y., Seo, K., & Fang, T. H. (2023). Demonstration of the feasibility of the Korean eLoran system as a resilient PNT in a testbed. *Remote Sensing*, *15*(14). 3586. https://doi.org/10.3390/rs15143586

Wikipedia contributors. (n.d.). *Azerbaijan Airlines Flight 8243*. Wikipedia. Retrieved June 6, 2025 from https://en.wikipedia.org/wiki/Azerbaijan_Airlines_Flight_8243

Wikipedia contributors. (n.d.). *Global Navigation Satellite System interference during the Russian-Ukrainian conflict*. Wikipedia. Retrieved June 6, 2025 from https://en.wikipedia.org/wiki/Global_Positioning_System_interference_during_the_Russian_invasion_of_Ukraine

Wikipedia contributors. (n.d.). *Electronic warfare in the Russian invasion of Ukraine*. Wikipedia. Retrieved June 6, 2025, from https://en.wikipedia.org/wiki/Electronic_warfare_in_the_Russian_invasion_of_Ukraine.

Wikipedia contributors. (n.d.). *Loran-C*. Wikipedia. Retrieved June 9, 2025, from https://en.wikipedia.org/wiki/Loran-C.

About the Author

Dr. Dünya Rauf Levent GÜNER / Integrated Naval Warfare Systems SE Dept. / Aselsan, TÜRKIYE / lguner[at]aselsan.com / ORCID: 0000-0002-0743-6902

Dr. Dünya Rauf Levent GÜNER graduated from Middle East Technical University Aerospace Engineering Department in 2000, received his master's degree on laser guided bombs, and Ph.D. on improvement of inertial navigation systems' performance in GNSS denied environments from Mechanical Engineering Department of METU. He has worked as a systems engineer at Aselsan for 25 years and has 15 years of experience in design and integration of inertial navigation systems onboard land/air and naval systems, 10 years of experience in design of unmanned air and naval systems. He participated in several projects like designing of artillery surveying systems, integration of navigation systems to multiple artillery systems, integration of indigenous inertial navigation systems to naval vessels of Turkish Navy, shipborne operations with UAV's and, design of UAV's and maritime unmanned systems (MUS). His areas of expertise are navigation systems, navigation in GNSS denied environments, unmanned systems concept development and systems engineering.

System Thinking for GPS Spoofing and Jamming Attacks Through Ships

Emre Düzenli
Istanbul Technical University

Gizem Kayişoğlu
Istanbul Technical University

Selen Uygur
Sakarya University of Applied Sciences

Pelin Bolat
Istanbul Technical University

Abstract

Global Navigation Satellite Systems (GNSS), with GPS at the forefront, are central to contemporary maritime navigation and provide precise positioning, route planning, and collision avoidance. But a growing number of GPS spoofing and jamming attacks represent a considerable menace to ships' operational safety and cybersecurity. This study employs a systems thinking approach to create and analyze the intricate interconnections among technical vulnerabilities, human factors, organizational responses, and external threat vectors relating to GNSS disruptions in the maritime sector. Systems thinking is a cognitive anchor that concentrates on comprehending entire systems and their interactions instead of just examining separate components in isolation. It is extremely useful when dealing with complex dynamic systems. The goal is to create a model that illustrates the system and the dynamics clearly and shows the necessity of understanding the dynamics to fully grasp the implications of GPS spoofing and jamming attacks for the ships. The causal loop model created reveals key feedback mechanisms that reinforce navigational uncertainty, degrade timely decision-making, and heighten the possibility of collision or grounding. Also, the study recognizes principal leverage points, including crew training, hybrid navigation, and incident reporting processes, by which risks can effectively be mitigated and system resilience enhanced. The study demonstrates the pressing requirement for coordinated cyber-physical risk management strategies with maritime security operation center (SOC) analysts for responding to GPS-dependent dangers in maritime operation, especially in congested or geopolitically restricted waters. This research contributes to provide comprehensive framework for GPS spoofing and jamming attacks that enhances our understanding and response to navigation-related cyber threats onboard ships.

Keywords

GPS Spoofing and Jamming, Maritime Cybersecurity Systems, Thinking Approach, Causal Loop Diagrams (CLDs, Navigation Safety at Sea)

Introduction

Modern systems and devices commonly rely on the Global Navigation Satellite Systems (GNSS) for positioning, navigation, and timing (PNT) (Burbank et al., 2024). Supporting accurate and timely navigational decision-making, ship captains utilize the Global Positioning System (GPS), a component of the GNSS. However, systems like GPS are vulnerable to cyber-attacks. Jamming and spoofing cyber-attacks of GPS are critical threats to maritime navigation systems. These types of cyber-attacks can lead to data manipulation and modification, insertion of malicious content and fake data, hijacking, availability disruption, bandwidth usurpation (Androjna & Perkovič, 2021).

Jamming disrupts signal reception by overwhelming GPS frequencies with noise, leading to a complete loss of positioning data. In contrast, spoofing deceives the receiver by broadcasting fake satellite signals, causing it to compute false positions without triggering alarms. While jamming is easier to detect, spoofing is more dangerous due to its ability to mislead vessels without immediate suspicion. Both attacks undermine navigational accuracy, situational awareness, and operational safety at sea (Androjna et al., 2020).

According to Darwish (2017), In 2017, approximately 450 ships locations changed from sea to airports in Sochi, St. Petersburg and Gelendzhik. The reason for this spoofing activity is explained by the experts as a defense tactic to protect the president. Moreover, In 2018, the U.S Maritime Administration reported that GPS distruptions in the Port of Haifa, Port Said, Strait of Hurmus, around the island of Cyprus and coastal side of Syria (U.S. Maritime Administration, 2018). In 2019, the U.S. Maritime Administration warns the vessels which are navigating in the Strait of Hormuz for spoofing and jamming situations. After that, the UK flagged tanker Stena Impero was spoofed in this strait and seized by Iranian forces (Bockmann, 2019). Chinese fishing fleet falsifying their location to make illegal fishing activities near the Galapagos protected waters. GPS spoofing and jamming is used for this type of malicious activities (Aitken, 2020). Recently, GPS jamming to The container ship MSC Antonia lead to grounding in the Red Sea. According to analysis, the ship navigational system data showed spoofed patterns before the incident. Inconsistent training of crew for cybersecurity, lack of awareness and preparedness among maritime personnel, unreliable equipments are one of the significant threat for ships (Marine Public, 2025).

In literature, Charitou (2025) talked about some countermeasures against GPS spoofing in the maritime sector. These involve training for maritime personnel to enable them to identify and respond to spoofing signals, the significance of reporting systems for incidents accompanied by awareness and ongoing training programs, and the requirement for robust international policies as well as regulatory measures to facilitate harmonized efforts and prevention strategies globally. Androjna and Perkovič (2021) called for the development of an international security protocol to discourage GPS jamming and spoofing. They identified the lack of encryption in data communication and the absence of authentication schemes as significant vulnerabilities.

The authors further demanded that manufacturers of devices must improve their cybersecurity features to be able to combat the threats effectively. Intertanko (2019) suggested that any GPS spoofing or jamming incidents must be reported immediately to the respective authorities in order to facilitate maritime situational awareness and synchronised response operations. Besides, a number of studies have suggested techniques for spoofing detection and countering with a view to improving the resilience of maritime navigation systems from these types of cyber attacks (Singh et al., 2022; Spravil et al., 2023).

On the other hand, systems thinking is an approach centered on the comprehension of intricate systems based on the examination of interconnections among their parts, rather than the separate examination of such elements (Flint, 2008). This systems perspective facilitates improved decision-making as well as problem-solving in a variety of areas, ranging from sustainability matters to business intelligence (Pandey & Kumar, 2016; Reyes, 2001). The method emphasizes interdependence between different elements in a system and recognizes that alteration in one section of the system can affect others (Boardman & Sauser, 2013). Systems thinking techniques such as systemigrams and system dynamics possess the potential to improve traditional problem-solving practices through the provision of an improved comprehension of problems (Boardman & Sauser, 2013). It has been utilized to offer solutions to a variety of problems, from child obesity to the development of business intelligence software, offering potential solutions where traditional approaches have failed (Pandey & Kumar, 2016).

The objective of this research that applies a system thinking methodology to investigating GPS spoofing and jamming in maritime environments is to carry out a thorough investigation of complex interactions between technological vulnerabilities, human factors, and organizational routines. The study aims to fully chart principal feedback loops and leverage points that shape the resilience of navigation systems utilized by the merchant ships. The primary goal is to gain a detailed insight into the effects of GPS spoofing and jamming on operational safety, and also to propose harmonized mitigation strategies to assist decision-making, situational awareness, and cyber-physical preparedness in maritime operations.

In the current study, a conceptual dynamic model has been developed to examine the implications of GPS spoofing and jamming on vessels from a system thinking perspective. The primary objective is to develop a deeper insight into how intricate interactions between technological, human, and organizational factors impact the resilience of maritime navigation. The structure of the paper is as follows: Section II presents an abstract; Section III reviews notable cyber attacks that employ GPS spoofing or jamming techniques; Section IV states the research approach, with subsections IV-I: Ship GPS Spoofing, IV-II: GPS Signal, and IV-III: Launching of Spoofing Attacks.

Section V reports the findings, and Section VI presents a critical review of the key findings. Finally, Section VII concludes the study by offering essential insights and real-world recommendations for enhancing cybersecurity protocols in maritime navigation systems.

GPS Spoofing Or Jamming Cyber Incidents

Examples of GPS spoofing or jamming incidents in maritime areas are provided in Table 1 (Charitou, 2025).

Incident	Location	Vessel	Impact	Responsible	Key Details
The White Rose Yacht Spoofing (2013)	Mediterranean Sea (Off Italy)	White Rose of Drachs	Gradual course deviation; crew unaware	University of Texas researchers (test)	Used $3,000 device to hijack navigation of $80M yacht
M/V Manukai Incident (2019)	Shanghai, China	M/V Manukai	GPS & AIS signal loss; multiple alarms; 300+ ships affected	Unknown	Sudden position jumps; false dockings observed
Shanghai Coastal Spoofing (2020)	Shanghai & Huangpu River, China	Multiple vessels	Massive navigation disruptions; spoofed GPS signals	Unknown (poss. smugglers or gov. tests)	Persistent spoofing affecting hundreds of ships
Eastern Med & Suez Canal Disruptions	Libya, Malta, Port Said, the island of Cyprus	Multiple vessels	GPS interference affecting critical shipping lanes	Unknown	Reported by US MARAD; commercial and security risks
Strait of Hormuz Spoofing	Strait of Hormuz	Multiple vessels incl. Stena Impero	Navigation issues; geopolitical tensions	Suspected state actors	Linked to ship seizures and drone incidents
GNSS Spoofing in Russia	Russia, Crimea, Syria	Multiple vessels	Strategic GPS disruptions	Russian Federation (C4ADS report)	Tactical use to mislead ships near sensitive areas
Black Sea Incident (2017)	Black Sea	20+ vessels	Fake GPS positions shown	Unknown	Confirmed by US NAVCEN
Hydrographers Passage Near Grounding (2022)	Australia	Unnamed Bulk Carrier	ECDIS showed false position; near grounding avoided	Unknown (spoofing not proven)	ATSB report noted GPS anomalies

Materials and Methods

Systems thinking serves as a theoretical foundation that emphasizes understanding entire systems and their interconnections, rather than examining components in isolation, making it particularly effective for analyzing complex and dynamic systems (Ramage & Shipp, 2009). In this study, systems thinking is operationalized through system dynamics, specifically using Causal Loop Diagrams (CLDs) as the primary methodological tool. CLDs offer a qualitative representation of cause-and-effect relationships within the system and help identify feedback mechanisms—reinforcing loops that intensify system behavior and balancing loops that stabilize it (Sterman, 2000).

These loops illustrate how changes in one variable influence others and eventually loop back to affect the original variable (Sterman, 2000). The study applies CLDs to map interactions among key variables and stakeholders, aiming to uncover how localized changes can produce broader systemic effects. To support model development, qualitative data were collected through a workshop involving four system dynamics experts with international experience, three of whom specialize in maritime cybersecurity, and three who hold expertise in maritime transportation management engineering. Fig. 1 shows the methodology process of this study.

Furthermore, quality of the research process is explained by Sterman (2000) highlights that several essential criteria that must be adequately addressed to build confidence in a system dynamics model. First, the purpose and boundaries of the model must be clearly defined. In this study, the model's purpose was determined during the initial problem formulation stage, informed by a literature review and internal discussions among the authors. The model boundaries were refined through variable elicitation exercises conducted during a workshop. Second, the model structure must reflect real-world decision-making processes. To ensure this, the structure was grounded in empirical data drawn from academic sources, expert consultations, and the practical experience of the research team. This was achieved through the workshop, and the review of relevant literature. Third, the study prioritizes comprehensive documentation and methodological transparency to support future replication and validation. While the reproducibility of the model may vary due to the evolving nature of GPS spoofing and jamming threats through ships, this research contributes a foundational framework for future system-based investigations into cyber-physical vulnerabilities in maritime navigation.

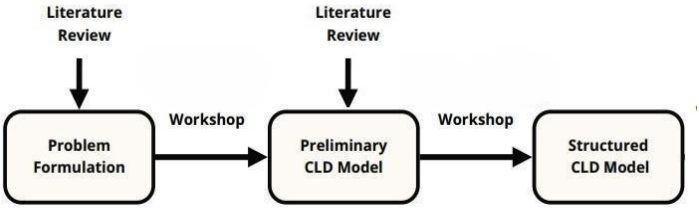

Figure 1
The process of methodology

Ship GPS Spoofing

Charitou (2025) refers to GPS spoofing, or GPS signal spoofing, or GNSS (Global Navigation Satellite System) spoofing, as a technique used by attackers to modify or generate counterfeit GPS signals, thus deceiving GPS receivers, including those used on maritime vehicles such as ships and boats. The impact of this practice can be considerable, impacting navigation, security, and safety at sea. Ship-specific GPS spoofing is the broadcasting of counterfeit GPS signals intended to deceive a ship's GPS receiver.

The false signals can cause the receiver to misinterpret its location, velocity, or direction. To counter the threats posed by GPS spoofing in the maritime sector, some countermeasures can be implemented.

Blocking	Blocking is the process of inhibiting the passage of the satellite signal to the receiver's antenna. Blocking may be physical in nature, like damage to or destruction of the antenna. The effect of blocking is GPS signal interference, making it impossible for the receiver to accurately fix its location.
Jamming	Jamming involves overwhelming a GPS receiver with interference or spurious signals, thereby degrading its capability to successfully identify valid GPS signals. This type of attack is usually referred to as a denial of service (DoS) attack. Jamming disrupts the receiver's potential to acquire and demodulate genuine satellite signals, ultimately resulting in GPS failure.
Spoofing	Spoofing, which is the centerpiece of this discussion, involves an attacker replacing the genuine satellite signal with a fabricated one. Unlike the blocking and jamming techniques, spoofing is a covert attack whereby the GPS receiver is deceived into calculating an incorrect position using the fake signal. This is a more sophisticated and subtle approach than the more brazen blocking and jamming techniques.

Table 2

Three primary methods to compromise a GPS receiver

GPS Signal

Each GPS satellite transmits two distinct signals: one for military and a second for civilian use. Most of the GPS users, including most DoD users, have access only to the civilian code GPS signal. Commercial ships at sea also use the civilian code, which consists of two significant data signals along with a carrier wave, as illustrated in Figure 2.

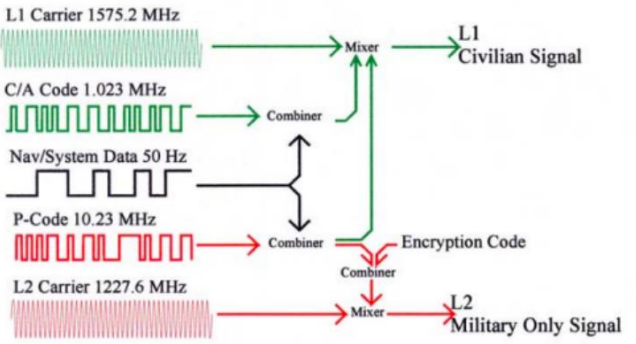

Figure 2
GPS Signal Waves

The navigation system data gives the GPS receiver essential information concerning the positional information of the satellites and accurate temporal information derived from the atomic clocks onboard the satellites. Each satellite possesses an individual identification code, the CIA code, which is repeated every millionth of a second. The navigation system data is merged with the CIA code, then modulated on the carrier wave.

The GPS receiver establishes contact with the signals transmitted by several GPS satellites concurrently. To keep things simple, we will consider the process of establishing contact with one satellite. The receiver is pre-programmed with a CIA identification string of each satellite.

The unit is constantly searching for GPS signals being transmitted from space, and once it detects a satellite signal, it utilizes the CIA code to identify the individual satellite. The receiver then creates an internal CIA code synchronized with the satellite's code. The internally generated code is correlated with the periodic CIA code from the satellite, which enables the receiver to calculate the signal travel time (ΔT), as indicated in Fig 3.

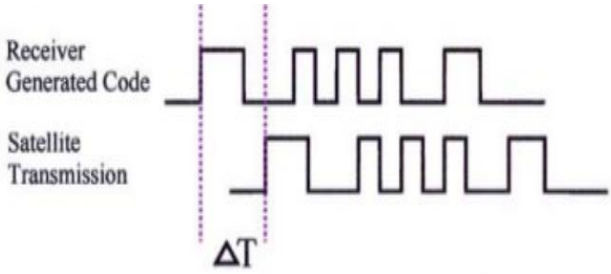

Figure 3
GPS Signal Time Delay

Once the travel time (ΔT) is determined, the receiver computes its distance from the satellite by the formula: Distance = ΔT x Speed of Light. Getting the distance to one satellite, however, is insufficient for precise location. Even when the precise position of the satellite is known, all that can be concluded is that the receiver is somewhere in a calculated distance from the satellite. Precise location needs the receiver to calculate distances to several satellites at once, usually four. As indicated in Figure 3, the range from various satellites measured by the GPS receiver does not, most of the time, intersect in one point. This is because of timing inaccuracies in the GPS receiver, which is less precise than the atomic clocks in the satellites. The area where the two incorrect ranges intersect gives the approximate location of the receiver.

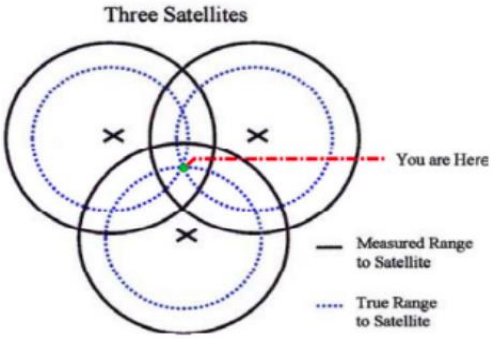

Figure 4
Representation of Finding Position

As illustrated in Figure 4, the GPS receiver then interpolates this overlap area to find the centre, providing two pieces of very important information: the receiver position and the clock error. The more satellites that are involved in this process, the smaller the area of overlap, and hence the better the position fix. The position is first given in an X, Y, Z Earth-centered/Earth-fixed coordinate system, and then converted to latitude, longitude, and altitude coordinates.

If the actions above are duly executed, this implies that the attacker can manipulate the real cross-track and along-track coordinates of the ship by presenting false positions to the ship's autopilot system or to the bridge crew, which are incorrectly calculated from the true position of the vessel, thereby successfully achieving his intention of attack.

Executing Spoofing Attacks

Spoofing Device: Another crucial element in a GPS spoofing attack is the spoofing device, which will have the capability to generate fake GPS signals, i.e., an antenna. The device is required for feeding fake positional information to the navigation systems of the targeted vessel. The spoofing device must have the capacity to create and transmit fake signals (Figure 5). Such capacity may also be complemented by software and applications with the capacity to generate fake signals.

Signal Source: In order to create spoofed GPS signals, the spoofer needs to have a decent signal source. This can be done either by manipulating real GPS signals or creating entirely spurious signals from scratch using some special equipment or computer programs. Thus, a mobile platform is required from which the spoofing device has to function. This recognizes that the closer the attacker is to the target, the higher the level of control he has over the attack. In addition, a system with the capability of signal transmission is required to overpower the genuine satellite signals received by the ships.

Knowledge and Skills: Conducting an effective GPS spoofing attack requires a good understanding of the GPS technology, signal modulation, and navigation systems. The attacker must possess the knowledge and skills required to effectively manipulate GPS signals without detection. An understanding of GPS signal manipulation is necessary, along with an understanding of the operational practices of vessels. Understanding ship operations, such as those conducted in port facilities, can make a difference in the success or failure of the attack.

Acquiring Access to the Target Ship's Navigation Systems: The attacker must gain access to the navigation systems of the target ship to be able to inject spoofed signals. This may involve physical proximity to the ship's GPS receiver or utilizing vulnerabilities in its communications protocols to inject spoofed signals remotely. A ship's navigation systems can be directly accessed, yet indirectly through the information available regarding the ship's navigation configuration and setup, such as the presence of GPS antennas, electronic charts, ECDIS, autopilot systems, and sensors on the ship.

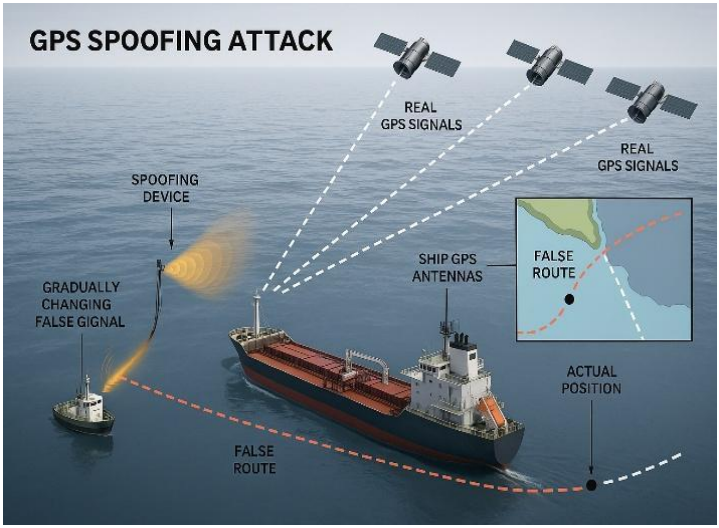

Figure 5
GPS Spoofing Attack

Results

The overarching model introduced here depicts the interactions between key maritime stakeholders in the event of GPS spoofing or jamming (refer to Figure 6). By outlining the roles and reactions of different entities within key domains, ranging from ship-level systems and human operators to shipping companies and regulatory or international bodies, the framework highlights that GPS spoofing and jamming in navigation systems create ripple effects that require coordinated reactions from various stakeholders.

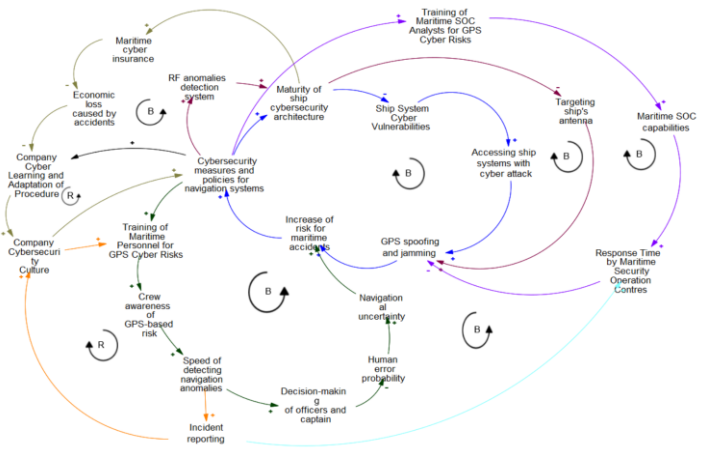

Figure 6
Overall Dynamics of GPS Spoofing and Jamming Attacks through Ships

In Figure 7, the first loop indicates a feedback process that stabilizes operation so that the development of a vessel's cybersecurity framework is of key importance in averting cyber threats and, especially, those arising from GPS spoofing and jamming. In this loop, growth in the cyber weaknesses of ship systems brings about heightened risk of breaching into these systems through cyberattacks. This kind of access enables attackers to interfere with GPS signals, leading to spoofing and jamming attacks that undermine navigation accuracy and heighten the risk of maritime accidents considerably.

With the risk of accidents looming, stakeholders in maritime are forced to introduce or enhance cybersecurity controls and policies for navigational systems. These controls—like anomaly detection, network segmentation, authentication protocols, and frequent patching—are essential in enhancing the overall maturity of the cybersecurity program of the ship. By extension, a mature cybersecurity solution serves to reduce existing vulnerabilities, thereby closing the loop by reducing future opportunities for successful cyber attacks associated with GPS technology.

This circular process underscores the merit of adopting a forward-looking and adaptive cybersecurity solution on vessels. Additionally, it calls for taking cybersecurity policies and translating them into concrete technical deployments that strengthen system robustness, in accordance with guidelines like IACS UR E26/E27.

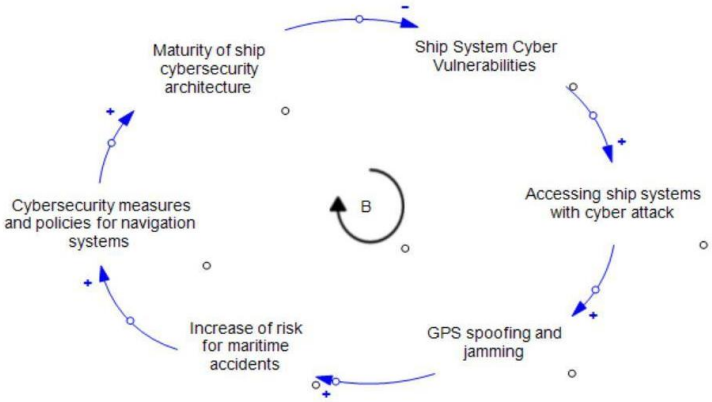

Figure 7
Loop1 – Core Cybersecurity Architecture Loop

In Figure 8, the cycle emphasizes antenna-targeted GPS spoofing attacks and the protective function of architectural maturity and technological detection systems. As ship systems are attacked via radio frequency (RF) manipulation, GPS spoofing and jamming become increasingly probable, with greater navigational uncertainty and accident vulnerability. In turn, ships implement stronger cybersecurity protections for navigation systems, such as the use of RF anomaly detection systems. These systems encourage early identification of hostile intrusions, thereby facilitating a general decrease in the effectiveness of spoofing attacks. The integration of these sophisticated detection technologies also increases the ship's cybersecurity system's level of sophistication. With an increase in the robustness of the system, there is a considerable reduction in the vulnerability of the ship's antenna and navigation systems, thereby creating a balance in the system. This trade-off highlights the paramount importance of the integration of detection technologies into maritime systems as a vital component in countering cyber threats related to GPS.

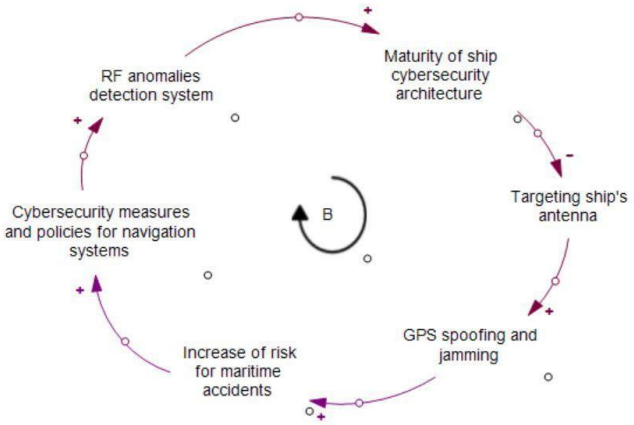

Figure 8
Loop2- Antenna-Based Attack Mitigation Loop

Loop 3, as illustrated in Figure 9, is a case of a balancing loop reflecting the impact of Maritime Security Operation Centers (MSOCs) on reducing incidences of GPS spoofing through facilitating organizational flexibility. Heightened risk of GPS spoofing and jamming has a causal relationship with the risk of maritime accidents. Maritime authorities strengthen the capacity of MSOCs, particularly by providing specialized training to analysts on GPS-based cyber threats. Enhanced SOC capabilities enhance the response time to navigation anomalies and cyberattacks, minimizing the operational effects of spoofing attacks. Minimization of attack effects further results in fewer accidents, which in itself makes investment in cybersecurity policy and training sustainable and justified. This cycle illustrates the intrinsic value of organizational preparedness and response timing to incidents in ensuring navigation security in an evolving cyber threat situation.

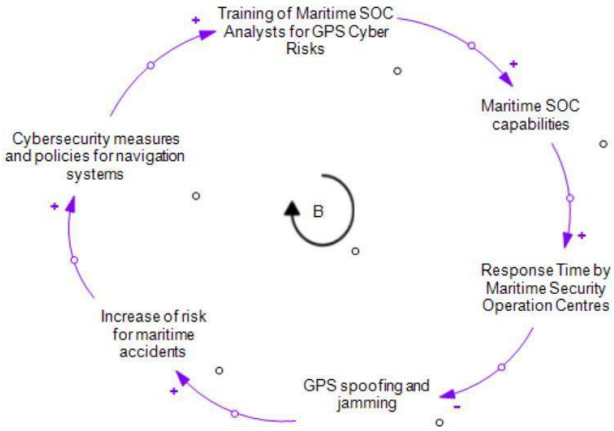

Figure 9
Loop3- Maritime Security Operation Centre (MSOC) Capability Loop

In Figure 10, the loop indicates a balanced relationship founded on economic incentives. The uptake of maritime cyber insurance has a strong motivation for shipowners to invest in good cybersecurity practice. As the financial consequences of incidents increase, the more the insurance firms insist on tighter adherence to cybersecurity controls, thus motivating ship operators to enhance cybersecurity practice for navigation systems.

These enhanced controls offset ship system weaknesses and improve cybersecurity architecture maturity, ultimately reducing the occurrence and severity of future attacks. This in turn reduces economic loss and closes the loop. The loop illustrates how external economic drivers—most notably cyber insurance policies—can solidify risk-awareness behavior and develop cybersecurity resilience across the maritime industry.

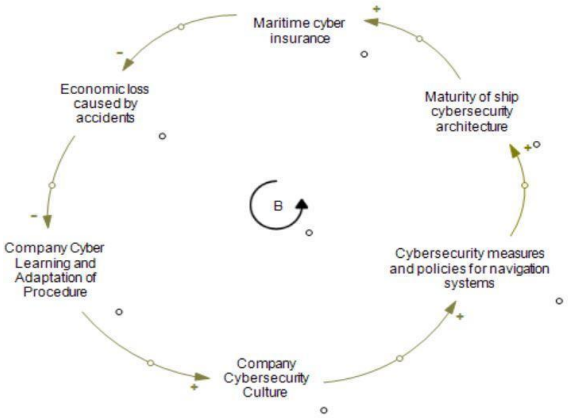

Figure 10
Loop4- Maritime Cyber Insurance Incentivization Loop

Figure 11 shows the manner in which internal learning processes strengthen an organization's preparedness to respond to cyber attacks through a reinforcing loop. If organizations face cyber events or near misses, they revise operating procedures along with learning lessons from them. Such adaptations guarantee the development of a strong culture of cybersecurity within the company, resulting in the long-term implementation of policies and practices for protecting navigation systems. As these practices evolve, the organization improves its ability to foresee and fend off likely cyber attacks. This is an instance of a relationship whereby cybersecurity culture and procedural knowledge development complement and result in sustained enhancement and resilience that persists long-term irrespective of GPS-type attacks.

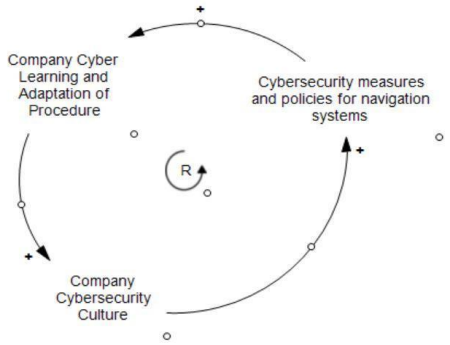

Figure 11
Loop5- Organizational Learning and Procedure Adaptation Loop

The reinforcing loop in Figure 12 indicates how cyber resilience can be increased by training in reporting behavior and increased awareness. Training programs aimed at GPS-related cyber threats increase the awareness of the crew regarding spoofing vulnerabilities and navigation anomalies. This heightened awareness enables the crew to identify anomalies more efficiently, thereby increasing the frequency of incident reporting. Improved reporting mechanisms enable a faster response, which in itself generates an improved cybersecurity culture in the organization. Conversely, a robust cybersecurity culture demands and assists in maintaining frequent training exercises, thereby establishing a positive feedback mechanism that promotes situational awareness and proactive countermeasures for cyber threats.

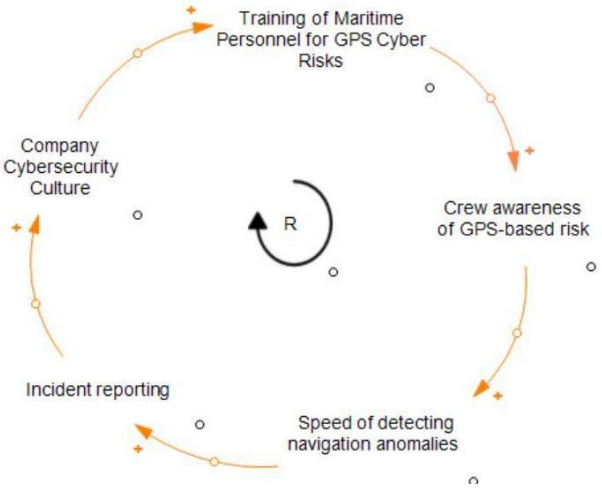

Figure 12
Loop6- Crew Awareness and Cyber Incident Reporting Loop

Figure 13 emphasizes navigation safety from a cognitive perspective, bringing to the forefront the significance of cyber attacks on human decision-making. The GPS spoofing and jamming incidents heighten navigation uncertainty, subsequently elevating the possibility of human error among officers and captains. Real-time anomaly detection and enhanced situational awareness, on the other hand, minimize uncertainty, thus guaranteeing well-informed and confident decision-making. The improvement in decision-making abilities minimizes the risk of maritime accidents, thereby encouraging ongoing investment in personnel training and cybersecurity. This is a circular impact that requires a fine balance in which human factors are integrated smoothly with technological and policy-based defense mechanisms to mitigate cyber-physical risks.

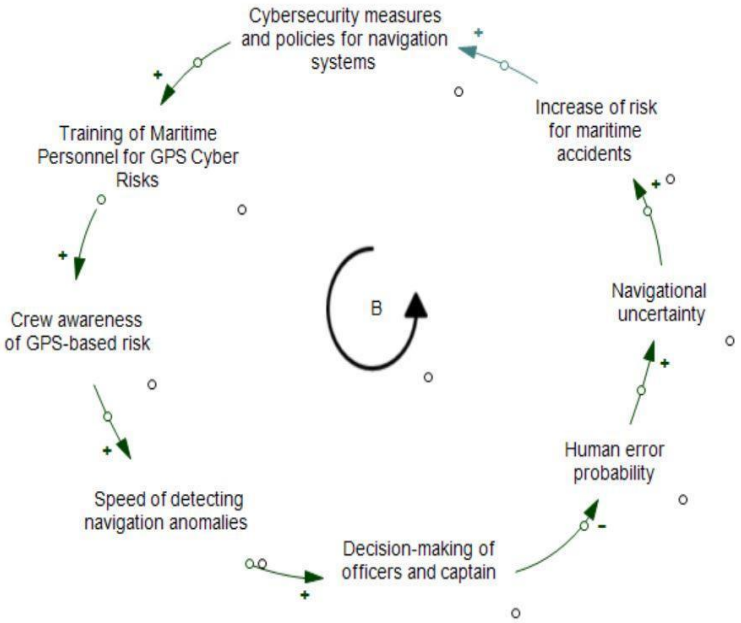

Figure 13
Loop7- Human Error and Navigational Decision-Making Loop

The last loop in Figure 14, it is the balancing loop that extends operational-level detection to organizational-level response. With increased crew awareness brought by training, so also is the likelihood and promptness of incident reporting of navigation anomalies. Prompt reporting enhances the response time of MSOCs, which are tasked to decrease the effect of spoofing and jamming. A response that is timely reduces the impact of cyber attacks, and hence a reduction in adverse events and less systemic vulnerability are observed. Better safety results further stress the role of reporting and training and thereby serve to stabilize the system. This feedback mechanism mandates the requirement of synchronized communication between the crew onboard and the cybersecurity team based on shore.

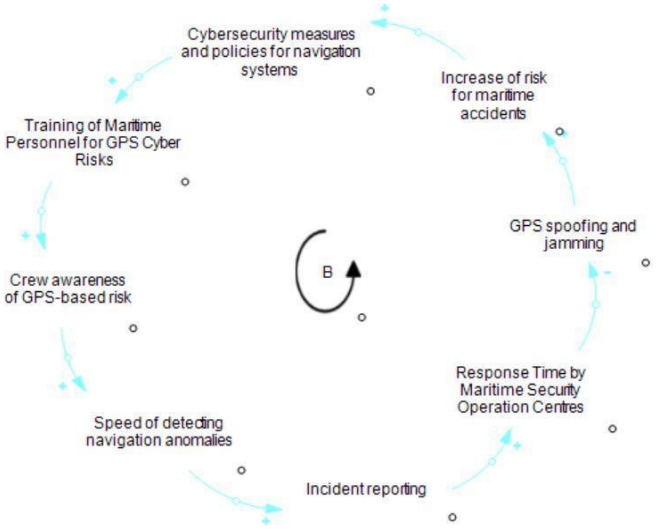

Figure 14
Loop8- Integrated SOC Response and Crew Reporting Loop

Discussion

The detailed causal loop diagram offers a bird's-eye perspective of the complex interaction among human, organizational, and technological factors in mitigating the risks of GPS jamming and spoofing in maritime systems. There are a number of balancing and reinforcing feedback loops that collectively convey the dynamic structure necessary to realize cyber resilience in maritime operations. At its core is ship cybersecurity architecture maturity that serves as both a product and a driver of efficient cybersecurity measures and regulation policies.Technical capabilities like RF anomaly detection systems, operational readiness of MSOCs, and ship-level detection systems help decrease system vulnerabilities and prevent or deter successful cyber intrusions. At the same time, feedback mechanisms of cyber culture and organizational learning mechanisms demonstrate that procedural and human factors, including crew situational awareness, incident reporting, and ongoing training, are able to enhance systemic resilience through guaranteeing preventive measures and internal adaptations.

Economic controls, specifically maritime cyber insurance under the current system offer extrinsic incentives for increasing maturity and compliance. Financial incentives enable the financing of cyber incidents by encouraging investments that reduce risk. Second, the symbiosis of human behavior and decision-making in situations of navigational uncertainty demonstrates the incorporation of behavior risk models in technical risk assessment methods.

The model shows how an effective and responsive maritime system capable of monitoring cyber threats is created by bridging feedback between people, technical systems, and the manner in which institutions respond. In short, this complex model provides an integrated view and emphasizes the imperative need to coordinate technology, train people, adhere to regulations, and learn in organizations in order to effectively deal with the complex threats posed by GPS spoofing and jamming to maritime operations.

Based on the integrated model, some strategic recommendations are proposed to enhance maritime cybersecurity. Firstly, it is necessary to build an integrated ship-shore cybersecurity system; this is done by incorporating onboard anomaly detection systems into MSOC operations in a manner that will enable real-time threat detection and concerted action. Second, it is essential that ongoing training is made compulsory for the crew members and SOC analysts to develop a solid knowledge base of GPS-related threats, reinforced with frequent assessments. Third, there needs to be the growth of a cybersecurity culture across all organizational levels—this includes promoting incident reporting and feedback mechanisms in line with adaptive learning processes. Fourth, cyber maturity needs to be fostered within regulatory and insurance regimes through the alignment of underwriting practices to IACS E26/E27 standards and IMO cybersecurity guidelines. Fifth, navigational uncertainty needs to be formally modeled and monitored, with GPS spoofing threats included in bridge simulator training and voyage planning decision support tools.

Conclusion

This study presented a system-based examination of GPS spoofing and jamming attacks on maritime navigation systems by developing a set of causal loop diagrams that collectively represent the socio-technical dynamics of ship cybersecurity. By deconstructing the GPS-based cyber threat landscape into networked balancing and reinforcing feedback loops, the study reveals how shipboard technical vulnerabilities, crew training, organizational culture, maritime security operation capability, and economic incentives such as cyber insurance influence one another to impact the threat of cyber-induced maritime accidents.

The analysis shows that the level of ship cybersecurity architecture acts as a critical component within the system and directly influences vulnerability exposure, as well as acting as a stabilizing force against escalating threats. Furthermore, the effectiveness of cybersecurity measures is enhanced by organizational learning, policy changes, and the deployment of resources towards technological tools such as RF anomaly detection systems. In particular, human factors like crew awareness, reporting behavior in case of incidents, and decision-making in navigation under uncertainty are shown to be significant determinants of system resilience. They must not be treated as residual threats but as inherent components of cyber defense strategy. Furthermore, the study underscores cross-level integration: shore-based MSOC response capacity must be aligned with onboard detection and reporting mechanisms to reduce response lag and damage potential. Finally, cyber insurance programs provide a systemic incentive for continuous improvement of cyber hygiene and adherence to regulation.

Lastly, this research demands an integrated model of cyber risk governance of maritime operations incorporating technical defenses, crew competence, organizational flexibility, and regulatory controls. The integrated system model formulated in this research offers a strategic framework for comprehending and thwarting the sophisticated, interconnected risks of GPS spoofing and jamming attacks on ships. Quantitative system dynamics modeling may be added to this framework in future research to experiment with possible interventions.

References

Aitken, P. (2020, August 16). Chinese fleet fishing near Galapagos protected waters, allegedly falsifying GPS location - Fox News - RNTF. RNTFND. https://rntfnd.org/2020/08/16/chinese-fleet-fishing-near-galapagos-protected-waters-allegedly-falsifying-gps-location-fox-news/

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering, 8(10), 776. https://doi.org/10.3390/jmse8100776

Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. Transactions on Maritime Science, 10(2), 361–373. https://doi.org/10.7225/toms.v10.n02.w08

Boardman, J., & Sauser, B. (2013). Systemic thinking: Building Maps for Worlds of Systems. John Wiley & Sons.

Bockmann, M. (2019, August 16). Seized UK tanker likely 'spoofed' by Iran. Lloyd's List. https://www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

Burbank, J., Greene, T., & Kaabouch, N. (2024). Detecting and mitigating attacks on GPS devices. Sensors, 24(17), 5529. https://doi.org/10.3390/s24175529

Charitou, N. (2025). Understanding and mitigating GPS spoofing attacks in shipping [Master Thesis, University of Piraeus]. https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/17419/Charitou_mpked2246.pdf?sequence=5&isAllowed=y

Darwish, M. (2017, November 3). Did Russia make this ship disappear? CNNBUSINESS. https://money.cnn.com/2017/11/03/technology/gps-spoofing-russia/index.html

Flint, S. (2008). Rethinking systems thinking. In Proceedings of the 14th ANZSYS Australia New Zealand Systems Society Conference (1st ed., Vol. 1). Edith Cowan University. https://researchportalplus.anu.edu.au/en/publications/rethinking-systems-thinking

INTERTANKO. (2019). Jamming and spoofing of Global Navigation Satellite Systems (GNSS). https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

Marine Public. (2025, May). Maritime GPS spoofing: MSC Antonia grounding & cyber threats. https://www.marinepublic.com/blogs/distress/952883-maritime-gps-spoofing-msc-antonia-grounding-cyber-threats

Pandey, A., & Kumar, A. (2016). System thinking approach to deal with sustainability challenges. In Proceedings of International Conference on Science, Technology, Humanities and Business Management. https://socrd.org/wp-content/uploads/2016/08/17BKK125-System-Thinking-Approach-to-Deal-with-Sustainability-Challenges.pdf

Ramage, M., & Shipp, K. (2020). Systems thinkers. Springer eBooks. https://doi.org/10.1007/978-1-4471-7475-2

Reyes, E. P. (2001). A systems thinking approach to business intelligence solutions based on cloud computing [Master Thesis, Massachusetts Institute of Technology]. https://dspace.mit.edu/handle/1721.1/59267

Singh, S., Singh, J., Singh, S., Goyal, S. B., Raboaca, M. S., Verma, C., & Suciu, G. (2022). Detection and mitigation of GNSS spoofing attacks in maritime environments using a genetic algorithm. Mathematics, 10(21), 4097. https://doi.org/10.3390/math10214097

Spravil, J., Hemminghaus, C., Von Rechenberg, M., Padilla, E., & Bauer, J. (2023). Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. Journal of Marine Science and Engineering, 11(5), 928. https://doi.org/10.3390/jmse11050928

Sterman, J. D. (2000). Business Dynamics: systems thinking and modeling for a complex world. http://gsme.sharif.edu/~sd/files/Resources/Old%20Resources/business%20dynamics%20chapter%203%20(6%20slides%20per%20page).pdf

U.S. Maritime Administration. (2018, November 1). 2018-014-Eastern Mediterranean Sea-GPS Interference. https://www.maritime.dot.gov/msci/2018-014-eastern-mediterranean-sea-gps-interference

About the Authors

Emre Düzenli / Istanbul Technical University, İstanbul, Türkiye / duzenli[at]itu.edu.tr / ORCID: 0009-0009-5179-1627

Emre Düzenli is a research assistant at Istanbul Technical University, Maritime Faculty. He is also a researcher at the Maritime Security and Cyber Threats Research Laboratory (CyberMarSec Lab). His research interests focus on maritime security and cybersecurity.

Dr. Gizem Kayisoglu / Istanbul Technical University, İstanbul, Türkiye / yukselg[at]itu.edu.tr / ORCID: 0000-0003-2730-9780

Dr. Gizem Kayisoglu is an Assistant Professor at Istanbul Technical University, Maritime Faculty. She serves as the Vice Head of the Department of Maritime Transportation Management Engineering. She is also a researcher at the CyberMarSec Lab. Her research focuses on maritime security and cybersecurity.

Selen Uygur / Sakarya University, Sakarya, Türkiye / selenuygur[at]subu.edu.tr / ORCID: 0000-0001-5945-8946

Dr. Selen Uygur is a lecturer at Sakarya University of Applied Sciences. She previously worked as an oceangoing watchkeeping officer. Her research focuses on decarbonization and modeling. She is also a researcher at the CyberMarSec Lab.

Pelin Bolat / Istanbul Technical University, İstanbul, Türkiye / yilmazp[at]itu.edu.tr / ORCID: 0000-0003-4262-3612

Dr. Pelin Bolat is the Research Coordinator at Istanbul Technical University, Maritime Faculty, and the Director of the CyberMarSec Lab. Her research focuses on maritime decarbonization, maritime security, nuclear energy, cybersecurity, and system modeling.

PART IV

Report by the Moderator on the Third Session: Leveraging Space-based and Underwater Technologies

Prof. James Kraska
Stockton Center for International Law
United States Naval War College

Abstract

Advancements in undersea, seabed, and outer space technologies are poised to revolutionize naval warfare, extending armed conflict at sea beyond traditional surface domains into multi-domain, integrated operations. Undersea innovations, such as autonomous unmanned underwater vehicles (UUVs), advanced sonar systems, enhance stealthy surveillance, mine countermeasures, and anti-submarine warfare. States will develop a persistent presence in contested waters. Seabed technologies, including fixed sensor networks, secure critical infrastructure like undersea cables while facilitating hybrid threats through concealed deployments. Outer space assets, from satellite constellations for real-time ISR (intelligence, surveillance, reconnaissance) to hypersonic weapons and anti-satellite capabilities, provide global command-and-control, disrupting adversaries' navigation and communications. Together, these technologies promote asymmetric strategies, cyber-physical integration, and domain dominance. New operational doctrine, reconsideration of international norms, and resilient alliances can mitigate horizontal and vertical escalation risks.

Keywords

Submarines, Undersea Warfare, SOSUS, Outer Space; Seabed Warfare; Outer Space Warfare; Satellites; Anti-Satellite; Autonomous Underwater Vehicle

Introduction

The panel "Leveraging Space-based and Underwater Technologies" brought together leading experts to discuss the increasing threats to maritime critical infrastructure (MCI) amid geopolitical tensions and technological advances. In a world where 97% of global communications travel through undersea cables and energy pipelines are vital for economic stability, hybrid attacks —ranging from physical sabotage to cyber intrusions —present threats to national security. The presentations examined how space-based assets, like satellites for real-time surveillance, and underwater technologies, including autonomous vehicles and acoustic sensors, can work together to improve detection, deterrence, and resilience. Drawing insights from NATO, regional analyses, and case studies on countries such as Russia and China, the panel highlighted the importance of civil-military cooperation, legal considerations, and offensive capabilities. Major themes included plausible deniability in gray-zone warfare, the essential role of subsea networks over satellites for high-volume data transfer, and the need for multi-domain operations combining space imagery with seabed robotics. By pointing out vulnerabilities in critical regions like the Baltic and Black Seas, the discussions emphasized collaborative strategies to counter asymmetric threats, promoting a proactive defense approach that uses AI-based analytics and international coordination to protect MCI.

Presentations

CDR Stanislas Frenzel, MARCOM's legal advisor, provided a detailed overview of NATO's strategy for protecting undersea infrastructure. He highlights its crucial economic and strategic importance in the contemporary world. Undersea cables transfer $10 trillion in daily financial transactions and seabed pipelines carry 70% of oil products. Frenzel outlined threats like sabotage from anchor dragging or explosives, including the 2022 Nord Stream blasts and 2023 Balticconnector damage. He criticized the limitations of international law, including UNCLOS Article 113, which lacks a provision of universal jurisdiction, and called for national legislation and new enforcement zones. MARCOM's role through the NATO Maritime Centre for the Security of Critical Undersea Infrastructure (NMCSCUI) combines data from seabed sensors and satellites to detect anomalies and issue real-time alerts. Technological advances like the Mainsail platform allow AI-powered pattern-of-life analysis at sea. Operations like Baltic Sentry 25 coordinated patrols and intelligence sharing may prevent plausible deniability. In relation to the panel theme, Frenzel emphasized using space radar for broad-area monitoring and underwater AUVs for close inspections, promoting deterrence through increased presence and private sector cooperation. His presentation called for updated legal frameworks to authorize boarding in EEZs and highlighted the importance of space-underwater cooperation in strengthening resilience against hybrid threats.

In their joint contribution, Can Ögütcü and Dr. Sijbren de Jong from NATO SHAPE examined Russia's strategic use of energy infrastructure as a hybrid warfare tool in the Black and Caspian Sea. They traced vulnerabilities from the Nord Stream sabotage to attacks on Ukraine's electrical grids, noting Russia's exploitation of "frozen conflicts" for plausible deniability and dominance. With Norway's 9,000 km pipelines vital for Europe's supply, the authors highlighted threats like cyber probes on Baltic states and PKK, and its extensions, affiliates or inspired groups or networks, disruptions to pipelines, causing multimillion-dollar losses. As Europe transitions away from Russian imports, the scholars advocate resilience through interconnections, diversified suppliers, and protection of emerging assets like hydrogen storage. The presentation emphasized NATO-EU cooperation for surveillance, integrating space-based imagery for threat tracking with underwater drones for infrastructure inspections. Key insights included the low-cost, high-impact nature of attacks and the need to prepare for electrified militaries reliant on undersea power cables. Ögütcü and de Jong warned of Russia's "controlled instability" strategy, undermining diversification through military presence in Crimea and exercises. Tying into the panel, they proposed space-underwater tech hybrids. These may be satellite-guided AUVs or other systems that monitor transit routes and counter geo-economic pressures.

Diren Doğan's presentation examined China's civil-military fusion (MCF) as a mechanism for transforming MCI into geopolitical leverage. Moscow has institutionalized this approach since 2016. Under the 2021 Critical Information Infrastructure Regulation, these efforts are expanding. In defining MCI as dual-use ports and surveillance networks like the "Great Underwater Wall," Doğan illustrated how MCF coordinates the PLA, Coast Guard, and state firms (e.g., COSCO, Huawei Marine) to integrate AI, satellites, and subsea sensors for power projection. Case studies of Sansha City and Fiery Cross Reef as dual-use platforms, along with Gwadar and Hambantota ports, demonstrated the importance of maritime infrastructure in naval logistics and gray-zone operations. Redundancy of logistics can help forces prevail in crises. Doğan critiqued limitations, including legal ambiguities under UNCLOS, cybersecurity vulnerabilities, and regional perception gaps fueling Indo-Pacific tensions. He argued MCF challenges the existing norms in contested waters, creating strategic asymmetries between China's centralized control and open systems, such as Western shipping transparency. Linking to the panel theme, Doğan highlighted space-based satellites for maritime extensions of the Belt and Road. The BRI is fused with underwater acoustic arrays for comprehensive surveillance. This fusion enhances intelligence in undersea data flows while undermining global norms. Ultimately, Doğan urged allies to counter with similar technology integrations. He advocates rethinking naval postures to mitigate China's leverage in hybrid domains.

Jan Stockbruegger from the German Aerospace Center provided a systematic analysis of hybrid attacks on offshore infrastructure, such as cables, pipelines, and windfarms, focusing on stealth strategies below the war threshold. He distinguished between operational stealth (delaying detection) and strategic stealth (ensuring plausible deniability) to avoid retaliation. Three strategies were outlined as three distinct options: “hiding in plain sight" (e.g., anchor-dragging as accidents, like the 2024 Estlink cut); “hiding in time” (timed explosives, as in Nord Stream); and “hiding in space” (remote drones, per the 2021 Mercer Street attack). Stockbruegger highlighted vulnerabilities such as post-incident forensics exposing attackers despite initial ambiguity. Countermeasures take advantage of these, including distributed acoustic sensing (DAS) for subsea monitoring, AUVs/USVs for inspections, and radar/satellites for broad surveillance. He stressed the importance of real-time detection combined with investigative tools to reduce deniability and prevent escalation. Supporting the panel, Stockbruegger suggested using space-based radars for anomaly detection over large areas, integrated with underwater AUVs to disrupt operations. His insights highlight the need for sensor expansion and data integration to manage grey-zone risks, preparing defenders for sophisticated threats from actors like Russia or China through multiple-domain technologies.

Dr. Münir Cansın Özden from ITU/DATUM explored offensive seabed warfare technologies, tracing developments from historical operations like Ivy Bells, which used submarines like NR-1 for cable tapping in the Sea of Okhotsk. He detailed manned mini-submarines, unmanned XLUUVs, and hybrid systems that require no crew but include human oversight during strike operations. He emphasized deep-water capabilities (e.g., Italy’s AE 90 SDV reaching 1,000m). Launch and recovery from surface ships or submarines enable covert deployments, with tools like manipulators for cutting or mining. Özden highlighted the grey area between automation and command, warning of ethical issues in unmanned combat. He included illustrations of undersea cable maps and ROVs used for sabotage. These capabilities require the integration of AI for navigation. Regarding the panel, he proposed combining space-based guidance like satellites used for for position, navigation and timing, with underwater vehicles to enhance precision in offensive operations. Strengthening these capabilities enhances deterrence against MCI threats. Özden advocated for diverse technologies to counter vulnerabilities, framing these advancements as dual-use for defense, such as protecting pipelines through offensive reconnaissance. His discussion calls for international norms to govern such capabilities, balancing innovation with stability in contested seabed regions.

Comments By The Moderator

CDR Frenzel's NATO perspective underscores vulnerabilities in legal frameworks like UNCLOS, where attacks such as the Nord Stream sabotage exploit plausible deniability in exclusive economic zones (EEZs).

Ögütcü and de Jong detail Russia's weaponization of energy assets in the Black Sea, using “frozen conflicts” for low-cost disruptions with high geopolitical impact. Doğan's analysis of China's civil-military fusion (MCF) reveals how dual-use ports and surveillance networks like the “Great Underwater Wall” extend strategic leverage, blurring civilian and military domains. Stockbruegger provides a three-part model of stealth strategies: “hiding in plain sight,” “time,” and “space.” These enable attackers to evade detection from dropped or dragged anchors, timed explosives, or drones. Özden explores offensive seabed technologies, from historical operations like Ivy Bells to emerging XLUUVs and “no manning required” mini submarines, facilitating covert strikes in depth.

These issues will profoundly shape future naval warfare by amplifying and grey-zone operations, where states achieve objectives without triggering full-scale conflict. Warfare will increasingly integrate space-based surveillance with underwater autonomy, fostering multi-domain battlespaces that demand AI-driven anomaly detection and rapid response. Civil-military fusion will erode traditional distinctions, enabling asymmetric advantages for actors like China and Russia, while heightening escalation risks in contested seas. Deterrence will pivot to denying deniability through forensic advancements and alliances. However, the proliferation of unmanned systems could democratize threats, leading to persistent low-intensity conflicts and necessitating resilient, diversified infrastructures. Ultimately, future wars may be won not on battlefields but through subtle MCI dominance, reshaping global power dynamics.

Concluding Remarks

The presentations at the 2025 MARSEC Conference highlight escalating hybrid threats to maritime critical infrastructure (MCI), including undersea cables, pipelines, and offshore platforms, which underpin global communications, energy security, and economic stability.

Collectively, these presentations illuminate how space-based and underwater technologies can transform MCI protection from reactive defense to a proactive strategy, addressing asymmetries in an interconnected maritime landscape. By bridging theory and practice, the panel advanced scholarly discourse on hybrid resilience.

About the Author

Prof. James Kraska / Stockton Center for International Law, United States Naval War College

James Kraska is chair and Charles H. Stockton Professor of International Maritime Law in the Stockton Center for International Law at the Naval War College, the first-established chair at the institution and visiting professor of law and John Harvey Gregory Lecturer on World Organization at Harvard Law School. He has served as visiting professor of law at the College of Law, University of the Philippines, visiting professor of law at Gujarat National Law University, Mary Derrickson McCurdy Visiting Scholar at Duke University Marine Laboratory and fellow-in-residence at the Marine Policy Center, Woods Hole Oceanographic Institution

Challenges to the Protection of Critical Undersea Infrastructure: NATO MARCOM's Perspective

Commander Stanislas Frenzel
Allied Maritime Command, NATO

Abstract

In the last three years, the increase of suspected acts of sabotage against critical maritime infrastructure, as part of larger hybrid campaigns, has been perceived as a significant risk to the Alliance and its member States. Acting within a restrictive legal framework and faced with highly deniable actions, Allied Maritime Command conducts, in coordination with coastal States, since January 2025, a multi-domain enhanced vigilance activity in the Baltic Sea looking to improve allies 'ability to respond to destabilizing acts. Baltic Sentry employs a wide range of military assets, provides an informational hub for private sector stakeholders and uses innovative new technologies such as data-fusion platforms providing real-time analytics.

Keywords
Protection of critical undersea infrastructure, Maritime security, NATO, New technologies, Informational hub

Introduction

The maritime environment is a vital hub for trade and energy transit connecting numerous Allied nations. The sea serves as a conduit for energy supplies, particularly natural gas and oil, and supports key underwater cables that transmit data between Europe, North America and beyond. These elements are crucial not only to the economies of the region, but also to the security of NATO Allies and Partners. With increasing reliance on undersea cables and pipelines, protecting this critical infrastructure is a continuing priority for NATO.

Faced with increasing threats and challenges to the security of critical undersea infrastructure in NATO's area of interest, and despite a constrained legal framework, Allied Maritime Command (MARCOM) has developed a new multi-domain approach to support Nations in enhancing the security of their infrastructure, notably through the use of new technologies.

The Vital Importance of Undersea Infrastructure.

a. Critical undersea infrastructure (CUI) includes undersea cables, pipelines, and energy installations that support global communications, energy supply, and economic stability. Undersea cables, laid on the ocean floor, transmit telecommunications signals, including internet and data, forming the backbone of global connectivity. This infrastructure is vital for energy distribution, the digital economy, and international communication but remains vulnerable to accidents, and intentional sabotage, making its protection a strategic priority.

b. Cables may be either communication cables – for transmission of data, for scientific purposes, for military purposes, for providing communications to offshore oil and gas platforms - or power cables. 97% of global communications are transmitted via cables lying deep beneath the oceans (Sunak, 2017, p. 12). Today's submarine network counts 213 independent cable systems and 545,018 miles of fibre. There is no alternative to using undersea cables. Satellite technology cannot effectively handle communication requirements of a modern digital economy and society. In a single day: cables carry $ 10 trillion of financial transfers and process some 15 million financial transactions (Wall, 2021).

c. Pipelines are pipes with pumps, valves, and control devices for conveying liquids, gases, or finely divided solids. Approximately 70% of crude oil and petroleum products are shipped by pipelines, and nearly all dry natural gas. There are 8,000 km of oil and gas pipelines across the North Sea alone.

Threats to critical undersea infrastructure

As global reliance on this infrastructure continues to grow, protecting it is a strategic priority for governments, industries, and security agencies to ensure resilience, secure communication, and uninterrupted global operations.

Any disruption, whether from accidental damage or targeted attacks, can lead to widespread outages, economic losses, and security threats. Similarly, damage to undersea cables and energy installations can disrupt fuel supplies, impact industrial operations, and create geopolitical tensions.

Threats to critical undersea infrastructure are various:

- Civilian ships (i.e. fishing trawlers) can be repurposed for sabotage, making detection and attribution challenging.
- Small vessels (i.e. sailing ships) can potentially be used for covert operations, underscoring the difficulty in monitoring and protecting such a vast domain.
- Merchant vessels can be responsible for cable cutting or deliberate damage to pipelines, using anchor dragging. They can operate in different locations during the same voyage. The delays in detecting and responding allow for subsequent damage.
- Several Nations have developed specific maritime capabilities dedicated to disruption of undersea infrastructure. They include specialized submarines designed for undersea operations. These advanced capabilities highlight the ability for state actors to engage in sophisticated and covert activities targeting CUI.

It is essential to insist of the asymmetric nature of threats to critical undersea infrastructure: the cost of conducting an attack is often minimal compared to the extensive resources required to ensure its protection.

Cases of damages to critical undersea infrastructure in the Baltic Sea

NATO has been working to enhance the security of critical undersea infrastructure for several years. Allies have committed to enhancing resilience of their critical infrastructure in line with Article 3 of the North Atlantic Treaty. They have increased the number of ships patrolling the North and Baltic Seas as part of vigilance activities.

Still, the Nordstream pipeline explosions on 26 September 2022 triggered new discussions inside the Alliance and unveiled the need to identify potential vulnerabilities and provide new responses to threats. A series of incidents involving damage to CUI highlighted the increasing threat developing in the Baltic Sea region:

- **Baltic Connector** (07-08 October 2023). The Baltic connector pipeline is a 77-kilometer-long gas pipeline connecting Finland and Estonia under the Baltic Sea. It was allegedly attacked on the night of 7-8 October 2023. The gas pipeline was damaged in Finland's EEZ. Also, a related communications cable disruption took place in Estonia's EEZ: two telecoms cables connecting Estonia to Finland and Sweden. Although the Finnish Prime Minister termed the Baltic Connector as caused by an ‘external attack’ (Armstrong & Sri-Pathma, 2023), the investigation by the Finnish and Estonian authorities have not ended conclusively.

A track came to surface over the course of investigation: a Chinese cargo ship named *Newnew Polar Bear*. The damage to the gas pipeline and two data cables coincided with the ship's voyage, merely within few hours of each other. The Finnish Navy also found a severed six-ton anchor from near the site of the damage. Later, the ship was spotted in St. Petersburg without its second anchor. In August 2024, China claimed the incident was due to weather conditions.

- **Cables in Swedish EEZ** (18 November 2024). A Chinese flagged bulk carrier, the *Yi Peng Three*, was suspected of having crossed several times over the position of two severed cables in Swedish EEZ. It was monitored by DNK, DEU and SWE patrol ships in international waters, before an investigation was led by chinese authorities. Investigators from DEU, SWE, FIN and DNK were allowed to get onboard and speak to the crew. However, China refused Sweden's chief prosecutor's request for diversion of the ship inside Sweden's territorial waters for further national investigation. The ship was eventually allowed to continue its voyage.
- **Estlink 2 incident** (25 December 2024). A power cable laid connecting Finland to Estonia was damaged in December 2024, resulting in cross-border was reduced from 1,016 MW to 358 MW. Tanker *Eagle S*, flying a Cook Islands flag, was spotted over the damaged cable with its anchors dragging. She was escorted by FIN coast guards inside finish territorial waters and boarded for investigation for the following offenses: act of sabotage, regulatory offense of circumvention of sanctions imposed on Russia on oil export and absence of a valid insurance. On 02 March 2025 the ship was allowed to continue its voyage. Three crew members remain in FIN territory with an interdiction to leave the country.

Limitations of the legal framework for protection of CUI

The international legal framework protecting submarine cables lags some way behind their contemporary importance. There are some sources of law specific to undersea cables and pipelines. Currently, the United Nations Convention on the Law of the Sea (UNCLOS), over forty years old itself, is the most contemporary, as seen in the table below:

1865 Constitution and Convention of the International Telecommunication Union
1884 International Convention for the Protection of Submarine Telegraph Cables
1907 Hague Convention
1958 Convention of the High Seas
1982 United Nations Convention on the Law of the Sea

Table 1

International legal framework governing the protection of critical undersea infrastructure

a. The **1884 Cable Convention** is still the only standalone framework addressing submarine cables – there is no standalone framework for pipelines. The primary goal of the 1884 Convention was to require State adoption of domestic legislation which protected cables outside of territorial waters. It makes the breaking or injury of submarine cables, done willfully or by culpable negligence a punishable offense. States can inspect the papers of (foreign) vessels suspected of intentional or negligent damage to submarine cables. While the Convention remains in force, there is very limited relevant State practice on its application. The extent to which the convention reflects customary law that is binding to non-States Parties is uncertain.

b. The **1958 Convention on the High Seas** has a few legal provisions to both types of infrastructure. It secured the legal principles that States could not obstruct the construction of undersea cables in international waters. It reaffirms the right of all States to lay undersea infrastructure on the bed of the high seas, extending that right and their protection not only to telegraph cables, but also high-voltage power cables, and pipelines.

c. Most provisions of these two conventions have been incorporated in the **1982 UNCLOS** or may be regarded as customary international law.

- In its article 113, UNCLOS replicates 1884 Cable convention with the requirement for States to enact laws that criminalize the breaking of undersea by vessels bearing their flag. However, many of the convention's signatories have not enacted this obligation.

- Moreover, there is a strong argument that intentional damage to an undersea infrastructure is a crime that attracts universal jurisdiction and all States should have jurisdiction over the offender. Something article 113 does not provide for (Sunak, 2017, p. 17).

- Eventually, article 113 falls short of giving warships a right to board a vessel suspected of intentionally damaging undersea cables in international waters.

None of these instruments provide for the right to visit, board, search or seize a vessel suspected of tampering with or breaking undersea cables. The only power a State has is the ability to require the master of a suspect vessel to produce documentation (re. state registration) before submission of a report to the Flag State, which is a clearly limited deterrence factor.

Difficulties mostly arise beyond TTW, with cable ownership presenting a particular challenge. Unlike vessels, submarine cables are not contained within any central/international registry. For any single cable the consortia of (usually private) companies that manufacture, own and operate it can and often does span various countries, as can the jurisdictional territory across which the cable lays.

Ownership cannot therefore be relied upon as jurisdiction or mandate for enforcement action. Critically, even if ownership of a particular cable could be established, the jurisdictional powers afforded by Art. 113 UNCLOS extend only to vessels flying a nation's own flag or to a person already subject to the coastal state's jurisdiction, presenting the obvious difficulties for ships operating under the operational command and control of NATO.

Preventing damage to CUI and enforcement actions

a. Prevention of damage

- Within their territorial waters, UNCLOS allows coastal States to adopt and enforce laws and regulations (e.g. on customs and fiscal matters, but also on protection of cables and pipelines), except for warships and governmental vessels enjoying immunity (UNCLOS, article 21). Coastal States can engage in port State control to verify that vessels comply with internationally accepted standards.

- In international waters, coastal States may conduct surveillance and patrolling activities inside their Exclusive Economic Zone (EEZ) and beyond.

- They may also create protection zones or exclusion zones to exclude e.g anchoring around CUI concentrations within their EEZ or continental shelf. While such protection zones appear to be useful, it is worth noting that these regulatory frameworks do not provide for enforcement measures against foreign vessels.

b. Enforcement actions

- Any vessel can be boarded in international waters when the flag State consents, or when it is without nationality (UNCLOS article 110).

- States can also leverage their exclusive jurisdiction over the exploitation of natural resources or marine scientific research in their EEZ and continental shelf. For instance, to prohibit fishing in CUI-sensitive areas, to protect cables connected with drilling rigs on their continental shelf, or to equip cables with acoustic sensors that can monitor marine life.
- The law of the sea permits enforcement action, in particular by coastal States, to prevent environmental pollution. These environmental competences are likely to be more relevant to pipelines than to cables.

- Even where no legal basis for boarding and/or arrest exists, the notion of a state of necessity may exceptionally be invoked to "excuse" what would otherwise be an unlawful maritime interdiction, to the extent that such action is the only way for the State to safeguard an essential interest against a grave and imminent peril (Art.25 Draft Articles on State Responsibility).

MARCOM and NMCSCUI's role in the protection of critical undersea infrastructure

On July 11, 2023, the importance of protecting CUI from potential threats was highlighted by NATO's Secretary General in the 2023 Vilnius Summit communiqué. While the protection of critical undersea infrastructure on Allies' territory remains a national responsibility, NATO stands ready to support Allies if and when requested (NATO, 2023).

To further enhance NATO's role in securing critical undersea infrastructure, Allies decided to establish NATO's Maritime Centre for the Security of Critical Undersea Infrastructure (NMCSCUI), based at MARCOM in Northwood, United Kingdom.

a. Roles and responsibilities

It is MARCOM's responsibility to provide operational-level support, facilitating information sharing and coordination with NATO Allies to enhance undersea infrastructure security. This support includes incident response coordination and the development of maritime response options.

As part of its mandate, NMCSCUI maintains the Operational CUI Network, which connects Points of Contact (POCs) from each NATO Ally. Its goal is to enhance collaboration by sharing threat assessments, best practices, and real-time information between military, governmental, and private sector actors. Through initiatives such as these, NMCSCUI enhances NATO's capacity to monitor, assess, and respond to threats targeting critical infrastructure.

b. A Multi-Domain Operation

Securing critical undersea infrastructure is taking part in a multi domain operation. It is the orchestration of military activities, across all operational domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance.

NMSCUI's ambition is to enhance its understanding of the maritime situational awareness through:

- **data collection**: sensor data and intelligence.
- **data fusion**: use of software, multiple data sources, study of patterns of life in vicinity of critical undersea infrastructure, use of artificial intelligence and anomaly detection.
- **knowledge**: information sharing, preventative/mitigating actions, denial of deniability.

c. Technological advancement

In collaboration with NMCSCUI, the Centre for Maritime Research and Experimentation (CMRE) has developed an operational prototype called MAINSAIL, aiming at enhancing the security of Critical Undersea Infrastructure (CUI) by improving Seabed-to-Space Situational Awareness (S3A).

MAINSAIL is a cloud-based data processing platform for analysis and reporting, built on Databricks and hosted on Microsoft Azure, with development funded by ACT. Unlike platforms reliant solely on AIS data, MAINSAIL can ingest data from a wide array of sources across the seabed-to-space spectrum. Its highly customizable alerts are designed to detect potential anomalies while avoiding operator overload. Key features for MAINSAIL include:

- Presenting CUI information
- Alerting key events
- Conducting historical analysis
- Generating detailed reports

d. MARCOM's response to incidents

Recent incidents in the Baltic Sea that damaged undersea infrastructure underscore the critical need for swift information sharing and close coordination among governmental, military, and private sector actors.

In the New New Polarbear case, 10 hours elapsed between the first and subsequent incidents, while the Yi Peng 3 case saw a 12-hour gap. Timely information about initial incidents could provide valuable opportunities to take preventive action and avoid further damage.

MARCOM responded as follows:

- The Battle Watch Captain and Duty Intelligence Officer received the initial information.
- The Duty Shipping Officer reviewed the merchant shipping picture to identify vessels active in the area at the relevant time.
- Contact was established with relevant national MOCs to verify the facts.
- Operational and tactical concerns were assessed to determine any required support.
- Maritime response options were developed by MARCOM.
- Coordination was maintained with affected nations, while Allies were engaged to ensure Maritime Situational Awareness (MSA). The affected nations retained ownership of the situation, with MARCOM acting in a support role.

Enhanced vigilance activity in the Baltic Sea – BALTIC SENTRY

On 14 January 2025, in Helsinki, NATO Secretary general Mr Rutte announced the launch of a new military activity by NATO to strengthen the protection of critical infrastructure. Baltic Sentry's mission is to enhance NATO's military presence in the Baltic Sea and improve Allies' ability to respond to destabilizing acts (NATO, 2025a).

Among the means, a wide range of assets are deployed in the Baltic Sea (warships, submarines, maritime patrol aircrafts, coastal radars, etc.) to help monitoring activity in vicinity of CUI. It includes the integration of Allies national surveillance assets. New technologies have also been tested in the Baltic Sea, including a small fleet of naval surface drones.

NATO fully interacts with the Critical Undersea Infrastructure Network, which includes industry, to explore further ways to protect infrastructure and improve resilience of underwater assets. NATO Maritime Centre for Security of Critical Underwater Infrastructure (NMCSCUI) assists ACO and NATO Allies in making decisions and coordinating action relating to critical undersea infrastructure protection and response (NATO, 2025b).

Finally, NATO Forces maintain a persistent presence in the Baltic Sea, conducting regular patrols and joint exercises to enhance readiness.

References

Allen, C. (2019). The peacetime right of approach and visit and effective Security Council sanctions enforcement at sea. Stockton Center for International Law.

Azaria, D., & Ulfstein, G. (2022). Are sabotage of submarine pipelines an attack triggering a right to self-defence? EJIL:Talk

European Commission. (2025). EU action plan on cable security.

Frazier, K. (2023). On protecting the undersea cable system. Lawfare.

Hinck, G. (2017). Cutting the cord: The legal regime protecting undersea cables. Lawfare.

Hinck, G. (2018). Evaluating the Russian threat to undersea cables. Lawfare.

Kaushal, S. (2023). Navies and economic warfare: Securing critical infrastructure and expanding policy options. Royal United Services Institute.

Koral, O. (2024). Use of force in protecting offshore critical infrastructure. NATO Maritime Security Centre of Excellence (MARSEC CoE).

Kraska, J. (2025). Undersea cables and international law. U.S. Naval War College, Stockton Center for International Law.

Monaghan, S., Svendsen, O., Darrah, M., & Arnold, E. (2023). NATO's role in protecting critical undersea infrastructure. Center for Strategic and International Studies (CSIS).

North Atlantic Council, Operations Policy Committee. (2022). The international legal framework governing undersea infrastructure.

Sari, A. (2025). Protecting maritime infrastructure from hybrid threats: Legal options. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Sunak, R. (2017). Undersea cables: Indispensable, insecure. Policy Exchange.

Wolf, S. (2011). Submarine pipelines and marine environmental protection: The example of the Baltic Sea under public international law.

About the Author:

Stanislas Frenzel / Legal advisor / NATO / stanislas.frenzel[at]nato.int

Commander Frenzel is the senior legal advisor at NATO's Allied Maritime Command, located in Northwood, United Kingdom. Cdr Frenzel joined the French naval academy in 2005. His early operational assignments include deployments onboard anti-submarine warfare frigate Montcalm and amphibious assault helicopter carrier Tonnerre. As a legal advisor, he has served in various overseas assignments and deployments at NATO's Maritime Command Naples, NATO's JFC Naples, EU Operation Atalanta, and European Operation Irini. He participated to Operation Active Endeavour, Operation Unified Protector in Libya, anti-piracy missions in the Horn of Africa and the implementation of the UN arms embargo on Libya. Cdr Frenzel has also held various positions on home soil, at the French Ministry of Defence, French Naval Staff, and French Naval inspection. He is a graduate from the French War College in Paris, a graduate from the Institut d'Etudes Politiques of Bordeaux and holds a master's degree in Law from the University of Paris Pantheon-Assas.

Hybrid Attack Strategies Against Offshore Infrastructures

Jan Stockbruegger
German Aerospace Center

Abstract

Hybrid attacks threaten offshore infrastructures, including wind farms, shipping lanes, subsea cables, and pipelines. In response, states are developing information-sharing platforms, advanced sensors, and unmanned systems to improve monitoring and threat detection. Yet what type of attacks offshore infrastructures need to be protected against remains unclear. This paper presents a comprehensive analysis of physical hybrid attack strategies targeting offshore infrastructures, encompassing both underwater and surface operations. It argues that attackers need to ensure plausible deniability to reduce the risk of conflict escalation. Yet making sure that attackers and their state-sponsors cannot be identified is a challenge due to the proliferation offshore sensors such as satellites, radar, and cameras. I identify three hybrid attack strategies aimed at ensuring plausible deniability, accident-based strategies, remote attack strategies, and escape strategies, each with specific operational focus, parameters and protection requirements. The findings can inform sensor configurations and protection measures to deter, detect, and disrupt hybrid attack operations.

Keywords

Hybrid Warfare, Offshore Infrastructure, Protection Plausible Deniability, Maritime Security, Unmanned and Autonomous Systems

Introduction

Hybrid attacks are a major threat to the maritime domain and offshore and underwater infrastructures such as windfarms, shipping lanes, and subsea cables and pipelines (Bueger & Liebetrau, 2023; 2021; Sari, 2025). Consequently, analysts, policymakers, and engineers increasingly develop solutions to protect infrastructures including information sharing platforms and innovative sensors and unmanned systems to better monitor infrastructures and collect data for maritime threat detection (Felemban et al., 2015; Wielgosz & Malyszko 2025; Voelsen, 2024).

Yet what exactly infrastructures need to be protected against remains largely unclear. So far, NATO countries have mainly been confronted with espionage and low-level sabotage attacks including civilian vessels that cut cables with their anchors (Praks, 2024). Yet hybrid warfare against offshore infrastructures could quickly escalate and become more intense as competition with Russia, China, and other countries with high technological and organizational capacities intensifies (Yazmyradov et al., 2024). Consequently, policymakers need to prepare for more sophisticated hybrid attack scenarios in the maritime domain involving advanced military grade weaponry and technologies including unmanned, autonomous and remotely operated systems.

A growing literature studies maritime cyberattack and legal strategies (Symes et al., 2024; Sari, 2025), as well as specific strategies, practices, and systems for physical attack (Savitz, 2024; Praks, 2024) against vessels, pipelines, cables, windfarms, and other platforms (Gabriel et al., 2022; Burgherr et al., 2023). However, few efforts have been made so far to analyse physical attack strategies systematically, including the strategic and operational parameters that influence specific hybrid attack operations, what maritime systems and technologies attackers could deploy, and how they can evade maritime sensors and other protection measures (Khawaja et al., 2022a; Savolainen et al., 2023). Consequently, we only have a limited understanding of hybrid attack risks against offshore infrastructures, how likely or unlikely certain attack scenarios are, and what can be done to prevent or deter them.
This paper tries to address this gap by offering a systematic analysis of physical hybrid attack strategies in the maritime domain focusing on both underwater und surface operations. I argue that actors engaged in hybrid warfare need to maintain plausible deniability by obscuring their involvement in attack operations. Yet doing so is difficult due to the proliferation of offshore sensor systems such as satellite and coastal radar and optical cameras (Felemban et al., 2015; Okafor-Yarwood et al., 2024). Attackers thus need to adjust their operations in a way that allows them to evade sensors and to make attack attribution difficult.

I analyze three strategies aimed at ensuring plausible deniability in hybrid maritime attacks. Accident attack strategies are operations in which the attacker obscures attacks as accidents and other safety incidents; remote attack strategies are operations in which the attacker increases the distance between itself and the site of the attack to evade surveillance systems; and escape strategies refer to operations whereby the attacker avoids detection by escaping from the site of the attack before they can be detected or detained and arrested. I argue that these strategies should be used to develop more specific attack scenarios and to configure sensor and protection systems to prevent and disrupt them.

I first discuss the notions of "hybrid" and "grey zone" warfare and "plausible deniability". I then introduce the concepts of "operational" and "strategic stealth" in hybrid attacks. After that I describe the challenge of ensuring strategic stealth and plausible deniability in attacks against offshore infrastructure, before analyzing three distinct hybrid attack strategies. I summarize my argument in the conclusion.

Hybrid attacks in the maritime grey zone

My paper contributes to the debate on "hybrid" or "grey zone" warfare strategies in the maritime domain. Both terms are relatively recent conceptual innovations that aim at capturing the transformation of warfare and competition in the modern age. Hybrid warfare refers to the broadening of warfare operations against an adversary beyond conventional military tools. A hybrid campaign uses multiple tools, vectors and activities to achieve its objective. This includes espionage, sabotage and cyberattacks, as well as engaging in election interference, propaganda or disinformation strategies to weaken and destabilize the enemy from within. Hybrid strategies are thus characterized by the blurring of lines between traditional warfare and other forms of conflict, such as irregular warfare, cyber warfare, and information warfare (Johnson, 2018).

The grey zone, on the other hand, refers to actions against an adversary below the threshold of war – that is actions that create a competitive space between peace (white) and war (black). Grey zone strategies leverage ambiguity and kinetic and non-kinetic means to achieve strategic objectives without escalating to traditional warfare. Grey zone strategies are thus characterized by actions that are intended to harm and weaken an adversary without justifying a conventional military response (Layton, 2021).

In the maritime domain, "grey zone" and "hybrid" warfare practices can include activities like naval patrols, cyberattacks on maritime infrastructure, economic coercion of countries with maritime assets, and the use of proxies to harass or interfere with maritime activities.

Grey zone and hybrid strategies can also include sabotage attacks against offshore infrastructures if these attacks are crafted and conducted in a way that they do not lead to a military response and open war (Patalano, 2018; Larsson, 2024). China (Patalano, 2018), Russia (Praks, 2024) and Iran (Eisenstadt, 2021) are commonly regarded as the main perpetrators of hybrid maritime warfare activities.

One of the ways in which attackers reduce the risk of conflict escalation in hybrid operations against offshore infrastructure is by ensuring plausible deniability – that is by making it difficult to pinpoint the source of an attack. Plausible deniability is crucial in hybrid attacks because it allows an actor to damage an opponent's interests without taking direct responsibility, making it difficult to attribute the actions and limiting the ability of the targeted state to respond decisively. The key aim of ambiguity is not necessarily to hide the true actor behind the activity, but ultimately to stymie a legitimate response by creating ambiguity.

To create plausible deniability, an attackers need to ensure that their operations do not produce evidence that could link them to the attack and justify counteractions including military retaliation (Mumford, 2020; Mumford & Carlucci, 2023). This includes legal evidence that could uphold in a court of law. As Mumford (Mumford, 2020, p. 4) argues, “if significant legal or forensic evidence emerges linking a state to a particular attack then the cloak of invisibility soon reveals itself to be the Emperor’s new clothes”, making deniability implausible. Next, I investigate the operational requirements to ensure plausible deniability in more detail.

Operational and strategic stealth

To better understand the operational implications of plausible deniability, it is useful to conceptualize it as a specific form of stealth that is required to conduct a physical attack. Hybrid attackers staging a physical attack against an offshore infrastructure rely on what might be called stealth at the operational and the strategic level. These two types of stealth overlap but capture distinct dimension and challenges in hybrid attack operations. Operational stealth refers to the attacker’s ability to delay attack detection, while strategic stealth refers to its ability to maintain plausible deniability. Both operational and strategic stealth are vital to carry out a successful grey zone operation, but the latter is the key factor that determines and constraints hybrid attack operations. Operational stealth refers to the attacker’s ability to carry out a successful attack against an adversary’s population or social, economic, or political system. Operational stealth does not mean that the attacker remains invisible and undetected. Instead, it implies that detection is too late for the initiation of countermeasures and to prevent or disrupt an attack operation. Operational stealth is therefore vital to overcome defensive measures and to stage a successful hybrid attack and to cause maximum damage to an adversary’s social, economic and political system.

Strategic stealth, on the other hand, refers to the attacker's ability to maintain plausible deniability and to make attack attribution difficult. Plausible deniability means that the perpetrator of an attack is unknown, or that the defender cannot produce sufficient evidence to prove its involvement in the operation. As pointed out before, plausible deniability is the key to reduces the risk of military retaliation in response to an attack on an infrastructure. If a defender can proof that an actor intentionally attacked its infrastructure, it has strong and justifiable reasons to retaliate militarily and to defend its territory and installations. Ensuring strategic stealth and plausible deniability is thus the top priority of actors engaged in hybrid warfare below the threshold war (Poznansky, 2022; Mumford, 2020).

Strategic stealth is not dependent on operational stealth. An attacker loses operational stealth when the defender detects the attack early enough to initiate countermeasures, even if it fails to attribute the attack to a specific actor. For example, states and private companies are often able to detect and disrupt cyberattacks against their systems, but they are usually unable to identify the individuals and states that carried out these attacks (Canfil, 2022).[16]

Yet even if operational stealth is ensured and a hybrid attack succeeds, the attacker can still lose strategic stealth if the defender is able to produce credible evidence that pinpoints to its involvement in the attack. For example, German authorities and investigators have been able to identify the individuals who carried out the attack against the Nord Stream pipeline in September 2022 and to collect evidence that implicates the Ukrainian state in the attack (Pancevski, 2024)

This perspective suggests that the effectiveness of protection systems that focus on operational rather than strategic stealth is limited. Such systems increase the likelihood that an attack will be detected and disrupted. However, they most likely do little to deter and prevent attacks as long as the attacker can remain anonymous and maintain plausible deniability, thus allowing it to continue attack operations without risking retaliatory countermeasures and conflict escalation (Pischedda & Cheon, 2023).

Cyberattacks, for example, are not only a common hybrid warfare strategy because they can produce significant damage, but also because it is so difficult to identify and prosecute the perpetrators of these attacks and to collect strong forensic evidence that clearly and unmistakenly links them to a state sponsor – even though the state's involvement in the attack is very likely (Simons et al., 2020).

[16] However, according to Canfil plausible deniability in the cyber domain has recently become more complicated in part due to enhanced investigative methods and practices of the U.S. Department of Justice and other authorities (Canfil, 2022).

In short, hybrid attacks require both operational and strategic stealth, but the latter is the key factor when it comes to designing hybrid attack operations and should therefore be at the center of our efforts to develop hybrid attack scenarios and infrastructure protection systems. Next, I apply this framework to investigate the challenges and strategies of hybrid attacks against offshore infrastructures.

Stealth and the "transparent" ocean

The debate on infrastructure protection has so far mainly focused on operational stealth and how to create real-time threat detection and early-warning systems to launch counter-measures and disrupt attack operations. The physical environment at sea makes surveillance over the water relatively easy. The seas are flat and there are little natural or human built physical structures where attackers can hide, such as mountains, hills, rocks, forests, or houses and other buildings.

Indeed, major efforts have been undertaken to monitor infrastructures and to install radar and other sensors on offshore platforms as well as efforts to share and fuse sensor data in a unified operational picture for maritime domain awareness (Balci & Pegg, 2006). This includes ship tracking systems and coastal or satellite radars as well as optical cameras, night-vision sensors and infrared sensors mounted on unmanned aerial vehicles, vessels, buoys and offshore infrastructures. Maritime surveillance is also being enhanced by machine learning algorithms that can help produce real-time situational awareness for anomaly detection and early warning applications (Felemban et al., 2015; Okafor-Yarwood et al., 2024; Wielgosz & Malyszko, 2025; Amani et al., 2022).

Yet creating real-time early warning system remains a major challenge. Poor weather and high waves can reduce visibility and make monitoring maritime activities difficult, especially if vessels have turned off their Automatic Identification Systems (Brandt et al., 2024; Androjna et al., 2024; Bunwaree, 2023). Sensor technologies such as radars and satellites are also costly, and not all offshore infrastructures are equipped with modern radar or other advanced sensor systems (Okafor-Yarwood et al., 2024).

Integrating different sensor data into a unified operational picture and threat detection mechanisms continues to be complicated. Security agencies and infrastructure operators are sometimes reluctant to share sensitive data, especially with other states. Consequently, many countries have not (yet) developed effective surveillance systems to detect threats to offshore infrastructures (Brewster & Bateman, 2024; Bueger, 2015).

Moreover, alert times at sea are often short because attackers can approach infrastructures on busy shipping lanes without raising suspicion. Additionally, offshore infrastructures cannot be fenced off to slow down an attack, and they are often located far off the coast and far away from ports and naval or coastguard assets, leading to long intervention times. Thus, even if security agencies are able to detect an attack, it might be too late for countermeasures to disrupt it and to stop a committed and well-prepared malicious actor from sabotaging a windfarm or an oil platform.

In short, targeting operational stealth to defend offshore infrastructures against attacks remains very difficult, despite the proliferation of maritime monitoring systems. There are many ways in which offshore infrastructures can be attacked and damaged by vessels, drones or other systems. For example, there is probably not much that security forces can do to prevent a large vessel from rapidly sailing into an offshore windfarm and to crash into a wind turbine, destroy a converter station with explosive devices, and attack sabotage pipelines with remotely operated vehicles.

And yet, the need to maintain strategic stealth and plausible deniability limits hybrid attack options. As a reminder, attackers need to design and conduct attacks in a way that do not produce evidence and that allow them to obscure their involvement in such operations – what I referred to as strategic stealth" in the previous section. Yet ensuring strategic stealth in the maritime domain is considerably more difficult. First, maintaining plausible deniability means that the attacker needs to escape from the site of an attack before security forces can arrive and arrest them. For example, the Finish authorities managed to stop and detain the Lion S., which had destroyed several subsea cables in the Baltic (Kauranen, 2025). Second, the defender can identify the vessels or individuals that carried out the attack and collect evidence that implicate specific actors in the attack.

Indeed, as indicated above, ship identification and monitoring capabilities have improved significantly in recent years. Especially satellite-based monitoring systems including synthetic aperture radar have proved effective to detect illicit activities and to identify ships that turn off their Automatic Identification System (Giompapa et al., 2009; Androjna et al., 2024; Helgesen et al., 2019). Thus, as pointed out before, the German authorities were able to identify the vessels and individuals involved in the Nord Stream pipeline attacks (Pancevski, 2024).

Next, I identify three strategies that attackers can use to avoid or limit strategic stealth risks and to maintain plausible deniability in hybrid attack operations.

Hybrid attack strategies against offshore infrastructure

This section introduces three hybrid attack strategies against offshore infrastructures. Each of these strategies is organized around a distinct approach to ensure strategic stealth and plausible deniability. These approaches are associated with specific operational parameters leading to specific attacking options. The strategies presented here are ideal types. In practice and reality, they often overlap so that specific attacks can include elements from different hybrid attack strategies. Here, however, we focus on these distinct ideal types.

I also show, however, that each of these hybrid attack strategies have problems and disadvantages, and that they sometimes increase the ability of defenders – such as security forces and infrastructure operators – to not only detect and identify attackers but also to prevent and disrupt attack operations.

Accident attack strategies

Accident attack strategies refer to a set of operations whereby an attacker obscures its malicious goals and intention by behaving "normally". The aim here is not to remain "invisible" but "inconspicuous" – that is not to engage in any suspicious practices that are clearly associated with an attack behavior. The key assumption here is that the more "normal" an attacker behaves, the more difficult it will be to prove that a certain activity was, indeed, an attack, creating ambiguity and plausible deniability.

A key example of this approach are operations where attacks that are being obscured as accidents, such as vessels or fishing boats that cut cables with their anchors or fishing gear. Such incidents happen frequently. They are difficult to detected, and it is nearly impossible to prevent them through timely interventions; and if they are detected, it is very hard to find evidence that prove malicious intent and that links the incident to a hostile state actor. For example, in December 2024 Finish authorities were able to detain a vessel suspected of cutting an underwater power cable, yet proving that the vessel's crew intentionally cut the cable has been difficult, despite extensive investigations, and the case is currently being handled by the courts (Kauranen, 2025).

Adversaries could also cause shipping accidents to disrupt shipping traffic and to create environmental catastrophes. For example, Russia has been accused of deploying old and unsafe "shadow tankers" for its oil exports, thus increasing the risk of a major oil spill in the Baltic Sea (Stockbruegger, 2023); and in 2023, a vessel accidentally sailed through a windfarm – without being detected by the windfarm operator or marine traffic authorities – and collided with a wind turbine (Federal Bureau of Maritime Casualty Investigation, 2025).

However, accidental cable cuts and vessel collisions are risky and their effectiveness is limited. For example, cutting cables with anchors is difficult as cables are often buried under the seabed and their precise location is unknown. Moreover, vessels engaged in such operations cannot carry with them sophisticated yet technical equipment to find, locate, and damage vulnerable cable sections, as such equipment could be detected in post-incident investigations. And while crashing a vessel in an offshore windfarm might be a more effective strategy, it would also lead to intense forensic investigations, thus requiring sophisticated planning and preparation to avoid or destroy any incriminating evidence (Kauranen, 2025).

Escape strategies

Escape strategies refer to a set of operations whereby an attacker aims at ensuring plausible deniability by escaping from the site of an attack before it is being noticed and before security forces can launch counteroperations to stop and arrest the perpetrator. The more time passes between escape and attack detection or the arrival of security forces, the more difficult it is to identify, detain, and investigate the attacker, thus increasing plausible deniability. An example of an escape operation would be if an attacker escapes before security forces arrive to detain and arrest it, thus making investigations to determine culpability more difficult.

The NewNew Polar Bear, for example, managed to escape before it could be detained for destroying subsea cables in the Baltic, thus making it difficult to investigate the vessel and to determine whether or not it had destroyed the cable intentionally (Ringbom & Lott, 2024).

Another example of escape operation is the attacks on the Nord Stream pipeline in September 2022. The attack involved explosives that were detonated several days after the material was planted at the pipelines. This allowed the attackers to escape from the site of the attack before the explosion took place and made it very hard for the authorities to identify and track them down. When the individuals who carried out the attack were eventually identified, they had already fled and could no longer be arrested and prosecuted (Pancevski, 2024). It is not inconceivable that a device explodes not days but weeks or even months after it is being planted at an infrastructure, thus making it nearly impossible for investigators to identify the platforms and persons involved in the operation.

Yet planning and carrying out escape operations is very complicated. Sometimes security forces manage to quickly identify and stop and detain vessels before they can escape. This happened, for example, when Finish authorities detained the Lion S. before it could leave Finish waters (Kauranen, 2025).

Explosive devices or other disruptive systems, moreover, can be found before they cause damage, and properly hiding such devices (e.g. by burying explosive devices at a cable under the sea) might require complex and time-consuming operations near an infrastructure, which increases the risk of detection. The attackers of the Nord Stream pipeline, for example, spent many days in the Baltic searching for the pipeline and placing the explosive devices on the bottom of the sea (Pancevski, 2024).

This does not mean that escape operations are impossible. For example, an attacker could launch autonomous underwater vehicles (AUV) from an unsuspicious vessel to identify vulnerable subsea infrastructures such as unburied cables and then launch remotely operated vehicles (ROV) to plant explosive devices (with timers) from another vessel operating several kilometers away from the infrastructure (Khawaja et al., 2022a; Eleftherakis & Vicen-Bueno, 2020).

Simpler escape operations include the use of sea mines to attack vessels or planting remotely controlled explosive devices at merchant ships or other infrastructures using small speed boats or unmanned systems.

Yet sea mines also endanger the attacker's vessels, and infrastructure sensors and crews might detect explosive devices or the platforms and systems used to plant them on an infrastructure. In other words, escape strategies remain viable, but they are also costly, difficult, and risky.

Remote attack strategies

Remote attack strategies refer to operations that are aimed at increasing the geographic distance between an attacker and the location of the attack. That is, the attacker ensures that the platform from which it launches the attack is far away from the location of the attack so that authorities cannot detect and identify its involvement in the attack. In other words, the key assumption of remote attack strategies is that the larger the distance between the attack platform and the attack location, the more difficult it will be for the authorities to find the attacker and to identify its state sponsor.

There are several ways in which an attacker can increase the distance between itself and the location of an attack. The most likely one is the use of unmanned surface or aerial vehicles that can be launched from a vessel that is located many kilometers away from the targeted infrastructure. Advanced unmanned systems can be operated over very large distances and have batteries that last many hours. Such systems are also commercially available across the world, and that they can be easily built and adjusted for specific operational purposes (Petritoli et al., 2020; Khawaja et al., 2022b; Bukovetskiy et al., 2019).

Hybrid attacks against maritime targets using unmanned systems have already occurred. The Houthi armed group in Yemen, for example, has used unmanned surface vehicles (USV) to attack merchant vessels in the Red Sea (Samaan, 2020; Haugstvedt, 2021), and Ukraine has used USV to damage Russian warships in the Black Sea (Kormych & Malyarenko, 2023; Kollakowski, 2025). Neither Ukraine nor the Houthis, however, tried to obscure their involvement in the attack.

Yet Unmanned systems have also been used to maintain plausible deniability in hybrid attack operations. In 2021, for example, the Israel-managed oil tanker MT Mercer Street was attacked by Unmanned Aerial Vehicles (UAVs) in the Gulf of Oman. Israeli, United States, and British officials blamed the attack on Iran, but Iran denied its involvement, which took place hundreds of kilometers off its coast (Gunawan et al., 2023). And on 23 December 2023, the tanker Chem Pluto was struck by an anti-ship missile or drone 320 km off India, leading the Indian Navy to board two Iranian vessels near the attack, yet without finding evidence of Iranian involvement in the attack (Phelan Chatterjee, 2023).

Attackers could deploy USVs or UAVs to conduct long-range strikes against offshore infrastructures from unsuspicious fishing or commercial vessels operating dozens of kilometers away from the targeted infrastructure. Especially small and low-flying UAVs cannot be detected easily by radar sensors, and even if they are detected, it will be difficult to identify the vessel from which they were launched. Small USVs can carry a higher payload than most UAVs and are very difficult to detect even with advanced optical and other sensors (The use of AUVs carrying explosive devices for attacks below the sea, however, is more complicated given the difficulty of effective underwater communication and navigation).

Conclusion

This paper has provided a systematic analysis of physical hybrid attack strategies against offshore infrastructures. It has argued that attackers must ensure plausible deniability to reduce the risk of conflict escalation. Yet ensuring that attackers and their state sponsors cannot be identified is challenging due to the proliferation of offshore sensors including satellites, radar, and cameras. I have developed three hybrid attack strategies aimed at ensuring plausible deniability—accident-based strategies, escape strategies, and remote attack strategies —each with generating specific operational parameters and protection requirements.

My paper has implications for how to protect offshore infrastructures against hybrid sabotage attacks aimed at avoiding conflict escalation and staying below the threshold of war. It suggests that the need to maintain plausible deniability makes hybrid attacks much more complicated than previously thought. Having to obscure their involvement in an attack increases the attacker's risks and vulnerabilities and creates opportunities for the defender to prevent and deter such operations.

Simple attack scenarios such as vessels crashing into offshore windfarms or short-range commercial drones attacking wind turbines are thus less likely because they expose the individuals and platforms that carry out these attacks and increase the risk that investigators produce incriminating evidence and that they can attribute the attack to a specific state actor.

References

Amani, M., Farzane M., Layegh, N. F., Nazari, M. E., Fatolazadeh, F., & Salehi, A. (2022). Remote sensing systems for ocean: A Review (Part 2: Active systems). IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 15, 1421–53. https://doi.org/10.1109/JSTARS.2022.3141980

Androjna, A., Pavić, I., Gucma, L., Vidmar, P., & Perkovič, M. (2024). AIS data manipulation in the illicit global oil trade. Journal of Marine Science and Engineering 12(1). https://doi.org/10.3390/jmse12010006

Balci, M., & Pegg, R. (2006). Towards global maritime domain awareness - Recent developments and challenges. 2006 9th International Conference on Information Fusion, July, 1–5. https://doi.org/10.1109/ICIF.2006.301702

Brandt, P., Munim, Z. H., Chaal, M., & Kang, H-S. (2024.) Maritime accident risk prediction integrating weather data using machine learning. Transportation Research Part D: Transport and Environment 136 (November): 104388. https://doi.org/10.1016/j.trd.2024.104388

Brewster, D., & Bateman, S. (2024). Maritime domain awareness 3.0: The future of information and intelligence-sharing in the Indian Ocean. Australian National University, National Security College.

Bueger, C. (2015). From dusk to dawn? Maritime domain awareness in Southeast Asia. Contemporary Southeast Asia, 37(2), 157–182. https://doi.org/10.1355/cs37-2a

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, 42(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129

Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? Marine Policy, 155, 105772. https://doi.org/10.1016/j.marpol.2023.105772

Bukovetskiy, A. V., Boyko, V. I., Gavrilov, P. M., Sheveleva, A. A., & Stepanov, B. P. (2019). Modeling of processes of security assurance from threats caused by unmanned air vehicles. Progress in Nuclear Energy, 115, 221–230. https://doi.org/10.1016/j.pnucene.2019.03.036

Bunwaree, P. (2023). The illegality of fishing vessels "going dark" and methods of deterrence. International and Comparative Law Quarterly, 72(1), 179–211. https://doi.org/10.1017/S0020589322000525

Burgherr, P., Siskos, E., Spada, M., Lustenberger, P., & Dupuy, A. C. (2023). Energy security in the context of hybrid threats: The case of the European natural gas network. In B. Hämmerli, U. Helmbrecht, W. Hommel, L. Kunczik, & S. Pickl (Eds.), Critical information infrastructures security (Vol. 13723, pp. — —). Lecture Notes in Computer Science. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35190-7_15

Canfil, J. K. (2022). The illogic of plausible deniability: Why proxy conflict in cyberspacemay no longer pay. Journal of Cybersecurity, 8(1), tyac007. https://doi.org/10.1093/cybsec/tyac007

Eisenstadt, M. (2021). Iran's gray zone strategy: Cornerstone of its asymmetric way of war. PRISM, 9(2), 77–97.

Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to increase the security of underwater communication cables: A review of underwater monitoring sensors. Sensors, 20(3), 737. https://doi.org/10.3390/s20030737

Federal Bureau of Maritime Casualty Investigation. (2025). Allision with an offshore wind turbine in the Gode Wind 1 wind farm by the PETRA L on 24 April 2023 (Investigation Report 192/23). Hamburg.

Felemban, E., Shaikh, F. K., Qureshi, U. M., Sheikh, A. A., & Qaisar, S. B. (2015). Underwater sensor network applications: A comprehensive survey. International Journal of Distributed Sensor Networks, 11(11), 896832. https://doi.org/10.1155/2015/896832

Gabriel, A., Tecklenburg, B., & Sill Torres, F. (2022). Threat and risk scenarios for offshore wind farms and an approach to their assessment. In Proceedings of the 19th ISCRAM Conference (pp. 162–173).

Giompapa, S., Gini, F., Farina, A., Graziano, A., Croci, R., & Distefano, R. (2009). Maritime border control multisensor system. IEEE Aerospace and Electronic Systems Magazine, 24(8), 9–15. https://doi.org/10.1109/MAES.2009.5256382

Gunawan, Y., Wati, E., & Corral, E. (2023). Iran's responsibility for the MV Mercer Street attack under international law. Brawijaya Law Journal, 10(1), 72–88. https://doi.org/10.21776/ub.blj.2023.010.01.05

Haugstvedt, H. (2021, September). Red Sea drones: How to counter Houthi maritime attacks. War on the Rocks. https://warontherocks.com/2021/09/red-sea-drones-how-to-counter-houthi-maritime-tactics/

Helgesen, Ø. K., Brekke, E. F., Helgesen, H. H., & Engelhardtsen, Ø. (2019, July). Sensor combinations in heterogeneous multi-sensor fusion for maritime target tracking. In 2019 22th International Conference on Information Fusion (FUSION) (pp. 1–9). https://doi.org/10.23919/FUSION43075.2019.9011297

Johnson, R. (2018). Hybrid war and its countermeasures: A critique of the literature. Small Wars & Insurgencies, 29(1), 141–163. https://doi.org/10.1080/09592318.2018.1404770

Kauranen, A. (2025, August 25). Suspects blame technical faults for Baltic Sea cable breaches. Reuters. https://www.reuters.com/business/media-telecom/suspects-blame-technical-faults-baltic-sea-cable-breaches-2025-08-25/

Khawaja, W., Semkin, V., Ratyal, N. I., Yaqoob, Q., Gul, J., & Guvenc, I. (2022a). Threats from and countermeasures for unmanned aerial and underwater vehicles. Sensors, 22(10), 3896. https://doi.org/10.3390/s22103896

Khawaja, W., Semkin, V., Ratyal, N. I., Yaqoob, Q., Gul, J., & Guvenc, I. (2022b). Threats from and countermeasures for unmanned aerial and underwater vehicles. Sensors, 22(10), 3896. https://doi.org/10.3390/s22103896

Kollakowski, T. (2025). War in the Black Sea: The revival of the Jeune École? Journal of Strategic Studies, 1–33. https://doi.org/10.1080/01402390.2025.2471067

Kormych, B., & Malyarenko, T. (2023). From gray zone to conventional warfare: The Russia-Ukraine conflict in the Black Sea. Small Wars & Insurgencies, 34(7), 1235–1270. https://doi.org/10.1080/09592318.2022.2122278

Larsson, O. L. (2024). Sea blindness in grey zone preparations. Defence Studies, 24(3), 399–420. https://doi.org/10.1080/14702436.2024.2359913

Layton, P. (2021, August 11). Responding to China's unending grey-zone prodding. Royal United Services Institute. https://rusi.org/explore-our-research/publications/commentary/responding-chinas-unending-grey-zone-prodding

Mumford, A. (2020). Ambiguity in hybrid warfare. The European Centre of Excellence for Countering Hybrid Threats.

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security, 8(2), 192–206. https://doi.org/10.1017/eis.2022.19

Okafor-Yarwood, I., Eastwood, O., Chikowore, N., & De Oliveira Paes, L. (2024). Technology and maritime security in Africa: Opportunities and challenges in Gulf of Guinea. Marine Policy, 160, 105976. https://doi.org/10.1016/j.marpol.2023.105976

Pancevski, B. (2024, August 14). A drunken evening, a rented yacht: The real story of the Nord Stream pipeline sabotage. The Wall Street Journal. https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c

Patalano, A. (2018). When strategy is 'hybrid' and not 'grey': Reviewing Chinese military and constabulary coercion at sea. The Pacific Review, 31(6), 811–839. https://doi.org/10.1080/09512748.2018.1513546

Petritoli, E., Cagnetti, M., & Leccese, F. (2020). Simulation of autonomous underwater vehicles (AUVs) swarm diffusion. Sensors, 20(17), 4950. https://doi.org/10.3390/s20174950

Chatterjee, P. (2023, December 24). Tanker hit off India coast by drone from Iran, says US. BBC News. https://www.bbc.com/news/world-asia-india-67811929

Pischedda, C., & Cheon, A. (2023). Does plausible deniability work? Assessing the effectiveness of unclaimed coercive acts in the Ukraine war. Contemporary Security Policy, 44(3), 345–371. https://doi.org/10.1080/13523260.2023.2212464

Poznansky, M. (2022). Revisiting plausible deniability. Journal of Strategic Studies, 45(4), 511–533. https://doi.org/10.1080/01402390.2020.1734570

Praks, H. (2024). Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage. The European Centre of Excellence for Countering Hybrid Threats.

Ringbom, H., & Lott, A. (2024). Sabotage of critical offshore infrastructure: A case study of the Balticconnector incident. In A. Lott (Ed.), Maritime security law in hybrid warfare. Brill | Nijhoff. https://doi.org/10.1163/9789004707993_008

Samaan, J. L. C. (2020). Missiles, drones, and the Houthis in Yemen. Parameters, 50(1), 51–63.

Sari, A. (2025). Protecting maritime infrastructure from hybrid threats: Legal options. The European Centre of Excellence for Countering Hybrid Threats.

Savitz, S. (2024). Uncrewed maritime vessels: Shaping naval power in hybrid threat operations. The European Centre of Excellence for Countering Hybrid Threats.

Savolainen, J., Gill, T., Schatz, V., & Giannoulis, G. (2023). Handbook on maritime hybrid threats: 15 scenarios and legal scans (Vol. 16). Hybrid CoE Paper. The European Centre of Excellence for Countering Hybrid Threats.

Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: Creating legal and operational dilemmas. Global Change, Peace & Security, 32(3), 337–342. https://doi.org/10.1080/14781158.2020.1732899

Stockbruegger, J. (2023). Reducing Russia's oil revenues: Does the allied price cap work? The RUSI Journal, 268(5), 34–42.

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the maritime sector: A literature review. Journal of Marine Science and Application, 23(4), 689–706. https://doi.org/10.1007/s11804-024-00443-0

Voelsen, D. (Ed.). (2024). Maritime kritische Infrastrukturen: Strategische Bedeutung und geeignete Schutzmaßnahmen (Version 1). Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/10.18449/2024S03/

Wielgosz, M., & Malyszko, M. (2025). A method for early identification of vessels potentially threatening critical maritime infrastructure. Applied Sciences, 15(15), 8716. https://doi.org/10.3390/app15158716

Yazmyradov, S., Lee, H., Lee, Y. S., Kamolov, A. A., & Kang, D.-W. (2024). Innovations and challenges in submarine security systems: A comprehensive analysis of modern threats and countermeasures. International Journal of Advanced Smart Convergence, 13(4), 111–121. https://doi.org/10.7236/IJASC.2024.13.4.111

About the Author

Dr. Jan Stockbruegger / German Aerospace Center /
jan.stockbruegger[at]dlr.de / ORCID: 0000-0002-1563-5434

Dr. Jan Stockbruegger leads the research group Marine Safety and Security at the Institute for the Protection of Maritime Infrastructures at the German Aerospace Center. He has a PhD in Political Science from Brown University and was previously a Postdoctoral Research Fellow in the Ocean Infrastructure Research Group at the University of Copenhagen's Department of Political Science. His current work focuses on methods to develop and evaluate maritime physical protection systems, including through the integration of sensors, security, and data analysis technologies and by increasing information sharing and operational coordination between infrastructure operators and security agencies.

Emerging Technologies for the Offensive Seabed Warfare

Asst. Prof. Dr. Münir Cansın Ozden
Istanbul Technical University

Abstract

Seabed warfare has emerged as a crucial domain in modern naval strategy due to the global reliance on undersea infrastructure and its vulnerability to covert attacks. This paper examines the rising importance of seabed warfare, catalyzed by the Nord Stream pipeline sabotage, and surveys the strategic capabilities of key maritime powers including the United States, Russia, France, China, and Italy. The paper concludes by evaluating commercial solutions such as Datum's GURNARD submersible as viable options for nations seeking to enhance their seabed warfare capacity.

Keywords

Seabed, cui, mine, sabotage, subsea

Introduction

Undersea infrastructure, including telecommunications cables, energy pipelines, and sensor networks, forms the backbone of the global economy and military communications. As states increasingly recognize the strategic importance of the seabed, seabed warfare has emerged as a new frontier in maritime defense and competition. The Nord Stream pipeline sabotage in 2022 dramatically underscored these vulnerabilities and accelerated global interest in seabed defense capabilities.

The Nord Stream Sabotage: Catalyst for Strategic Shift

In 26 September 2022, North Streamline Sabotage remind once again how important is the underwater domain and how fragile it is for covert operations. The destruction of the Nord Stream 1 and 2 pipelines in September 2022 represented a pivotal moment in seabed security (Vincent & Wieder, 2022). The incident, which occurred in international waters and involved precision demolition of critical energy infrastructure, demonstrated the covert nature and strategic impact of seabed operations. In response, NATO and its member states prioritized seabed surveillance, protection, and offensive capabilities in their defense planning NATO (2023).

Underwater Cables

%99 of international data traffic relies on underwater cables and since the war in Ukraine started at least 11 incidents happened in just Baltic Sea caused of the damage of underwater cables they are due to sabotage or anchor damage.

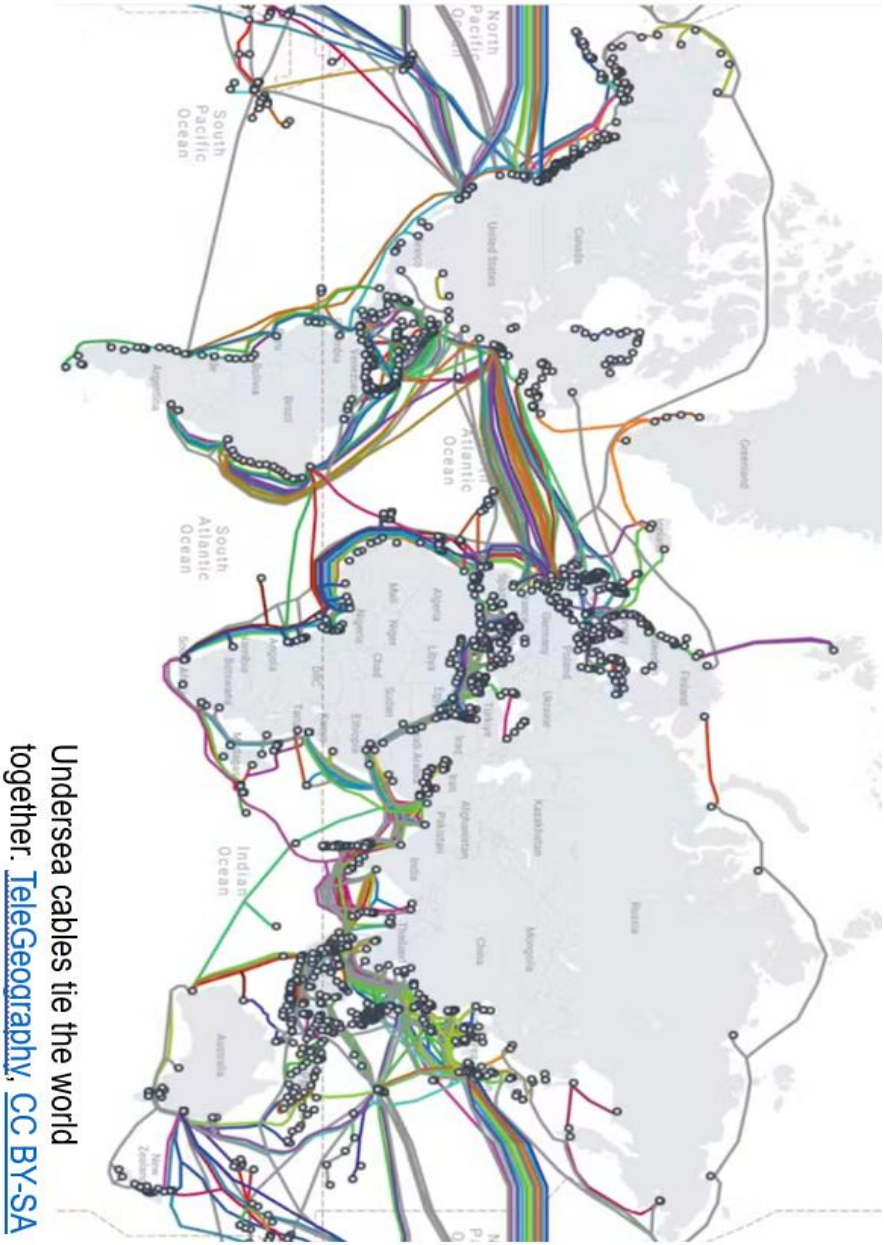

Figure 1
World undersea cables Telegeography (2025, 11 October)

When a country shut downs and aircraft of the opponent, it causes a serious conflict. Once an underwater cable is damaged it is not hard to understand it. You just restart your modem in your living room and if internet does not blink, it means somebody touched your cable. But it is very hard to find where it is damaged and operation to repair the damaged cable and effect of that damaged cable on the economy costs far more than an aircraft.

Figure 2

Underwater electric cable Karlskrona Submarine Museum, Sweden (ABB, 2025)

An underwater electric cable or a network cable has a shield to protect the cable from environmental conditions but it very vulnerable for physical damages. Cable grippers and cutters are already in use with offshore industry.

National Capabilities in Seabed Warfare

4.1 United States: NR-1 and Legacy Capabilities

Although Nord Stream reminded the name Seabed Warfare, it is not new and both Russia and the USA has very interesting submarine designs for this very important purpose. One very famous operation was Ivy Bells where US Navy wiretapped Soviet communication cables. Some of these special purpose submarines are large nuclear submarines which are converted for seabed warfare operations while others are specifically designed mini nuclear submarines operated by CIA or GRU. USS Halibut which was used in Ivy Bells was converted SSGN.

The U.S. Navy has a historical foundation in seabed warfare, particularly through the now-retired NR-1 nuclear-powered research submarine. Operational from 1969 to 2008, the NR-1 was specially built micro nuclear submarine for Seabed Warfare and she was the smallest ever built nuclear submarine with just 400tons displacement. The sub could reach depths of 900 meters and was equipped with manipulator arms, seabed wheels, and a diver lockout chamber (U.S. Navy Historical Archives, 2008). Though decommissioned, its legacy informs ongoing classified programs aimed at seabed intelligence, surveillance, and sabotage.

Figure 3
NR1 Seabed warfare submarine

Russian Federation: A Sophisticated Seabed Fleet and Covert Activities
Russia maintains the most diverse and capable fleet of seabed warfare submarines (Sutton, 2024), many operated under the Main Directorate for Deep-Sea Research (GUGI):

- Project 1910 Kashalot: A nuclear-powered auxiliary submarine capable of deep-sea operations and recovery missions.
- Project 1851 Nelma: Small nuclear-powered submarines designed for seabed reconnaissance and covert operations.
- Project 18511 Halibut: Modified diesel-electric submarines for cable tapping and sabotage, with diver support features.
- Project 10831 Losharik (Norsub-5): A titanium-hulled deep-diving nuclear sub capable of operating below 6000 meters, used for strategic cable tapping and seabed manipulation.

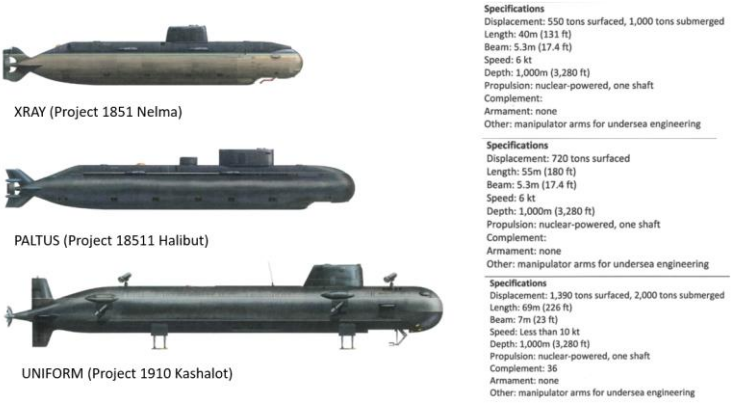

Figure 4

Russian midget submarines for Seabed Warfare (Sutton & Davis, 2017)

Yantar Support Ship: A special-purpose vessel equipped with cranes and facilities to deploy small submersibles such as Rus, Konsul, and Klavesin-2R-PM, used for cable operations and seabed surveillance. Nowadays, underwater research ships such as Yantar or even mega yachts with launching systems for touristic mini submarines can be used as mother ships of covert seabed warfare operations.

Recent reports indicate that Russian-installed seabed sensors have been discovered near key underwater cable routes off the coast of the United Kingdom. According to an investigative report by The Sunday Times on 05.03.2025, British intelligence agencies suspect these sensors are capable of monitoring undersea communications, Vanguard class submarines' activities and possibly coordinating future sabotage operations The Sunday Times (2024). These revelations have intensified concerns about Russian seabed espionage activities in Western maritime zones.

France: Strategic Depth to 6000 Meters

The French Navy has implemented a seabed warfare doctrine targeting operational capabilities down to 6000 meters which covers %98 percent of world's oceans (French MAF, 2023). The strategy includes deploying deep-diving autonomous and remotely operated vehicles (AUVs and ROVs), infrastructure mapping, and seabed monitoring systems. France seeks to defend critical seabed assets and counteract foreign intrusions.

4.4 China: Cable-Cutting Tools to 4000 Meters

China, in 22th March 2025, became the first country which publicly announced that they their military-industrial complex has developed tools capable of identifying and severing undersea cables at depths of up to 4000 meters (South China Morning Post, 2025).

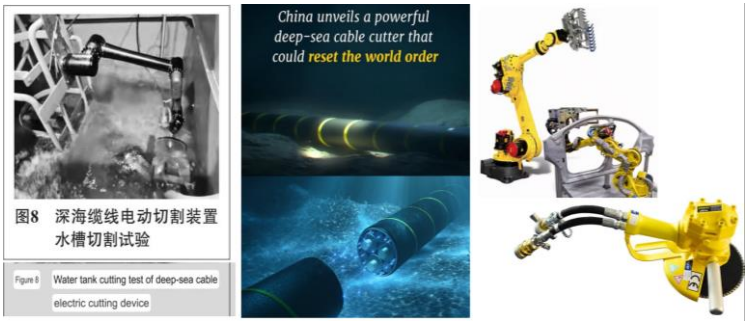

Figure 5

China's underwater cable cutter

China already has vehicles which can operate deeper than these depths and this arm can be attached to these vehicles. As we see on the Figure-5 it is not different than an industrial robot arm which you can see inside all new automated factories but a hydraulic cutter is attached to that and motors get waterproof. These capabilities, though not widely publicized, are believed to be part of a broader doctrine of information dominance and strategic disruption in undersea warfare.

Italy: AE90 Seabed Warfare Submersible

Italian Navy since WWII is very well-known for their world leading technologies in covert operations, latest seabed warfare platform, the AE90 submersible, exemplifies its growing commitment to maritime infrastructure protection and covert underwater operations Italian Defence Ministry (2024). It reflects Italy's expanding role in Mediterranean and NATO undersea security. The AE90 is a modular, deep-diving vehicle intended for cable inspection, sabotage prevention, and reconnaissance. Looks like it can be carried piggyback on Italian conventional submarines Saura and Todaro without a requirement for a dry deck shelter.

Like a wet type swimmer delivery vehicle, divers can swim inside underwater but the vehicle is very stiff with very thick pressure hull walls and acrylic windows which clearly indicates an expected to dive down to 1000m and can launch undersea mines from the tube at the aft of the vehicle.

Figure 6

Italian wet/dry type seabed warfare swimmer delivery submersible AE-90 (Militaria, 2024)

These types of vehicles can also be launched from mission bays or aft ramps from surface ships. But also, from commercial ships or mega yachts via their moonpools.

Emerging technologies shows us that manned/unmanned mini submarines will be part of surface ships but also, they will launch from larger submarines too.

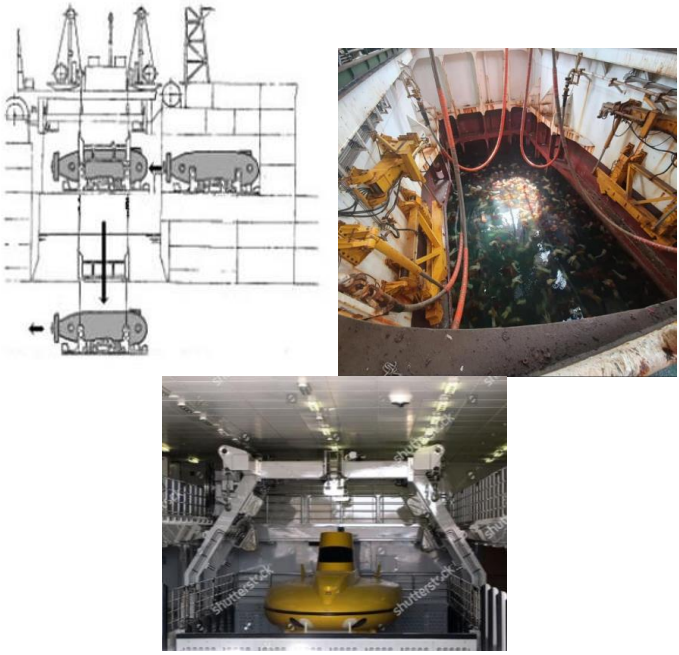

Figure 7

Launch/recovery of submersibles from moon pools of motherships

Commercial Solutions: Datum's GURNARD Submersible

Datum's first submarine, also the first indigenous mini submarine design of Turkey and first submarine classified by Turkish Lloyd is multipurpose mini submarine (or Çok Amaçlı Mini Denizalti – ÇAMD) is funded and owned by the Presidency of Defence Industries of Turkey (Navalnews, 2023). Datum has different designs for emerging undersea requirements like ÇAMD's more weaponized version Trança mini attack and special forces submarine (Navalnews, 2024).

The GURNARD is a deep-diving wet/dry submersible capable of transporting operators and tools to the seabed. It is fitted with modular payload bays, including cable grappling and cutting tools. According to Datum Subsea, the GURNARD is designed for flexible deployment in inspection, sabotage, and defensive operations (Datum, 2025).

Figure 8

Gurnard Deep Diving Wet & Dry Seabed Warfare Submarine Concept of Operation

Datum's latest design, Gurnard is a deep-diving wet/dry submersible capable of transporting operators and tools to the seabed and designed to conduct seabed warfare to damage underwater communication/electric cables via its manipulator and it can deliver 2 Malaman Mines for larger targets. Gurnard represents a commercially available solution for states seeking seabed warfare capabilities without extensive military R&D programs.

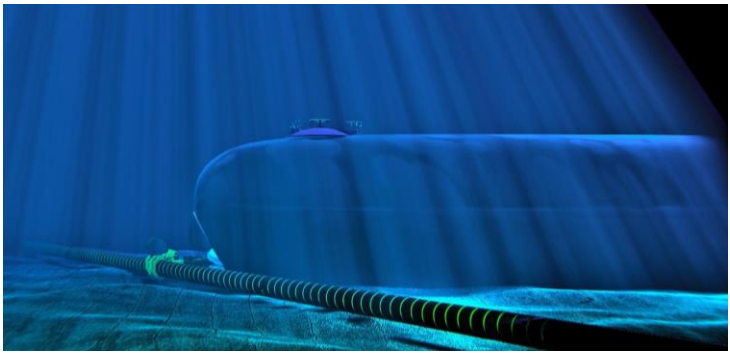

Figure 8

Gurnard Deep Diving Wet & Dry Seabed Warfare Submarine

Gurnard is designed for flexible deployment in inspection, sabotage, and defensive operations. Vessel has a tube at the aft to lay two Turkish indigenous sea bottom mine. Malaman is Turkey's indigenous seabottom mine developed by Koç Savunma, MKE A.Ş. and TÜBİTAK-SAGE. Gurnard is designed to be transported by cargo aircrafts, launched from a submarine or a surface vehicle. Vessel has an acrylic window in the front. It can detect an underwater pipeline or a cable by the help of side scan sonars and the vessel can conduct precise operations which can either help mine countermeasure or a specially designed replaceable hydraulic manipulator allow operators to grab and cut underwater cables.

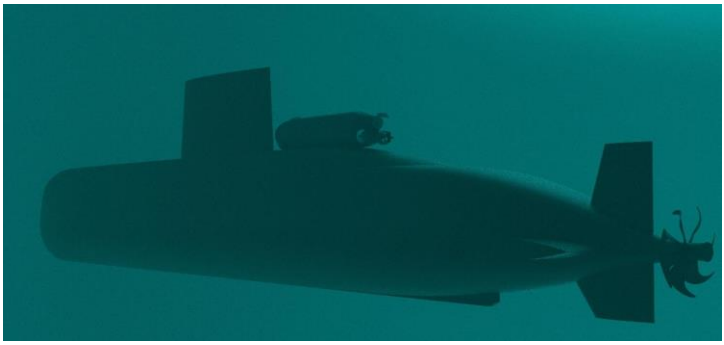

Figure 10

Gurnard's piggyback transport on a larger mother submarine

Gurnard can be launched from a surface ship or on a trailer from the shore but a specially designed connection mechanism allow the minisub be carried piggyback on larger submarines. Exterior structure of Gurnard can withstand a diving depth of 600m while inside is water resistant down to 50m. As a result, Gurnard can be carried without a need for a dry deck shelter on a submarine. Its water proof interior allows combat swimmers wet entry into the vehicle and conduct operation without need of mother submarine to surface.

Gurnard can be transported inside a standard 40 foot container. This allows a transport inside a ship container via sea, air or land transportation covertly. Two combat swimmers can operate vehicle. Gurnard can be operated in very shallow waters where large submarines can not manoeuver. Also can be operated in very deep waters where seawater pressure is so high that largers submarines can not resist. Its size allows it to get closer to ports, offshore platforms and other critical infrastructures. Gurnard Deep Diving Wet & Dry Seabed Warfare Submarine can be delivered inside TCG Anadolu or similar Platform Docks or amphibious crafts.

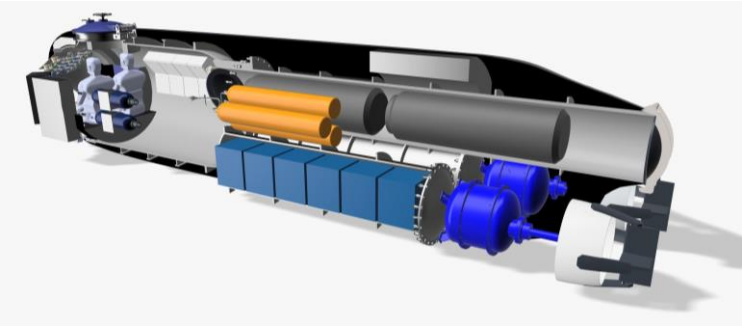

Figure 9

Gurnard's cutaway view where a stern tube for two Malaman Mines are visible

GENERAL SPECIFICATIONS			
Length (L_{OA})	9 m	Navigation	GNSS (Surface) INS+DVL (Underwater)
Beam (B)	1.8 m		
Height (D)	2.2 m	Propulsion	2x12kW electric motor Lithium Iron Phosphate Batteries
Displacement (∇)	12 ton		
Diving Depth	600m		
Operation Speed	4 knot	Weapons	2 units Malaman Mine
Max Speed	6 knot	Sensors	Other: Forward looking sonar, side scan sonar
Range	100 nm (battery)		
Crew	2 Operator Combat Swimmers	Transport	40 foot container, airtransport via A400M
Communications	VHF, SATCOM(o)	Other	Manipulator cutter

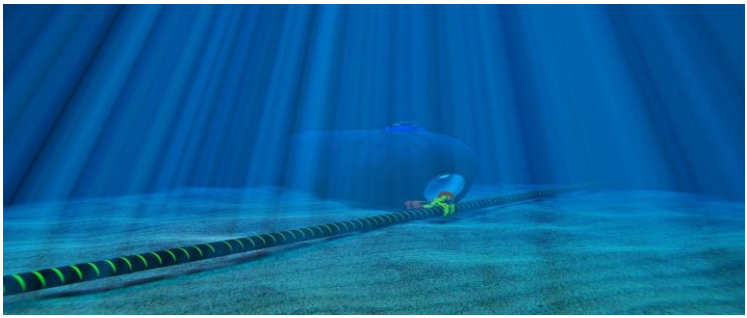

Figure 11
Gurnard's underwater cable cutter

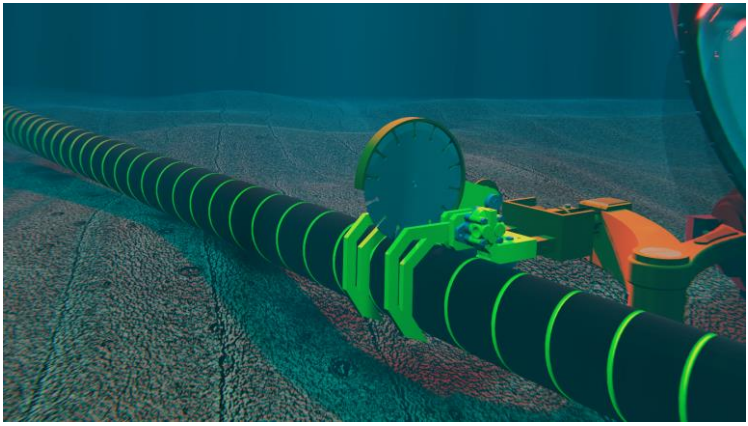

Figure 12
Gurnard's underwater cable cutter

Conclusion

Seabed warfare is a rapidly evolving strategic domain, driven by the criticality of undersea infrastructure and the demonstrated feasibility of covert attacks. From legacy U.S. platforms like NR-1 to Russia's deep-diving submersible fleet and the rising capabilities of France, China, and Italy, global powers are investing in seabed dominance. Commercial technologies like the Gurnard provide scalable entry points for nations seeking to defend their maritime infrastructure. The seabed is now a contested battlespace—one that demands readiness, innovation, and vigilance.

References

ABB's XLPE Submarine Cable Systems User's Guide (2025, 11 October) https://new.abb.com/docs/default-source/ewea-doc/xlpe-submarine-cable-systems-2gm5007.pdf

Covert Shores (2024). Russian Deep-Sea Submarine Capabilities.

Datum Denizalti Teknolojileri Uygulama ve Muhendislik AS Website. (2025, November 11). https://www.datum-subs.com

French Ministry of Armed Forces (2023). Seabed Warfare Doctrine.

Italian Defence Ministry (2024). AE90 Submersible Deployment Summary.

Militaria – storia militare (2024, 17 March) "Sommergibile Midget AE-90 incursori della marina COM SUB IN." https://www.youtube.com/watch?v=yZ6lzazIj54

Navalnews, (2023, December 01). "Turkiye is working on multipurpose mini submarine project". https://www.navalnews.com/naval-news/2023/12/turkiye-is-working-on-multipurpose-mini-submarine-project/

Navalnews, (2024, October 27). "TRANÇA mini attack submarine breaks cover in Turkey". https://www.navalnews.com/naval-news/2024/10/tranca-mini-attack-submarine-breaks-cover-in-turkey/

NATO (2023). Critical Undersea Infrastructure Coordination Cell Reports.

South China Morning Post (22.03.2025). China unveils a powerful deep-sea cable cutter that could reset the world order

Sutton, H.I., Davis, C.E., (2017) World Submarines: Covert Shores Recognition Guide

Telegeography (2025, 11 October). https://submarine-cable-map-2025.telegeography.com/

The Sunday Times (05.04.2024). Revealed: Russia's secret war in UK waters. https://www.thetimes.com/uk/defence/article/russia-secret-war-uk-waters-submarines-dpbzphfx5

U.S. Navy Historical Archives (2008). NR-1 Program Overview.

Vincent, E., Hivert, A.-F., & Wieder, T. (2022, October 10). Investigation into Nord Stream pipeline sabotage reignites the race to control the seabed. Le Monde.

About the Author

Dr. Munir Cansin Ozden / Istanbul Technical University / ozden[at]itu.edu.tr

Dr. Munir Cansin Ozden completed his Bachelor's, Master's, and Ph.D. studies at Istanbul Technical University in the Department of Naval Architecture and Marine Engineering. He is currently serving as an Assistant Professor in the same department. Dr. Özden teaches the courses Underwater Acoustics and Fundamentals of Submarine Design. In 2013, Dr. Özden founded DATUM Submarine Technologies Engineering Inc., where he continues to serve as Chairman of the Board. DATUM is carrying out the Multi-Purpose Mini Submarine Development Project, which is the first submarine whose detailed design has been approved by Turkish Lloyd for the Presidency of Defense Industries of the Republic of Türkiye.