Review

AIS Cybersecurity: Challenges, Vulnerabilities, and Mitigation Strategies

Silvie Levy *, Ehud Gudess , Danny Hendler

Posted Date: 14 May 2026

doi: 10.20944/preprints202605.0928.v1

Keywords: automatic identification system (AIS); maritime anomaly detection; maritime cyber challenges; maritime cyber security

 doi:10.20944/preprints202605.0928.v1

Review

AIS Cybersecurity: Challenges, Vulnerabilities, and Mitigation Strategies

Silvie Levy *, Ehud Gudess and Danny Hendler

Department of Computer Science, Ben-Gurion University of the Negev, Beersheba, Israel
* Correspondence: silvial@post.bgu.ac.il

Abstract

Maritime operations rely on the Automatic Identification System (AIS), an open broadcast protocol whose unauthenticated, self-reported Messages are easily abused. This survey takes an *AIS-first*, *security-focused* view, grounded in a comprehensive review of prior AIS-security research. We (i) explain how AIS works and use that to expose fundamental weaknesses; (ii) synthesize from the literature the main threats and their technical and operational impacts; (iii) categorize, from the surveyed works and operational practice, mitigations by the layers they target and, for each mitigation, indicate whether it primarily prevents, detects, responds, or supports recovery; and (iv) provide practical recommendations. Bringing together cybersecurity, maritime operations, and data-science perspectives, we consolidate recommendations for securing AIS-based systems and assess their current use in practice, thus highlighting the gaps that standards and implementations still need to address.

Keywords: automatic identification system (AIS); maritime anomaly detection; maritime cyber challenges; maritime cyber security

---

1. Introduction

Maritime operations depend on the Automatic Identification System (AIS) for collision avoidance, traffic management, and wide-area monitoring. Yet AIS is an open VHF broadcast of unauthenticated, self-reported data. Anyone within range can listen; with the right equipment, attackers can inject, alter, or suppress messages, and AIS's reliance on Global Navigation Satellite Systems (GNSS) makes it sensitive to spoofing and jamming. These weaknesses have safety, commercial, and geopolitical consequences: they can degrade bridge situational awareness, disrupt port and logistics flows, and enable sanctions evasion or misinformation.

This survey takes an AIS-first, security-focused view. Drawing on an extensive review of prior AIS-security research, standards, and incident reports, we synthesize and organize findings across the literature. We explain the protocol mechanics to surface first-principles weaknesses; map the threat surface, from on-air injection and GNSS spoofing/jamming to feed tampering and endpoint compromise; link these to technical and operational effects; and organize mitigations by the layers they target (protocol/crypto, endpoints & networks, analytics, and governance & resilience). For each mitigation, we note whether it primarily prevents, detects, responds, or supports recovery. We also summarize behavior-aware detection methods (including ML/statistical approaches) and cross-sensor checks with radar/EO and satellite AIS. Finally, we distill practical recommendations and point to where standards and implementations still need to catch up.

We combine specification-level review, bridge/shore operating practice, and detection/ML results from the literature to offer practical guidance, evaluate what is used today, and thus identify where standards and implementations fall short.

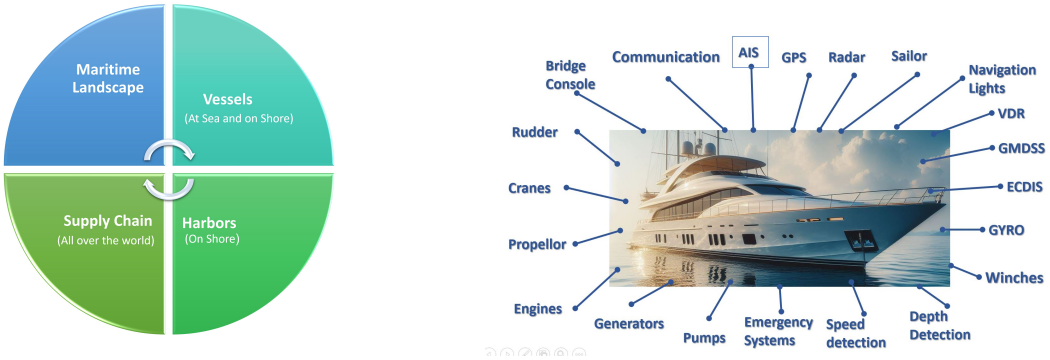
1.1. Maritime Landscape

The maritime domain represents a highly interconnected and multifaceted ecosystem that includes vessels (both at sea and docked), port infrastructure and logistics operations, the global cargo supply

 doi:10.20944/preprints202605.0928.v1

chain, and the shipping companies responsible for vessel ownership and operation [1]. As illustrated in Figures 1(**b**) - 1(**a**), this ecosystem presents an extensive and diverse attack surface. The accelerating digitalization of the maritime sector, driven by advancements in automation and the adoption of machine learning technologies, necessitates deeper integration between information technology (IT) and operational technology (OT) systems.

Figure 1(**b**) depicts typical onboard IT and OT devices, demonstrating how their interconnectivity extends the cyberattack surface to encompass vital functions across vessels, ports, and logistics networks, including navigation, communications, cargo handling, and booking/payment systems. This increasing reliance on internet-connected infrastructure, often operated by personnel with limited cybersecurity training and without comprehensive security evaluations, introduces substantial vulnerabilities to unauthorized access and cyberattacks targeting critical maritime systems [2]. Furthermore, inadequate cybersecurity measures place sensitive data, such as personal and operational information, at risk of exposure, raising serious concerns regarding adherence to data protection frameworks such as the European Union's General Data Protection Regulation (GDPR) [3].



(**a**) Maritime landscape with lanes and ports. (**b**) Onboard IT/OT devices and segments.

Figure 1. Maritime landscape and onboard IT/OT devices.

As the maritime industry undergoes rapid digitalization, operational efficiency improves, but so does its vulnerability to cyberattacks [4–6]. The consequences of successful cyberattacks can be severe, including disruptions to port operations, delays in cargo deliveries, supply chain vulnerabilities, environmental damage, and considerable financial losses. Several high-profile incidents illustrate the sector's susceptibility to such threats.

- 2023: A ransomware attack on DNV ShipManager, widely used for fleet management, forced a shutdown, affecting 1,000 vessels [7].

- 2021: Ransomware targeted Greek shipping companies via vulnerabilities in a major IT consulting firm, highlighting industry-wide risks [8].

- 2017: The NotPetya cyberattack severely disrupted Maersk's global operations, crippling 76 ports and 800 vessels, with financial damages exceeding 300 million [9–11].

These incidents highlight the growing sophistication of maritime cyberattacks and their far-reaching consequences. They reinforce the urgency of developing comprehensive, resilient cybersecurity strategies to safeguard global shipping infrastructure.

1.2. Factors Influencing Cybersecurity Vulnerabilities and Threats in the Maritime Sector

Industry stakeholders like the International Chamber of Shipping (ICS) [12] report a significant increase in cyberattacks targeting critical maritime infrastructure, particularly navigation and communication systems [13–15]. Such attacks pose a growing threat to national security, potentially hindering military operations and disrupting vital infrastructure. This necessitates collaboration between governments, regulators, shipping companies, and technology providers to implement robust measures, raise awareness, and invest in secure communication protocols.

 doi:10.20944/preprints202605.0928.v1

ENISA's study of cyber incidents in the transport sector (January 2021–October 2022) highlights key threats: Distributed Denial of Service (DDoS) attacks (53%), ransomware (19%), data-related threats (14%), and intrusion attacks (8%). These cyber threats primarily target the maritime sector, including port authorities, operators, and manufacturers. Additionally, state-sponsored actors frequently engage in politically motivated cyberattacks, disrupting port and vessel operations.

The industry's vulnerability stems from outdated technology, multiple stakeholders involved in ship operation and leasing, extensive online interactions with service providers and partners, and a weak cybersecurity culture due to a lack of awareness, training, and cybersecurity professionals.

1.3. Guidelines and Regulations

Regulatory bodies, industry organizations, and risk-management experts have established a robust framework of guidelines and best practices to address maritime cyber risks [16]. The International Maritime Organization (IMO) [17] plays a central role—most notably through its Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.3, 2025), a concise, high-level guide for integrating cyber risk into existing safety and security management [18]. Complementing this guidance, IMO Resolution MSC.428(98) mandates that shipping companies and vessel operators incorporate cyber-risk management into their Safety Management Systems (SMS); adopted in 2017 and mandatory since 1 January 2021, compliance is verified at the first annual audit of the company's Document of Compliance thereafter [19,20].

In addition, other notable organizations have made substantial contributions to enhancing maritime cybersecurity. The International Chamber of Shipping (ICS) [12,21] and BIMCO [22] have issued guidance to help industry stakeholders address the evolving landscape of cyber threats. In the United States, the Navigation and Vessel Inspection Circular (NVIC) 01-20 [23] outlines specific requirements for managing cyber risks in Marine Transportation System facilities. At the European level, the Network and Information Systems (NIS) Directive [24] establishes a comprehensive cybersecurity framework for critical service sectors, including maritime transport.

Contributions in brief.

We offer an *AIS-first, security-focused* survey. We (i) give a clear primer on how AIS works and why its open, self-reported broadcasts invite abuse, (ii) map the threat landscape from common manipulations to technical and operational effects, (iii) organize available mitigations, from protocol and device hardening to monitoring and procedures, and show how they fit together, (iv) review how ML/statistical methods detect unusual AIS behaviour, highlighting what tends to work and how to evaluate fairly, and (v) distill practical guidance and a short research agenda. Our survey draws on more than 300 publications—peer-reviewed papers, standards, and incident reports, surveyed through November 2024.

The remainder of this article is organized as follows. Section 2 provides a technical overview of AIS. Section 3 characterizes AIS threats and vulnerabilities. Section 4 presents mitigation strategies grouped into protocol/authentication, endpoint/network hardening, analytics, and resilience/governance. Section 5 situates our review within prior surveys. Section 6 synthesizes the findings and outlines recommendations. The appendices offer brief, quick-reference glossaries of key terms and acronyms in three areas: cybersecurity, maritime navigation/safety, and cryptography & network security. The appendices appear as supplementary material to this article.

2. An Overview of the Automatic Identification System

The Automatic Identification System (AIS) is a fundamental component of maritime safety and navigation, utilizing a dedicated Very High Frequency (VHF) data link protocol to facilitate communication between vessels and shore stations [25]. AIS enhances navigational safety by providing real-time transmission of essential data, including a ship's Maritime Mobile Service Identity (MMSI), position, course, speed, and additional operational information [26]. Displayed on dedicated screens or integrated into electronic navigational charts, this data significantly improves situational awareness

 doi:10.20944/preprints202605.0928.v1

for shipboard officers and assists in collision avoidance [17]. Maritime authorities rely on AIS data for effective traffic monitoring and vessel tracking. Despite its critical role, AIS relies on self-reported data, making it inherently vulnerable to cybersecurity threats, which are further examined in this study [27].

Ships navigating through remote waterways face numerous challenges, including adverse weather, piracy, and collisions [28]. To mitigate these risks, the International Maritime Organization (IMO) mandated the installation of AIS under the Safety of Life at Sea (SOLAS) Convention. This regulation applies to all vessels over 300 gross tonnage (GT) on international voyages, all passenger ships regardless of size, and cargo ships exceeding 500 GT on domestic routes [17]. By ensuring widespread AIS adoption, the mandate enhances maritime safety and improves vessel traffic oversight.

An AIS installation comprises a VHF transceiver, a Global Navigation Satellite System (GNSS) receiver (commonly GPS), and shipboard sensors (e.g., a gyrocompass) [25]. Together, these elements broadcast and receive vessel data, which is ingested by coastal base stations and satellites equipped with AIS receivers. For brevity, we use "GPS" to refer to GNSS [26].

2.1. Types of AIS Systems

AIS is categorized into Class A and Class B systems, alongside AIS base stations [17]. Class A, the initial standard, offers high transmission power and is mandatory for larger vessels due to its frequent position reporting and support for voyage-related data [29]. Class B provides a cost-effective solution, fostering broader adoption and significantly increasing maritime communication data volume [26]. Following Class B's introduction, regulatory frameworks, such as the European Union's 2010 mandate, required AIS on most commercial inland vessels and fishing vessels over 15 meters, expanding AIS deployment [30].

2.1.1. AIS Class A

Class A equipment complies with IMO standards, transmitting position data autonomously every 2-10 seconds, depending on speed and course changes, or every three minutes when stationary [31]. It also transmits static and voyage-related information every six minutes, supports safety-related text messaging, and transmits Application-Specific Messages (ASM) for meteorological and navigational data.

2.1.2. AIS Class B

Class B AIS equipment is compatible with all AIS systems but transmits at lower power and less frequently than Class A [26]. While it can communicate with all other AIS stations, it does not meet all performance standards adopted by the IMO. When the vessel is anchored, it reports its position every three minutes or less using message type 18[1]. Additionally, it transmits static data every six minutes, though it does not include voyage-related information. Class B AIS can receive safety-related text and application-specific messages, but it lacks the capability to transmit them, limiting its role in active communication scenarios.

Class B AIS transponders are categorized into two types: Carrier Sense Time-Division Multiple Access-based Class B (CSTDMA-based B/CS) and Self-Organized Time-Division Multiple Access-based Class B (SOTDMA-based B/SO) systems. SOTDMA-based B/SO transponders improve transmission reliability and increase the frequency of position updates by reserving future communication slots, thereby securing higher transmission priority in congested environments. In contrast, CSTDMA-based B/CS transponders operate by sensing available transmission slots before sending data, offering a more cost-effective solution but with lower transmission priority and potentially less frequent updates in busy maritime areas [29].

[1] AIS message type 18 is the Standard Class B Equipment Position Report. It is used by Class B AIS transponders to broadcast vessel position and movement data. See Table 1.

 doi:10.20944/preprints202605.0928.v1

2.1.3. AIS Base Station

Shore-based AIS stations transmit identity, time synchronization, and text messages using AIS message type 4 at ten-second intervals[2]. In addition, these stations broadcast Aid to Navigation (AtoN) reports and Application-Specific Messages (ASM) containing meteorological data. In the United States, regulations restrict the operation of private AIS base stations to ensure compliance with maritime safety standards and prevent unauthorized interference.

2.1.4. AIS Aid to Navigation (ATON)

AIS ATONs, shore-based or mobile, broadcast navigational aid information using messages 6 and 8[3], with U.S. ATONs identified by MMSI numbers starting with 993 and listed in the United States Coast Guard (USCG) Light List [29]. Aids to navigation include lights, sound signals, buoys, daybeacons, and other navigational aids.

2.1.5. AIS Search and Rescue Transmitter (SART)

AIS SARTs aid in locating lifeboats and life rafts, transmitting 'SART TEST' or 'ACTIVE SART' using AIS message type 14[4] and position data using message type 1[5] every minute [26]. AIS SARTs are also used in maritime survivor locating devices (MSLD) or man overboard (MOB) devices. Standard AIS SARTs can be identified by MMSI numbers beginning with 970.

2.1.6. Search and Rescue Aircraft

Search and rescue aircraft report position every ten seconds [17] using message type 9.[6]

2.2. AIS Use Cases

AIS enhances maritime safety and efficiency through various functionalities:

Navigation Safety:

Provides real-time vessel data for collision avoidance and traffic management [26]. Vessel Traffic Service (VTS) utilizes AIS data in busy waterways for traffic management and enhanced safety.

Maritime Security: Assists in vessel identification and differentiation within exclusive economic zones [27].

Navigation Aids: Broadcasts locations of stationary objects and virtual markers. "Artificial AIS" messages transmit the position of virtual markers or warnings about restricted areas [26].

Search and Rescue: Enhances coordination by providing vessel locations [17].

Accident Investigation: Provides detailed records of vessel movements [28].

Informational Messages: Transmits weather conditions and navigational instructions using ASM [29].

2.3. How AIS works

2.3.1. TDMA Protocol

AIS utilizes Self-Organized TDMA (SOTDMA), Carrier-Sense TDMA (CSTDMA), Fixed Access TDMA (FATDMA), Incremental TDMA (ITDMA), and Random Access TDMA (RATDMA) protocols [25]. SOTDMA dynamically allocates transmission slots, ensuring efficient communication in busy maritime environments through time synchronization, slot mapping, avoiding data collision, and

[2] AIS message type 4 is used for Coordinated Universal Time (UTC) synchronization and base station identification [29]. See Table 1.

[3] AIS messages 6 and 8 are used for transmitting application-specific binary data. Message 6 is sent to a specific MMSI number, whereas message 8 is broadcast to all AIS recipients within range. See Table 1.

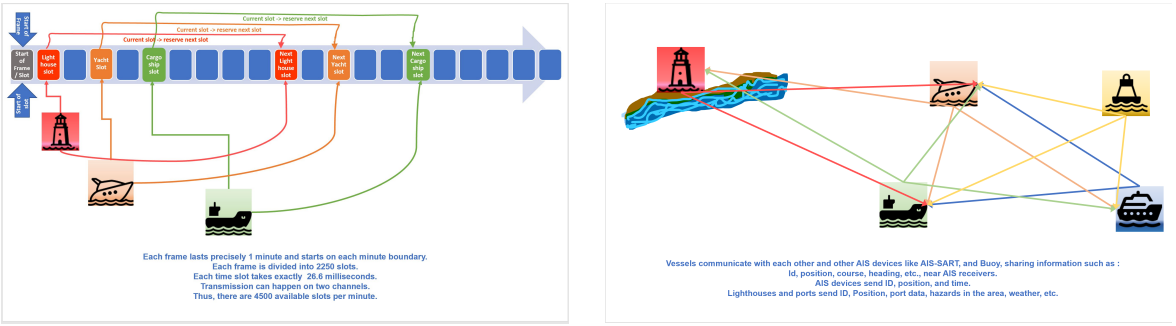
[4] AIS Message Type 14 is the Safety-Related Broadcast Message. It is used to transmit important safety information to all AIS-equipped vessels within range. See Table 1.

[5] AIS Message Type 1 is a Standard Class A Position Report used by vessels equipped with Class A AIS transponders. It provides essential navigational data to other ships and shore stations. See Table 1.

[6] AIS message type 9 is the message used by search and rescue aircraft. See Table 1

 doi:10.20944/preprints202605.0928.v1

dynamic slot allocation [26]. As vessels move and encounter new stations, AIS stations adjust their slot selections dynamically to avoid conflicts. AIS transmissions and TDMA type depend on vessel size, with SOTDMA enabling slot reuse for optimized capacity, while smaller vessels and yachts typically use CSTDMA. AIS signal range isn't uniform and depends on factors like antenna height and environment. Transmission range extends up to 74 kilometers horizontally and 400 kilometers vertically [29]. The technical details about frame lengths and slot numbers are illustrated in Figure 2(**b**).



(**a**) AIS slot communication scheme [32]. Each UTC-synchronized minute is divided into 2,250 time slots (≈ 26.67 ms). Stations access slots by reservation (SOTDMA, Class A), carrier-sense use of free slots (CSTDMA, Class B), or fixed assignments (FATDMA for AtoN/base). Two VHF channels operate in parallel, each with the same frame structure.

(**b**) AIS broadcast communication scheme [32]. AIS messages are one-to-many broadcasts received by all stations within VHF range (ships, AtoN/buoys/lighthouses, and coastal receivers). Lines illustrate simultaneous reception; both AIS channels carry such broadcasts in parallel.

Figure 2. AIS slot structure and AIS broadcast communication.

The link layer controls access to VHF channels using TDMA techniques and defines frame and message formats. Each frame lasts precisely one minute, begins at the minute boundary, and is synchronized to UTC time. Each frame is divided into 2250 individual transmission slots per channel. Each time slot occupies 26.6 milliseconds and contains a 256-bit data payload. AIS transmissions can occur on two separate channels, resulting in a total of 4500 available slots per minute. While multiplying the number of slots by the slot duration should ideally total 60 seconds, small discrepancies arise due to guard intervals, synchronization overhead, and reserved slots. Guard times between transmissions help prevent interference, while UTC-based synchronization ensures consistency across AIS devices worldwide. Figure 3 provides a visual representation of the AIS Transmission Slot Structure, including a detailed Payload Breakdown.

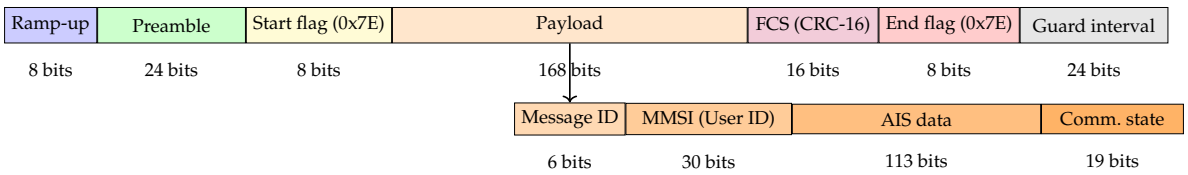


Figure 3. AIS single-slot burst (one VHF channel). At 9.6 kb/s each TDMA slot carries a 256-bit frame: 8-bit TX ramp-up, 24-bit preamble, 8-bit start flag (0x7E), payload (example shown: 168-bit Class A position report), 16-bit FCS (CRC-16), 8-bit end flag (0x7E), and a 24-bit guard interval. Example payload fields: Message ID (6 b), MMSI/User ID (30 b), AIS data (113 b), and communication state (19 b; SOTDMA). Other message types may differ in length, and some span multiple slots.

AIS data originates from vessel navigation sensors, including a GNSS receiver and a gyroscopic compass. Static information like the vessel's name and VHF call sign is programmed into the AIS system during installation and transmitted regularly.

AIS information is displayed on dedicated equipment or integrated into electronic navigational charts, providing crew situational awareness and aiding collision avoidance.

 doi:10.20944/preprints202605.0928.v1

2.3.2. Benefits of SOTDMA in AIS

Increased Channel Capacity:

Multiple vessels can share the same channel through efficient time slot allocation.

Improved Communication Reliability: Reduced data collisions and errors enhance transmission reliability.

Enhanced Navigation Safety: Timely and accurate information about nearby vessels is crucial for collision avoidance and safe navigation.

2.3.3. Limitations of TDMA (Partially Applicable to AIS)

Limited Flexibility:

Fixed time slots may not always suit dynamic maritime conditions, but SOTDMA mitigates this by adapting slot allocation as needed.

Increased Complexity: Efficient scheduling and management of time slots require coordination to avoid transmission conflicts.

Scalability Limits: The number of available time slots restricts the number of vessels that can share a single channel, which is particularly relevant in densely trafficked maritime areas. This limitation has an immediate impact on AIS communication efficiency, as slot availability is a determining factor in whether ships can transmit navigational data reliably and in real time, affecting overall maritime situational awareness.

These limitations are inherent to TDMA protocols and are not unique to AIS. However, SOTDMA's dynamic slot allocation makes it a valuable choice for AIS, enabling reliable and efficient communication in the dynamic maritime environment. TDMA's adaptability and efficiency have also made it a popular protocol in various wireless communication systems beyond AIS.

2.4. AIS Messages

AIS systems comply with maritime-specific protocols and standards, including the National Marine Electronics Association (NMEA) standard and the AIS protocol [25,29,33]. The NMEA interface standard is used worldwide across maritime industry segments. The standard is intended to support one-way serial data transmission from a single talker to one or more listeners. AIS protocol includes 64 types of AIS messages, of which 27 are currently in use. The rest (37) are reserved for the future. Table 1 lists the AIS messages that are currently in use.

Table 1. List of AIS Message Types.

Message ID	Name	Description	Priority	Access Scheme
1	Position Report Class A	Scheduled position report from Class A shipborne equipment; provides vessel position, speed, and course	High	SOTDMA
2	Position Report Class A (Assigned)	Assigned scheduled position report from Class A shipborne equipment; provides vessel position, speed, and course	High	SOTDMA
3	Special Position Report (Response to Interrogation)	Position report transmitted in response to an interrogation	High	SOTDMA or RATDMA
4	Base Station Report	Sent by base stations with time and location information	High	FATDMA
5	Static and Voyage Related Data	Ship's static details and voyage information	Medium	SOTDMA

Continued on next page

 doi:10.20944/preprints202605.0928.v1

Continued from previous page

Message ID	Name	Description	Priority	Access Scheme
6	Binary Addressed Message	Binary data addressed to specific targets	Low	FATDMA or RATDMA
7	Binary Acknowledge	Acknowledgment of receipt of a binary message	Low	FATDMA or RATDMA
8	Binary Broadcast Message	Broadcast binary data transmission	Low	FATDMA or RATDMA
9	Standard SAR Aircraft Position Report	Position report from search and rescue aircraft	High	RATDMA
10	UTC/Date Inquiry	Request for UTC/date information from a station	Low	FATDMA or RATDMA
11	UTC/Date Response	Response with UTC/date information	Low	FATDMA or RATDMA
12	Addressed Safety-Related Message	Safety-related text to a specific station	Medium	FATDMA or RATDMA
13	Safety-Related Acknowledgment	Acknowledgment of addressed safety-related message	Medium	FATDMA or RATDMA
14	Safety-Related Broadcast Message	Broadcast safety-related text message	Medium	FATDMA or RATDMA
15	Interrogation	Request for specific information from another AIS station	Low	FATDMA or RATDMA
16	Assignment Mode Command	Assigns specific time slots to a station	Low	FATDMA or RATDMA
17	GNSS Broadcast Binary Message	Broadcast of GNSS corrections for navigation accuracy	High	FATDMA
18	Standard Class B Equipment Position Report	Position data for Class B vessels	Medium	CSTDMA or SOTDMA (Class B SO)
19	Extended Class B Equipment Position Report	Additional voyage/static data for Class B vessels	Medium	CSTDMA or SOTDMA (Class B SO)
20	Data Link Management Message	Management of data link parameters	Low	FATDMA
21	Aids-to-Navigation Report	Position/status of an aid to navigation (e.g., buoy, beacon)	High	FATDMA or RATDMA
22	Channel Management	Management of AIS channels	Low	FATDMA
23	Group Assignment Command	Command assigning actions to a group of AIS stations	Low	FATDMA or RATDMA
24	Static Data Report (Class B)	Static data such as name and call sign from Class B equipment	Medium	CSTDMA or SOTDMA (Class B SO)
25	Single Slot Binary Message	Single-slot binary message for addressed or broadcast communication	Low	FATDMA or RATDMA
26	Multiple Slot Binary Message with Communications State	Multi-slot binary message with communication-state information	Low	FATDMA or RATDMA
27	Long-Range AIS Broadcast Message	Position report for long-range applications (reduced content/rate)	High	RATDMA

 doi:10.20944/preprints202605.0928.v1

3. Threats & Vulnerabilities in AIS

This section surveys the evolving landscape of AIS threats, focusing on protocol-, signal-, and data-layer vulnerabilities and known exploitation techniques. We highlight how AIS's open, self-reported broadcast model and dependence on GNSS[7] expose it to spoofing, jamming/denial-of-service, and data manipulation attacks. We treat mitigation strategies in Section 4, where we group defenses into four families: protocol/authentication, endpoint/network hardening, analytics for detection, and resilience/governance.

3.1. The Growing Threat Landscape

Recent literature highlights the evolving landscape of maritime cybersecurity within Industry 4.0[7], driven by increasing digitization and reliance on interconnected systems. While these advancements enhance operational efficiency and sustainability, they also introduce significant vulnerabilities. For example, forged warship tracks reported off Crimea in June 2021 illustrate how manipulated AIS can heighten geopolitical tensions and mislead operators [34].

Figure 4 charts the AIS threat landscape in an end-to-end view, connecting the overarching drivers, principal attack vectors, immediate technical effects, and downstream operational and safety impacts. We discuss these elements in detail in the sections that follow.

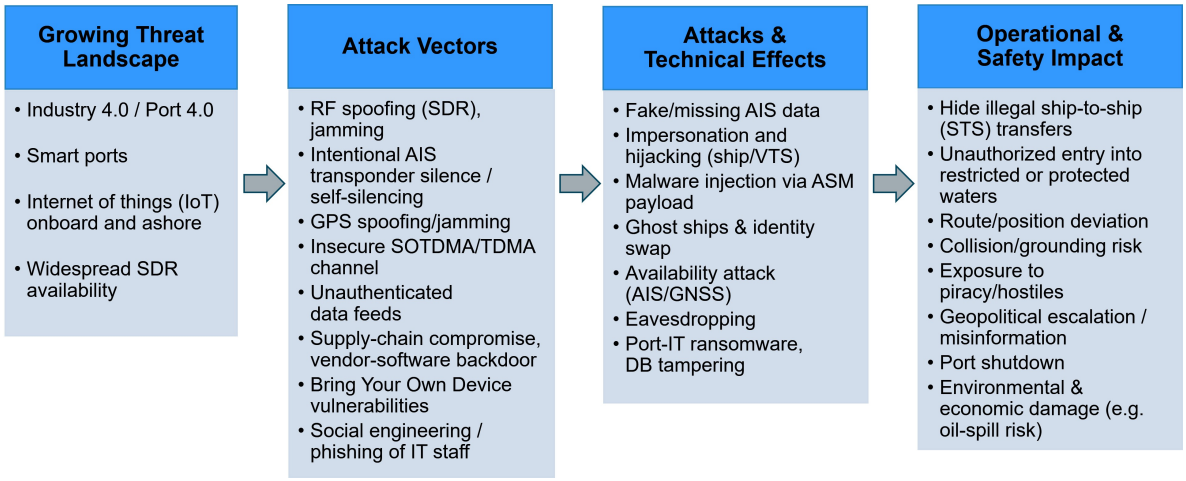


Figure 4. AIS threats flow: drivers, attack vectors, technical effects, and operational/safety impacts.

Ajayi et al. [35] and Nayernia et al. [36] analyze Industry 4.0, examining its core principles, enabling technologies, applications, and key challenges. Industry 4.0—often referred to as the fourth industrial revolution—seamlessly integrates digital and physical systems through advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Big Data Analytics (BDA), robotics, and cloud computing. These technologies collectively drive automation and support data-driven decision-making.

Barthwal and Agarwal [37] examine the security challenges associated with deploying Industry 4.0 technologies in the maritime sector, along with the industry's preparedness to mitigate these risks. Integrating IoT and cloud-based systems enhances real-time tracking, anomaly detection, and predictive threat mitigation, improving the security and efficiency of maritime operations. However, increased connectivity also expands the attack surface, exposing AIS data to cyber threats like spoofing, jamming, and unauthorized data manipulation.

Imran et al. [38] analyze the escalating cybersecurity threats in the maritime industry resulting from the increasing integration of Internet of Things (IoT) technologies. Their research identifies critical vulnerabilities in shipboard systems, including sensors, communication tools, navigation technologies

[7] For detailed definitions, see Appendix section in the supplementary material file named: ***maritime_and_CyberSecurity_terms.pdf***

 doi:10.20944/preprints202605.0928.v1

(ECDIS[7], AIS, GPS[7]), and emergency response mechanisms. Several factors exacerbate these vulnerabilities: limited onboard technical expertise, hindering the implementation and maintenance of effective cybersecurity measures; reliance on outdated software systems lacking essential security features and regular updates, exposing ships to known exploits; and the heterogeneity of security devices from different vendors, complicating system integration and creating inconsistencies in security practices. The absence of standardized cybersecurity protocols further compounds these challenges, leading to fragmented and inconsistent security measures across the industry. Consequently, they emphasize the need for a comprehensive strategy encompassing enhanced crew training, timely software updates, and establishing standardized, industry-wide cybersecurity protocols to bolster defenses against emerging threats.

Ignacio de la Peña Zarzuelo analyzes the increasing importance of cybersecurity in the maritime and port sectors, focusing on the transformative impact of Industry 4.0 and the emergence of smart ports (Port 4.0) [39]. His study demonstrates how increasing automation, IoT integration, and reliance on digital technologies in these advanced environments enhance operational efficiency and sustainability while introducing significant cybersecurity vulnerabilities. As critical links in the global supply chain, ports are attractive cyberattack targets due to their strategic importance and potential for cascading global disruptions. This inherent vulnerability is compounded by the convergence of cyber-physical systems (CPS[7]) with extensive wireless networks, particularly in automated terminals, and the proliferation of IoT devices and sensors, which expands the attack surface.

Incidents like the 2017 NotPetya attack [9,11] on Maersk and breaches at Antwerp and Rotterdam [40–42] highlight the tangible risks and financial repercussions of cybersecurity failures. Threat actors range from organized crime and state-sponsored entities to disgruntled employees and human error. Mitigation requires combining established frameworks like the NIST Cybersecurity Framework [43], ISO/IEC 27001 [44], and ENISA[7] guidelines with port-specific initiatives which promote information sharing and collaboration [45]. Robust employee training and awareness programs are also essential. The IT/OT convergence in Port 4.0 necessitates robust safeguards for operational and informational infrastructures to safeguard operational continuity and global supply chain integrity.

Sepehri et al. [46] explored how Industry 4.0 technologies, cloud computing, Cyber-Physical Systems, the Internet of Things (IoT), and Big Data Analytics (BDA), can enhance maritime safety, with a particular emphasis on collision prevention, a central theme identified in up to 67% of accident types. Their findings underscore the transformative potential of "Safety Through Technology" innovations facilitated by Industry 4.0, mainly through integrating existing navigational tools, such as AIS and Automatic Radar Plotting Aid (ARPA)[7], with these advanced technologies. This integration enables several key advancements: autonomous vessel navigation through systems that augment decision-making and mitigate human error; real-time information access for crews to enhance situational awareness and facilitate more effective responses to dynamic conditions; and enhanced risk management through sophisticated strategies informed by real-time data and advanced analytics. This integrated approach is crucial for achieving more robust decision-making capabilities at sea.

Hyra [47] analyzed the cybersecurity posture of transportation systems, specifically focusing on maritime vessels. The study identifies current cyber threats in the maritime domain, examines the functionality and financial impact of malware, and highlights the scale of cybersecurity challenges faced by ships. It explores the vulnerabilities inherent in maritime systems, emphasizing the motivations behind cyberattacks on the sector and the operational methods of maritime cyber pirates. The paper reviews notable cyber incidents in the maritime industry and the responses from international bodies and frameworks such as the IMO[7], SOLAS[7], UN, EU, and US. Additionally, it outlines risk management strategies and assessment methods suitable for maritime cybersecurity analysis. Using an Asset-Based Risk method, Hyra provides a detailed analysis of ship components, underscoring the critical need for enhanced cybersecurity measures. The findings reveal that most shipboard systems are inadequately protected, making them highly susceptible to cyberattacks, with even shore-based

 doi:10.20944/preprints202605.0928.v1

systems at risk. The study concludes that immediate and decisive actions are necessary to strengthen maritime cybersecurity and prevent an escalation in compromised systems.

Prior research has established the strategic importance of cyber operations in modern military contexts. Sub-Lieutenant Christopher Argles [48] analyzed cyber operations doctrines of major naval powers, focusing on the Royal Navy's approach, revealing key differences between Western and Eastern military thinking. While the US Department of Defense designates cyberspace as an operational domain alongside land, air, sea, and space, Chinese and Russian doctrine conceptualize it more broadly as part of information warfare aimed at cognitive control. Argles highlighted unique cyber defense challenges for naval forces, including autonomous operation with limited bandwidth, the complexity of networked maritime systems, and difficulties in updating deployed vessels' software. His examination of organizational structures, training, and capability development provides a crucial foundation for understanding naval cyber operations.

Akash [49] highlighted the growing cybersecurity risks in the maritime sector due to increasing reliance on digital systems such as AIS, GPS, and ECDIS. The study underscores the vulnerabilities of these systems to GPS spoofing, malware, and unauthorized access, drawing attention to incidents like the GPS spoofing of an $80 million yacht, which was hijacked using low-cost equipment. The article emphasizes the need for robust cyber risk management, aligning with IMO's guidelines for comprehensive risk assessment, personnel training, and adherence to international standards like ISO/IEC 27001 [19,44,50–52]. The British Code of Practice: Cyber Security for Ships is a nationally adopted guideline that offers practical measures for securing shipboard IT and OT systems [53].

Chupkemi et al.[54] highlight the complexities of maritime cybersecurity training, emphasizing challenges such as evolving cyber threats, Bring Your Own Device (BYOD[7]) vulnerabilities, and operational constraints. Their work underscores the need for continuous, scenario-based training and customized programs. These challenges parallel those in AIS cybersecurity, where outdated protocols and emerging threats demand adaptive security measures. The authors propose AI-driven training solutions and immersive technologies that can be extended to AIS systems for anomaly detection and secure operations. By incorporating this approach, AIS security can benefit from dynamic training models, ongoing threat assessments, and the integration of human factors, enhancing resilience against spoofing, jamming, and other cyber threats to maritime navigation and communication systems. Furthermore, their work highlights the growing interconnectedness of maritime operations—including ports and critical onboard systems such as sensors, communication tools, navigation technologies, and emergency mechanisms—leading to increased vulnerabilities. As a result, a holistic risk management approach is essential, one that integrates technical, human, organizational, regulatory, and collaborative measures to ensure seaworthiness and safeguard both civilian and military cyber operations.

Kanwal et al.[55] emphasize the critical importance of cybersecurity in maritime systems, drawing parallels to vulnerabilities in AIS systems, which are similarly susceptible to spoofing, jamming, and data manipulation. Their study highlights the roles of training, regulatory frameworks, and system readiness as key factors in enhancing AIS cybersecurity. Building on their findings, AIS systems can benefit from structured training programs, robust compliance monitoring, and adopting advanced cybersecurity measures such as encryption, anomaly detection, and multi-factor authentication to mitigate emerging threats.

Afenyo et al.[56] identify significant gaps and future research directions in maritime cybersecurity, many of which align with the challenges faced by AIS systems. The authors' call for real-time data acquisition and improved training resonates with AIS-specific concerns, where data accuracy and operator proficiency are essential for anomaly detection. Their emphasis on enhancing legal frameworks and updating policies also reflects the regulatory shortcomings in AIS cybersecurity, particularly the lack of consistent international standards. Furthermore, the paper highlights the value of holistic approaches and stakeholder collaboration, supporting the integration of multi-source data fusion and cooperative monitoring in AIS operations. The research underscores the importance of continuous assessment and adaptation, suggesting that AIS systems could benefit from similar

 doi:10.20944/preprints202605.0928.v1

methodologies, including real-time threat detection, economic impact analysis, and comprehensive operator training programs, to mitigate cyber threats effectively.

3.2. AIS Vulnerabilities and Exploitation

Developed in the late 1990s, the Automatic Identification System (AIS) underpins modern maritime safety, traffic management, and collision-avoidance. It continuously broadcasts dynamic data such as position, course, and speed, alongside static details (MMSI[7], ship name, type, hazardous-cargo codes) over a Self-Organizing TDMA (SOTDMA) VHF link. Because AIS relies on unencrypted, unauthenticated self-reported data and lacks integrity and replay protection[7], it is vulnerable to spoofing, eavesdropping, and message manipulation. These gaps can disrupt traffic flow, compromise vessel safety, and facilitate illicit activities ranging from smuggling and piracy to illegal fishing.

A substantial body of research addresses these protocols and ecosystem weaknesses. In the following sections, we survey this work by vulnerability class; Section 4 then links causes to concrete mitigations such as cryptographic protections, endpoint/network hardening, analytics for detection, and resilience/governance measures.

3.2.1. Data Falsification

Malicious actors can manipulate AIS data, for example, by altering location information to conceal illicit activities, including piracy, smuggling, and unauthorized fishing in restricted zones. Although AIS provides valuable opportunities for monitoring fishing activities, it also presents significant challenges due to its reliance on self-reported data, which is vulnerable to falsification [57], [58]. Deliberate AIS signal disruptions, particularly "silence anomalies," where vessels disable their AIS transponders to engage in illegal fishing, are commonly observed near Exclusive Economic Zones (EEZs) and Marine Protected Areas (MPAs) [59].

3.2.2. TDMA insecurity

The TDMA protocol underpinning AIS lacks essential security features such as encryption and authentication, exposing it to spoofing, data corruption, and hijacking [25,26].

3.2.3. Eavesdropping and Unauthorized Access

The unencrypted nature of AIS transmissions allows attackers to intercept sensitive information, increasing the risk of unauthorized access [60].

3.2.4. Unreliable Data Sources

Many public ship-tracking websites rely on unauthenticated data feeds, making them vulnerable to manipulation through fake AIS packets transmitted via Software-Defined Radio (SDR)[7]. Androjna and Perkovič [61] conducted a case study examining several vessels involved in AIS data manipulation. This includes recent incidents related to Ship-to-Ship (STS) transfers, a common practice in the shipping industry for transferring large quantities of oil or other cargo between vessels. Their investigation into suspicious STS oil transfers revealed falsified or missing position data and confirmed that AIS messages can be spoofed, disrupted, deliberately falsified, or simply switched off.

3.2.5. Communication Disruption

Advanced equipment can disrupt ship-to-ship communication through jamming or interference with transponder signals, compromising situational awareness (e.g., GPS spoofing or SDR techniques) [62–64].

3.2.6. AIS Data Manipulations, Spoofing, and Jamming

While AIS spoofing involves transmitting false data to misrepresent a vessel's identity or location, requiring control over an AIS transmitter, AIS jamming disrupts communication by overwhelming the

 doi:10.20944/preprints202605.0928.v1

system with high-power transmissions, preventing data reception without sending false information [65].

The reliability of the Automatic Identification System (AIS) is intrinsically tied to Global Positioning System (GPS) signals, rendering it highly susceptible to jamming and spoofing attacks that can compromise maritime safety. Designed for interoperability, AIS lacks inherent security features, making it vulnerable to GPS spoofing, which poses significant security risks. Exploiting this vulnerability, malicious actors can conceal illicit activities, escalate maritime tensions, or disrupt navigation by causing vessels to disappear from AIS displays, appear at incorrect locations, or exhibit implausible movements and formations [66–69]. Such attacks can severely impact the maritime community, threatening regional stability and disrupting global trade.

While Class B AIS transponders exhibit some resilience to spoofing—owing to factors such as type-approval testing[8], reliance on internal GPS, and single-slot transmission (which limits the complexity of spoofed messages compared to the multi-slot transmissions used by larger vessels)—they nonetheless remain vulnerable to sophisticated forms of manipulation.

AIS spoofing has been used in various contexts, ranging from electronic warfare (EW) to conceal military maneuvers, to non-military applications intended to disrupt commercial shipping operations [34,70]. Zorri et al. [71] provide a detailed analysis of AIS spoofing incidents, including cases involving NATO vessels in the Black Sea and commercial ships in the Strait of Hormuz, highlighting the absence of authentication and data integrity mechanisms in the AIS protocol. Their study emphasizes the urgent need for cryptographic safeguards and the adoption of resilient, terrestrial navigation backups such as eLORAN[7] [72] (Enhanced Long Range Navigation), a ground-based radio navigation system designed to provide robust positioning, navigation, and timing (PNT)[7] services even in the event of satellite system disruption or spoofing. Additionally, the research underscores the importance of training maritime personnel to detect AIS anomalies and advocates for implementing multi-layered security architectures to strengthen maritime situational awareness and operational resilience.

Grant et al. [73] further highlight the critical impact of GPS jamming on AIS functionality, demonstrating how signal disruption leads to erroneous AIS positions, compromised data synchronization, and significant maritime hazards. The authors advocate for integrating eLORAN as a backup system for PNT to mitigate these vulnerabilities, stressing the importance of redundant navigation systems and comprehensive crew training in alternative navigation methods to ensure operational continuity in the face of GPS denial attacks.

Androjna et al. [2,66,67,69] examined the cybersecurity challenges in maritime transportation systems, with a specific focus on vulnerabilities in Global Navigation Satellite Systems (GNSS), the AIS, and maritime critical infrastructure (MCI). Their studies emphasize how the increased digitalization of maritime operations, driven by IoT, cloud computing, big data analytics, and automation, introduces significant cyber risks. These vulnerabilities threaten navigation, port operations, cargo handling, and maritime situational awareness (MSA), with potential consequences for global trade, environmental safety, and national security. Their research presented empirical case studies - such as the Elba Island AIS spoofing incident (2019) [66] - to illustrate the real-world impacts of AIS/GNSS vulnerabilities. It demonstrates how attackers can inject false AIS signals, disrupt vessel navigation, and overload maritime monitoring systems, resulting in operational disruptions and navigation hazards. The authors demonstrated the potential for AIS data spoofing through real-world examples, highlighting the use of Software-Defined Radio (SDR) to inject false information. Studies assessing cyber threats to maritime critical infrastructure and the cybersecurity of navigation systems further underscore these vulnerabilities. Key findings include:

* AIS/GNSS spoofing and jamming, which result in inaccurate navigation data.

[8] Type approval refers to the regulatory certification process through which AIS transponders are tested and validated to ensure compliance with international standards for performance, interoperability, and safety, such as those set by the International Maritime Organization (IMO) and the International Telecommunication Union (ITU). This process helps ensure that devices behave predictably and securely under defined operational conditions.

 doi:10.20944/preprints202605.0928.v1

* Ransomware and malware attacks targeting port logistics systems.
* Social engineering and phishing campaigns aimed at maritime personnel.
* Supply chain attacks, often enabled through compromised third-party systems.

Balduzzi et al. [64] conducted a comprehensive security evaluation of AIS, highlighting critical vulnerabilities in both the protocol's specifications and its software and radio frequency (RF) implementations. Their study revealed that AIS is susceptible to spoofing, hijacking, and denial-of-service attacks, which can undermine vessel navigation, collision avoidance, and maritime traffic management. The authors developed an AIS VHF Data Message (AIVDM) encoder to generate and inject arbitrary AIS messages, enabling the creation of false vessel signals, spoofed navigational aids, and bogus distress alerts. Additionally, they implemented AISTX, a software-defined radio-based AIS transmitter, to demonstrate real-world signal manipulation over distances of up to 16.5 kilometers. Their attack simulations exposed vulnerabilities such as slot starvation, frequency hopping, and AIS hijacking, all of which pose serious threats to the integrity and availability of AIS communications.

Spoofing Techniques and Examples: Spoofing methods include using AIS base stations, SDR platforms, and transponder interface exploitation to transmit unauthorized messages [65,73]. Several techniques have been used to demonstrate and conduct AIS spoofing attacks, with varying degrees of sophistication and impact.

Vessel spoofing: In this technique, an attacker broadcasts falsified AIS information—static fields such as MMSI or call-sign and, more critically, dynamic fields like position, speed, or course—to create a phantom vessel. By manipulating those dynamic parameters, the adversary can mask illicit behaviour, including unauthorised approaches, incursions into restricted zones, route deviations, or suspicious AIS on/off cycles [64]. DiRenzo et al. [74] highlight AIS exposure to spoofing, jamming, and denial-of-service, and advocate cryptographic authentication together with eLORAN as a complementary navigation system. Mednikarov et al. [75] reach similar conclusions, stressing network segmentation, intrusion detection, and encryption to bolster AIS security.

GNSS Spoofing: Androjna et al. present a comprehensive analysis of spoofing incidents targeting Global Navigation Satellite Systems (GNSS) in maritime traffic between 2008 and 2020, highlighting the growing threat to systems reliant on satellite-based positioning [66–68].

Territorial disputes, heightened tensions, and AIS data-layer injection: Harris [76] documents incidents in which false AIS tracks for naval vessels were injected into public AIS aggregators' feeds via uplinks attributed to terrestrial feeder stations (shore-based gateways), rather than broadcast over VHF. These cases show that adversaries can remotely place phantom ships on public AIS maps without access to shipboard equipment. However, because they do not alter the local RF AIS picture used by ships and authorities, their primary impact is to sow confusion and heighten tensions in contested waters. The article also notes mitigation approaches, such as anomaly detection and cross-checking with satellite AIS, to curb such fabrications. Illustrative examples include forged war-ship positions off Crimea (June 2021) [34,76], North-Korean vessels cycling identities to evade sanctions (June 2019) [77], and bogus Swedish-navy tracks near Kaliningrad (March 2021) [70]. Together, these cases show how AIS manipulation can construct false narratives and heighten geopolitical tension [78].

Real-World Test and Academic Research: A 2013 University of Texas at Austin experiment successfully spoofed a yacht's GPS, exposing vulnerabilities in onboard navigation systems [79,80]. Similarly, a 2008 UK trial using GPS jamming equipment demonstrated potential disruptions to onboard AIS and navigation systems [73,81].

Fake Weather Forecasts: One application of AIS is the communication of dynamic data reflecting the changing environment, such as currents and climate conditions. A special type of message, namely a binary message, is used to convey such information. Spoofing may be used to broadcast false weather forecasts—for example, reporting heavy fog when visibility is actually clear [64].

Navigation and Closest Point of Approach (CPA) Spoofing: AIS utilizes an algorithm to calculate the Closest Point of Approach (CPA) between vessels by considering their respective positions and trajectories. This system can be configured to generate visual or audible alerts when a potential collision

 doi:10.20944/preprints202605.0928.v1

is detected, causing the vessels to perform evasive maneuvers. However, deliberately fabricating a false imminent collision scenario targeting a specific vessel can trigger erroneous CPA alerts, potentially inducing unnecessary and even hazardous evasive actions. In critical situations, such maneuvers could inadvertently result in collisions with physical obstacles, such as rocks or shoals, or cause grounding, particularly in shallow waters during low tide.

In December 2019, an attack near Elba Island generated spoofed data from fictitious Dutch naval vessels, saturating the area and disrupting genuine AIS transmissions, thereby jeopardizing safe navigation [66,67]. Androjna et al. [82] simulated the data that would have appeared on the ECDIS[7] screen of one of the ships present during the incident. The bridge display (radar/ECDIS with AIS overlay) would have shown a hazardous situation in which the vessel appeared to be on a collision course with over a dozen phantom merchant vessels, potentially prompting inappropriate decisions by the officer of the watch (OOW).

AIS-SART Spoofing: As pointed out by Androjna and Perkovič [68], False Search and Rescue Transponder (SART[7]) alerts can lure vessels into hostile waters under the pretense of aiding distressed ships.

Denial-of-Service (DoS) Attacks: Denial-of-Service (DoS) attacks on AIS aim to disrupt maritime communication by overwhelming or manipulating the system, thereby hindering the transmission and reception of critical navigational data. Several studies have examined the impact of DoS attacks on AIS communication [64,65,74]. Khandker et al. [65] transmitted 200,000 AIS type 1 frames using an SDR. Their evaluation showed that nearly 90% of the tested hardware/software configurations were affected by the DoS attack, resulting in issues such as output congestion, unresponsiveness, or system crashes. Balduzzi et al. [64] identified and analyzed several radio-frequency-based DoS techniques targeting AIS communication:

1. **Slot Starvation:** This technique prevents legitimate AIS communication by exploiting transmission slot allocation mechanisms. It can be executed in two primary ways:
   (a) **Impersonation:** Attackers impersonate maritime authorities to reserve the entire AIS transmission "address space," effectively occupying all available slots. This action prevents other AIS stations within range from transmitting, leading to widespread communication failure.
   (b) **Flooding:** The system is inundated with fabricated AIS messages, saturating available bandwidth and overwhelming processing capacity. This disruption hinders the reception and processing of legitimate messages, impairing vessel coordination and situational awareness.
2. **Frequency Hopping:** Attackers impersonate authoritative entities to issue commands that force AIS transponders to switch frequencies. This tactic disrupts communication and undermines system reliability.
3. **Timing Attacks:** These attacks exploit AIS timing mechanisms by repeatedly altering transmission schedules, delaying messages, or sending renewal commands. The resulting interference may cause vessels to disappear from radar displays, creating navigational confusion and increasing the risk of collisions.

Aids to Navigation (AtoN) Spoofing: Aids to Navigation (AtoNs)[7], such as buoys and lighthouses, are critical for managing vessel traffic and warning of navigational hazards like shallow waters and rocks. AtoN spoofing refers to generating false or misleading information about these aids, potentially deceiving vessels, and compromising navigational safety. For example, attackers may fabricate nonexistent buoys near a harbor entrance to disrupt maritime traffic or mislead vessels into hazardous areas, increasing the risk of collisions, groundings, or other incidents. Balduzzi et al. [64] demonstrated that their SDR-based attack successfully injected fake AtoNs. As noted by Androjna et al. [66], in a 2020 incident at Ponce de Leon Inlet, Florida, attackers used AIS spoofing to inject entirely fabricated virtual buoys, illustrating how digital AtoNs can be manipulated to threaten maritime safety.

 doi:10.20944/preprints202605.0928.v1

AIS Hijacking: As defined by Balduzzi et al. [64], AIS hijacking refers to the manipulation or overriding of the AIS signal of a real, existing vessel. In such an attack, the adversary attempts to assume a legitimate vessel's identity or communication channel and alters its broadcasted data (such as location, speed, heading, or identity). Walde and Einar [83] demonstrate that AIS hijacking is feasible using the AISTX, an open-source software-defined AIS transmitter developed by Balduzzi et al. [64].

Application-Specific Messages (ASM): Although not directly involved in manipulating core AIS data, sophisticated attackers can exploit binary messages to inject malware and compromise vessel systems. Amro et al. [84] explored cybersecurity threats in maritime environments by demonstrating how AIS can serve as a covert channel for Command & Control (C&C)[7] in cyberattacks. Their work highlights inherent AIS vulnerabilities, particularly its lack of encryption and authentication, which makes it susceptible to unauthorized transmissions and cyber manipulation.

The authors introduced a novel attack vector in which AIS messages are used to transmit commands to compromised shipboard systems, underscoring the risks to autonomous maritime operations. Using the MITRE[7] framework, they developed a threat model focusing on C&C and defense evasion techniques. Their proof of concept demonstrated how encrypted commands could be embedded within AIS Type 8 messages using AES encryption and Base32 encoding. Furthermore, they simulated two cyber kill chains[7] targeting an autonomous passenger ship (APS), illustrating the feasibility of remote malware control via AIS.

3.2.7. Consequences of AIS Manipulations

AIS manipulation can have far-reaching consequences across various domains:

Safety and Navigation: Manipulated AIS data can mislead vessels, potentially causing deviations from planned routes, collisions, groundings, and other navigational hazards. Such incidents endanger crew safety and pose significant risks of environmental damage, including oil spills and marine ecosystem disruptions.

Khandker et al. [65] highlighted the critical role of AIS in vessel tracking, collision avoidance, and maritime traffic management while emphasizing its lack of encryption and authentication mechanisms, making it susceptible to spoofing, jamming, and Denial-of-Service (DoS) attacks. Their study conducted a detailed AIS data analysis, detecting anomalous vessel behaviors and identifying unexpected course deviations through live AIS data streams. By simulating AIS spoofing and jamming attacks using SDRs, the authors demonstrated the impact of these threats on navigation safety and operational efficiency. They employed machine learning-based anomaly detection, utilizing clustering algorithms (K-means, DBSCAN) and neural networks for real-time detection of AIS anomalies. A quantitative risk assessment framework was also developed, integrating multi-criteria decision analysis (MCDA) to prioritize cyber risk mitigation strategies. They used cryptographic techniques for data integrity and authenticity and multi-source data fusion methods to mitigate spoofing risks. The authors advocated for enhanced cybersecurity policies aligned with IMO MSC.428(98) [19], contributing to the ongoing research efforts in securing maritime navigation systems.

Security and Law Enforcement: The transmission of falsified AIS information can obscure a vessel's true identity, hindering law enforcement efforts to monitor and intercept illicit activities such as smuggling, piracy, and illegal fishing. This compromises maritime security and facilitates unlawful operations.

Geopolitical and Strategic: Fabricating AIS data in sensitive maritime regions can escalate geopolitical tensions, leading to miscalculations or military confrontations. AIS spoofing can also be leveraged to create false narratives, manipulate maritime traffic patterns, and gain strategic advantages in contested waters.

4. Proposed AIS Security Measures

Although AIS plays a crucial role in maritime safety, navigation, and traffic management, it remains susceptible to cyber threats such as spoofing, hijacking, data manipulation, and denial-of-

 doi:10.20944/preprints202605.0928.v1

service, posing substantial risks to maritime security and operational reliability [85]. This motivates the deployment of effective security measures.

This section surveys measures proposed in the literature and organizes them along two axes: (i) *categories*: Protocol & Cryptography; Endpoints & Network; Analytics & Detection; Resilience & Redundancy; and Governance, People & Ecosystem; and (ii) *incident lifecycle phase*: Prevent (P), Detect (D), Respond (R), Recover (Rv). The taxonomy appears in Figure 5. The measures are designed to operate within AIS's open architecture while accommodating key management constraints and maintaining backward compatibility with legacy maritime systems.

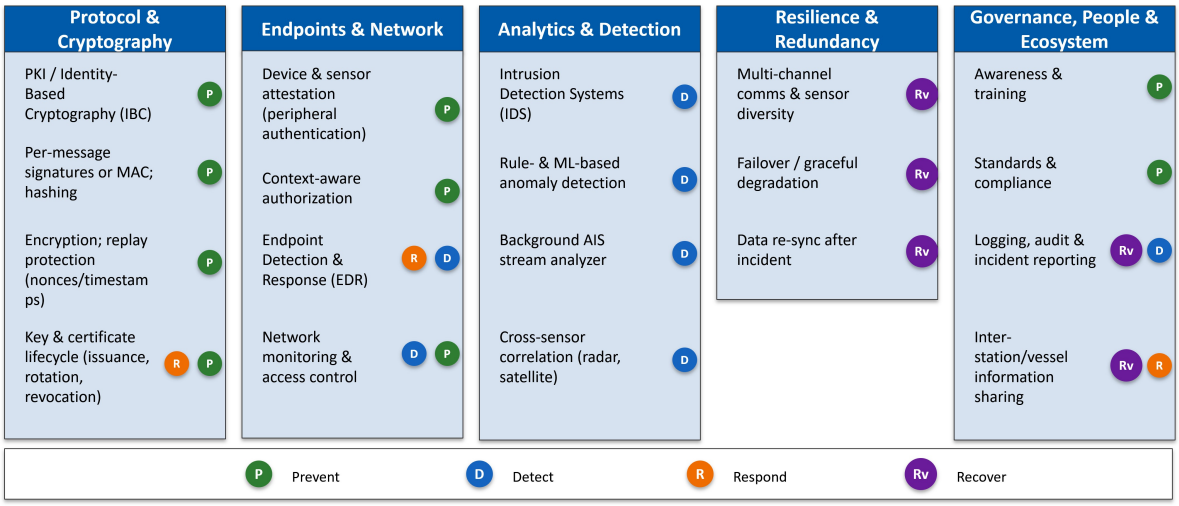


Figure 5. AIS Security Measures: Categories & Lifecycle Coverage.

4.1. Design Constraints for AIS Security Measures

4.1.1. Open Broadcast Model

AIS relies on an open Self-Organizing Time-Division Multiple Access (SOTDMA) broadcast without built-in authentication, integrity, or replay protection[7]. These properties enable spoofing and data manipulation. Any enhancement must preserve interoperability and receiver compatibility across the installed base.

4.1.2. Key Management

Cryptographic assurances (signatures/MACs[7], encryption, replay protection) depend on scalable *key management* across a worldwide fleet with intermittent connectivity and diverse equipment. Approaches include public key infrastructure (PKI)[7] and context-bound symmetric authorization (e.g., deriving short-lived keys from time and small geographic tiles using a lightweight cipher such as RC5 [86], suitable for underwater assets that surface only briefly) [87]. Keys should be generated under audited multi-person control and distributed securely when assets surface; lifecycle operations (issuance, rotation, revocation/status) must be feasible at sea.

4.1.3. Backward Compatibility

Security enhancements must coexist with legacy AIS transponders and infrastructure. Proposals should support gradual deployment and graceful degradation so that authenticated messages remain consumable by non-upgraded receivers.

4.2. Security Measures by Category

4.2.1. Protocol & Cryptography

Per-message authentication and confidentiality.

Message-authentication codes (cryptographic MACs)[7], digital signatures such as the Elliptic Curve Digital Signature Algorithm (ECDSA)[7], authenticated encryption with associated data (AEAD)[7],

 doi:10.20944/preprints202605.0928.v1

replay protection (timestamps/nonces[7]), and even signal-domain watermarking have been proposed to provide authenticity and integrity for AIS payloads [88–90]. Public-key cryptography has [91] likewise been explored for AIS messages (including Message 8, see Table 1) [90,92]. Because baseline AIS lacks these primitives, effective key management is a prerequisite for any deployment [93]. Taken together, these controls *prevent* spoofing and in-transit manipulation by binding each message to a verifiable sender and rejecting replays, and *support response* through rapid credential revocation and re-keying after compromise.

Identity-based and modular authentication. SecAIS leverages Identity-Based Cryptography (IBC)[7] with symmetric anonymization to simplify key distribution relative to classic PKI[7] [60,88,94]. Auth-AIS is a modular protocol that enables flexible authentication (signatures or MACs) while maintaining backward compatibility [95,96]. These approaches primarily *prevent* spoofing and content tampering via authenticity/integrity. Key rollover is the periodic replacement and revocation of keys, *supports response* to credential compromise.

Location/time-bound symmetric authorization. Time- and area-scoped keys authorize transmissions for specific contexts (e.g., underwater assets) where PKI[7] is impractical [87]. Binding authorization to place and time *prevents* unauthorized transmissions outside the designated parameters.

Attribute-based security and secure aggregation. For ship- and shore-side devices, attribute-based encryption (ABE[7]) with zero-knowledge proofs[7] gives policy-based, fine-grained access to data. It also enables integrity-preserving aggregation: combining readings from many devices into summaries (such as counts or averages) with cryptographic evidence that the summary hasn't been tampered with, even if individual readings stay hidden. These controls *prevent* unauthorized access and forgery while scaling to large fleets and port installations [97].

4.2.2. Endpoints & Network

Device & sensor attestation and RFF

Peripheral authentication and context-aware authorization act *preventively* by admitting only devices that can cryptographically attest their identity and state (e.g., challenge–response with signed measurements), blocking rogue or tampered sensors; they act *detectively* by continuously checking attestation results and Radio-Frequency Fingerprints (RFFs[7]) against enrolled profiles to flag changes in a device's RF "signature," detect copied or relayed transmitters, and highlight other signs of spoofing [98].

EDR and IDS on vessel/shore endpoints. Endpoint Detection and Response (EDR) combines continuous monitoring with automated containment or remediation on compromised endpoints. Monitoring, anomaly alerts, and forensic visibility contribute to *detection*, while containment and remediation actions serve the *response* phase. Complementing EDR, Intrusion Detection Systems (IDS) provide rule-based or anomaly-based identification of suspicious traffic, strengthening *detection* but typically lacking built-in response capabilities. Together, EDR and IDS extend protection beyond cryptographic mechanisms by covering runtime compromise and malicious behavior on both shipborne and shore-based AIS endpoints [99,100].

Secure transport between Remote Base Stations (VPN)[7] VPNs create encrypted, mutually authenticated tunnels between RBSs and shore systems. This *prevents* eavesdropping, tampering, and session hijacking across the links between remote base stations and shore systems by enforcing confidentiality and integrity at the transport/network layer (e.g., IPsec/TLS[7] with forward secrecy, so past sessions stay confidential even if a long-term key is later compromised). They complement message-level authentication for AIS content integrity end-to-end [101].

Network monitoring & access control. Port-based network access control (IEEE 802.1X/EAP-TLS; a switch only forwards normal traffic after the device authenticates) and switch-port security (limit each port to known MACs, disable unused ports, auto-shut on violations) on wired/wireless edges [102], together with least-privilege ACLs (permit only required flows) and VLAN/micro-segmentation that separates IT from OT and confines breaches [43,45,103,104], *prevent* unauthorized attachment and

 doi:10.20944/preprints202605.0928.v1

lateral movement[7]. Flow and packet monitoring, integrated with IDS/IPS and a SIEM[7] and compared to traffic baselines, helps *detect* policy violations and unusual network traffic [43,104].

4.3. Analytics & Detection

4.3.1. ML/Statistical Anomaly Detection

Model-based and ML approaches, such as deep learning models [105], unsupervised clustering [106], and time-series/state-space models [107], *detect* motion irregularities, shutdowns, transshipment patterns, and identity/route anomalies by exploiting position/velocity/heading/rate-of-turn time series, inter-message gaps, and identity–trajectory consistency [89].

Trajectory prediction (baselines for "normal"). Sequence models [108] learn expected paths and next-step motion so that deviations can be scored as anomalies, using recurrent or other sequential architectures [109]; these strengthen detection of spoofed tracks and implausible Closest Point of Approach (CPA) alerts [110–116].

Learning normal route patterns from clustering Clustering historical AIS trajectories learns the normal *traffic context*: main shipping lanes and port-approach routes, typical speed and turn-rate profiles, and usual anchorages and waiting areas for a given region, season, or vessel class [117–122]. Vessels that deviate from these learned routes or cluster structures are flagged as outliers. To keep computation tractable at scale, trajectories are first simplified (e.g., adaptive Douglas–Peucker [118]) and then processed on distributed platforms (e.g. Apache Spark [123]).

General anomaly detectors. Practical systems use simple motion features plus ML to flag vessels going dark, making unusual maneuvers, or showing long gaps/shutdowns. Typical designs combine clustering with sequence models and apply missing-data reconstruction checks; for example, they interpolate over short gaps and verify that the implied speeds/turn rates remain physically plausible [124–127].

Behavior/state classification. Supervised models classify movement or navigational status from trajectories to support rule- and risk-based alerting [128–130].

Event-type detectors. Purpose-built methods target close-approach/rendezvous and at-sea transfer patterns, improving precision for sanction-relevant behaviors [131].

Operational monitoring. Production systems turn the detection techniques described above into practical tools for watchstanders: continuous monitoring, clear and prioritized alerts (with context), and smooth integration into existing workflows for triage and follow-up [132].

4.3.2. Scalable Pipelines for Large AIS Corpora

Distributed data platforms such as Apache Spark [123] and Hadoop [133] let teams process large AIS archives in parallel, accelerating trajectory cleaning, feature extraction, and clustering for detection at scale [122,123,133]. A common pipeline first simplifies raw tracks with the Douglas–Peucker algorithm [134] to reduce points, then clusters the simplified trajectories with DBSCAN [135] to recover main routes; deviations from these routes can be flagged as anomalies [119,134,135]. Statistical models over the clustered data then estimate how typical each movement pattern is and highlight low-probability behavior, improving precision on risky patterns [136].

4.3.3. Text–Sensor Inconsistency Detection

Prieur et al. [137] propose UMBAR, an end-to-end system that ingests AIS/radar ("hard data") and news/open-source intelligence (OSINT)[7] ("soft data"), builds a maritime knowledge base, and cross-checks events across sources. In practice, it *detects* mismatches in a vessel's identity, location, or dates between sources; *supports response* by ranking flagged items with simple similarity scores and short explanations for operator review; and *aids recovery* by keeping provenance so records can be corrected later. On its own, it does not *prevent* forged or replayed messages; pair it with cryptographic authentication and device attestation for prevention.

 doi:10.20944/preprints202605.0928.v1

4.3.4. Background AIS Stream Analyzer

Lightweight, rule-based checks (e.g., rate limits, MMSI[7] reuse, physically impossible movement) can *detect* simple abuses quickly and provide triage before ML models run [85,89].

4.3.5. CTI-Driven Maritime IoT Detection

Deep-learning pipelines that use cyber threat intelligence (CTI) together with network telemetry can classify attack types and *detect* new malicious patterns in maritime IoT traffic [138].

4.4. Resilience & Redundancy

4.4.1. Cross-Sensor Validation and Coverage Gaps

Fusion of AIS with radar, satellite, electro-optical (EO), and infrared (IR) imagery, and maritime OT maintains continuity and cross-checks AIS claims when AIS is incomplete or manipulated [65,139–144]. Empirical work uses dedicated *aerial surveys*, that is, survey aircraft carrying EO/IR cameras plus an onboard AIS receiver, to estimate the share of non-AIS vessels and to correct vessel-density maps (vessels per km^2) by accounting for the surveyed area, i.e., the water surface actually observed along flight transects (transect length $\times$ effective strip width adjusted for detection probability) [145].

4.4.2. Failover, Graceful Degradation, and Data Re-Sync

In operational deployments, AIS and related systems are commonly engineered with backup channels and sensors, along with defined fallback modes to maintain service during outages or interference [141–143]. During the *recovery* phase, typical actions include reloading missing AIS data, reconciling any altered records, and preserving explicit provenance (what data came from where and when) throughout restoration, consistent with maritime cyber-resilience guidance [16,23,51].

4.5. Governance, People & Ecosystem

4.5.1. Risk Assessment and Cyber Situational Awareness

Continuous risk assessment and cyber situational awareness (CSA) (seeing what is happening, understanding it, and anticipating what may happen next) support early warning and *detection*. Common tools include (i) Failure Modes and Effects Analysis (FMEA) per IEC 60812 to list and score failure modes by severity, likelihood, and detectability, and (ii) Bayesian networks (BNs) to update those risk scores as new evidence arrives (e.g., sensor readings, alerts). Many works combine the two: FMEA structures the hazards, then key factors are mapped into a BN so probabilities can be updated online [2,100,146–152]. Broader taxonomies frame vulnerabilities and mitigations at the system-of-systems scope [153].

4.5.2. Taxonomies and Holistic Frameworks

Sector-wide frameworks help plan mitigations and resilience across technical and human factors. Examples include MaCRA, which models assets, threats, and operating context (route/ship/area) to rank risks and test mitigations, and the policy framework of Tam & Jones, which maps stakeholders (ship, company, port/authority, regulator) and ship/shore attack surfaces to guide defense-in-depth and risk management [154,155].

4.5.3. Crew Training and Awareness

Training to spot GPS/AIS inconsistencies (e.g., jumps, illogical motion, cross-sensor conflicts) and to handle systems securely *prevents* human-factor incidents and improves *detection* when data is suspect [18,45,53,54].

4.5.4. Collaboration and Information Sharing

Trusted information-sharing initiatives and verification of nearby vessel activity strengthen *prevention* and coordinated *response* [156–158].

 doi:10.20944/preprints202605.0928.v1

4.5.5. Regulation and Compliance

Key frameworks and standards include: *IMO/ISM*—cyber risk integrated into the Safety Management System with guidance for preparation, detection, response, and restoration [19,20,50–52]; *EU NIS/NIS2*—risk-management measures and incident reporting for essential/important entities [24]; *Classification and national guidance*—defense-in-depth objectives and operational practices [16,23,53]; and *ISO/IEC 27001*—an ISMS for ongoing risk treatment and improvement [44].

5. Previous Surveys

This section summarizes prior survey papers spanning maritime cybersecurity, AIS analytics, anomaly detection, human/organizational aspects, and enabling methods. Table 2 groups surveys by theme and highlights their scope and relevance to AIS security.

Positioning & contributions beyond prior surveys.

In contrast to anomaly/application-only reviews or broad maritime-cyber surveys, our work is AIS-first and security-focused. Specifically, we:

* **Protocol-centric AIS overview.** We provide a standards-referenced AIS primer (message set, TDMA access, terrestrial vs. satellite reception, NMEA framing) and use it to surface first-principles weaknesses (unauthenticated broadcast, integrity/replay gaps, GNSS dependency) that drive downstream attack classes (e.g., [102, 104, 106], representative exploits, and threat demonstrations [4, 6, 7, 17, 84, 86]).

* **Synthesize protocol and operational defenses.** Beyond anomaly-detection surveys (e.g., [159]), we connect broadcast-authentication proposals and their compatibility limits (e.g., [52, 83, 131, 158]) with endpoint/network hardening, governance, and resilience practices across the ship/shore ecosystem, organizing measures by category and incident-lifecycle phase (e.g., [39, 66, 101, 105, 109, 112, 119, 123, 139]).

* **Operationalization guidance.** We consolidate evaluation practice (spatiotemporal CV; leakage avoidance), alerting/triage patterns, multi-sensor fusion ([119]), and MLOps/monitoring for live AIS analytics ([101])—topics typically outside anomaly-centric or policy-centric surveys (e.g., [16, 159]).

* **Gap analysis and research agenda.** We articulate open problems by contrasting anomaly/application surveys ([103, 146, 159, 164]), sectoral cybersecurity/policy work ([21, 113, 130]), and protocol/authentication proposals ([52, 83, 131, 158]).

Table 2. Representative surveys relevant to AIS security, anomaly detection, and maritime cyber risk.

Category	Main Research Topic	Reference	Scope and relevance to AIS security
Data mining methods for maritime mobility	Methods and tasks in maritime data mining (route extraction, anomaly detection, ETA, etc.)	Troupiotis-Kapeliaris et al. [159]	Methodological overview framing AIS as rich, free-space mobility data; motivates task taxonomies used by AIS anomaly detectors.
AIS anomaly detection (surveys)	AIS track anomalies: taxonomies, methods, datasets	Wolsing et al. [89]	Consolidates anomaly types (route deviation, AIS-silent operation, close approach, zone entry) and families of methods; baseline for evaluating AIS-specific ML.
Vessel anomaly detection (SLRs using AIS and fused sensors)	Abnormal vessel behaviour detection using AIS (sometimes SAR/radar fusion)	Ferlansyah et al. [139]	Systematic review of anomaly targets and pipelines; complements Wolsing's taxonomy with sensor-fusion angles.

Continued on next page

 doi:10.20944/preprints202605.0928.v1

Continued from previous page

Category	Main Research Topic	Reference	Scope and relevance to AIS security
General anomaly detection (method survey)	ML anomaly detection techniques (classification, clustering, statistical, information-theoretic)	Toshniwal et al. [160]	Technique-level survey; provides algorithmic choices and trade-offs that appear in AIS detectors.
AIS data for intelligent navigation	AIS for route estimation, collision prediction, anomaly detection, path planning	Tu et al. [161]	End-to-end view of AIS applications; clarifies data quality issues that affect ML-based AIS security analytics.
AIS applications (broad)	AIS applications 2003–2018 (safety, behaviour, environment, trade, performance)	Yang et al. [162]	Maps "basic/extended/advanced" AIS applications; situates security analytics within broader AIS use.
Big data/AI in maritime (bibliometric)	Bibliometric review of AI/big-data applications in maritime	Munim et al. [163]	Identifies clusters and trends (including AIS analytics); useful to position contributions.
Maritime cybersecurity (broad, system/port focus)	Cybersecurity advances and challenges on vessels and in ports	Ben Farah et al. [164]	Taxonomy of maritime cyberattacks (incl. spoofing/jamming) and vulnerable components; motivates AIS hardening and detection.
Maritime cybersecurity (incidents/perspective)	Threats, notable incidents, sector challenges	Park et al. [165]; CyberKeel [80]	Early incident- and threat-oriented views that include GNSS/AIS misuse; provides operational context for AIS threats.
Cyber seaworthiness / policy	Cyber risk, regulation, and implications for seaworthiness	Schinas et al. [166]	Policy/assurance perspective; highlights need for training, patching, and reporting—complements technical AIS countermeasures.
Human/organizational factors and risk perception	HOF techniques; cyber risk perception in maritime	Wu et al. [167]; Larsen et al. [168]	Shows how operator behaviour, training, and perception impact detection/response to AIS spoofing/jamming/data manipulation.
MASS cybersecurity	Cybersecurity for Maritime Autonomous Surface Ships (MASS)	Tabish et al. [169]	Overlapping attack surface (GNSS/AIS comms); discusses IDS/ML and protocol hardening applicable to AIS ecosystems.
OT data fusion for cyber/ops awareness	Fusion of AIS, radar, DF/SIGINT for anomaly and incident detection	Potamos et al. [143]	Evidence that multi-sensor fusion improves detection robustness vs. AIS-only signals; relevant for anti-spoofing.
MLOps in maritime	ML lifecycle and orchestration in maritime settings	Morariu et al. [170]	Argues for pipelines/retraining/monitoring, directly addressing deployment of AIS anomaly detectors at scale.
Vision-based maritime awareness	Vision-based situational awareness (detection, ReID, tracking)	Qiao et al. [140]	Non-AIS sensing that can corroborate AIS-based detections and reduce false alarms via multi-modal fusion.
Supply-chain cybersecurity (impacts/defences)	Cyber-attack impacts/defences in maritime supply chains	Clavijo Mesa et al. [171]	Sector-level practices (18 best practices) that include securing AIS data flows and response procedures.

Continued on next page

 doi:10.20944/preprints202605.0928.v1

Continued from previous page

Category	Main Research Topic	Reference	Scope and relevance to AIS security
Trajectory prediction for anomaly detection (SLR)	AI for ship trajectory prediction / anomaly detection (regional SLR)	Badrudin et al. [172]	Focused SLR; catalogues trajectory-modelling techniques that underpin many AIS anomaly detectors.

Collectively, prior surveys (i) catalog AIS anomaly/misuse types [89,139], (ii) review ML methods and deployment patterns for AIS security [160–162,170], and (iii) describe the operational, human, and policy contexts [143,164–169,171]. Our review offers a comprehensive, up-to-date, security-first synthesis that unifies these strands.

6. Discussion and Recommendations

This section builds on the protocol mechanics (Section 2), the threats and vulnerabilities organized as a threat taxonomy (Section 3), and the mitigation families (Section 4) to set out concise, actionable recommendations for practice and priorities for research. In brief, AIS's open, self-reported SOTDMA broadcast (see timing/slot structure in Figure 2(**b**)) exposes known attack avenues: spoofing, VHF-channel denial-of-service (jamming), and data manipulation. We use the taxonomy in Figure 5 to organize our recommendations across *Protocol & Cryptography*, *Endpoint & Network*, *Analytics & Detection*, and *Governance & Resilience*, aligned to incident-lifecycle phases.

6.1. Protocol & Authentication Priorities

We recommend deployable authentication that respects AIS's legacy ecosystem (design constraints in Section 4) while improving message integrity and replay resistance. Practical options include carrying short signatures/MACs in application-specific binary AIS messages (e.g., application-specific binary payloads) or in standard optional/reserved fields where permissible, plus lightweight replay protection. When cryptographic keys are unavailable, auxiliary/physical-channel verification may be used to link the claimed MMSI to the actual vessel; for example, RF-emitter fingerprints [98] or peripheral/optical-attribute schemes adapted from vehicular systems [173–175].

Current status. No cryptographic message authentication or digital signatures are defined in the *International Telecommunication Union – Radiocommunication Sector* (ITU–R) Recommendation M.1371 for AIS; AIS management messages (e.g., 20/22/23) address channel/group management rather than message signing [176]. The *VHF Data Exchange System* (VDES) per ITU–R M.2092 integrates AIS, Application-Specific Messages (ASM), and VDE links and provides higher-capacity bearers in which authentication schemes could be carried; however, there is currently no IMO/ITU/IEC mandate for cryptographic authentication in AIS/VDES [177]. Auxiliary physical-channel verification is an active research direction, including radio-frequency specific emitter identification (RF-SEI) and optical/peripheral attribute binding adapted from vehicular systems [178–180].

6.2. Advanced Anomaly Detection

Detection should move beyond inactivity/silence flags toward behavior-aware models (Section 4; see field semantics in Table 1 and TDMA timing in Figure 2(**b**)). Models must be stress-tested against falsification tactics surveyed in Section 3, and regularly updated to track SDR-enabled attack evolution. Pointers to specific approaches appear in Section 4.3.

Current status. Behavioral anomaly/spoofing detection is widely deployed *shore-side* by commercial analytics providers and NGOs (e.g., "dark shipping," AIS position validation, identity/track inconsistency detection); these are operational practices rather than prescriptive AIS standards, and no IMO/ITU/IEC text specifies particular ML models [181–184].

 doi:10.20944/preprints202605.0928.v1

6.3. Fuse AIS with Independent Sensors and Cross-Check Discrepancies

In practice, combine AIS with independent sources (e.g., ship/shore radar, satellite AIS, EO/IR imagery) and automatically flag inconsistencies. Handle flagged cases using defined incident-response procedures during the *Detect* and *Respond* phases in Figure 5. Section 4.4.1 outlines integration patterns and how to balance latency with operator triage.

Current status. Operational today on bridge and ashore: *International Electrotechnical Commission* (IEC) standards specify radar performance and AIS target handling/association (IEC 62388) and the portrayal of navigation information on shipborne displays (IEC 62288); IMO circulars standardize how navigation symbols are shown, and ECDIS, radar, and AIS systems implement these rules to associate AIS with radar targets and flag inconsistencies [185–187].

6.4. Machine Learning Operations (MLOps), Evaluation, and Datasets

Live analytics should ship with versioned datasets, leakage-safe evaluation, drift monitoring, and reproducible benchmarks tied to the misuse categories in Section 3 and the coverage taxonomy in Figure 5. This supports safe iteration as traffic patterns and attacker behavior change.

Current status. These practices are common in vendor/authority analytics stacks but are *not* prescribed by maritime technical standards; IMO cyber guidance is intentionally high-level and process-oriented [18].

6.5. Governance, Collaboration, and Human Factors

Because AIS operates in a heterogeneous, safety-critical ecosystem, controls must include crew training, Standard Operating Procedures (SOPs), and clear authority and hand-off rules across Vessel Traffic Service (VTS); shore-based traffic management and bridge workflows (the ship's on-watch, pilotage, and decision-making processes), not only technical hardening (cf. Governance & Resilience in Figure 5). Where appropriate, cooperative consistency checks and secure consensus among stations (for example, Byzantine agreement to corroborate shared alerts) can strengthen collective defense [188].

Current status. At the *process* level, these controls are mandated via the *International Safety Management (ISM) Code* through IMO Resolution MSC.428(98) (requiring cyber risk to be addressed in the Safety Management System) and the updated IMO MSC-FAL.1/Circ.3/Rev.3 guidelines [18,19].

6.6. Resilience, Recovery, and Broader Implications

It is recommended to engineer for graceful degradation and rapid recovery (see Prevent/Detect/Respond/Recover in Figure 5). During slot congestion or RF interference, prioritize safety-critical traffic and temporarily defer or down-sample low-priority transmissions (e.g., static/voyage fields, nonessential ASM) so essential collision-avoidance information continues to flow. When authentication is unavailable, don't blank the display: continue to show AIS targets but (i) flag them as unverified/low-trust, (ii) throttle and inspect the stream, and (iii) validate against other sensors (radar/EO/GNSS/eLoran). Blocking every unauthenticated message can degrade situational awareness. For recovery, rely on clear, tested incident-response and restoration procedures: isolate the fault, switch to alternate sensors/links, re-synchronize and reconcile delayed or suspect data, restore normal configuration, and conduct a post-incident review.

Current status. *VHF Data Link (VDL)* load/channel management and group assignment are supported by AIS management messages (e.g., 20/22/23) in ITU–R M.1371 and by *International Association of Marine Aids to Navigation and Lighthouse Authorities* (IALA) Recommendation A-124 and its appendices on channel and VDL management; VDES (ITU–R M.2092) adds extra data links so operators can prioritize traffic by service. Per IEC 62288/IMO guidance, bridge displays use standardized symbols and show lost/degraded target alerts; there is no standardized "cryptographic trust" flag because AIS has no protocol-level signing standard [176,177,186,187,189,190].

 doi:10.20944/preprints202605.0928.v1

Author Contributions: Main contribution by the first author. Second and third authors contributed equally.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Cybersecurity-Related Terms

In this appendix, we provide a short glossary of key cybersecurity terms.

Attack Surface

The attack surface is the full set of ways an adversary could interact with or reach a system: software and firmware interfaces, network services, hardware ports, exposed data, third-party dependencies, and human/operational processes.

Attack Vectors

Attack vectors are the specific paths used to exploit vulnerabilities, such as credential compromise (e.g., phishing), weak or default passwords, misconfiguration or exposed services, unpatched software or firmware, supply-chain compromise, and physical intrusion.

BYOD (Bring Your Own Device)

A policy or practice allowing personnel to use personally owned phones, tablets, or laptops for work purposes. BYOD expands the attack surface through heterogeneous, variably managed endpoints that may lack enterprise-grade controls.

Command & Control (C2)

Command-and-Control (C2) is the communication channel by which an attacker remotely issues instructions to compromised systems, moves data (exfiltration), stages payloads, and coordinates follow-on actions.

CPS (Cyber-Physical Systems)

Systems in which computational components (software, networking) tightly interact with physical processes via sensors and actuators. In maritime settings, CPS include navigation, propulsion, and cargo-handling subsystems.

GDPR

The General Data Protection Regulation (GDPR) is the EU's data-protection law governing the processing of individuals' personal data in the EU/EEA. It grants data-subject rights, imposes duties on controllers/processors, and enables significant penalties for non-compliance. It can apply extraterritorially to organizations outside the EU/EEA that offer goods/services to or monitor EU/EEA data subjects.

IT

Information Technology (IT) encompasses computing and networking systems that process business and administrative data (e.g., enterprise applications, databases, email, identity services), distinct from OT systems that directly monitor or control physical processes.

Kill Chain

The (Cyber) Kill Chain is a model that decomposes an intrusion into stages (e.g., reconnaissance, weaponization, delivery, exploitation, installation, C2, actions on objectives). Many teams also use MITRE ATT&CK to describe tactics and techniques across these stages.

 doi:10.20944/preprints202605.0928.v1

Lateral Movement

The set of actions an adversary takes after initial access to move within a network, reusing credentials, exploiting trust and permissions, and pivoting between hosts, to reach higher-value systems or data.

MITRE ATT&CK (and D3FEND)

MITRE ATT&CK is a curated knowledge base of adversary tactics, techniques, and procedures derived from real intrusions (with Enterprise and ICS matrices). MITRE D3FEND complements it by mapping defensive countermeasures to ATT&CK techniques.

OSINT (Open-Source Intelligence)

Information gathered from publicly available sources (e.g., news, social media, public records) used to support threat analysis, attribution, and situational awareness.

OT

Operational Technology (OT) comprises hardware and software that monitor or control physical processes in industrial environments (e.g., SCADA, PLCs, maritime sensors/actuators). OT systems emphasize safety and real-time operation and often interface with critical infrastructure.

Physical Attacks

Physical attacks target facilities, devices, or media (e.g., unauthorized entry, hardware tampering, device theft, interdiction), potentially leading to disruption or data compromise.

Risk

Risk is the potential for loss or harm when a threat exploits a vulnerability, commonly considered as a function of likelihood and impact.

Threat

A threat is a potential cause of an unwanted incident (actor, capability, or event) that could exploit a vulnerability.

Appendix B. Maritime Safety and Navigation System Terms

This appendix provides a short glossary of key navigation system terms.

ARPA

Automatic Radar Plotting Aid (ARPA) automatically acquires/tracks targets and computes course, speed, closest point of approach (CPA), and time to CPA (TCPA). By displaying this data with collision alarms, ARPA supports rapid manoeuvring decisions without manual plotting.

AtoNs

Aids to Navigation (AtoNs) are physical or electronic markers (e.g., buoys, beacons, lights) that indicate routes and hazards. AIS enables AIS AtoNs—real, remote, or virtual signals transmitted for display on electronic charts to improve situational awareness.

ECDIS

Electronic Chart Display and Information System (ECDIS) integrates electronic navigational charts (ENCs) with sensor inputs (e.g., GNSS, radar, AIS). ECDIS supports route planning/monitoring and, for certain vessels, meets SOLAS carriage requirements.

 doi:10.20944/preprints202605.0928.v1

eLORAN

eLORAN is a modernized, low-frequency terrestrial PNT system that derives position, velocity, and timing from high-power pulses. Its ground-based, high-power signals make it a resilient backup when GNSS is unavailable, degraded, or spoofed [72].

ENISA

The European Union Agency for Cybersecurity (ENISA) provides expertise, supports policy, and coordinates with Member States and industry on risk management, incident response, and best practices [191].

GMDSS

The Global Maritime Distress and Safety System (GMDSS) is an internationally mandated framework that uses satellite and terrestrial communications to carry distress alerts, safety communications, and navigational warnings.

GNSS

Global Navigation Satellite Systems (GNSS) are satellite constellations that provide positioning, navigation, and timing (PNT) services worldwide. Examples include the U.S. Global Positioning System (GPS) and the European Union's Galileo [192]. Maritime systems commonly fuse GNSS with other sensors for resilience.

GPS

The Global Positioning System (GPS) is a U.S. GNSS providing precise position and time using signals from a constellation of satellites. Receivers compute position by trilateration from multiple satellites.

IMO

The International Maritime Organization (IMO) is the UN specialized agency for shipping safety, security, and environmental performance.

Industry 4.0

Industry 4.0 refers to the integration of AI, IoT, cloud computing, and data analytics into industrial processes to create highly automated, data-driven production systems [35,193].

MMSI

The Maritime Mobile Service Identity (MMSI) is a unique nine-digit identifier assigned (via national authorities/ITU processes) to ships, coast stations, and other maritime radios for use in DSC, AIS, and GMDSS.

PNT (Positioning, Navigation, and Timing)

A collective term for the position, navigation, and time references required by maritime and other systems. PNT is typically provided by GNSS and can be augmented by terrestrial systems (e.g., eLORAN) and onboard sensors.

SART

An AIS Search and Rescue Transmitter (AIS-SART) broadcasts its position and a unique identifier to nearby AIS-equipped vessels and rescue centers, aiding rapid localization during emergencies.

 doi:10.20944/preprints202605.0928.v1

SDR

A Software-Defined Radio (SDR) implements radio functions (e.g., filtering, modulation, decoding) in software rather than fixed hardware, enabling flexible transmit/receive across bands. In AIS contexts, SDRs can be used to eavesdrop, spoof, or jam communications.

SOLAS

The International Convention for the Safety of Life at Sea (SOLAS) [28] sets minimum safety standards in construction, equipment, and operation of merchant ships. Among other things, SOLAS establishes carriage requirements relevant to navigation and communications (e.g., AIS and, for certain vessels, ECDIS).

SOTDMA

Self-Organized Time-Division Multiple Access (SOTDMA) is a TDMA variant in which participants reserve and reuse timeslots without a central controller. In AIS, SOTDMA underpins slot self-organization within VHF channels as specified in ITU-R M.1371.

VDR

Voyage Data Recorder (VDR) continuously records key navigational and operational data (including bridge audio) to support incident reconstruction and safety investigations.

Appendix C. Cryptography & Network-Security Terms

In this appendix, we provide a short glossary of Cryptography & Network-Security Terms.

ABE (Attribute-Based Encryption)

A public-key scheme where decryption rights are tied to attributes or policies, enabling fine-grained access control across many devices/users [194].

AEAD (Authenticated Encryption with Associated Data)

Encryption that simultaneously provides confidentiality and integrity for the ciphertext and optionally authenticates unencrypted, associated headers [195].

ECDSA

Elliptic Curve Digital Signature Algorithm, a compact digital-signature scheme used to authenticate data and bind it to a key pair [196].

IBC (Identity-Based Cryptography)

A public-key paradigm where a user's identity (e.g., an MMSI) serves as the public key, simplifying distribution at the cost of a trusted private-key generator [197,198].

MAC (Message Authentication Code)

A symmetric integrity tag computed over a message and a shared key, used to detect forgery and tampering [199].

Nonce

A number used once (e.g., counter or random value) to ensure uniqueness for replay protection and to derive per-message keys [200].

PKI

Public Key Infrastructure: the processes and roles (CAs, certificates, revocation) that manage key lifecycles for entities at scale [201].

 doi:10.20944/preprints202605.0928.v1

Replay Protection

A mechanism that prevents duplicated or stale messages from being accepted by verifying freshness data and keeping per-sender state so replays and out-of-order messages are rejected.

RFF (Radio-Frequency Fingerprint)

Device-unique analog/PHY artifacts (e.g., IQ impairments) learned from RF emissions to help distinguish genuine transmitters from clones/relays [202].

SIEM

Security Information and Event Management: centralized collection, correlation, and alerting over logs/telemetry for detection and response [203].

TLS

Transport Layer Security: a widely used protocol that provides channel confidentiality and integrity for TCP-based connections (e.g., HTTPS, VPN tunnels) [204].

VPN

Virtual Private Network: an authenticated, encrypted tunnel (e.g., TLS-, IPsec-, or WireGuard-based) protecting data in transit across untrusted networks [205].

Zero-Knowledge Proof (ZKP)

A cryptographic protocol that proves a statement is true without revealing the underlying secret (e.g., membership or attribute possession) [206].

References

1. of Ports, I.A.; (IAPH), H.; the International Cargo Handling Coordination Association (ICHCA).; Club, T.; (WPSP)., W.P.S.P. *PORT COMMUNITY CYBER SECURITY*. International Association of Ports and Harbors, 2020. https:https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf.
2. Androjna, A.; Twrdy, E. Cyber Threats to Maritime Critical Infrastructure. In *Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection*; Ministry of Defence, Republic of Slovenia; Institute for Corporative Security Studies; Joint Special Operations University: Ljubljana, Slovenia, 2020; pp. 163–170.
3. the European Parliament.; of the Council of 27 April 2016. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. European Union, 2016.
4. United Nations Conference on Trade and Development (UNCTAD). Review of Maritime Transport 2023. https://unctad.org/publication/review-maritime-transport-2023, 2023. United Nations.
5. Loomis, W.; Singh, V.V.; Kessler, G.C.; Bellekens, X. RAISING THE COLORS: Signaling for Cooperation on Maritime, Cybersecurity. Technical report, Atlantic Council : Scowcroft Center for Strategy and Security, 2021.
6. Trade, U.; (UNCTAD), D. Review of Maritime Transport 2024, 2024.
7. Carly, P. Maritime giant DNV says 1,000 ships affected by ransomware attack, 2023.
8. Kouras, B. Cyberattack Hits Multiple Greek Shipping Firm, 2021.
9. Valour Consultancy. Maersk cyber attack: lessons learned. https://valourconsultancy.com/maersk-cyber-attack-lesson-learned/, 2017. Blog post.
10. Pownall, C. The Context and Impact of Maersk's NotPetya cyber attack. Master's thesis, King's College London, Department of War Studies, 2019.
11. Steinberg, S.; Stepan, A.; Neary, K. NotPetya: A Columbia University Case Study, 2021.
12. BIMCO.; of Shipping of America, C.; of Shipping (ICS), I.C.; Al.. *The Guidelines on Cyber Security Onboard Ships V4*. International Chamber of Shipping (ICS); BIMCO; Chamber of Shipping of America, 2021. https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf.

 doi:10.20944/preprints202605.0928.v1

13. of Ports, I.A.; Harbors. *IAPH Cybersecurity Guidelines for Ports and Port Facilities Verson 1.0*. International Association of Ports and Harbors, 2021. https://safety4sea.com/wp-content/uploads/2021/09/IAPH-Cybersecurity-Guidelines-2021_09.pdf.
14. B., D.; Trowbridge, B.; B., S.; B., M.; Curran, C.; Freeh, J.; Kim, L.; K., N.; Moore, L.; Park, C.H.; et al. U.S. Maritime Trade and Port Cybersecurity. Technical report, Homeland Security: DHS Public-Private Analytic Exchange Program, 2023.
15. Volz, D. Espionage Probe Finds Communications Device on Chinese Cranes at U.S. Ports, 2024.
16. DNV-GL, R.p.D.R.. *Cyber security resilience management for ships and mobile offshore units in operation*. DNV GL, 2016. https://www.dnv.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585/.
17. International Maritime Organization (IMO). International Maritime Organization (IMO) — official website. https://www.imo.org/, 2024. Accessed 2025-09-07.
18. Organization, I.M. Guidelines on Maritime Cyber Risk Management. IMO Circular MSC-FAL.1/Circ.3/Rev.3, 2025.
19. Organization, I.M. Maritime Cyber Risk Management in Safety Management Systems. IMO Resolution MSC.428(98), 2017.
20. Organization, I.M. *The International Safety Management (ISM) Code*. International Maritime Organization, 1993. https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx.
21. International Chamber of Shipping (ICS). International Chamber of Shipping (ICS) — official website. https://www.ics-shipping.org/, 2024. Accessed 2025-09-07.
22. Baltic and International Maritime Council (BIMCO). BIMCO — official website. https://www.bimco.org/, 2024. Accessed 2025-09-07.
23. of Homeland Security, U.D. *NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 01-20, GUIDELINES FOR ADDRESSING CYBER RISKS AT MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATED FACILITIES*. U.S. Department of Homeland Security, United States Coast Guard, 2020. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023.
24. Parliament, E.U. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. European Union, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L11483.
25. of ITU, I.R.R.S. *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band, Recommendation ITU-R M.1371-5*. International Telecommunication Union, 2014. https://www.itu.int/en/ITU-R/Pages/default.aspx.
26. for Marine Aids to Navigation, I.T.I.O. *IALA Guideline 1082 – An overview of AIS*. International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), 2016. Edition 2.0.
27. Raga, A.A. The Bab el-Mandeb Strait: Geopolitical considerations of the strategic chokepoint. Technical Report 18/2020, Instituto Español de Estudios Estratégicos (IEEE), 2020.
28. (IMO), T.I.M.O. *International Convention for the Safety of Life at Sea (SOLAS), 1974*. The International Maritime Organization (IMO), 1974. https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx.
29. November, U.S.C.G.A. AIS Messages, 2024.
30. Parliament, E.U. *DIRECTIVE 2010/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. European Union, 2010. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0065.
31. International Maritime Organization (IMO), London. *Guidance on the Use of AIS Application-Specific Messages (SN.1/Circ.289)*, 2010. Issued June 2010.
32. Icons8 LLC. Icons by Icons8. https://icons8.com, 2024. Icon set used in figures; accessed 2025-09-07.
33. (NMEA), T.N.M.E.A. *NMEA 0183 Interface Standard, Version 4.30*. The National Marine Electronics Association (NMEA), 2023.
34. Sutton, H.I. Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base, 2021.
35. Ajayi, O.; Bagula, A.; Maluleke, H. The Fourth Industrial Revolution: A Technological Wave of Change. In *Industry 4.0*; Gordan, M.; Ghaedi, K.; Saleh, V., Eds.; IntechOpen: London, United Kingdom, 2023. https://doi.org/10.5772/intechopen.100147.
36. Hamed, N.; Hanna, B.; Savvas, P. A systematic review of the implementation of industry 4.0 from the organisational perspective. *International Journal of Production Research* **2022**, *60*, 4365–4396. https://doi.org/10.1080/00207543.2021.2002964.

 doi:10.20944/preprints202605.0928.v1

37. Barthwal, N.; Agarwala, N. Industry 4.0 in the Shipping Industry: Challenges and Preparedness—The Prevailing Scenario the Digital Revolution in the Shipping Industry. 2019, 2019.
38. Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y.B.; Nosheen, S. A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems* **2023**, *24*, 2677–2690. https://doi.org/10.1109/TITS.2022.3164678.
39. de la Peña Zarzuelo, I. Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy* **2021**, *100*, 1–4. https://doi.org/https://doi.org/10.1016/j.tranpol.2020.10.001.
40. Boyes, H.; Isbell, R.; Luck, A. Code of practice: cyber security for ports and port systems. Technical report, Institution of Engineering and Technology (IET); Department for Transport, London, United Kingdom, 2016.
41. Boyes, H.; Isbell, R. Code of Practice Cyber Security for Ships. Technical report, Institution of Engineering and Technology (IET); Department for Transport, London, United Kingdom, 2017/2023.
42. Cruz, J.D. Rotterdam: Europe's Largest Port Targeted in Cyberattack Linked to Pro-Russian Hackers, 2023.
43. Pascoe, C.; Quinn, S.; Scarfone, K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) NIST.CSWP.29, National Institute of Standards and Technology, Gaithersburg, MD, 2024. https://doi.org/https://doi.org/10.6028/NIST.CSWP.29.
44. International Organization for Standardization (ISO).; International Electrotechnical Commission (IEC). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001.html, 2022. International standard.
45. Drougkas, A.; Sarri, A.; Kyranoudi, P. Cyber Risk Management for Ports: Guidelines for Cyber Security in the Maritime Sector. Technical report, European Union Agency for Cybersecurity (ENISA), 2020. Catalogue No. TP-02-20-790-EN-N.
46. Sepehri, A.; Vandchali, H.R.; Siddiqui, A.W.; Montewka, J. The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review. *Ocean Engineering* **2022**, *243*, 110162. https://doi.org/https://doi.org/10.1016/j.oceaneng.2021.110162.
47. Hyra, B. Analyzing the attack surface of ships, 2019. M.S. thesis, DTU Comput. Dept. Appl. Math. Comput. Sci., Technical Univ. Denmark, Lyngby, Denmark.
48. Argles, C.; Zaluska, E. A Conceptual Review of Cyber-Operations for the Royal Navy. *The Cyber Defense Review* **2018**, *3*, 43–56.
49. RANA, A. Commercial Maritime and Cyber Risk Management. *Safety & Defense, Vol.5 (1)* **2019**, *5*, 46–48.
50. International Maritime Organization (IMO). Recommendation on incorporating cyber risk management into Safety Management Systems. https://www.imo.org/, 2022. See circular MSC-FAL.1/Circ.3 and subsequent revisions.
51. International Association of Classification Societies (IACS). Recommendation on Cyber Resilience. IACS Recommendation 166 (Rec. 2020/Corr. 2, 2022), The International Maritime Organization (IMO), London, 2022. Corrigendum 2, April 2022.
52. International Maritime Organization (IMO), London. *MSC-FAL.1/Circ.3/Rev.2: Guidelines on Maritime Cyber Risk Management*, 2022. Adopted 7 June 2022.
53. for Transport, U.D. *Cyber Security Code of Practice for Ships*. Institution of Engineering and Technology (IET); Department for Transport, 2023.
54. Chupkemi, D.C.; Mersinas, K. Challenges in Maritime Cybersecurity Training and Compliance. *Marine Science and Engineering* **2024**, *12*, 1844–1858.
55. Kanwala, K.; Shi, W.; Kontovas, C.; Yang, Z.; Chang, C.H. Maritime cybersecurity: are onboard systems ready? *MARITIME POLICY & MANAGEMENT* **2024**, *51*, 484–502.
56. Afenyo, M.; Caesar, L.D. Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management* **2023**, *236*, 106493. https://doi.org/https://doi.org/10.1016/j.ocecoaman.2023.106493.
57. Chen, S.; Lin, W.; Zeng, C.; Liu, B.; Serres, A.; Li, S. Mapping the fishing intensity in the coastal waters off Guangdong province, China through AIS data. *Water Biology and Security* **2023**, *2*, 100090. https://doi.org/https://doi.org/10.1016/j.watbs.2022.100090.
58. Yan, Z.; He, R.; Ruan, X.; Yang, H. Footprints of fishing vessels in Chinese waters based on automatic identification system data. *Journal of Sea Research* **2022**, *187*, 102255. https://doi.org/https://doi.org/10.1016/j.seares.2022.102255.
59. Rodríguez, J.P.; Irigoien, X.; Duarte, C.M.; Eguíluz, V.M. Identification of suspicious behavior through anomalies in the tracking data of fishing vessels. *EPJ Data Science* **2024**, *13*, 23. https://doi.org/https://doi.org/10.1140/epjds/s13688-024-00459-0.

 doi:10.20944/preprints202605.0928.v1

60. Goudossis-Goudosis, A.A.; Katsikas, S.K. Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology* **2018**, *24*, 410 – 423.
61. Androjna, A.; Perković, M. AIS Data Falsification—How Long Will It Be Before We Can No Longer Trust AIS? In Proceedings of the 2024 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea), Piscataway, NJ, USA, 2024; pp. 301–306.
62. Glomsvoll, O.; Bonenberg, L.K. GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea. *Journal of Navigation* **2017**, *70*, 33–48. https://doi.org/10.1017/S0373463316000473.
63. Klör, F.; Bauer, J.; Paulus, S.; Rademacher, M. Dude, Where's That Ship? Stealthy Radio Attacks Against AIS Broadcasts. In Proceedings of the 2024 IEEE 49th Conference on Local Computer Networks (LCN), Toulouse, France, 2024; pp. 1–7. https://doi.org/10.1109/LCN60385.2024.10639674.
64. Balduzzi, M.; Wilhoit, K.; Pasta, A. A Security Evaluation of AIS. Technical report, Trend Micro Forward-Looking Threat Research Team, New Orleans, LA, USA, 2014. https://doi.org/10.1145/2664243.2664257.
65. Khandker, S.; Turtiainen, H.; Costin, A.; Hämäläinen, T. Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience. *IEEE Access* **2022**, *10*, 29493–29505. https://doi.org/10.1109/ACCESS.2022.3158943.
66. Androjna, A.; Perkovič, M.; Pavic, I.; Mišković, J. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences* **2021**, *11*, 5015. https://doi.org/10.3390/app11115015.
67. Androjna, A.; Perkovic, M.; Pavic, I. CYBER SECURITY CHALLENGES FOR SAFE NAVIGATION AT SEA. In Proceedings of the 14th Annual Baška GNSS Conference: Technologies, Techniques and Applications Across PNT and The 1st Workshop on Smart, Blue and Green Maritime Technologies, Baška, Krk Island, Croatia, 05 2021; pp. 47–62.
68. Androjna, A.; Perkovič, M. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Transactions on Maritime Science* **2021**, *10*, 361–373. https://doi.org/10.7225/toms.v10.n02.w08.
69. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering* **2020**, *8*. https://doi.org/10.3390/jmse8100776.
70. Bateman, T. HMS Defender: AIS spoofing is opening up a new front in the war on reality, 2021.
71. Zorri, D.M.; Kessler, G.C. Position, Navigation, and Timing Weaponization in the Maritime Domain: Orientation in the Era of Great Systems Conflict, 2024.
72. Safar, J.; Vejražka, F.; Williams, P. Assessing the Limits of eLoran Positioning Accuracy. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* **2011**, *5*, 93–101. https://doi.org/10.12716/1001.05.01.08.
73. Grant, A.; Williams, P.; Ward, N.; Basker, S. GPS Jamming and the Impact on Maritime Navigation. *Journal of Navigation* **2009**, *62*, 173–187. https://doi.org/10.1017/S0373463308005213.
74. DiRenzo, J.; Goward, D.A.; Roberts, F.S. The Little-known Challenge of Maritime Cyber Security. In Proceedings of the Proceedings of the 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 2015; pp. 1–5. https://doi.org/10.1109/IISA.2015.7388071.
75. Mednikarov, B.; Tsonev, Y.; Lazarov, A. Analysis of Cybersecurity Issues in the Maritime Industry. *Information & Security: An International Journal,47 no. 1* **2020**, *47*, 27–43.
76. Harris, M. Phantom Warships Are Courting Chaos in Conflict Zones - The latest weapons in the global information war are fake vessels behaving badly, 2021.
77. Zwirko, C. North Korean vessels exploiting tracking system flaws to evade sanctions: report, 2019.
78. Reevell, P. UK denies Russia fired warning shots near British warship, 2021.
79. Humphreys, T. UT Austin Researchers Spoof Superyacht at Sea. Technical report, UT Austin Cockrell School of Engineering, 2013.
80. CyberKeel.; Copenhagen.; Denmark. MARITIME CYBER-RISKS. Technical report, CyberKeel, 2014.
81. GLA. General Lighthouse Authorities, The United Kingdom and Ireland, 2024.
82. Androjna, A.; Perkovič, M.; Pavic, I.; Mišković, J. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences* **2021**, *11*, 5015. https://doi.org/10.3390/app11115015.
83. Walde, A.; Hanus, E.G. The feasibility of AIS-and GNSS-based attacks within the maritime industry. Master's thesis, NTNU, 2020.
84. Amro, A.; Gkioulos, V. From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks. In Proceedings of the Computer Security – ESORICS 2022; Atluri, V.; Di Pietro, R.; Jensen, C.D.; Meng, W., Eds., Cham, 2022; pp. 535–553.

 doi:10.20944/preprints202605.0928.v1

85. Iphar, C.; Ray, C.; Napoli, A. Uses and Misuses of the Automatic Identification System. In Proceedings of the OCEANS 2019 - Marseille, Marseille, France, 2019; pp. 1–10. https://doi.org/10.1109/OCEANSE.2019.8867559.
86. Rivest, R.L. The RC5 Encryption Algorithm. In Proceedings of the Fast Software Encryption: Second International Workshop, Leuven, Belgium, 14–16 December 1994, Proceedings, Berlin, Heidelberg, 1995; Vol. 1008, *Lecture Notes in Computer Science*, pp. 86–96. https://doi.org/10.1007/3-540-60590-8_7.
87. Teglasy, B.; Katsikas, S. A Location-Based Global Authorization Method for Underwater Security. arXiv preprint arXiv:2210.07666, 2022. https://doi.org/10.48550/arXiv.2210.07666.
88. Goudosis, A.K.; Katsikas, S.K. Secure AIS with Identity-Based Authentication and Encryption. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* **2020**, *14*, 287–298.
89. Wolsing, K.; Roepert, L.; Bauer, J.; Wehrle, K. Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches. *Journal of Marine Science and Engineering* **2022**, *10*, 112. https://doi.org/10.3390/jmse10010112.
90. Wimpenny, G.; Vastardis, N.; Šafář, J. Authentication in Maritime Communications. In Proceedings of the Proceedings of the 20th IALA Conference 2023, International Association of Marine Aids to Navigation and Lighthouse Authorities, Rio de Janeiro, Brazil, May 2023; pp. 133–1–133–7.
91. Diffie, W.; Hellman, M.E. New Directions in Cryptography. *IEEE Transactions on Information Theory* **1976**, *22*, 644–654. https://doi.org/10.1109/TIT.1976.1055638.
92. Wimpenny, G.; Šafář, J.; Grant, A.; Bransby, M. Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *Journal of Navigation* **2022**, *75*, 333–345. https://doi.org/10.1017/S0373463321000837.
93. Shyshkin, O. Cybersecurity Providing for Maritime Automatic Identification System. In Proceedings of the 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), Las Vegas, NV, USA, 2022; pp. 736–740. https://doi.org/10.1109/ELNANO54667.2022.9926987.
94. Goudosis, A.; Katsikas, S. Secure Automatic Identification System (SecAIS): Proof-of-Concept Implementation. *Journal of Marine Science and Engineering* **2022**, *10*, 805. https://doi.org/10.3390/jmse10060805.
95. Sciancalepore, S.; Tedeschi, P.; Aziz, A.; Di Pietro, R. Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts. *IEEE Transactions on Dependable and Secure Computing* **2022**, *19*, 2709–2726. https://doi.org/10.1109/TDSC.2021.3069428.
96. Aziz, A.; Tedeschi, P.; Sciancalepore, S.; Pietro, R. SecureAIS - Securing Pairwise Vessels Communications. In Proceedings of the 2020 IEEE Conference on Communications and Network Security, CNS 2020, Avignon, France, Jun 2020; pp. 1–9. DBLP License: DBLP's bibliographic metadata records provided through http://dblp.org/ are distributed under a Creative Commons CC0 1.0 Universal Public Domain Dedication. Although the bibliographic metadata records are provided consistent with CC0 1.0 Dedication, the content described by the metadata records is not. Content may be subject to copyright, rights of privacy, rights of publicity and other restrictions., https://doi.org/10.1109/CNS48642.2020.9162320.
97. Wang, C.; Shen, J.; Vijayakumar, P.; Gupta, B.B. Attribute-Based Secure Data Aggregation for Isolated IoT-Enabled Maritime Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* **2023**, *24*, 2608–2617. https://doi.org/10.1109/TITS.2021.3127436.
98. Qian, Y.; Qi, J.; Kuai, X.; Han, G.; Sun, H.; Hong, S. Specific Emitter Identification Based on Multi-Level Sparse Representation in Automatic Identification System. *IEEE Transactions on Information Forensics and Security* **2021**, *16*, 2872–2884. https://doi.org/10.1109/TIFS.2021.3068010.
99. Izuazu, U.; Ihekoronye, V.; Kim, D.S.; Lee, J.M. Leveraging Deep Learning for Anomaly Detection in AIS for Secured Maritime Navigation. In Proceedings of the 2023 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, South Korea, 09 2023.
100. Jacq, O.; Laso, P.M.; Brosset, D.; Simonin, J.; Kermarrec, Y.; Giraud, M.A. Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles. In Proceedings of the IST-174 Symposium on Cyber Defence and Security for the Maritime Domain (CDSM), Copenhagen, Denmark, 2019; pp. 9–1 – 9–16.
101. Maulidi, A.; Abdullah, M.; Handani, D. Virtual private network (VPN) model for AIS real time monitoring. *IOP Conference Series: Earth and Environmental Science* **2022**, *1081*, 012028. https://doi.org/10.1088/1755-1315/1081/1/012028.
102. IEEE Standards Association. IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control. IEEE Standard 802.1X-2020, Institute of Electrical and Electronics Engineers (IEEE), 2020. Revision of IEEE Std 802.1X-2010 incorporating 802.1Xbx-2014 and 802.1Xck-2018, https://doi.org/10.1109/IEEESTD.2020.9018454.

 doi:10.20944/preprints202605.0928.v1

103. Zisi, A.; Sarri, A.; Drougkas, A.; Kyranoudi, P. Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector. Report, European Union Agency for Cybersecurity (ENISA), Heraklion, Greece, 2019. Publications Office of the European Union, https://doi.org/10.2824/328515.
104. Milenkovic, G.; Dekker, M. Guideline on Security Measures under the EECC (4th Edition). Report, European Union Agency for Cybersecurity (ENISA), Heraklion, Greece, 2021. Publications Office of the European Union, https://doi.org/10.2824/44013.
105. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*; MIT Press: Cambridge, MA, 2016.
106. Jain, A.K.; Murty, M.N.; Flynn, P.J. Data Clustering: A Review. *ACM Computing Surveys* **1999**, *31*, 264–323. https://doi.org/10.1145/331499.331504.
107. Durbin, J.; Koopman, S.J. *Time Series Analysis by State Space Methods*, 2 ed.; Oxford Statistical Science Series, Oxford University Press: Oxford, 2012. https://doi.org/10.1093/acprof:oso/9780199641178.001.0001.
108. Graves, A. *Supervised Sequence Labelling with Recurrent Neural Networks*; Vol. 385, *Studies in Computational Intelligence*, Springer: Berlin, Heidelberg, 2012. https://doi.org/10.1007/978-3-642-24797-2.
109. Vaswani, A.; Shazeer, N.; Parmar, N.; Uszkoreit, J.; Jones, L.; Gomez, A.N.; Kaiser, Ł.; Polosukhin, I. Attention Is All You Need. In Proceedings of the Advances in Neural Information Processing Systems 30 (NeurIPS 2017), Long Beach, CA, USA, 2017; pp. 5998–6008, [1706.03762].
110. Gao, M.; Shi, G.; Li, S. misc Prediction of Ship Behavior with Automatic Identification System Sensor Data Using Bidirectional Long Short-Term Memory Recurrent Neural Network. *Sensors* **2018**, *18*. https://doi.org/10.3390/s18124211.
111. Capobianco, S.; Millefiori, L.M.; Forti, N.; Braca, P.; Willett, P. Deep Learning Methods for Vessel Trajectory Prediction based on Recurrent Neural Networks. *IEEE Transactions on Aerospace and Electronic Systems* **2021**, *58*. https://doi.org/10.1109/TAES.2021.3096873.
112. Lu, B.; Lin, R.; Zou, H. A Novel CNN-LSTM Method for Ship Trajectory Prediction. In Proceedings of the 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Haikou, China, 2021; pp. 2431–2436. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00366.
113. Zhang, Z.; Ni, G.; Xu, Y. Ship Trajectory Prediction based on LSTM Neural Network. In Proceedings of the 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 2020; pp. 1356–1364. https://doi.org/10.1109/ITOEC49072.2020.9141702.
114. Wang, S.; He, Z. A prediction model of vessel trajectory based on generative adversarial network. *Journal of Navigation* **2021**, *74*, 1161–1171. https://doi.org/10.1017/S0373463321000382.
115. Wang, J.; Hu, B.; Zhu, J.; Gao, D. Ship trajectory prediction model based on PSO-LSTM. In Proceedings of the 2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Nanchang, China, 2022; pp. 81–86. https://doi.org/10.1109/ICBAIE56435.2022.9985836.
116. Alizadeh, D.; Alesheikh, A.A.; Sharif, M. Vessel Trajectory Prediction Using Historical Automatic Identification System Data. *Journal of Navigation* **2021**, *74*, 156–174. https://doi.org/10.1017/S0373463320000442.
117. kai Zhang, S.; you Shi, G.; jiang Liu, Z.; wei Zhao, Z.; lin Wu, Z. Data-driven based automatic maritime routing from massive AIS trajectories in the face of disparity. *Ocean Engineering* **2018**, *155*, 240–250. https://doi.org/https://doi.org/10.1016/j.oceaneng.2018.02.060.
118. Tang, C.; Wang, H.; Zhao, J.; Tang, Y.; Yan, H.; Xiao, Y. A method for compressing AIS trajectory data based on the adaptive-threshold Douglas-Peucker algorithm. *Ocean Engineering* **2021**, *232*, 109041. https://doi.org/https://doi.org/10.1016/j.oceaneng.2021.109041.
119. Pedroche, D.S.; Herrero, D.A.; Herrero, J.G.; López, J.M.M. Clustering of maritime trajectories with AIS features for context learning. In Proceedings of the 2021 IEEE 24th International Conference on Information Fusion (FUSION), Sun City, South Africa, 2021; pp. 1–8. https://doi.org/10.23919/FUSION49465.2021.9626956.
120. Xiong, L.; Xiong, X.; Zhang, F.; Chen, H. Unsupervised Deep Embedding Clustering for AIS Trajectory. In Proceedings of the IGARSS 2022 - 2022 IEEE International Geoscience and Remote Sensing Symposium, Kuala Lumpur, Malaysia, 2022; pp. 2283–2286. https://doi.org/10.1109/IGARSS46834.2022.9884800.
121. Jain, R.P.; Brekke, E.F.; Rasheed, A. Unsupervised Clustering of Marine Vessel Trajectories in Historical AIS Database. In Proceedings of the 2022 25th International Conference on Information Fusion (FUSION), Linköping, Sweden, 2022; pp. 1–6. https://doi.org/10.23919/FUSION49751.2022.9841274.

 doi:10.20944/preprints202605.0928.v1

122. Chu, X.; Lei, J.; Liu, X.; Wang, Z. KMEANS Algorithm Clustering for Massive AIS Data Based on the Spark Platform. In Proceedings of the 2020 5th International Conference on Control, Robotics and Cybernetics (CRC), Virtual Conference, 2020; pp. 36–39. https://doi.org/10.1109/CRC51253.2020.9253451.
123. Zaharia, M.; Xin, R.S.; Wendell, P.; Das, T.; Armbrust, M.; Dave, A.; Meng, X.; Rosen, J.; Venkataraman, S.; Franklin, M.J.; et al. Apache Spark: A Unified Engine for Big Data Processing. *Communications of the ACM* **2016**, *59*, 56–65. https://doi.org/10.1145/2934664.
124. Singh, S.K.; Heymann, F. Machine Learning-Assisted Anomaly Detection in Maritime Navigation using AIS Data. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Bengaluru, India, 2020; pp. 832–838. https://doi.org/10.1109/PLANS46316.2020.9109806.
125. Anne, D.; Suhardi.; Muhamad, W. Prediction of Ship Track Anomaly based on AIS data using Long Short-Term Memory (LSTM) and DBSCAN. In Proceedings of the 2022 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 2022; pp. 107–112. https://doi.org/10.1109/ICITSI56531.2022.9970940.
126. Li, J.; Liu, J.; Zhang, X.; Li, X.; Wang, J.; Wu, Z. A Novel Hybrid Approach for Detecting Abnormal Vessel Behavior in Maritime Traffic. In Proceedings of the 2023 7th International Conference on Transportation Information and Safety (ICTIS), Wuhan, China, 2023; pp. 1–7. https://doi.org/10.1109/ICTIS60134.2023.10243728.
127. Guo, S.; Mou, J.; Chen, L.; Chen, P. An Anomaly Detection Method for AIS Trajectory Based on Kinematic Interpolation. *Journal of Marine Science and Engineering* **2021**, *9*, 609. https://doi.org/10.3390/jmse9060609.
128. Chen, X.; Liu, Y.; Achuthan, K.; Zhang, X. A ship movement classification based on Automatic Identification System (AIS) data using Convolutional Neural Network. *Ocean Engineering* **2020**, *218*, 108182. https://doi.org/https://doi.org/10.1016/j.oceaneng.2020.108182.
129. Wijaya, W.M.; Nakamura, Y. Ship Navigational Status Classification Based on the Geometrical and Spatiotemporal Features of the AIS-Generated Trajectory. In Proceedings of the 2024 9th International Conference on Big Data Analytics (ICBDA), Fukuoka, Japan, 2024; pp. 103–112. https://doi.org/10.1109/ICBDA61153.2024.10607233.
130. Pohontu, A.; Deliu, A.D.; Vertan, C. Ship Type Classification: a Handwriting Signature Verification Approach for Maritime Trajectories. In Proceedings of the 2023 8th International Symposium on Electrical and Electronics Engineering (ISEEE), Craiova, Romania, 2023; pp. 110–115. https://doi.org/10.1109/ISEEE58596.2023.10310540.
131. Vasudevan, R.; Chola, C. AI Based Approach for Transshipment Detection in the Maritime Domain. In Proceedings of the 2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2024; pp. 1–6. https://doi.org/10.1109/ICITIIT61487.2024.10580624.
132. Luangwilai, T. Improving Maritime Security Via Automated Navigational Monitoring. *Contemporary Issues in Air and Space Power* **2023**, *1*, bp31180108. https://doi.org/10.58930/bp31180108.
133. Shvachko, K.; Kuang, H.; Radia, S.; Chansler, R. The Hadoop Distributed File System. In Proceedings of the 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST), Incline Village, NV, USA, 2010; pp. 1–10. https://doi.org/10.1109/MSST.2010.5496972.
134. Douglas, D.H.; Peucker, T.K. Algorithms for the Reduction of the Number of Points Required to Represent a Digitized Line or its Caricature. *The Canadian Cartographer* **1973**, *10*, 112–122. https://doi.org/10.3138/FM57-6770-U75U-7727.
135. Ester, M.; Kriegel, H.P.; Sander, J.; Xu, X. A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. In Proceedings of the Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96), Portland, OR, USA, 1996; pp. 226–231.
136. Rong, H.; Teixeira, A.; Guedes Soares, C. Data mining approach to shipping route characterization and anomaly detection based on AIS data. *Ocean Engineering* **2020**, *198*, 106936. https://doi.org/https://doi.org/10.1016/j.oceaneng.2020.106936.
137. Prieur, M.; Gahbiche-Braham, S.; Gadek, G.; Gatepaille, S.; Vasnier, K.; Justine, V. K-pop and fake facts: from texts to smart alerting for maritime security. In Proceedings of the Findings of the Association for Computational Linguistics: ACL 2023, Toronto, Canada, 2023; pp. 8394–8400.
138. Kumar, P.; Gupta, G.P.; Tripathi, R.; Garg, S.; Hassan, M.M. DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* **2023**, *24*, 2472–2481. https://doi.org/10.1109/TITS.2021.3122368.

 doi:10.20944/preprints202605.0928.v1

139. Nova Muhammad Ferlansyah, S. A Systematic Literature Review of Vessel Anomaly Behavior Detection Methods Based on Automatic Identification System (AIS) and another Sensor Fusion. *Advances in Science, Technology and Engineering Systems Journal* **2020**, *5*, 287–292. https://doi.org/10.25046/aj050237.
140. Qiao, D.; Liu, G.; Lv, T.; Li, W.; Zhang, J. Marine Vision-Based Situational Awareness Using Discriminative Deep Learning: A Survey. *Journal of Marine Science and Engineering* **2021**, *9*, 397. https://doi.org/10.3390/jmse9040397.
141. Pan, Q.; Lin, S.; Lu, W.; Wang, Z.; Wu, L.; Zou, Y.; Ai, B.; Zhong, Z. Space-Air-Sea-Ground Integrated Monitoring Network-Based Maritime Transportation Emergency Forecasting. *IEEE Transactions on Intelligent Transportation Systems* **2022**, *23*, 2843–2852. https://doi.org/10.1109/TITS.2021.3134838.
142. O'Hara, P.D.; Serra-Sogas, N.; McWhinnie, L.; Pearce, K.; Le Baron, N.; O'Hagan, G.; Nesdoly, A.; Marques, T.; Canessa, R. Automated identification system for ships data as a proxy for marine vessel related stressors. *Science of The Total Environment* **2023**, *865*, 160987. https://doi.org/https://doi.org/10.1016/j.scitotenv.2022.160987.
143. Potamos, G.; Stavrou, E.; Stavrou, S. Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis. *Sensors* **2024**, *24*. https://doi.org/10.3390/s24113458.
144. Cherrak, O.; Ghennioui, H.E.; Thirion-Moreau, N.; Abarkan, E.H. Blind separation of complex-valued satellite-AIS data for marine surveillance: a spatial quadratic time-frequency domain approach, 2019.
145. Serra-Sogas, N.; O'Hara, P.D.; Pearce, K.; Smallshaw, L.; Canessa, R. Using aerial surveys to fill gaps in AIS vessel traffic data to inform threat assessments, vessel management and planning. *Marine Policy* **2021**, *133*, 104765. https://doi.org/https://doi.org/10.1016/j.marpol.2021.104765.
146. Iphar, C.; Napoli, A.; , Cyril, R.; Alincourt, E.; Brosset., D. Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety. In Proceedings of the Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of the 26th European Safety and Reliability Conference (ESREL 2016), Glasgow, UnitedKingdom, September 2016; pp. 606–613. hal-01421905.
147. Iphar, C.; Napoli, A.; Ray, C. An expert-based method for the risk assessment of anomalous maritime transportation data. *Applied Ocean Research* **2020**, *104*, 102337. https://doi.org/https://doi.org/10.1016/j.apor.2020.102337.
148. Mohsendokht, M.; Li, H.; Kontovas, C.; Chang, C.H.; Qu, Z.; Yang, Z. Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. *Ocean Engineering* **2024**, *312*, 119078. https://doi.org/https://doi.org/10.1016/j.oceaneng.2024.119078.
149. Chang, C.H.; Shi, W.; Zhang, V.; Park, C. Evaluating cybersecurity risks in the maritime industry: a literature review, 2020.
150. Commission, I.E. IEC 60812:2018 — Failure modes and effects analysis (FMEA and FMECA). Technical report, International Electrotechnical Commission (IEC), Geneva, Switzerland, 2018. Second edition.
151. Langseth, H.; Portinale, L. Bayesian networks in reliability. *Reliability Engineering & System Safety* **2007**, *92*, 92–108. https://doi.org/10.1016/j.ress.2005.11.037.
152. Weber, P.; Medina-Oliva, G.; Simon, C.; Iung, B. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence* **2012**, *25*, 671–682. https://doi.org/10.1016/j.engappai.2010.06.002.
153. C., K.G.; P., C.J.; C., H.J. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 12(3).* **2018**, *12*.
154. Tam, K.; Jones, K. Factors Affecting Cyber Risk in Maritime. In Proceedings of the Maritime 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, Oxford, UK, 06 2019. https://doi.org/10.1109/CyberSA.2019.8899382.
155. Kimberly, T.; Kevin, J. Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector. *International Journal on Cyber Situational Awareness, 4(1)* **2019**, *4*, 40–68.
156. Verhoeven, P. *WORLD PORTS SUSTAINABILITY REPORT 2020, The World Ports Sustainability Program (WPSP).* International Association of Ports and Harbors (IAPH), 2020.
157. Gorkem, B.N.; Caglayan, B.; Karaca, E.; Karabulut, C.; Korcak, O. Dark Activity Detection in AIS-Based Maritime Networks. In Proceedings of the 2023 34th Conference of Open Innovations Association (FRUCT), Helsinki, Finland, 2023; pp. 35–40. https://doi.org/10.23919/FRUCT60429.2023.10328171.
158. Yang, C.H.; Wu, C.H.; Shao, J.C.; Wang, Y.C.; Hsieh, C.M. AIS-Based Intelligent Vessel Trajectory Prediction Using Bi-LSTM. *IEEE Access* **2022**, *10*, 24302–24315. https://doi.org/10.1109/ACCESS.2022.3154812.

 doi:10.20944/preprints202605.0928.v1

159. Troupiotis-Kapeliaris, A.; Zissis, D.; Kohlbrenner, S.; Kastrisios, C. Mobility Data Mining: the Maritime Use Case. In Proceedings of the 2024 11th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Milan, Italy, 2024; pp. 207–212. https://doi.org/10.1109/MetroAeroSpace61015.2024.10591577.
160. Toshniwal, A.; Mahesh, K.; Jayashree, R. Overview of Anomaly Detection techniques in Machine Learning. In Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020; pp. 808–815. https://doi.org/10.1109/I-SMAC49090.2020.9243329.
161. Tu, E.; Zhang, G.; Rachmawati, L.; Rajabally, E.; Huang, G.B. Exploiting AIS Data for Intelligent Maritime Navigation: A Comprehensive Survey From Data to Methodology. *IEEE Transactions on Intelligent Transportation Systems* **2018**, *19*, 1559–1582. https://doi.org/10.1109/TITS.2017.2724551.
162. Yang, D.; Wu, L.; Wang, S.; Jia, H.; Li, K.X. How big data enriches maritime research – a critical review of Automatic Identification System (AIS) data applications. *Transport Reviews* **2019**, *39*, 755–773. https://doi.org/https://doi.org/10.1080/01441647.2019.1649315.
163. Munim, Z.H.; Dushenko, M.; Jimenez, V.J.; Shakil, M.H.; Imset, M. Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions. *Maritime Policy & Management* **2020**, *47*, 577–597, [https://doi.org/10.1080/03088839.2020.1788731]. https://doi.org/10.1080/03088839.2020.1788731.
164. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information* **2022**, *13*, 22. https://doi.org/10.3390/info13010022.
165. Park, C.J.; Shi, W.; Zhang, W.; Kontovas, C.; Chang, C.H. Cybersecurity in the maritime industry: a literature review. In Proceedings of the The 19th Annual General Assembly of the International Association of Maritime Universities Conference (IAMU AGA 2019), Tokyo, Japan, 2019; pp. 231–239.
166. Schinas, O.; Metzger, D. Cyber-seaworthiness: A critical review of the literature. *Marine Policy* **2023**, *151*, 105592. https://doi.org/https://doi.org/10.1016/j.marpol.2023.105592.
167. Wu, B.; Yip, T.L.; Yan, X.; Guedes Soares, C. Review of techniques and challenges of human and organizational factors analysis in maritime transportation. *Reliability Engineering & System Safety* **2022**, *219*, 108249. https://doi.org/https://doi.org/10.1016/j.ress.2021.108249.
168. Larsen, M.H.; Lund, M.S. Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 144895–144905. https://doi.org/10.1109/ACCESS.2021.3122433.
169. Tabish, N.; Chaur-Luh, T. Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. *IEEE Access* **2024**, *12*, 17114–17136. https://doi.org/10.1109/ACCESS.2024.3357082.
170. Morariu, A.R.; Ahmad, T.; Iancu, B.; Poikonen, J.; Björkqvist, J. Analysing MLOps and its Applicability in the Maritime Domain through a Systematic Mapping Study. In Proceedings of the 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS), St. John's, NL, Canada, 2024; pp. 1–8. https://doi.org/10.1109/ICPS59941.2024.10639945.
171. Mesa, M.V.C.; Patino-Rodriguez, C.E.; Carazas, F.J.G. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information, 15* **2024**, *45*, 710.
172. Badrudin, A.; Sumantri, S.H.; Gultom, R.A.G.; Nengah, I.; Apriyanto, P.; Wijaya, H.R.; Sutedja, I. SHIP TRAJECTORY PREDICTION FOR ANOMALY DETECTION USING AIS DATA AND ARTIFICIAL INTELLIGENCE: A SYSTEMATIC LITERATURE REVIEW. *Journal of Theoretical and Applied Information Technology* **2023**, *101*, 50929–50937.
173. Dolev, S.; Panwar, N. Peripheral Authentication for Autonomous Vehicles. In Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Piscataway, NJ, USA, 2016; pp. 282–285. https://doi.org/10.1109/NCA.2016.7778601.
174. Dolev, S.; Krzywiecki, L.; Panwar, N.; Segal, M. Optical PUF for Non Forwardable Vehicle Authentication. In Proceedings of the 2015 IEEE 14th International Symposium on Network Computing and Applications, Berlin, Germany, 2015; pp. 204–207. https://doi.org/10.1109/NCA.2015.25.
175. Dolev, S.; Krzywiecki, L.; Panwar, N.; Segal, M. Brief announcement: Vehicle to vehicle authentication. In Proceedings of the Stabilization, Safety and Security of Distributed Systems - 17th International Symposium, SSS 2015, Proceedings; Pelc, A.; Schwarzmann, A., Eds., Germany, Jan 2015; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 275–277. 17th International Symposium on Stabilization, Safety and Security of Distributed Systems, SSS 2015 ; Conference date: 18-08-2015 Through 21-08-2015.

 doi:10.20944/preprints202605.0928.v1

176. of ITU, I.R.R.S. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band. Technical Report Recommendation ITU-R M.1371, International Telecommunication Union – Radiocommunication Sector (ITU–R), 2021. Latest public listing page; defines AIS technical characteristics and management messages (e.g., 20/22/23).
177. of ITU, I.R.R.S. Technical characteristics for a VHF data exchange system (VDES) in the VHF maritime mobile band. Technical Report Recommendation ITU-R M.2092-1, International Telecommunication Union – Radiocommunication Sector (ITU–R), 2022.
178. Jiang, Q.; et al. RF Fingerprinting Identification in Low SNR Scenarios for AIS Satellite Links. *IEEE Transactions on Wireless Communications* **2024**, *23*, 2070–2083. https://doi.org/10.1109/TWC.2023.3294988.
179. Tyler, J.H.; et al. Considerations, Advances, and Challenges Associated with Specific Emitter Identification. *Information* **2023**, *14*, 479. https://doi.org/10.3390/info14090479.
180. Dolev, S.; Krzywiecki, Ł.; Panwar, N.; Segal, M. Optical PUF for Non-Forwardable Vehicle Authentication. *Computer Communications* **2016**, *93*, 52–67. https://doi.org/10.1016/j.comcom.2016.07.004.
181. Windward. The Dark Side of AIS: Staying Ahead in a Sea of Spoofing, 2024.
182. MarineTraffic. Understanding AIS & GNSS Spoofing, 2024.
183. Spire Global. Understanding a Vessel's True Journey: Using AIS Position Validation to Expose Illegal Trade, 2024.
184. Global Fishing Watch. Systematic Data Analysis Reveals False Vessel Tracks, 2021.
185. (IEC), I.E.C. Maritime navigation and radiocommunication equipment and systems — Shipborne radar — Performance requirements, methods of testing and required test results. Technical Report IEC 62388:2013, International Electrotechnical Commission (IEC), 2013.
186. (IEC), I.E.C. Maritime navigation and radiocommunication equipment and systems — Presentation of navigation-related information on shipborne navigational displays — General requirements, methods of testing and required test results, 2021.
187. Organization, I.M. Guidelines for the Presentation of Navigation-Related Symbols, Terms and Abbreviations. IMO Circular SN.1/Circ.243/Rev.2, 2019.
188. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382–401. https://doi.org/10.1145/357172.357176.
189. for Marine Aids to Navigation, I.T.I.O. Recommendation A-124: On the AIS Service (Revised). Technical report, International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), 2012. Includes appendices on VDL loading and management.
190. for Marine Aids to Navigation, I.T.I.O. Appendix 17: Channel Management by an AIS Service. Technical report, International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), 2011.
191. European Union Agency for Cybersecurity, E. *ENISA THREAT LANDSCAPE: TRANSPORT SECTOR*. European Union Agency for Cybersecurity (ENISA), 2023. https://www.enisa.europa.eu/sites/default/files/all_files/03-cooperation-information-sharing-03-enisa-theocharidou.pdf.
192. EU Agency for the Space Programme (EUSPA). Galileo, 2025. Overview of the EU's Global Navigation Satellite System.
193. Lasi, H.; Fettke, P.; Kemper, H.G.; Feld, T.; Hoffmann, M. Industry 4.0. *Business & information systems engineering* **2014**, *6*, 239–242.
194. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP), Oakland, CA, USA, 2007; pp. 321–334. https://doi.org/10.1109/SP.2007.11.
195. McGrew, D.A. An Interface and Algorithms for Authenticated Encryption. RFC 5116, Internet Engineering Task Force, 2008.
196. of Standards, N.I.; Technology. Digital Signature Standard (DSS). FIPS PUB 186-5, National Institute of Standards and Technology, 2023.
197. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In Proceedings of the Advances in Cryptology – CRYPTO '84, Berlin, Heidelberg, 1985; Vol. 196, *LNCS*, pp. 47–53. https://doi.org/10.1007/3-540-39568-7_5.
198. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. In Proceedings of the Advances in Cryptology – CRYPTO 2001, Santa Barbara, CA, USA, 2001; Vol. 2139, *LNCS*, pp. 213–229. https://doi.org/10.1007/3-540-44647-8_13.
199. of Standards, N.I.; Technology. The Keyed-Hash Message Authentication Code (HMAC). FIPS PUB 198-1, National Institute of Standards and Technology, 2008.

 doi:10.20944/preprints202605.0928.v1

200. NIST. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D, National Institute of Standards and Technology, 2007.
201. Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, Internet Engineering Task Force, 2008.
202. Danev, B.; Čapkun, S. Transient-based Identification of Wireless Sensor Nodes. In Proceedings of the Proceedings of the 2009 International Conference on Information Processing in Sensor Networks (IPSN), Montreal, Canada, 2009; pp. 25–36. https://doi.org/10.1145/1602165.1602169.
203. Stouffer, K.; Jansen, W.; Scarfone, K.; Taylor, C. Guide to Computer Security Log Management. NIST Special Publication 800-92, National Institute of Standards and Technology, 2006.
204. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force, 2018.
205. Kent, S.; Seo, K. Security Architecture for the Internet Protocol. RFC 4301, Internet Engineering Task Force, 2005.
206. Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing* **1989**, *18*, 186–208. https://doi.org/10.1137/0218012.