

# Emerging Maritime Threats in Global Geopolitics: GPS Spoofing as a Tool of Hybrid Warfare in Strategic Maritime Chokepoints

Emilio Rodriguez-Diaz

[emilio.rodriquez@uca.es](mailto:emilio.rodriquez@uca.es)

University of Cádiz

**Manuel Santamaria**

University of Cádiz

**Jose Manuel Prieto**

University of Cádiz

**Juan Ignacio Alcaide**

University of Cádiz

---

## Article

**Keywords:** GPS spoofing, maritime security, hybrid warfare, electronic warfare, navigation systems, Red Sea, Persian Gulf, GNSS interference

**Posted Date:** March 19th, 2026

**DOI:** <https://doi.org/10.21203/rs.3.rs-8901159/v1>

**License:**   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

**Additional Declarations:** No competing interests reported.

---

# Abstract

This research examines the operational deployment of GPS spoofing as an emerging threat to maritime security, analyzing critical incidents in strategically vital waterways that demonstrate sophisticated electronic warfare capabilities against commercial shipping. Through detailed case study analysis of the May 2025 MSC ANTONIA grounding in the Red Sea and the 2019 Stena Impero seizure in the Strait of Hormuz, this paper reveals how GPS spoofing has evolved from theoretical vulnerability to operational weapon within hybrid warfare strategies. The research identifies systematic campaigns employing sophisticated spoofing techniques that gradually manipulate vessel positioning while maintaining apparent signal integrity, making detection extremely challenging. Evidence indicates state-level involvement through proxy forces, particularly in regions of strategic importance, utilizing advanced electronic warfare capabilities that exceed typical non-state actor resources. The study reveals critical vulnerabilities in modern maritime navigation systems, including excessive GPS dependence, inadequate spoofing detection capabilities, and insufficient crew training for electronic warfare scenarios. Strategic implications encompass disruption of critical maritime chokepoints, erosion of trust in fundamental navigation systems, and escalation potential threatening global trade flows. The paper proposes comprehensive countermeasures encompassing technical solutions, procedural improvements, enhanced training requirements, and regulatory reforms to address this evolving threat to maritime security and international commerce.

## 1. Introduction

The maritime domain has become increasingly vulnerable to sophisticated electronic warfare attacks that exploit the critical dependence of modern vessels on Global Positioning System (GPS) technology. Electronic warfare (EW), traditionally defined as warfare involving the use of the electromagnetic spectrum (EM spectrum) or directed energy to control the spectrum, attack an enemy, or impede enemy operations, has evolved from its original military applications to encompass attacks against civilian maritime targets (Grant & Collins, 1982; Spezio, 2002). Recent analysis suggests that the MSC Antonia's grounding likely resulted from deliberate interference, underscoring persistent concerns for maritime navigation including GNSS dependency, where most commercial vessels rely heavily on GNSS as their primary position source, often without cross-verification from radar, visual bearings, or inertial navigation (Androjna et al., 2020).

The evolution of electronic warfare from purely military applications to hybrid warfare targeting civilian infrastructure represents a significant shift in contemporary conflict dynamics. NATO has adopted an encompassing approach to EW (*Electromagnetic Warfare / NATO Topic*, n.d.), recognizing the electromagnetic environment (EME) as an operational maneuver space and warfighting environment. Electronic warfare consists of three major subdivisions: electronic attack (EA), involving the offensive use of electromagnetic energy weapons; electronic protection (EP), measures used to protect against electronic attacks; and electronic warfare support (ES), actions taken to detect, intercept, identify, locate, and localize sources of electromagnetic energy.

This research examines the emerging threat of GPS spoofing in maritime environments, with particular focus on incidents in strategically vital waterways. The study grounds its analysis in two documented incidents: the May 10, 2025, grounding of the 7,000 TEU container ship MSC Antonia near the Eliza Shoals south of Jeddah Port in the Red Sea (*MSC Antonia Grounding in the Red Sea Attributed to Suspected GNSS Spoofing - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design*, n.d.), and the July 19, 2019, seizure of the UK-flagged product tanker Stena Impero by the Islamic Revolutionary Guard Corps (*Seized UK Tanker Likely 'Spoofed' by Iran :: Lloyd's List*, n.d.). These cases are positioned within the broader strategic context of hybrid warfare—the deliberate blending of conventional, irregular, and cyber warfare techniques to achieve strategic objectives while maintaining plausible deniability (Hoffman, 2014; Hunter & Pernik, 2015).

The deployment of military-grade electronic warfare capabilities against civilian maritime targets represents a significant evolution in hybrid warfare methodologies. Electronic warfare has played major roles in military operations from the Vietnam War (Deitchman, 2008) through the 2007 Israeli attack on a suspected Syrian nuclear site during Operation Outside the Box (Follath & Stark, 2009), and extensively during the 2022 Russian invasion of Ukraine where Russian EW disrupted Ukraine's air defense radars and communications (Willett, 2023). The transition of these sophisticated military capabilities to target civilian merchant vessels represents a concerning development in contemporary conflict dynamics.

This research addresses a significant gap in the academic literature by moving beyond theoretical vulnerability assessments to examine real-world incidents with documented operational impacts. Risk Intelligence warns of GPS jamming incidents (*Maritime Dangers of GPS/AIS Spoofing and Jamming in the Baltic Sea*, n.d.; *Sensors on the Baltic Frontline - CEPA*, n.d.) ranging from the Baltic to the Eastern Mediterranean, Black Sea, Red Sea, Persian Gulf, Gulf of Aden, Sudan's coastline, and China's coastal waters. GPS spoofing is not just a technical nuisance—it must be viewed as a strategic threat capable of disrupting regional and global trade, destabilizing geopolitics, and endangering lives at sea (*IMarEST / The Potentially Catastrophic Threat of GPS Spoofing in Shipping*, n.d.).

The research objectives are threefold: first, to analyze the technical methodologies and operational effectiveness of GPS spoofing attacks against commercial vessels; second, to assess the geopolitical context and attribution patterns of these operations within regional security dynamics; and third, to evaluate vulnerabilities in current maritime navigation systems and propose comprehensive countermeasures to address this emerging threat.

## 2. Materials and Methods

### 2.1 Research Design

This research employs a qualitative case study methodology combining incident analysis, technical assessment, and geopolitical evaluation to examine GPS spoofing operations in maritime environments (K Robert, 2018). The methodological approach draws upon established frameworks for explanatory

case studies, utilizing multiple data sources to develop comprehensive understanding of complex phenomena within their real-world contexts (Adamy, 2006). The research design integrates technical analysis of spoofing methodologies, operational assessment of incident impacts, and strategic evaluation of geopolitical contexts to provide holistic understanding of GPS spoofing as a maritime security threat.

## 2.2 Case Selection Criteria

Two primary cases were selected based on their significance as documented instances of GPS spoofing with verifiable maritime impacts: the 2025 MSC ANTONIA incident and the 2019 Stena Impero seizure. Selection criteria included documented evidence of GPS manipulation based on technical analysis from multiple sources, verified operational impacts on vessel safety or operations, availability of multiple independent data sources for triangulation, and geographic relevance to strategic maritime chokepoints. These cases provide temporal breadth allowing analysis of tactical and technological evolution, geographic diversity encompassing both Red Sea and Persian Gulf operational environments and varying operational contexts from direct maritime casualty to seizure pretext.

## 2.3 Data Collection Methods

### 2.3.1 Primary Data Sources

Primary data collection encompassed maritime incident reports and technical analyses from maritime intelligence firms. Maritime data intelligence providers, including Windward, MarineTraffic, and Pole Star Global (*Pole Star Confirms GPS Interference Caused MSC ANTONIA Grounding*, n.d.), have released analyses pointing to probable GNSS spoofing or jamming as contributing factors in the MSC ANTONIA incident. Following a review of the available data, Captain Steve Bomgardner, Vice President of Shipping and Offshore at Pole Star Global, concluded that the vessel's AIS was subject to GPS jamming, where threat actors introduced fake signals that gave the crew inaccurate positioning information (*Pole Star Confirms GPS Interference Caused MSC ANTONIA Grounding*, n.d.). Additional primary sources included vessel tracking data from Automatic Identification System (AIS) networks. Analysis of AIS data by Lloyd's List Intelligence shows that Stena Impero fitted the pattern (*Seized UK Tanker Likely 'Spoofed' by Iran :: Lloyd's List*, n.d.) for a spoofing attack when it was seized by the Islamic Revolutionary Guard Corps.

### 2.3.2 Secondary Data Sources

Secondary sources included intelligence assessments from governmental and commercial maritime security organizations, technical specifications for navigation systems, academic literature on GNSS vulnerabilities and electronic warfare capabilities, and open-source intelligence reports on regional security developments. The U.S. Department of Transportation's Maritime Administration issued an advisory to ships traveling in the Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea and Red Sea, documenting official recognition of GPS interference threats (*2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and Its Proxies | MARAD*,

n.d.). Additionally, reports from the United Kingdom Maritime Trade Operations (UKMTO) and the International Maritime Organization's Maritime Safety Committee provided supplementary documentation of regional GPS interference patterns (International Maritime Organization, 2021; UKMTO, 2025).

## **2.4 Analytical Framework**

The analytical framework integrated technical, operational, and strategic dimensions of GPS spoofing incidents. Technical analysis examined spoofing methodologies through assessment of signal characteristics, positioning accuracy degradation patterns, and system response behaviors, incorporating comparative analysis with documented interference patterns in the Baltic Sea to establish baseline signatures for state-level electronic warfare capabilities. GPS spoofing occurs when false GPS signals are transmitted to mislead navigational systems; shipboard systems lock on to the false signal and if not identified by the bridge watch keeper, these can lead to a loss of situational awareness, navigational errors and increased risk of maritime accidents (Radoš et al., 2024).

Operational analysis evaluated immediate impacts on vessel operations, crew responses, and broader maritime traffic patterns across multiple theaters including the Red Sea, Persian Gulf, and Baltic regions. Strategic analysis considered broader geopolitical contexts through examination of regional security dynamics, proxy force capabilities, and state-level electronic warfare programs, with particular attention to convergent patterns between Russian operations in the Baltic and Iranian-affiliated activities in Middle Eastern waterways.

## **2.5 Data Validation and Triangulation**

Multiple data sources were utilized to validate findings and ensure analytical rigor. Technical findings were corroborated through independent analysis by multiple maritime intelligence firms and cross-regional comparison with documented GPS interference incidents in the Baltic Sea, where systematic jamming and spoofing operations have been extensively documented since 2022. Cross-theater pattern validation, comparing spoofing signatures and operational characteristics between Baltic, Red Sea, and Persian Gulf incidents, strengthened attribution assessments and established the global scope of maritime GPS spoofing as a systematic strategic threat rather than isolated regional phenomena.

## **2.6 Ethical Considerations and Limitations**

Research procedures adhered to established ethical guidelines for security studies research. The research focused on publicly available information and analytical conclusions derived from open sources. Limitations include restricted access to classified intelligence assessments, limited availability of detailed technical data from affected vessels due to commercial sensitivity, and temporal constraints limiting follow-up analysis of long-term impacts. Additionally, the rapidly evolving nature of electronic warfare capabilities means that technical assessments may not capture the most recent developments in spoofing methodologies.

## 3. Results

### 3.1 Technical Analysis Findings

#### 3.1.1 GPS Spoofing Methodologies and Escalation

Analysis reveals significant escalation in GPS spoofing capabilities and impacts over recent years. According to Windward's data, the average distance vessels "jump" to when their AIS is jammed grew dramatically from 600km in Q4 2024 to 6,300km in Q1 2025, representing not merely growing frequency but technological sophistication advancement. The Red Sea area, particularly near Sudan, has become a major hotspot, with more than 180 vessels affected in Q1 2025 alone (*Top 5 Geopolitical Disruptions – Q1 2025*, n.d.). This geographic concentration and impact scale indicate systematic rather than opportunistic operations.

The technical characteristics of observed spoofing attacks suggest deployment of software-defined radio (SDR) platforms capable of generating GPS-like signals with sufficient power to overwhelm authentic satellite signals. Modern spoofing systems can gradually shift reported positions to avoid abrupt changes that might alert watchkeepers, while more aggressive attacks create instantaneous position jumps that can displace vessel positions by thousands of kilometers. Both methodologies have been observed in the documented incidents, suggesting adversaries possess versatile capabilities adaptable to different operational objectives.

#### 3.1.2 Sophisticated Attack Methodologies

Technical analysis of the MSC ANTONIA incident reveals deployment of sophisticated spoofing techniques. Maritime intelligence firms quickly identified GPS spoofing as the probable cause of the grounding. Windward reported that the Antonia's navigational data showed clear indicators consistent with spoofing activity before the incident (*Russian GPS Games in the Baltic Sea Region - Jamestown*, n.d.), involving gradual position manipulation designed to avoid detection while achieving operational effects. This pattern indicates technological advancement enabling more precise and effective position manipulation compared to earlier documented incidents.

#### 3.1.3 Detection Challenges and System Vulnerabilities

The incidents reveal fundamental detection challenges in current maritime systems. While Bomgardner noted that the MSC ANTONIA jamming incident was characterized as relatively basic compared to other recent attacks, he stressed that electronic warfare of any complexity level poses significant risks. Even relatively simple spoofing operations can achieve significant operational impacts against current maritime navigation architectures. Existing shipboard systems may lack built-in alerting mechanisms to distinguish authentic satellite signals from spoofed ones. In contested regions, bridge crews may face additional challenges in interpreting conflicting position information without immediate indicators of signal compromise, highlighting fundamental architectural vulnerabilities in current navigation system designs.

## 3.2 Incident Analysis Results

### 3.2.1 MSC ANTONIA Grounding (May 2025)

On May 10, 2025, the 7,000 TEU container ship MSC Antonia ran aground near the Eliza Shoals south of Jeddah Port in the Red Sea. The vessel, flagged in Liberia and operated by MSC, was transiting from Marsa Bashayer, Sudan, to Jeddah when it deviated from its intended course and grounded in shallow waters. This incident represents the most significant documented case of GPS spoofing directly causing a maritime casualty (*MSC-Operated Boxship Runs Aground off Jeddah :: Lloyd's List*, n.d.).

Satellite imagery and AIS data showed the ship's track making sudden abrupt positional discontinuities and course deviations near the shoals before stalling in shallow water, providing technical evidence of navigation system compromise preceding the grounding (*MSC Containership Aground in Red Sea Is a Possible Victim of GPS Jamming*, n.d.). The operational impact extended beyond the immediate casualty. While the grounding itself did not block the main shipping lane to Jeddah, it strained salvage resources and raised insurance concerns. Cargo interests were advised to notify claim agents immediately, as general average declarations became likely. The incident demonstrated how GPS spoofing can create cascading operational and economic impacts throughout maritime supply chains (*GPS Spoofing Suspected in Containership's Grounding Near Jeddah Port*, n.d.; *MSC Container Ship Stranded In Red Sea After Suspected GPS Spoofing*, n.d.).

### 3.2.2 Stena Impero Seizure (July 2019)

The UK-flagged product tanker was seized by Iranian forces on July 19, 2019, in what was widely regarded as retaliation for the impounding of the Iranian-controlled very large crude carrier Grace 1 in waters off Gibraltar on July 4. However, technical analysis reveals sophisticated GPS manipulation preceding the seizure.

Analysis of AIS data by Lloyd's List Intelligence shows that Stena Impero fitted the pattern for a spoofing attack. Evidence appears to show that the vessel received "spoofed" Automatic Identification System signals, sending it off course into Iranian waters as it transited the Strait of Hormuz. Lloyd's List Intelligence analysis revealed anomalous messages. The messages contradicted the speed and trajectory of the vessel and were therefore discarded.

The incident demonstrates evolution from GPS spoofing as standalone capability to integration within broader operational frameworks. Cybersecurity experts assessed the incident as a clear case of state-sponsored GPS spoofing.

### 3.2.3 Additional Documented Incidents

Beyond the primary cases, numerous additional incidents corroborate the systematic nature of GPS spoofing threats. In the Black Sea, vessels have reported GPS systems showing positions miles inland (Graham, 2011; *Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025 | GPSPATRON.Com*,

n.d.), demonstrating the geographic scope of the phenomenon. Ships operating near Russian-controlled Crimea have experienced persistent navigation anomalies attributed to electronic warfare systems deployed in the region. In Chinese coastal waters, fishing vessels and commercial ships have reported GPS interference events, though attribution remains more challenging due to multiple potential sources including military exercises and alleged illicit activities.

## 3.3 Geopolitical Pattern Analysis

### 3.3.1 Geographic Distribution and Strategic Targeting

Analysis reveals systematic targeting of strategic maritime chokepoints and approaches. Risk Intelligence reports that spoofing capabilities have become more advanced and now affect not only the Red Sea but also the Baltic, Eastern Mediterranean, Black Sea, Persian Gulf, Gulf of Aden, and China's coastal waters (*Maritime Navigation Under Threat: GFSS Spoofing*, n.d.). The geographic distribution of incidents correlates strongly with regions of geopolitical tension and strategic competition, suggesting coordinated deployment rather than random occurrence.

Recent instances where GPS interference served as a defensive measure against drone and missile threats targeting critical infrastructure include the Israeli coast and the Red Sea during the Israel-Hamas conflict as well as the Persian Gulf and Arabian Gulf. The Bab el-Mandeb Strait, connecting the Red Sea to the Gulf of Aden, has experienced particularly intense spoofing activity coinciding with Houthi attacks on commercial shipping since late 2023. Similarly, the Turkish Straits and approaches to the Black Sea have shown increased interference patterns correlated with the Russia-Ukraine conflict. This pattern indicates systematic deployment as component of broader regional conflict strategies rather than isolated technical phenomena.

### 3.3.2 State-Level Attribution and Capability Assessment

Evidence points to state-level involvement in systematic GPS spoofing operations. According to U.S. intelligence assessments reported by CNN, Iran has placed GPS jammers on Iran-controlled Abu Musa Island (*Iran Spoofing Ship GPS Signals, Warns US :: Lloyd's List*, n.d.), which lies in the Persian Gulf close to the entrance of the Strait of Hormuz. Iran's goal is for ships and aircraft to wander into Iranian waters or airspace, justifying a seizure. The capability requirements suggest advanced state-sponsored programs rather than ad hoc operations.

Similarly, the increase in GPS and AIS spoofing and jamming in the Baltic Sea is part of a broader Russian strategy of hybrid warfare directed against the West. Since 2022 (Solli, 2024), extensive interference has been documented affecting civilian aviation and maritime traffic in the Baltic region, with operational patterns suggesting coordination with broader geopolitical objectives. Russian electronic warfare units have demonstrated sophisticated capabilities including the Krasukha-4 and Tirada-2 systems (*Electronic Warfare in Ukraine - Joint Air Power Competence Centre*, n.d.), originally developed for military applications but now apparently adapted for use against civilian infrastructure.

## 3.4 Vulnerability Assessment Results

### 3.4.1 Navigation System Architecture Weaknesses

Current maritime navigation systems exhibit fundamental vulnerabilities to GPS spoofing attacks. Most commercial vessels rely heavily on GNSS as their primary position source (Androjna et al., 2020), often without cross-verification from radar, visual bearings, or inertial navigation. This excessive dependence creates single points of failure that sophisticated spoofing can exploit. High-profile spoofing incidents have been reported in the Black Sea, where ships' GPS systems showed them located miles inland (*Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025* | GPSPATRON.Com, n.d.), demonstrating the global scope of navigation system vulnerabilities. The integration of GPS into virtually all bridge systems—from ECDIS to AIS to autopilot—means that a single corrupted GPS signal can cascade through multiple critical navigation functions.

### 3.4.2 Detection and Response Inadequacies

Analysis reveals significant gaps in spoofing detection capabilities and response procedures. Compliance professionals face challenges in verifying vessel movements accurately because of GPS jamming and spoofing, making it harder to detect illicit activities such as sanctions-busting (*The Real Impact of GPS Jamming on Maritime Operations*, n.d.). Multiple instances of GNSS signal spoofing have illustrated that such manipulations can be executed even with inexpensive equipment and minimal expertise (Radoš et al., 2024), reducing the threshold for malicious attacks with potentially severe repercussions. This accessibility concern indicates potential for threat proliferation beyond state actors to include criminal organizations and terrorist groups.

### 3.4.3 Training and Procedural Deficiencies

Current maritime training and procedures inadequately address GPS spoofing threats. Aviation industry professionals have noted the disparity between sectors (*IMarEST | The Potentially Catastrophic Threat of GPS Spoofing in Shipping*, n.d.). Maritime cybersecurity specialists have highlighted the absence of robust cyber defenses. This represents a fundamental gap in maritime cybersecurity preparedness for electronic warfare scenarios (Greene & David, 1984).

## 3.5 Impact Assessment Results

### 3.5.1 Operational and Economic Impacts

GPS spoofing operations create significant operational disruption and economic costs across the maritime industry. Navigation disruptions from jamming and spoofing interfere with the accuracy of navigational systems, leading to potential misrouting, collisions, and grounding of vessels (Cichocki & Wójcik, 2025). The MSC ANTONIA grounding alone resulted in salvage operations costing millions of dollars, cargo delays affecting hundreds of containers, and potential general average declarations that distribute losses across all cargo interests. Operational delays caused by navigation system disruptions

affect the timely delivery of goods, leading to increased operational costs and economic losses for shipping companies. The just-in-time supply chain models prevalent in modern manufacturing are particularly vulnerable to such delays.

The heightened risk of accidents and the potential for cargo loss or damage due to navigation errors have led to increased insurance premiums for vessels operating in affected areas. War risk insurance premiums for Red Sea transits increased substantially following the escalation of Houthi attacks and associated GPS interference (*GPS Jamming, Spoofing and Hacking* | NorthStandard | Marine Insurance, n.d.), with some insurers adding specific exclusions or conditions related to electronic warfare threats. Industry estimates suggest that GPS spoofing incidents have contributed to additional insurance costs exceeding tens of millions of dollars annually across the global fleet operating in high-risk regions. Furthermore, some vessel operators have chosen to reroute around affected areas entirely, adding thousands of nautical miles and days to voyages, with corresponding increases in fuel costs, crew expenses, and schedule disruption.

### **3.5.2 Strategic and Security Implications**

The strategic implications extend beyond individual operational impacts. The goals of electronic warfare campaigns against maritime targets likely include undermining alliance cohesion by disrupting navigation systems and creating uncertainty, testing response capabilities and unity, and eroding confidence in the ability to protect member states and maintain secure navigation routes (Ertan et al., 2020). Additionally, targeting commercial maritime traffic through electronic warfare serves as a tactic to create economic instability without direct military confrontation. Regional trade flows have remained on edge, with UKMTO continuing to publish navigation alerts and merchant ships increasing reliance on alternative navigation methods when GPS data appears unreliable.

## **4. Discussion**

### **4.1 Technical Evolution and Capability Advancement**

The findings demonstrate that maritime GPS spoofing has evolved significantly beyond theoretical vulnerability to become a sophisticated operational capability with documented strategic impacts. The ten-fold increase in spoofing range capabilities between Q4 2024 and Q1 2025 represents unprecedented technological advancement in electronic warfare capabilities deployed against civilian maritime targets. This evolution suggests systematic investment and development rather than ad hoc capability deployment, indicating state-level resources and planning.

The worst-case scenario of maritime GPS spoofing could be a large-scale, coordinated attack that disrupts global shipping lanes, ports and naval operations, leading to severe economic, environmental and geopolitical consequences (Tsailas, 2025). The sophistication observed, particularly the coordination between electronic warfare and conventional maritime enforcement in the Stena Impero

case, indicates integration of spoofing within broader operational frameworks rather than standalone capability deployment.

## 4.2 Evolution from Military to Hybrid Warfare Applications

The findings demonstrate a concerning evolution of electronic warfare capabilities from traditional military applications to hybrid warfare targeting civilian maritime infrastructure. The historical development of electronic warfare—from its earliest documented use during the Second Boer War of 1899–1902 when the British Army used searchlights to signal and the Boers attempted to jam those signals, through World War II's "Battle of the Beams" involving navigational radar interference, to modern sophisticated systems—demonstrates continuous advancement of EW capabilities (Adamy, 2015).

The transition of military electronic warfare technologies to civilian targets represents a fundamental shift in hybrid warfare strategies. During the Russia-Ukraine conflict, Russian forces employed systems like Krasukha-4 and Tirada-2 to spoof GNSS signals (*Electronic Warfare in Ukraine - Joint Air Power Competence Centre*, n.d.), confusing drones, missiles, and aircraft. The Russian Army deployed their first land-based multifunctional electronic warfare system known as Borisoglebsk 2 in December 2010, intended to suppress mobile satellite communications and satellite-based navigation signals. The adaptation of such military systems for use against civilian maritime targets demonstrates the blurring of distinctions between military and civilian targets in contemporary hybrid warfare.

## 4.3 Geopolitical Context and Strategic Implementation

The geographic and temporal correlation of GPS spoofing incidents with regional conflicts and strategic competition indicates systematic rather than opportunistic deployment. Far from being a theoretical concern, recent incidents in geopolitical conflict zones have underscored the very real and immediate dangers posed by compromised global navigational satellite systems (Sabanadze & Galip, 2025; Zorri & Kessler, 2024).

GPS spoofing is not only a technical anomaly but could be a powerful tool of asymmetric or electronic warfare, capable of misleading aircraft, disrupting airspace surveillance, and endangering civilian lives while undermining national security without direct confrontation (*How Russia Is Jamming GPS around Europe* / *Royal United Services Institute*, n.d.; Zorri & Kessler, 2024). The capability transfer to proxy forces, particularly evident in Red Sea operations, represents significant development in hybrid warfare methodology, providing strategic advantages including enhanced deniability, reduced escalation risk, and ability to maintain continuous pressure without committing state military assets.

## 4.4 Systemic Vulnerabilities and Detection Challenges

The vulnerability assessment reveals how the attitude of industry prioritization of cost reduction through technology adoption and crew minimization has created vulnerabilities that sophisticated adversaries can systematically exploit. The excessive dependence on GPS technology, combined with inadequate backup systems and detection capabilities, creates critical single points of failure throughout maritime operations. Unmanned vessels relying on GNSS lacking real-time human intervention face heightened

risks from spoofing attacks, as they may struggle to verify their positions and react promptly (Androjna et al., 2020; Cichocki & Wójcik, 2025).

Most spoofing is carried out by states, although in Southeast Asia and the Red Sea, pirates are using rudimentary spoofing systems bought on the internet to direct ships to danger areas (*GNSS Spoofing Threat in China and beyond / Maritime Security*, n.d.), indicating both state-level sophistication and concerning proliferation of military-derived technologies to criminal actors. Traditional navigation methods such as radar and inertial navigation can provide some level of redundancy, but they are not foolproof against coordinated electronic warfare attacks. Electronic warfare support (ES)—involving actions taken to detect, intercept, identify, locate, and localize sources of electromagnetic energy—is virtually absent in civilian maritime operations (Beckman et al., 2025).

## 4.5 Strategic Implications and Escalation Potential

The strategic implications extend beyond individual incidents to encompass broader threats to maritime security architecture and global supply chain reliability. A single compromised vessel could block a port, create an environmental disaster, or disrupt global trade—as demonstrated by the Ever Given incident in the Suez Canal in 2021. That incident, caused by natural factors, blocked one of the world's most critical waterways for six days and disrupted an estimated \$9.6 billion in trade daily (*Suez Blockage Is Holding up \$9.6bn of Goods a Day*, n.d.). A deliberate GPS spoofing attack designed to cause a similar blockage at a strategic chokepoint could have even more severe consequences, particularly if combined with additional attacks or timed to coincide with geopolitical tensions.

The integration of advanced electronic warfare capabilities into hybrid warfare strategies creates new categories of asymmetric threat that existing international frameworks struggle to address. GPS spoofing exists in a gray zone between acts of war and acceptable peacetime activities, allowing state actors to maintain plausible deniability while achieving strategic effects. The lack of clear international norms regarding electronic interference with civilian navigation systems creates ambiguity that sophisticated adversaries exploit.

The development of cognitive electronic warfare (CEW), utilizing AI in electronic warfare systems, represents the next evolution of threats that civilian maritime systems will face. CEW can improve situation-assessment and electronic support measures through automatic detection and classification of new signals, potentially making military-grade electronic warfare even more effective against civilian targets. Machine learning algorithms could enable spoofing systems to adapt to countermeasures in real-time, creating an escalating technological competition between attackers and defenders. The escalation potential is particularly concerning given demonstrated capabilities could potentially be deployed in more critical maritime chokepoints during periods of heightened international tension.

## 4.6 Comparative Analysis: Aviation vs. Maritime Approaches

The contrast between aviation and maritime approaches to GPS spoofing threats provides important insights for countermeasure development. The aviation industry has developed comprehensive protocols for GPS spoofing recognition and response, including mandatory crew training, multiple backup navigation systems, and ground-based radio navigation stations. Commercial aircraft routinely carry inertial navigation systems (INS), VOR/DME receivers, and are supported by ground-based radar systems that provide independent position verification. Pilots receive specific training in recognizing GPS anomalies and have established procedures for reverting to alternative navigation methods when GPS integrity is compromised.

In contrast, the maritime industry has been slower to adopt equivalent safeguards. While SOLAS regulations require vessels to carry multiple navigation systems, the practical reliance on GNSS has increasingly marginalized traditional navigation skills and equipment. Many modern seafarers have limited experience with celestial navigation, radar-based position fixing, or visual pilotage techniques that were standard practice before GPS ubiquity. The European Union Aviation Safety Agency (EASA) has issued multiple safety bulletins on GNSS interference in European airspace, particularly affecting the Baltic and Eastern Mediterranean regions, demonstrating proactive regulatory response that the maritime sector has yet to match (*Global Navigation Satellite System (GNSS) Outages and Alterations* / EASA, n.d.).

The aviation industry's experience with GPS interference in conflict zones, particularly over Eastern Europe and the Middle East, has driven rapid adaptation of procedures and equipment. Airlines operating in affected areas have implemented enhanced navigation monitoring protocols and increased reliance on inertial reference systems. The maritime industry could benefit significantly from studying aviation's response to similar threats and adapting relevant practices for shipboard implementation, recognizing the different operational constraints and capabilities of vessels compared to aircraft.

## 4.7 Future Threat Landscape

The threat landscape for maritime GPS spoofing is likely to continue evolving in the coming years. The proliferation of software-defined radio (SDR) technology has dramatically reduced the cost and complexity of GPS spoofing equipment, enabling a wider range of actors to develop offensive capabilities (Radoš et al., 2024). Academic research has demonstrated that effective GPS spoofers can be constructed for a few hundred dollars using commercially available components, lowering the barrier to entry for criminal organizations and terrorist groups.

The increasing autonomy of maritime systems presents additional concerns. Autonomous and remotely operated vessels, currently in development and early deployment phases, lack the human judgment and situational awareness that can identify spoofing anomalies. These vessels rely entirely on electronic systems for navigation, creating potential for catastrophic consequences if those systems are compromised. As the maritime industry moves toward greater automation, the importance of spoofing-resistant navigation architectures will only increase.

## 5. Countermeasures and Recommendations

### 5.1 Technical Countermeasures

A multi-layered approach to technical countermeasures is essential for ensuring operational continuity and security against GPS spoofing threats. Multi-constellation GNSS receivers utilizing GPS, Galileo, GLONASS, and BeiDou simultaneously can provide cross-validation of position data, making spoofing significantly more difficult as attackers would need to simultaneously spoof multiple satellite constellations operating on different frequencies and signal structures. Advanced anti-spoofing receivers capable of detecting signal anomalies through analysis of signal characteristics, carrier phase measurements, and signal power levels offer another layer of protection. These receivers can identify inconsistencies between expected and received signal parameters that indicate potential spoofing attempts (Radoš et al., 2024).

The revival of enhanced Long Range Navigation (eLoran) as a terrestrial backup to satellite-based navigation offers robust resistance to GPS spoofing due to its high signal power and ground-based transmission. Unlike GPS signals, which arrive at receivers with extremely low power levels easily overwhelmed by spoofing transmitters, eLoran signals are approximately one million times stronger (*US Weighs UAS-Friendly GPS Backup System - Inside Unmanned Systems*, n.d.), making them virtually impossible to spoof with portable equipment. Several nations including the United Kingdom, South Korea, and Russia have maintained or expanded eLoran infrastructure specifically as a GPS backup for maritime navigation (*Back To The Future: LORAN – IFATCA*, n.d.).

Integration of inertial navigation systems (INS) with GNSS receivers enables position continuity during GPS outages and provides anomaly detection capability when INS-derived positions diverge from GPS-reported positions. Modern fiber-optic gyroscope and ring laser gyroscope INS units can maintain navigational accuracy for extended periods without external updates, though cost remains a barrier to widespread adoption on commercial vessels. Radar-based positioning using shore-based radar stations and shipborne radar can provide independent position verification in coastal waters and port approaches. Additionally, the emerging field of quantum navigation based on cold atom interferometry may offer future spoofing-resistant positioning capabilities independent of external signals (Geiger et al., 2020).

### 5.2 Procedural and Training Improvements

Enhanced crew training programs should incorporate GPS spoofing recognition and response procedures as mandatory competencies within STCW certification frameworks. Bridge teams must be trained to recognize spoofing indicators including sudden position jumps, inconsistencies between GPS and radar returns, compass anomalies, and implausible vessel speeds or courses. Training should include practical exercises using spoofing simulators that allow watchkeepers to experience navigation system anomalies in controlled environments before encountering them at sea. Standard operating

procedures should mandate cross-verification of GPS positions using radar, visual bearings, and depth soundings when transiting high-risk areas.

Voyage planning should incorporate GPS interference risk assessments for transits through identified high-risk areas, with pre-planned alternative navigation strategies and waypoints verified through multiple sources. Masters and navigation officers should develop contingency plans for GPS denial scenarios, including predetermined radar conspicuous navigation marks and visual pilotage routes. Bridge resource management training should emphasize maintaining situational awareness independent of electronic systems and the importance of challenging anomalous navigation data. The traditional skills of celestial navigation, while not practical for precision pilotage, should be retained as emergency backup capabilities.

Companies should establish clear reporting protocols for suspected GPS spoofing incidents, ensuring that observations are documented and shared with relevant authorities and industry organizations. Post-incident analysis should be incorporated into safety management systems to capture lessons learned and improve response procedures. Regular drills simulating GPS failure or spoofing scenarios should be incorporated into shipboard emergency training programs alongside existing drills for fire, collision, and abandon ship procedures.

## **5.3 Regulatory and Policy Reforms**

The International Maritime Organization (IMO) should consider amendments to SOLAS Chapter V to mandate carriage requirements for GPS spoofing detection equipment on vessels transiting identified high-risk areas (International Maritime Organization (, 1974). Current SOLAS requirements for navigation systems were developed before GPS spoofing emerged as a significant threat and do not adequately address electronic warfare vulnerabilities. Updates to the International Ship and Port Facility Security (ISPS) Code should incorporate electronic warfare threats within the maritime security framework, requiring ship security assessments to address navigation system vulnerabilities and port facility security plans to consider the potential for spoofing attacks affecting vessels in approaches and harbor areas.

National maritime authorities should establish GPS interference reporting requirements and develop shared databases of spoofing incidents to enable pattern analysis and early warning capabilities. The existing voluntary reporting frameworks through organizations like UKMTO should be formalized and expanded to create comprehensive global coverage. Classification societies should develop notations for vessels equipped with enhanced spoofing detection and resilient navigation capabilities, potentially enabling insurance premium reductions that incentivize adoption.

International cooperation mechanisms should be strengthened to address state-sponsored GPS spoofing as a violation of international law, particularly the UN Convention on the Law of the Sea provisions regarding freedom of navigation and safety of life at sea. The deliberate interference with navigation systems that endangers vessels could constitute a violation of UNCLOS Article 94 obligations

regarding flag state duties for safety at sea (United Nations Convention on the Law of the Sea (UNCLOS), 1982). Diplomatic channels should be utilized to raise GPS spoofing as a matter of international concern, potentially leading to new international instruments specifically addressing electronic interference with civil navigation systems. Flag states should consider requiring spoofing detection capabilities as conditions of vessel registration for ships trading in high-risk regions.

## 6. Conclusions

This research has demonstrated that GPS spoofing has evolved from a theoretical vulnerability to an operational weapon systematically deployed within hybrid warfare strategies targeting maritime chokepoints. Analysis of the MSC ANTONIA grounding and Stena Impero seizure provides compelling evidence that state actors are utilizing advanced electronic warfare capabilities against civilian maritime targets to achieve strategic objectives while maintaining plausible deniability. The sophistication and coordination observed in these incidents indicate deliberate strategic planning rather than opportunistic attacks.

The ten-fold increase in spoofing effectiveness observed between late 2024 and early 2025 indicates accelerating technological advancement and systematic investment in offensive capabilities. The geographic scope of documented incidents—spanning the Red Sea, Persian Gulf, Baltic Sea, Black Sea, and Eastern Mediterranean—demonstrates that GPS spoofing has become a global maritime security threat rather than an isolated regional phenomenon. The convergent patterns observed across these geographically distinct theaters, combined with the technical sophistication required, point to state-level programs with significant resources and strategic intent.

Critical vulnerabilities in current maritime navigation systems—including excessive GNSS dependence, inadequate detection capabilities, and insufficient crew training—create systemic exposure that sophisticated adversaries can exploit. The maritime industry's pursuit of efficiency through technology adoption and crew reduction has inadvertently created single points of failure that undermine resilience. The contrast with aviation industry practices, where multi-layered navigation redundancy and comprehensive crew training for GPS anomalies are standard, demonstrates that effective countermeasures exist but have not been adequately adopted in the maritime sector.

The strategic implications extend beyond operational disruption to encompass threats to global supply chain reliability, alliance cohesion, and international maritime order. Maritime commerce depends fundamentally on the freedom of navigation and the reliability of position, navigation, and timing services. The weaponization of GPS spoofing against civilian vessels represents a direct challenge to these foundations of the international maritime system. The proliferation of spoofing capabilities to non-state actors and criminal organizations further compounds these concerns, suggesting the threat will continue to expand.

If the maritime community waits for a high-profile disaster before it decides to act, it will be too late. A proactive, layered, and globally coordinated response is not just preferable—it is imperative. This

response must encompass technical countermeasures including multi-constellation GNSS receivers, eLoran backup systems, and integrated INS solutions; enhanced crew training and procedural reforms that restore traditional navigation skills alongside electronic systems; and regulatory updates through IMO instruments that address this evolving threat. Future research should prioritize development of real-time spoofing detection algorithms, assessment of cognitive electronic warfare implications for maritime systems, comprehensive economic impact analysis to support evidence-based policy development, and exploration of emerging technologies such as quantum navigation that may provide inherently spoofing-resistant positioning capabilities.

## Declarations

## Author Contribution

E.R.D. conceived the study, developed the analytical framework, conducted the research, and wrote the main manuscript text. M.S. and J.M.P. contributed to the geopolitical analysis and provided critical review of the hybrid warfare framework. J.I.A. contributed to the maritime security assessment and reviewed the policy recommendations. All authors reviewed and approved the final manuscript.

## Data Availability

This research is based exclusively on publicly available open-source data and does not involve the collection or generation of proprietary datasets. The primary data sources underpinning the analysis are as follows:

(1) AIS vessel tracking data and incident analyses published by maritime intelligence platforms, including Windward, whose specific reports are available at [https://windward.ai/knowledge-base/top-5-geopolitical-disruptions-q1-2025/#gps\\_jamming](https://windward.ai/knowledge-base/top-5-geopolitical-disruptions-q1-2025/#gps_jamming) and <https://windward.ai/blog/gps-jamming-is-now-a-mainstream-maritime-threat/>; MarineTraffic (<https://www.marinetraffic.com>), a real-time vessel tracking platform providing Automatic Identification System data whose vessel movement records do not generate permanent URLs; and Pole Star Global, whose analysis of the MSC ANTONIA incident is documented at <https://gcaptain.com/pole-star-confirms-gps-interference-caused-msc-antonia-grounding/>;

(2) incident documentation and technical analysis published by Lloyd's List Intelligence, including specific reports available at <https://www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran>, <https://www.lloydslist.com/LL1153446/MSC-operated-boxship-runs-aground-off-Jeddah>, and <https://www.lloydslist.com/LL1128704/Iran-spoofing-ship-GPS-signals-warns-US>;

(3) official maritime advisories issued by the United States Maritime Administration (MARAD), specifically available at <https://www.maritime.dot.gov/msci/2019-012-persian-gulf-strait-hormuz-gulf->

oman-arabian-sea-red-sea-threats-commercial-vessels, and the United Kingdom Maritime Trade Operations (UKMTO), available at <https://www.ukmto.org>;

(4) safety documentation from the International Maritime Organization (IMO), specifically circular MSC.1/Circ.1644 on deliberate interference with GNSS, available through the IMO document repository at [https://rntfnd.org/wp-content/uploads/IMO-Circular-MSC.1-Circ.1644-Deliberate-Interference-With-The-United-States-Global-Positioning-System-Gps-And-Other...-Secretariat.pdf\\_safe.pdf](https://rntfnd.org/wp-content/uploads/IMO-Circular-MSC.1-Circ.1644-Deliberate-Interference-With-The-United-States-Global-Positioning-System-Gps-And-Other...-Secretariat.pdf_safe.pdf);

(5) peer-reviewed academic literature and open-source intelligence reports cited fully in the reference list.

All cited sources are identified in the manuscript references and can be accessed through their respective publishers or institutional repositories. No restricted, classified, or proprietary data were used. There are no obstacles to the transparency of the data sources underpinning this research.

## References

1. Spezio AE. Electronic warfare systems. *IEEE Trans Microw Theory Tech.* 2002;50(3):633–44.
2. Grant PM, Collins JH. Introduction to electronic warfare. In: *IEE Proceedings F (Communications, Radar and Signal Processing)*. IET; 1982. p. 113–32.
3. Androjna A, Brcko T, Pavic I, Greidanus H. Assessing cyber challenges of maritime navigation. *J Mar Sci Eng.* 2020;8(10):776.
4. Electromagnetic warfare | NATO Topic [Internet]. [cited 2025 Nov 20]. Available from: <https://www.nato.int/en/what-we-do/deterrence-and-defence/electromagnetic-warfare>
5. MSC Antonia Grounding in the Red Sea Attributed to Suspected GNSS Spoofing - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design [Internet]. [cited 2025 Nov 20]. Available from: <https://insidegnss.com/msc-antonia-grounding-in-the-red-sea-attributed-to-suspected-gps-spoofing/>
6. Seized UK tanker likely 'spoofed' by Iran :: Lloyd's List [Internet]. [cited 2025 Nov 20]. Available from: <https://www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran>
7. Hoffman FG. Hybrid warfare and challenges. In: *Strategic studies*. Routledge; 2014. p. 329–37.
8. Hunter E, Pernik P. The challenges of hybrid warfare. *JSTOR*; 2015.
9. Deitchman SJ. The "Electronic Battlefield" in the Vietnam War. *J Mil Hist.* 2008;72(3):869–87.
10. Follath E, Stark H. How Israel Destroyed Syria's Al Kibar Nuclear Reactor. *Spiegel Online.* 2009;11:22–6.
11. Willett M. The cyber dimension of the Russia–Ukraine war. In: *Survival: October–November 2022*. Routledge; 2023. p. 7–26.
12. Maritime Dangers of GPS/AIS Spoofing and Jamming in the Baltic Sea [Internet]. [cited 2025 Nov 20]. Available from: <https://www.riskintelligence.eu/analyst-briefings/maritime-dangers-of-gps/ais->

spoofing-and-jamming-in-the-baltic-sea

13. Sensors on the Baltic Frontline - CEPA [Internet]. [cited 2025 Nov 20]. Available from: <https://cepa.org/article/sensors-on-the-baltic-frontline/>
14. IMarEST | The potentially catastrophic threat of GPS spoofing in shipping [Internet]. [cited 2025 Nov 20]. Available from: <https://www.imarest.org/resource/mp-the-potentially-catastrophic-threat-of-gps-spoofing-in-shipping.html>
15. K Robert Y. Case study research and applications design and methods. In Library of Congress Cataloging-in-Publication Data; 2018.
16. Adamy DL. Introduction to electronic warfare modeling and simulation. Vol. 2. SciTech Publishing; 2006.
17. Pole Star Confirms GPS Interference Caused MSC ANTONIA Grounding [Internet]. [cited 2025 Nov 20]. Available from: <https://gcaptain.com/pole-star-confirms-gps-interference-caused-msc-antonia-grounding/>
18. 012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and its Proxies | MARAD [Internet]. [cited 2025 Nov 20]. Available from: <https://www.maritime.dot.gov/msci/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels>
19. International Maritime Organization. Deliberate interference with the United States' Global Positioning System (GPS) and Gothen Global Navigation Satellite Systems (GNSS). London; 2021. Report No.: MSC.1/Circ.1644.
20. UKMT0. JMIC Weekly Dashboard for the Middle East. 2025. Report No.: Week 41-2025 (06 October – 12 October).
21. Radoš K, Brkić M, Begušić D. Recent advances on jamming and spoofing detection in GNSS. Sensors. 2024;24(13):4210.
22. Top 5 Geopolitical Disruptions – Q1 2025 [Internet]. [cited 2025 Nov 20]. Available from: [https://windward.ai/knowledge-base/top-5-geopolitical-disruptions-q1-2025/#gps\\_jamming](https://windward.ai/knowledge-base/top-5-geopolitical-disruptions-q1-2025/#gps_jamming)
23. Russian GPS Games in the Baltic Sea Region - Jamestown [Internet]. [cited 2025 Nov 20]. Available from: <https://jamestown.org/russian-gps-games-in-the-baltic-sea-region/>
24. MSC-operated boxship runs aground off Jeddah :: Lloyd's List [Internet]. [cited 2025 Nov 20]. Available from: <https://www.lloydslist.com/LL1153446/MSC-operated-boxship-runs-aground-off-Jeddah>
25. MSC Containership Aground in Red Sea is a Possible Victim of GPS Jamming [Internet]. [cited 2025 Nov 21]. Available from: <https://maritime-executive.com/article/msc-containership-aground-in-red-sea-is-a-possible-victim-of-gps-jamming>
26. MSC Container Ship Stranded In Red Sea After Suspected GPS Spoofing [Internet]. [cited 2025 Nov 21]. Available from: <https://www.marineinsight.com/shipping-news/msc-container-ship-stranded-in-red-sea-after-suspected-gps-spoofing/>

27. GPS Spoofing Suspected in Containership's Grounding Near Jeddah Port [Internet]. [cited 2025 Nov 21]. Available from: <https://gcaptain.com/gps-spoofing-suspected-in-containerships-grounding-near-jeddah-port/>
28. Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025 | GPSPATRON.com [Internet]. [cited 2025 Nov 20]. Available from: <https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/>
29. Graham A. Communications, radar and electronic warfare. John Wiley & Sons; 2011.
30. Maritime Navigation Under Threat: GFSS spoofing [Internet]. [cited 2025 Nov 20]. Available from: <https://www.riskintelligence.eu/analyst-briefings/maritime-navigation-under-threat>
31. Iran spoofing ship GPS signals, warns US :: Lloyd's List [Internet]. [cited 2025 Nov 21]. Available from: <https://www.lloydslist.com/LL1128704/Iran-spoofing-ship-GPS-signals-warns-US>
32. Solli PE. Differentiating Hybrid Threats against the High North and Baltic Sea regions. JSTOR; 2024.
33. Electronic Warfare in Ukraine - Joint Air Power Competence Centre [Internet]. [cited 2025 Nov 20]. Available from: <https://www.japcc.org/articles/electronic-warfare-in-ukraine/>
34. The Real Impact of GPS Jamming on Maritime Operations [Internet]. [cited 2025 Nov 20]. Available from: <https://windward.ai/blog/gps-jamming-is-now-a-mainstream-maritime-threat/>
35. Greene D, David JL. A research design for generalizing from multiple case studies. Eval Program Plann. 1984;7(1):73–85.
36. Cichocki R, Wójcik P. Cybersecurity in Maritime Transport Systems: Threats, Trends, and Countermeasures in the Last Decade. TransNav: International Journal on Marine Navigation & Safety of Sea Transportation. 2025;19(3).
37. GPS Jamming, Spoofing and Hacking | NorthStandard | Marine Insurance [Internet]. [cited 2025 Nov 21]. Available from: <https://north-standard.com/insights-and-resources/resources/articles/gps-jamming-spoofing-and-hacking>
38. Ertan A, Floyd K, Pernik P, Stevens T. Cyber Threats and NATO 2030: Horizon Scanning and Analysis [Internet]. 2020 [cited 2025 Nov 20]. Available from: [https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\\_Horizon-Scanning-and-Analysis.pdf](https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf)
39. Tsailas DN. RISKS AND THREATS IN THE 21ST CENTURY MARITIME SECURITY. Security Science Journal. 2025;6(1):106–44.
40. Adamy DL. EW 104: electronic warfare against a new generation of threats. Artech House; 2015.
41. Zorri DM, Kessler GC. Position, navigation, and timing weaponization in the maritime domain: Orientation in the era of great systems conflict. Joint Force Quarterly. 2024;112(1):3.
42. Sabanadze N, Galip D. Understanding Russia's Black Sea strategy. How to strengthen Europe and NATO's approach to the region [Internet]. 2025 [cited 2025 Nov 20]. Available from: [www.chathamhouse.org/sites/default/files/2025-07/2025-07-28-russias-black-sea-strategy-sabanadze-dalay.pdf](http://www.chathamhouse.org/sites/default/files/2025-07/2025-07-28-russias-black-sea-strategy-sabanadze-dalay.pdf)

43. How Russia is jamming GPS around Europe | Royal United Services Institute [Internet]. [cited 2025 Nov 20]. Available from: <https://www.rusi.org/news-and-comment/in-the-news/how-russia-jamming-gps-around-europe>
44. GNSS spoofing threat in China and beyond | Maritime security [Internet]. [cited 2025 Nov 20]. Available from: <https://www.riskintelligence.eu/background-and-guides/background-gnss-spoofing-in-china-and-beyond>
45. Beckman J, Carter CM, Diebold MC, Ghaffari R, Lonstein W, Malhotra V, et al. Connected, Complex, Compromised (Murthy & Ghaffari). MARITIME TRANSPORTATION SYSTEMS. 2025;
46. Suez blockage is holding up \$9.6bn of goods a day [Internet]. [cited 2025 Nov 21]. Available from: <https://www.bbc.com/news/business-56533250>
47. Global Navigation Satellite System (GNSS) Outages and Alterations | EASA [Internet]. [cited 2025 Nov 21]. Available from: <https://www.easa.europa.eu/en/domains/air-operations/global-navigation-satellite-system-outages-and-alterations>
48. US Weighs UAS-Friendly GPS Backup System - Inside Unmanned Systems [Internet]. [cited 2025 Nov 21]. Available from: <https://insideunmannedsystems.com/us-weighs-uas-friendly-gps-backup-system/>
49. Back To The Future: LORAN – IFATCA [Internet]. [cited 2025 Nov 21]. Available from: <https://ifatca.org/article/back-to-the-future-loran/>
50. Geiger R, Landragin A, Merlet S, Pereira Dos Santos F. High-accuracy inertial measurements with cold-atom sensors. AVS Quantum Science. 2020;2(2).
51. International Maritime Organization (. International Convention for the Safety of Life at Sea (SOLAS). London; 1974.
52. United Nations. United Nations Convention on the Law of the Sea (UNCLOS). United Nations; 1982.