

Review

Uncovering the Security Landscape of Maritime Software-Defined Radios: A Threat Modeling Perspective

Erasmus Mfodwo ¹, Phani Lanka ¹, Ahmet Furkan Aydogan ²  and Cihan Varol ^{1,*} ¹ Department of Computer Science, Sam Houston State University, Huntsville, TX 77340, USA; exm251@shsu.edu (E.M.); pklanka@shsu.edu (P.L.)² Department of Computer Science, University of North Carolina Wilmington, Wilmington, NC 28403, USA; aydogana@uncw.edu

* Correspondence: cxv007@shsu.edu

Abstract

Maritime transportation accounts for approximately 80 percent of global trade volume, with modern vessels increasingly reliant on Software-Defined Radio (SDR) technologies for communication and navigation. However, the very flexibility and reconfigurability that make SDRs advantageous also introduce complex radio frequency vulnerabilities exposing ships to threats that jeopardize vessel security, and this disrupts global supply chains. This survey paper systematically examines the security landscape of maritime SDR systems through a threat modeling lens. Following Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines, we analyzed 84 peer-reviewed publications (from 2002 to 2025) and applied the STRIDE framework to identify and categorize maritime SDR threats. We identified 44 distinct threat types, with tampering attacks being most prevalent (36 instances), followed by Denial of Service (33 instances), Repudiation (30 instances), Spoofing (23 instances), Information Disclosure (24 instances), and Elevation of Privilege (28 instances). These threats exploit vulnerabilities across device, software, network, message, and user layers, targeting critical systems including Global Navigation Satellite Systems, Automatic Identification Systems, Very High Frequency or Digital Selective Calling systems, Electronic Chart Display and Information Systems, and National Marine Electronics Association 2000 networks. Our analysis reveals that maritime SDR threats are multidimensional and interdependent, with compromises at any layer potentially cascading through entire maritime operations. Significant gaps remain in authentication mechanisms for core protocols, supply chain assurance, regulatory frameworks, multi-layer security implementations, awareness training, and standardized forensic procedures. Further analysis highlights that securing maritime SDRs requires a proactive security engineering that integrates secured hardware architectural designs, cryptographic authentications, adaptive spectrum management, strengthened international regulations, awareness education, and standardized forensic procedures to ensure resilience and trustworthiness.



Academic Editor: Christos Bouras

Received: 24 November 2025

Revised: 17 December 2025

Accepted: 5 January 2026

Published: 13 January 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

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

Keywords: maritime radio systems; maritime security; STRIDE; SDR defense measures; SDR frameworks; SDR RF attacks; SDR threat; SDR threat modeling; SDR vulnerability

1. Introduction

Maritime transportation constitutes the cornerstone of global trade, accounting for approximately 80 percent of the total volume of goods transported worldwide. As of early 2024, the global merchant fleet exceeded 109,000 vessels, each possessing an internal cargo capacity of at least 100 gross tons, calling attention to the magnitude of global reliance

on maritime logistics. Although the sector faced notable disruptions in 2023, the United Nations Conference on Trade and Development (UNCTAD) projects that seaborne trade will continue to expand at an average annual rate of 2.4 percent through 2029 [1–3]. Sustaining this projected growth trajectory increasingly depends on the maritime industry's capacity to secure and optimize its digital infrastructures. Modern ships now depend heavily on interconnected systems for navigation, communication, and cargo management. This means that cybersecurity and technological resilience are essential for maintaining the global distribution of goods and the economies of countries.

Within this broader shift toward digitalization, software-defined radio technology has emerged as a pivotal enabler of maritime communication and control. By decoupling traditional radio hardware and transferring radiofrequency (RF) signal processing into software, SDRs introduce unprecedented flexibility, scalability, and adaptability to shipboard communication architectures. Their multi-waveform compatibility, rapid reconfiguration capabilities, and reduced lifecycle costs provide operational advantages over legacy radio systems. More critically, SDRs facilitate seamless interoperability across heterogeneous maritime networks, allowing vessels to dynamically adjust to evolving communication and navigational demands. This real-time adaptability, even under adverse weather or contested electromagnetic environments, has rendered SDRs indispensable to the safe, efficient, and resilient operation of contemporary maritime fleets.

Yet, the very strengths that make SDRs advantageous also broaden their attack surfaces. Unlike conventional Information Technology (IT) or Operational Technology (OT) systems, SDRs operate at the intersection of hardware, software, and spectrum, creating a uniquely complex risk profile [4]. Adversaries equipped with even low-cost SDR platforms can exploit weak authentication mechanisms, unencrypted communication protocols, and unsecured firmware to execute attacks such as spoofing, jamming, tampering, replay, unauthorized waveform reconfigurations, and many more. These phenomena are leading to many cases of misdirected navigations, disrupted safety broadcasts, hijack of vessel-to-shore coordination, ultimately compromising the integrity of maritime operations in vessel voyages [5].

These challenges highlight the inadequacy of applying traditional IT-centric controls to maritime SDR ecosystems [6]. Securing SDR technologies requires specialized, focused approaches that integrate threat modeling and penetration testing. As vessels become increasingly interconnected and autonomous, the consequences of SDR exploitation extend beyond individual ships to affecting global supply chains, port operations, and national security interests. Addressing these risks demands systematic methodologies capable of identifying, categorizing, and mitigating threats specific to the maritime SDR domain.

In this survey, we used the STRIDE framework as a baseline. The study reviews and categorizes SDR-related attacks documented in literature, maps them to the most maritime-targeted protocols and systems, and analyzes existing defensive strategies. In doing so, it not only consolidates the current knowledge but also highlights existing SDR threats and research gaps that must be addressed to build resilient and secure maritime SDR ecosystems within the broader naval network.

The paper is organized as follows: Section 2 provides background on SDR policies, regulations, and evaluation frameworks, as well as a comparative analysis of applicable SDR frameworks. Section 3 outlines the methodology, describing the data sources, criteria used for categorizing SDR-related threats, and analytical approaches. Section 4 discusses threats within the STRIDE framework, examining documented attacks, attack processes, and targeted maritime protocols and systems, including their corresponding defense mechanisms reported in the literature. Section 5 presents results and discussions. Section 6 summarizes SDR research challenges. Section 7 highlights key research gaps and future

directions, identifying areas requiring further study to strengthen maritime SDR resilience. Finally, we concluded the paper in Section 8, summarizing the main findings.

2. Background

Recognizing the increasing exposure of maritime systems to cyber threats, multiple international and national bodies have introduced regulatory policies and regulations aimed at strengthening cyber security of vessels. These policies and regulations collectively seek to minimize incidents, disrupt potential attack vector orchestration, and enhance the resilience of maritime equipment, networks, and software applications. This section also explains applicable SDR frameworks that are potentially helpful in achieving these security goals.

2.1. Policies and Regulations

This section describes how multiple regulatory and standards bodies collectively shape maritime cyber resilience across IT, OT, and RF systems. It explains that these efforts span strategic policy from the International Maritime Organization (IMO), operational guidance from industry associations and national authorities, and technical standards for OT/ICS and spectrum management.

First, the IMO establishes top-level requirements for cyber risk management in shipping. Resolution MSC.428(98) mandates integration of cyber risk into the Safety Management System, with compliance checked during Document of Compliance audits after 1 January 2021, ensuring cybersecurity becomes part of routine safety governance. The updated Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3, Rev.3, 2025) structure expectations around identification, protection, detection, response, and recovery, and encourage alignment with existing best practices and standards [7,8].

Second, shipping industry associations translate IMO principles into practical shipboard measures. BIMCO's 2024 "Guidelines on Cyber Security Onboard Ships" (Version 5) provide detailed interpretations of IMO guidance, clarifying how operators should handle IT versus OT environments in practice. These guidelines stress third-party and vendor management, supply-chain complexity, and integrating cybersecurity into the SMS to achieve a sustainable, system-wide security posture [9].

Third, U.S. national authorities reinforce maritime cyber resilience in the domestic context. USCG's NVIC 01-20 requires MTSA-regulated facilities to embed cyber risk into Facility Security Assessments and Plans, explicitly referencing the NIST Cybersecurity Framework and NIST SP 800-82 for OT environments to align maritime and national practices. MARAD and USCG's MSCI Advisory 2023-013 highlight threats such as GPS disruption and AIS spoofing, calling for contingency navigation plans and timely incident reporting through NAVCEN to support situational awareness and coordinated response [10,11].

Fourth, OT/ICS security standards provide technical foundations that complement these policies. NIST SP 800-82 Rev.3 extends OT security guidance beyond traditional industrial control systems to include safety, dependability, and performance aspects relevant to maritime operations, promoting risk management that is both technically robust and operationally realistic. ISA/IEC 62443 adds a lifecycle model for securing Industrial Automation and Control Systems, including security levels, secure development, and zoning or segmentation, which are increasingly applied to shipboard OT and shore systems [12,13].

Fifth, classification societies contribute domain-specific methodologies that tie safety and cyber together. DNV Recommended Practice RP-0496 defines a barrier-based approach with tiered evaluation levels and mitigation measures, aligning cyber risk management with existing maritime safety frameworks. By embedding cyber controls within the SMS and OT domains, this model helps ensure consistent security and safety postures across ships, offshore installations, and mobile assets [14].

Finally, these regulatory standards and spectrum-management measures collectively form a layered governance ecosystem for maritime cyber resilience. At the RF layer, ITU-R M.1371 and IALA guidance define and refine AIS technical and operational parameters in the VHF maritime band, ensuring interoperable and reliable communications [15,16]. Together with IMO policy; industry guidelines; national directives; and OT/ICS standards such as NIST SP 800-82, ISA/IEC 62443, and DNV RP-0496, they jointly address cybersecurity, safety, SDR resilience, and spectrum integrity in modern maritime operations.

2.2. Applicable SDR Frameworks

The systematic evaluation of cyber threats in maritime software-defined radio environments requires the use of robust and adaptable frameworks capable of mapping diverse attack vectors across both hardware and software domains. Several well-established cybersecurity frameworks originally designed for general IT, industrial control, or space-based systems have been adapted or proposed as relevant baselines for SDR threat assessment. As shown in Figure 1, STRIDE, MITRE ATT&CK for ICS, SPARTA, and PASTA stand out as key methodologies that collectively provide complementary perspectives on adversarial behavior, system vulnerabilities, and maritime organizational risk posture.

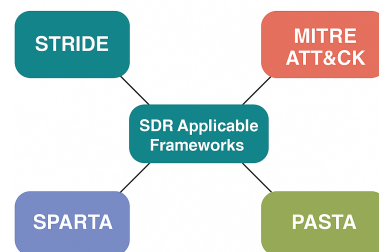


Figure 1. Applicable frameworks for SDR Threat modeling.

2.2.1. STRIDE

STRIDE is a threat modeling methodology developed by Microsoft engineers that categorizes security threats into six types: spoofing, tampering, repudiation, information disclosure, denial of service, and Elevation of privilege. STRIDE's structured taxonomy enables analysts to identify and assess vulnerabilities across various layers of an SDR architecture, from application software to firmware and radio interfaces. In maritime SDR contexts, STRIDE proves useful for classifying signal-level attacks such as GPS and AIS spoofing, where falsified navigation and identification data can compromise vessel operations and situational awareness. Additionally, attacks involving unauthorized firmware modification or malicious SDR reconfiguration align well with the framework's Tampering and Elevation of Privilege categories. Owing to its adaptability and extensibility, STRIDE serves as a foundational baseline for maritime SDR threat modeling and can be integrated with more behaviorally oriented frameworks for greater depth [17].

2.2.2. MITRE ATT&CK

While STRIDE focuses primarily on categorization, the MITRE ATT&CK framework for Industrial Control Systems (ICS) provides a complementary thus behavior-centric methodology. This framework documents adversarial Tactics, Techniques, and Procedures (TTPs) observed in real-world attacks, emphasizing the sequential and operational nature of cyber intrusions. Initially developed for industrial control environments, MITRE ATTACK for ICS is highly relevant to SDRs integrated into maritime operational technology systems. Software-Defined Radios deployed in navigation, communications, and monitoring subsystems are susceptible to unauthorized access, malware injection, and RF-layer manipulation threats that can be effectively modeled within the MITRE ATT&CK matrix. Its focus on observable at-

tacker behaviors facilitates detailed analysis of how adversaries penetrate, persist, and exploit vulnerabilities in maritime SDR networks. Furthermore, the framework's extensibility allows researchers to map SDR-specific attack patterns and expand its taxonomy to accommodate maritime communication protocols such as AIS, DSC, and NMEA 2000 [18,19].

2.2.3. SPARTA

A closely related and specialized framework, Space Attack Research and Tactic Analysis (SPARTA), was developed by The Aerospace Corporation as an adaptation of the MITRE ATT&CK methodology tailored for space systems. SPARTA adopts a mission-centric approach and places strong emphasis on radio frequency (RF)-layer vulnerabilities and signal-based adversarial tactics. It organizes attacker behavior into a structured sequence of phases, including reconnaissance, initial access, execution, persistence, defense evasion, lateral movement, exfiltration, and impact, each mapped to specific operational or RF-layer behaviors. Although its original scope is within space communications, SPARTA's detailed representation of RF attack phases makes it particularly relevant to maritime SDR systems, which share similar dependencies on wireless spectrum, real-time telemetry, and command and control links. By focusing on RF-signal integrity, waveform manipulation, and spectrum denial, SPARTA introduces analytical depth that complements both STRIDE's categorical simplicity and MITRE's behavioral specificity [20].

2.2.4. PASTA

In contrast, the Process for Attack Simulation and Threat Analysis (PASTA) framework offers a risk- and business-aligned methodology that spans seven iterative phases, ranging from business objective definition to impact analysis and remediation planning. PASTA's goal-oriented structure encourages organizations to assess threats in relation to mission-critical processes and operational continuity. In maritime SDR environments, PASTA can be utilized to model both shipboard and shoreside threat scenarios, simulating potential attack paths on reconfigurable radios and their downstream effects on navigation safety, communication reliability, and system interoperability. Its systematic and modular design enables integration with broader enterprise risk management systems, supporting the alignment of technical threat modeling with organizational and regulatory objectives [21].

Table 1 compares the above four frameworks based on their focus areas, relevance to SDR security, and limitations. It highlights key differences in how each framework approaches behavior modeling, radio-layer threats, and mission risk, helping researchers choose or adapt the most suitable method for maritime SDR systems.

Table 1. Comparative Analysis of Threat Modeling Frameworks applicable for SDR Security [17–21].

Frameworks	Focus Areas	Strengths for SDRs	Limitations
STRIDE	Threat categorization	Simple, adaptable taxonomy; effective for small, modular SDR systems	Limited behavioral insight; lacks temporal attack context
MITRE ATT&CK	Adversary behavior	Real-world TTPs; rich behavioral mapping for SDR-related exploitation	Requires SDR-specific mapping and protocol adaptation
SPARTA	Mission-centric RF threats	Deep RF-layer modeling; structured procedural attack phases	Initially designed for space assets; limited direct scalability
PASTA	Risk and business alignment	End-to-end simulation linking risk to mission impact	Abstract modeling; needs SDR-specific contextualization

3. Methodology

To ensure transparent, reproducible, and standard reporting in our work, this survey uses systematic literature review methods based on the PRISMA guidelines. PRISMA

stands for Preferred Reporting Items for Systematic Reviews and Meta-Analyses, and its methodology is organized into six main steps: defining objectives, formulating research questions, setting inclusion or exclusion criteria, executing a search and categorization plan, extracting and analyzing data, and presenting and interpreting findings [22].

3.1. Research Objectives and Questions

The primary objective of this survey is to explore, identify, categorize, and find the most prevalent attacks and also create an attack classification for SDR threats targeting maritime systems through a threat modeling lens. Specifically, the survey aims to identify and classify SDR-related attacks using the STRIDE framework. It further highlights gaps in current literature and proposes future research directions. To guide this process, these research questions were formulated:

- What types of cyberattacks have been documented against maritime SDR systems, and which ones are most prevalent?
- How can these attacks be systematically categorized using the STRIDE framework?
- What threat modeling methodologies are most applicable to SDR-based maritime systems?
- What maritime systems or protocols are mostly attacked?
- What are some of the research gaps that currently exist in maritime SDR security?
- What are some of the emerging SDR attacks that should be expected?
- How do we safeguard systems from specific SDR exploits?

3.2. Literature Search and Categorization Strategy

To identify articles pertinent to our review topic, we searched four major databases: IEEE Xplore, Science Direct, ACM Digital Library, and Springer, utilizing the search terms “Software Defined Radio Frequency Attacks on Maritime” OR “SDR Threats on Maritime” OR “SDR Attacks on NMEA 2000 Network” OR “SDR Vulnerabilities in Maritime.” The terms were entered into the databases to refine the search results to identify more relevant articles. Relevant articles comprised publications from the last 2 decades (2002–2025), predominantly between 2022 and 2025. The research papers were systematically categorized using the STRIDE framework, which comprises spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Each publication was reviewed to identify the kinds of attacks addressed, the attack processes, and the proposed preventive mechanisms. Figure 2 presents the distribution of articles across the years surveyed in our study.

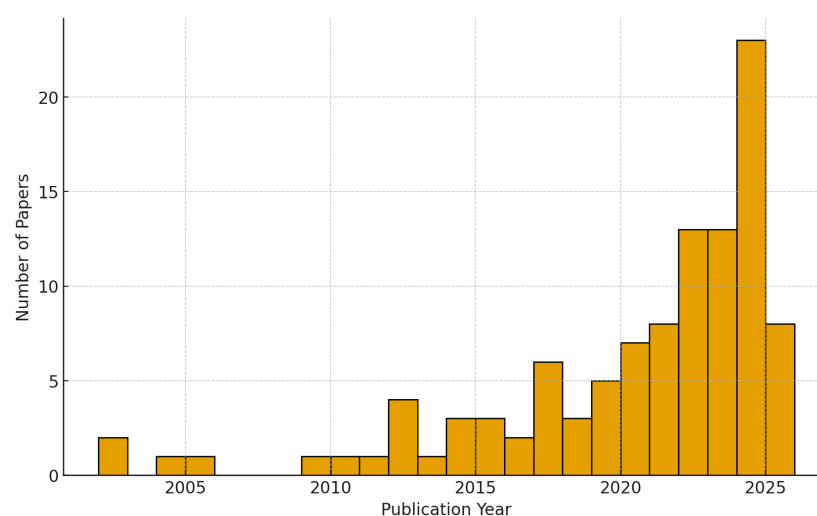


Figure 2. Distribution of articles.

3.3. Inclusion and Exclusion Criteria

In ensuring relevance and quality, the survey applied specific inclusion and exclusion criteria. Based on the title and abstract, 127 out of the 143 papers were evaluated and downloaded. We reduced the number to 89 by leaving out those that did not address the subject of SDR-related cyberattacks in maritime and broader RF communication environment security available in full text. The chosen papers were thoroughly reviewed, and a subsequent evaluation was conducted based on the specified criteria. The initial criterion selected articles with and without empirical data, including abstracts, editorials, conference summaries, brief papers, and book chapters. Secondly, all articles written in languages other than English were excluded. Third, analogous duplicate articles were eliminated. Upon fulfilling these requirements, 81 articles remained. After these decisions, we performed an additional backward reference search to enhance the clarity of the development of this body of knowledge. This approach examined the citations in the chosen articles linked to the previously searched terms. Consequently, we included 25 additional publications, bringing the total to 106 reviewed articles, as shown in Figure 3.

Among the reviewed literature were journal and conference papers that provided technical insights into key threat vectors such as spoofing, jamming, tampering, replay attacks, and NMEA 2000 network attacks.

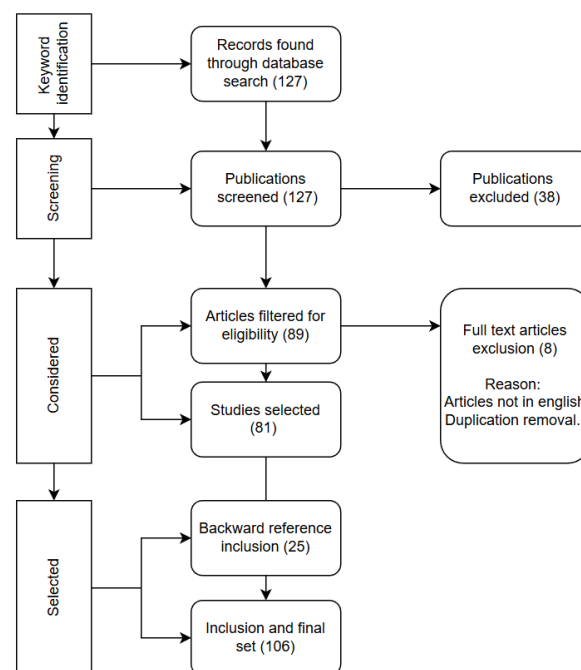


Figure 3. Process used to identify papers reviewed.

3.4. Data Extraction and Analysis

For each selected research paper, key data points were extracted, including the threat type and its technical process (e.g., GPS spoofing, AIS message manipulation, VHF signal jamming), the targeted maritime SDR protocol or system (e.g., AIS, GPS, VHF, radar, ECDIS, sensors), and any proposed defense mechanisms or mitigation strategies (e.g., anomaly detection algorithms, encryption techniques, authentication protocols, and frequency hopping). Additionally, information on research methodologies such as simulation studies, field experiments, testbed evaluations, and metrics used to assess threat impact was collected. This structured approach facilitated the construction of a comparative threat landscape, enabling the identification of recurring attack patterns, trends across different maritime systems, and gaps in existing threat modeling and mitigation efforts.

3.5. Study Types and Reliability Assessment

To assess the reliability of the reviewed body of work, three study types were distinguished: (i) empirical and testbed-based experiments conducted on real maritime platforms, operational SDR hardware, or hardware-in-the-loop testbeds; (ii) simulation or emulation studies in which SDR behaviour, maritime channels, or traffic patterns were modeled in software; and (iii) analytical or conceptual contributions that primarily proposed threat taxonomies, frameworks, or attack scenarios without experimental validation.

Empirical and testbed studies were treated as providing higher ecological validity because they capture realistic RF conditions, protocol implementations, and system integrations, although they often involve a limited number of vessels, devices, or operational environments. Simulation-based works enable systematic exploration of large parameter spaces and complex attack scenarios that would be impractical or unsafe to reproduce at sea, but their conclusions can be sensitive to modeling assumptions and may not fully reflect multipath propagation, interference, or mixed-vendor deployments encountered in real maritime operations. Analytical and conceptual studies are valuable for identifying emerging attack surfaces and guiding future measurements; however, findings from these works are interpreted as qualitative risk indicators or hypotheses until supported by empirical or testbed evidence.

This classification is used in the results and discussion section to differentiate between threats that have been repeatedly demonstrated under realistic conditions and those that are currently supported mainly by simulations or conceptual analyses.

3.6. Threat Modeling Framework Evaluation

To further organize and interpret these threats, each publication was evaluated and mapped to one or more STRIDE categories. The STRIDE model was selected for its simplicity, adaptability, and applicability to both software and hardware layers, making it particularly effective for analyzing SDR vulnerabilities in standard vessels. By combining this structured data with STRIDE-based categorization, the survey establishes a foundation for identifying patterns, assessing system risks, and highlighting areas requiring further research not only from the STRIDE categories but also from attack surfaces and attack trees.

3.7. Limitations and Scope

This study specifically concentrates on maritime Software-Defined Radio systems and excludes general SDR applications in aviation and terrestrial domains, except where their relevance to the maritime context is explicitly established. Furthermore, within the STRIDE-based classification of attacks, the analysis was limited to primary attack types to maintain consistency and focus in the threat categorization process.

4. STRIDE Analysis of Existing SDR Maritime Attacks

To systematically evaluate the cyber threats affecting SDR-enabled maritime communication and navigation systems, this study adopts the STRIDE threat modeling framework. The framework facilitates a comprehensive understanding of the security implications at both the software and hardware abstraction layers, highlighting the relationships between adversarial intent, attack execution, and system impact. In this section, each STRIDE category is discussed in detail with an emphasis on technical characteristics, attack processes, and targeted SDR protocols and systems, including defensive mechanisms reported in the literature. This structure highlights common methodologies, exploits, and attack surfaces usually targeted to compromise critical maritime systems such as GNSS, AIS, NMEA-based navigation, and VHF communication infrastructures by threat actors.

4.1. Spoofing

This occurs when a threat actor transmits falsified RF signals or protocol messages (GNSS/AIS/NMEA/VHF/DSC) forged to appear as legitimate marine infrastructure or vessels, causing the wrong location, false identity, and false sensor inputs in shipboard navigation and situational awareness systems. Researchers demonstrated that low-cost SDR transmitters can generate counterfeit GNSS signals and manipulate NMEA sentences to mislead maritime navigation systems [23]. The same researchers also developed an NMEA sentence integrity monitor (MANA) that detects anomalies produced by practical spoofing experiments [23]. Multiple case studies have shown situations where fabricated AIS messages produced ghost vessels or obscured real vessel tracks [24]. Spoofing attacks can disrupt automated navigation and collision-avoidance systems, erode operator trust in GNSS and AIS reliability, and degrade maritime domain awareness across integrated monitoring networks. Moreover, spoofing may serve as a precursor to more advanced cyber operations, leading to severe navigational errors, collisions, or environmental incidents [25–27].

4.1.1. Description and Attack Methodology

During our study, we found that common spoofing vectors against maritime navigation and communication systems include the injection of counterfeit GNSS/GPS satellite signals to induce erroneous time or position fixes. Examples include fabrication or replay of AIS and NMEA sentences, falsified VHF/DSC calls, and injection of malicious NMEA-2000 messages [23,25]. Most experiments typically leverage low-cost software-defined radio platforms to synthesize protocol-compliant waveforms, replicating modulation schemes, message timing, and message framing so that legitimate receivers accept forged frames as authentic. Empirical studies and field demonstrations have shown that these capabilities enable a range of effects from transient mispositioning to sustained deception of shipboard situational-awareness systems [28,29].

The operational sequence of practical SDR spoofing attacks generally follows a repeatable pattern:

1. **Reconnaissance:** Passive monitoring of target spectrum bands and message formats to collect baseline signal characteristics (carrier frequencies, modulation parameters, timing, message structures, and typical signal power levels).
2. **Counterfeit waveform construction:** Generation of forged signals that replicate the target protocol's physical and link layer characteristics so that the spoofed transmissions are protocol-compliant and thus plausible to victim receivers.
3. **Signal Manipulation and Dominance:** This is the control of transmission to achieve receiver acquisition of the counterfeit source. This may involve increasing local signal power, manipulating relative time offsets, or exploiting receiver acquisition algorithms so the victim locks to the spoofed signals instead of the legitimate source.
4. **Persistence:** Gradual or persistent manipulation of the victim's state to achieve the adversary's objective (for example, slow displacement of GNSS position fixes, injection of false AIS tracks, or timed replay to create transient ambiguity while avoiding rapid detection).

Figure 4 illustrates the above spoofing attack stages, and each of these stages exploits the programmability of SDRs to refine waveform parameters and adapt to local conditions, enabling attackers to balance stealthiness, effectiveness, and persistence [23–25,27–29].

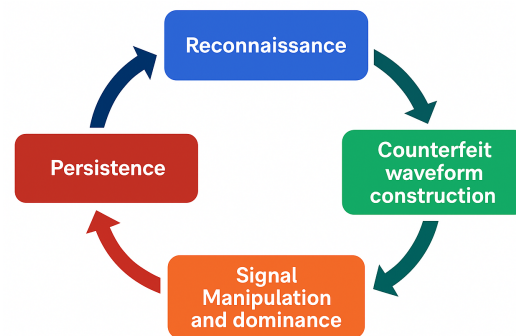


Figure 4. Spoofing Attack Methodology.

4.1.2. Targeted Systems and Protocols

Spoofing attacks in maritime environments overwhelmingly target systems and protocols that rely on unauthenticated and unencrypted signals. GNSS-based navigation is the most exploited, with attackers using SDRs to inject counterfeit satellite signals and mislead vessel positioning systems [23]. This manipulation cascades into dependent systems such as the Electronic Chart Display and Information System (ECDIS) and Long-Range Identification and Tracking (LRIT), which rely on GNSS inputs for route plotting and vessel tracking [28,30]. AIS protocols are also vulnerable, allowing attackers to fabricate vessel identities, simulate ghost ships, and sometimes suppress real traffic [31]. Digital Selective Calling (DSC), a core protocol for maritime distress and routine calling, has been spoofed to trigger false alerts and impersonate legitimate vessels [26].

Beyond navigation and identification, spoofing extends to communication and safety-critical systems. Emergency Position-Indicating Radio Beacons (EPIRBs) can be spoofed to simulate false distress locations, while Navigational Telex (NAVTEX) broadcasts are susceptible to injected misinformation, including fake weather alerts and navigational warnings [32]. Satellite communication systems such as Inmarsat and Iridium have been shown to be vulnerable to spoofed uplinks and downlinks, disrupting ship-to-shore coordination [33]. Even radar and VHF voice channels have been manipulated using SDRs to simulate phantom targets with impersonated voice traffic [34]. These attacks exploit legacy protocol weaknesses, highlighting the urgent need for authentication and signal integrity mechanisms across maritime systems.

4.1.3. Defensive Measures

Several defensive strategies against maritime spoofing attacks have been proposed in the literature, which targets both signal-level anomalies and protocol-level enhancements. One widely discussed approach is signal-level detection, which involves monitoring GNSS signal characteristics such as signal-to-noise ratio, Doppler shift, and satellite geometry changes. These indicators, along with NMEA sentence integrity checks, help identify inconsistencies and abrupt shifts in time or position that may be orchestrated by a signal spoofing attack [23,29]. Complementing this, cross-sensor fusion techniques compare GNSS-derived positions with independent sources such as gyrocompass, radar, and AIS feeds to detect contradictions and also to reinforce situational awareness [18].

Protocol-level defenses are also effective, which include the use of authenticated navigation messages where digital signatures and challenge-response mechanisms are embedded within AIS and NMEA sentence structures to verify message origin and integrity [27,35]. Additionally, RF-fingerprinting and power or timing analysis methods have been employed to detect spoofing by identifying deviations in signal power or waveform characteristics that differ from expected satellite and shore station identities [36]. Finally, operational controls such as structured crew training and standardized incident response

procedures serve as a human layer of defense that enables operators to recognize and respond to implausible navigation fixes during transient spoofing events [31].

4.2. Tampering

SDR tampering encompasses any unauthorized modification of the SDR device's configuration, software, or signal path that change how it transmits, receives, and processes radio signals. This can occur locally via compromised firmware or configuration files and remotely through software vulnerabilities in control interfaces such as GNU Radio, USRP Hardware Driver (UHD), and remote SDR management Application Programming Interfaces (APIs). Common forms include firmware modification, base processing manipulation, and waveform injections. Tampering compromises data integrity and trust in both signal processing and control layers. They usually lead to the generation of deceptive signals, creation of covert transmission channels, and persistence mechanisms that will allow continuous compromise of maritime communication bands [37–39].

4.2.1. Description and Attack Methodology

SDR-based tampering leverages programmable software to generate, modify, and replay radio-frequency waveforms (IQ samples) at GNSS and VHF/AIS bands or other targeted bands. This allows an attacker to create controlled interference (jamming), counterfeit timing/position signals, and forged or replayed AIS/VHF frames (message injection or replay). Commodity software-defined radios such as HackRF, LimeSDR, and BladeRF, when paired with open-source toolchains, can generate waveforms that closely resemble legitimate maritime communication protocols. Without cryptographic authentication or strong sensor fusion, many maritime receivers accept these signals as valid [25,40]. Detection methods (NMEA integrity checks, multi-sensor fusion, anomaly detectors) mitigate risk but are not yet universally deployed [23,36].

A standard tampering attack unfolds through the steps listed below and represented in Figure 5:

1. **Signal survey:** This involves identifying target frequencies, receiver types, antenna geometry, and local signal characteristics using an SDR in receive mode [36].
2. **Attack vector selection:** This step entails determining whether to pursue jamming (denial), spoofing (GNSS deception), AIS injection (identity or position forgery), or replay, based on operational goals and environmental constraints [31,39].
3. **Waveform generation:** This involves crafting protocol-conformant IQ waveforms to tamper with communication flow. GNSS tampering requires synthesizing satellite-like signals with controlled pseudorange and timing, while AIS injection entails constructing bit-framed VHF messages with valid callsigns, Maritime Mobile Service Identity (MMSI), and position fields. Commodity SDRs capable of transmission support these capabilities [39].
4. **Power and timing planning:** At this stage, attackers estimate transmission power levels and timing offsets, then select a tampering strategy. Options include high-power takeover or gradual coherent pull-off to shift receiver fixes. Effective planning of this attack can reduce the likelihood of detection [36].
5. **Testing:** This step validates the effectiveness of the crafted signals by observing receiver responses such as NMEA position changes or AIS track generation either in a controlled environment or through passive monitoring [23].
6. **Execution:** The malicious waveform is transmitted at the designated time and location. For mobile targets, transmission parameters are dynamically adjusted to sustain the illusion of legitimate signaling. Replay attacks may also be employed by injecting previously captured legitimate frames at alternate times or locations [31].

7. **Persistence:** This involves sustaining the intended effect through adaptive transmissions that respond to countermeasures or ceasing transmission to avoid detection once operational objectives are achieved [36].

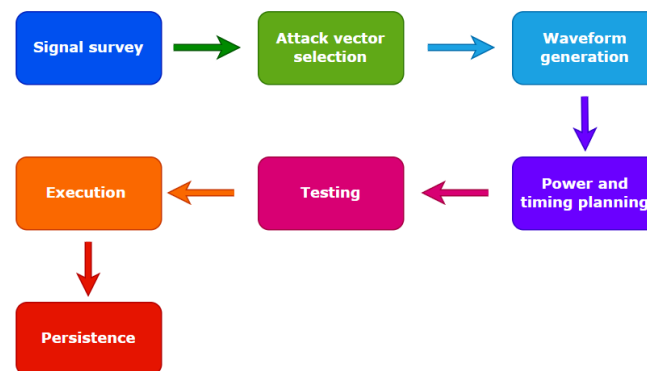


Figure 5. Tampering Attack Methodology.

4.2.2. Targeted Systems and Protocols

SDR-enabled tampering, similar to spoofing also targets several core maritime communication and navigation systems by exploiting their open and unauthenticated radio protocols. The most prominent target is the Global Navigation Satellite Systems, including GPS, Galileo, GLONASS, and Beidou, where attackers use SDRs to jam or spoof navigation signals to falsify vessel positions and timing data [23,41]. The Automatic Identification System is similarly vulnerable, allowing attackers to inject, replay, or alter AIS messages to fabricate ghost vessels or obscure real locations [25,42]. VHF-based communication protocols such as the VHF Data Exchange System (VDES) and Digital Selective Calling are also susceptible to SDR manipulation since attackers can synthesize and transmit legitimate-looking VHF data frames without authentication [35,43].

Beyond communication systems, tampering can compromise bridge navigation and situational awareness systems, including ECDIS, Automatic Radar Plotting Aid (ARPA) radar overlays, and NMEA data buses, by corrupting their upstream GNSS and AIS inputs [23]. Such manipulation can lead to erroneous chart updates, unsafe routing, or false collision alerts. Additionally, shore-based systems such as Vessel Traffic Services and Long-Range Identification and Tracking can receive falsified tracking data due to spoofed AIS or GNSS inputs, as observed in recent Baltic Sea incidents [44,45]. Collectively, these vulnerabilities highlight the systemic risk of SDR-based tampering across the maritime cyber-physical ecosystem, where the lack of cryptographic safeguards continues to expose essential protocols to manipulation [46].

4.2.3. Defensive Measures

GNSS, AIS, VDES, and onboard navigation devices are known to be vulnerable to tampering. At the signal level, integrating multiple sensors such as radar, GNSS, AIS, and inertial measurement units helps detect anomalies, including sudden position jumps, improbable speeds, and inconsistencies between reported and observed vessel movements [23]. Monitoring signal characteristics such as power, correlation distortion, and direction of arrival can reveal jamming or spoofing attacks or attempts. Operational procedures, including maintaining radar and visual navigation as backups, suspicious signals reporting, and cross-checking alternate position sources, further reduce risk. Redundancy, for instance, using multiple GNSS constellations or independent AIS/VTS feeds, also increases system resilience against attack [30,47,48].

In addition to signal-level defenses, securing the SDR platform itself is essential to prevent attackers from introducing malicious waveforms or tampering with firmware. Techniques such as code signing and secure boot ensure that only verified firmware and waveform binaries run on the device [40]. Access control and authentication mechanisms that includes mutual Transport Layer Security (TLS) and role-based permissions protect management interfaces from unauthorized access [49]. Secured software update pipelines with integrity checks and rollback capabilities prevent malicious modifications during distribution [40]. Runtime monitoring of memory and system state can detect abnormal behavior in real time while executing waveforms in constrained containers or hypervisors. This minimizes potential damage if a waveform is compromised. Combining signal monitoring with robust platform security creates a comprehensive defense against SDR-enabled tampering, helping to protect critical maritime systems and maintain operational safety [50,51].

4.3. Repudiation

Repudiation attacks occur when there is no reliable way to verify the origin of a message, a system change, or an operator who triggered the incident or event, particularly in the absence of cryptographic signatures or sufficient audit trails. Attackers exploit this vulnerability by faking or tampering with system logs, overwriting local records to conceal their actions, sending unsigned messages that cannot be traced to a source, or triggering false errors to erase evidence. For instance, after compromising an SDR, an attacker may delete logs to eliminate traces of their intrusion. These may undermine forensic investigations, compromise vessel system accountability, and also delay or distort responses to safety-critical incidents [52,53].

4.3.1. Description and Attack Methodology

Repudiation is prominent in systems lacking non-repudiation mechanisms, mostly where local event logs are incomplete and audit capabilities are limited [42,52]. SDRs lower the technical bar for gathering information and preparing the deceptive signal steps while weak update or authentication practices enable gaining access and tampering with local records [53]. Figure 6 breaks down the steps that characterize an orchestrated repudiation attack.

1. **Signal Reconnaissance:** Attackers begin by mapping the target environment to identify active maritime protocols such as AIS, VDES, GNSS, and NMEA feeds. During this phase, they record traffic patterns, locate logging and management endpoints, and capture baseline messages for future replay scenarios [53,54].
2. **Gain Foothold and Access:** The attacker compromises an SDR device, onboard system, shore-based server, or operator account. Entry points include weak credentials, exposed management interfaces, software logic flaws, or physical access. AIS implementations are especially vulnerable due to poor error handling and logic validation [52].
3. **Repudiation actions:** Repudiation is not a direct attack vector but rather denotes a class of threats wherein actors can deny responsibility for actions due to the absence of verifiable evidence. Literature outlines several actions that lead to repudiation, and examples are:
 - (i) **Replaying artifacts:** This is when the attacker gets inside a host and then constructs protocol-compliant messages such as AIS or VDES packets or records legitimate transmission actions to obscure or overwrite recorded logs. SDR toolchains allow attackers to replicate these with minimal effort [42,53].

- (ii) **Forged messages:** Forged messages may be injected to simulate ghost vessels, false positions, and misled investigations. Alternatively, attackers may replay previously captured messages at different times or locations. Unsigned command messages may also be accepted by maritime systems to create events that cannot be reliably traced back to a source [52].
- (iii) **Tamper local records and logs:** To erase evidence, attackers overwrite, delete, or alter onboard logs, NMEA traces, and shore-based audit trails. Those with control over the SDR or host operating system can manipulate timestamps and storage contents to frustrate forensic analysis [31].
- (iv) **Trigger plausible errors or confusion:** Attackers may induce benign-looking faults such as AIS clutter or intermittent GNSS anomalies to mislead system auditors. These distractions cause anomalies to be wrongly attributed to environmental or technical issues rather than malicious intent [54,55].
- (v) **Jamming:** Access control systems may be jammed, and this may prevent log recording, creating gaps in logs and making it harder to attribute actions [55].

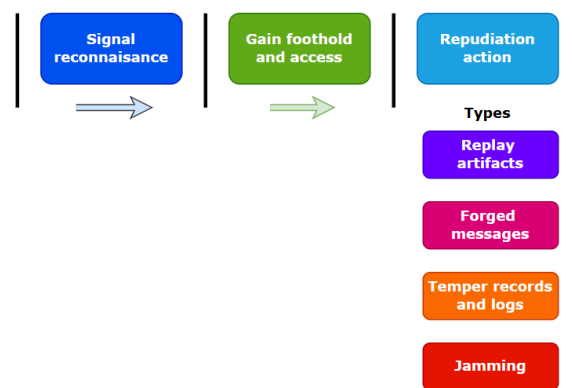


Figure 6. Repudiation Attack Methodology.

4.3.2. Targeted Systems and Protocols

Repudiation threats are prevalent across several maritime communication and navigation systems that lack message authentication or sufficient audit trails. The Automatic Identification System is particularly vulnerable due to its open, unauthenticated VHF broadcasts that allow attackers to inject or modify vessel identity, position, and status information without attribution [52]. Similarly, the Global Navigation Satellite System, which provides position and timing data to most maritime platforms, faces repudiation risks when logs or received signals lack cryptographic validation or tamper-evident storage, enabling malicious entities to deny involvement in spoofing or jamming incidents [56]. These vulnerabilities allow adversaries to manipulate or falsify maritime situational data while maintaining plausible deniability, making attribution and accountability difficult for operators and investigators.

Other critical systems, such as the Electronic Chart Display and Information System and Voyage Data Recorders, also face repudiation risks due to inadequate data integrity verification and weak access controls. In ECDIS, unlogged or unauthenticated updates to navigation charts and sensor data can lead to untraceable alterations that distort navigational awareness [53]. Similarly, if VDR logs can be deleted or overwritten without tamper protection, malicious users can erase evidence of unauthorized actions, impeding post-incident forensics [57]. The absence of secure audit mechanisms and cryptographic non-repudiation in these systems highlights the need for robust logging, digital signatures, and time-stamped audit trails to preserve accountability and ensure data integrity within maritime operations.

4.3.3. Defensive Measures

Defensive measures against repudiation in maritime systems emphasize ensuring message authenticity, integrity, and accountability. Implementing digital signatures and origin authentication, as demonstrated in Protected AIS and digital authentication prototypes, strengthens the traceability of transmitted data and prevents message forgery or denial of origin [27,35]. Similarly, robust cryptographic schemes such as public key infrastructure (PKI) and TLS-based validation provide secure identification for maritime services like AIS, VDES, and ECDIS, reducing the risk of entities repudiating transmitted information. Rahman et al. (2022) further highlight that resilient software logic and authenticated message exchange are essential to mitigate the exploitation of weak AIS implementations [52]. Complementary tamper-evident and immutable audit logs also support accountability by preserving the chain of evidence and ensuring system actions can be independently verified [16].

Additional mechanisms such as secure timestamping, replay detection, and sequence enforcement help establish verifiable event timelines, making it difficult for actors to deny prior communications or actions [8]. Integrating multi-sensor correlation, for example, comparing radar, GNSS, and AIS data, further enhances non-repudiation by exposing inconsistencies across independent sources [31,44]. Finally, designing maritime systems with non-repudiation principles, including role-based access, authenticated updates, and cryptographically verifiable records, ensures long-term accountability and operational trust.

4.4. Information Disclosure

In the STRIDE threat model, information disclosure refers to the unauthorized exposure of sensitive data. This compromises confidentiality, which adversaries can exploit for surveillance, exfiltration of operational data, and system takeovers in maritime environments. Such disclosures often result from insecure system configurations, unencrypted communications, or inadequate access controls [27,58].

4.4.1. Description and Attack Methodology

Attackers seeking to cause information disclosure in maritime systems typically proceed from reconnaissance to exploitation and then data exfiltration, often beginning with a passive radio or network survey to discover exposed broadcasts and endpoints [59,60]. Exploitation leverages protocol weaknesses, implementation faults, or misconfiguration to access sensitive vessel or sensor data [31,44,52]. Sophisticated adversaries may also use side channels or covert radio emissions to leak secrets from isolated systems, showing that disclosure risks are not limited to conventional networks [61].

Information disclosure in maritime systems occurs through multiple vectors. As discussed in the context of repudiation, information disclosure also involves **signal reconnaissance** and **gaining access**. Once access is gained, the process of disclosing sensitive information continues. The following are the various types of information disclosure actions explained below and summarized in Figure 7.

- (i) **Passive Eavesdropping:** Attackers intercept unencrypted maritime broadcasts using low-cost SDRs to collect AIS, VDES, or other radio communications, obtaining real-time vessel and system information and operational data [59,62].
- (ii) **Protocol Exploitation:** Weaknesses in maritime communication protocols, such as insufficient message authentication or error handling. This allow attackers to extract or infer sensitive data from system responses [27,52].
- (iii) **Side-Channel and Covert Channels:** Advanced attacks exploit hardware. For example, RAM-based emissions from isolated systems can reveal secret information

even from air-gapped computers, demonstrating that data leakage is not limited to networked channels [62].

- (iv) **Misconfigurations and Improper Access Control:** Inadequate system configurations, weak passwords, or lack of encryption can inadvertently expose data to unauthorized entities enabling easy capture or monitoring of sensitive communications [60].
- (v) **Data Aggregation and Analytics:** Anonymized or partial information can become sensitive when combined with external data. This may enable attackers to reconstruct vessel routes, schedules, or operational patterns [31,44,56].

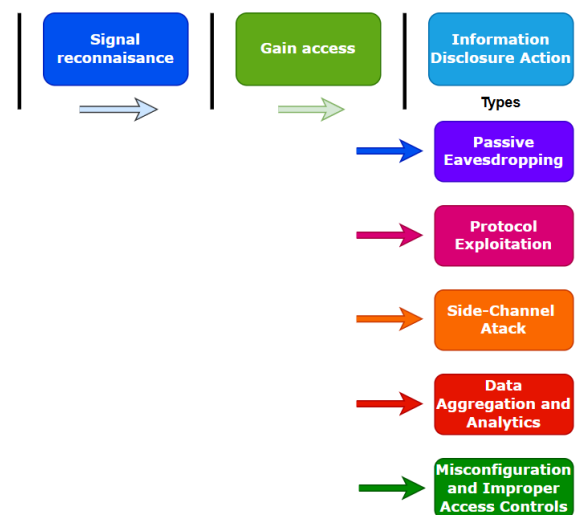


Figure 7. Information Disclosure Attack Methodology.

4.4.2. Targeted Systems and Protocols

Proceeding with the attack description and methodology, the following systems and protocols represent the primary targets where reconnaissance, exploitation, and exfiltration converge. Attackers first survey these channels for exposed data and then exploit the protocol or implement weaknesses to obtain leak-sensitive information [52,59]. The Automatic Identification System is a foremost example because its open broadcast design exposes vessel identities and real-time positions to anyone with basic SDR equipment, making passive collection and traffic analysis trivial [27,58]. Similarly, VHF Data Exchange System implementations, including VDES R-Mode carry operational messages whose handling flaws or insufficient protections can reveal routing, control, or status data to adversaries [63]. Electronic Chart Display and Information Systems can leak planned routes, waypoints, and navigational intent when misconfigured, which an attacker can combine with broadcast captures to reconstruct vessel behaviour [58].

Onboard archival and sensor systems also present significant disclosure risks that align with exploitation phases. Voyage Data Recorders store historical movements and communications that can be accessed if insecure [58]. Networked IoT sensors for engine telemetry, environmental monitoring, and autonomous navigation may inadvertently expose operational data when access controls are in place. This may lead to advanced eavesdropping and beam-based interception techniques that can capture data remotely [62]. Together, these systems form a contiguous attack surface where passive collection, protocol exploitation, and targeted data extraction produce information disclosure as outlined in the attack methodology.

4.4.3. Defense Measures

Mitigating information disclosure in maritime systems requires a multilayered approach that combines technical, procedural, and operational strategies. Encryption and

secure communication are fundamental, ensuring that AIS, VDES, DSC, GPS, sensor data, and other maritime channels remain confidential even if intercepted [27,42]. Authentication and access control further protect sensitive systems by enforcing strong credentials, role-based permissions, and mutual verification to prevent unauthorized access [35,58]. Maintaining tamper-evident logging and auditing allows operators to track access attempts and detect potential breaches in real time, while anomaly detection and multisensor correlation, thus integrating AIS, radar, GNSS, and visual data, helps identify inconsistencies and suspicious activity, providing an additional layer of defense [31,44,52,56,64].

Complementary measures focus on system resilience and operational discipline. System hardening and configuration management, including timely updates, patches, and careful network segmentation, reduce the risk of accidental data leaks from misconfigurations [60,61]. Additionally, user training and operational policies equip personnel to handle communications securely, recognize potential threats, and follow procedures that minimize inadvertent disclosures [58]. Together, these strategies create a comprehensive defense-in-depth framework to safeguard maritime systems against information disclosure.

4.5. Denial of Service

Denial of service in the maritime domain is the intentional disruption or degradation of legitimate radio or protocol service availability. Denial of service ranges from GNSS jamming, AIS channel flooding, and targeted physical-layer jamming of maritime VHF, leading to loss of navigation, communications, and situational awareness on water. Attacks may target radio frequency channels, shipboard and shore networks, and physical layer functions in radios and satellite links. Further impact may lead to loss of position and timing fixes to disruption of vessel traffic services and port operations with consequent safety and economic effects [41,65,66].

Many denial-of-service evaluations focus on isolated links or small-scale testbeds, so large-scale effects on integrated ship-shore networks and multi-vessel scenarios are often extrapolated rather than directly observed.

4.5.1. Description and Attack Methodology

Observations from incident analyses reveal that DoS attackers often initiate their operations with target selection and reconnaissance. Continuing with the workflow, they stage and execute the attack and then conclude with persistence and concealment as outlined in Figure 8 [67–70]. The following numbered steps capture the common methodology observations in experiments and incident analyses.

1. **Reconnaissance and Profiling:** Reconnaissance of the target environment includes radio spectrum surveys, identification of receiver types, observation of AIS and VDES traffic, and mapping of shipboard and shore network services using passive monitoring low-cost SDRs [67,68].
2. **Capability Staging:** This is the stage where attackers assemble required tools and resources, such as SDRs, amplifiers, and develop waveform or traffic generation scripts for the intended DoS vector [69,71].
3. **Initial Probing:** During this stage, threat actors may use low amplitude or intermittent interference and malformed packets to measure system tolerance and operator response thresholds while avoiding early detection [72,73].
4. **Execution of DoS Action:** This may include RF jamming or protocol-aware interference against GNSS, VHF, and application-layer networks against shipboard or shore services, including synchronization attacks on cellular or satellite links in maritime systems [67,69,70].

5. **Adaptive Escalation or Stealth Maintenance:** At this stage, cybercriminals vary power, timing, or traffic patterns of transmitted signals to prolong disruption while evading detection, or withdraw quickly after achieving objectives to reduce attribution risk [70,72].
6. **Persistence and Cleanup:** This includes maintaining footholds in compromised devices to enable repeated attacks or removing indicators of compromise to hinder post-incident analysis [52,73]. In maritime denial of services attacks, cleanups are not usually seen, but researchers have spoken about their possibility. Therefore, it is imperative to call for attention and solutions for future use.

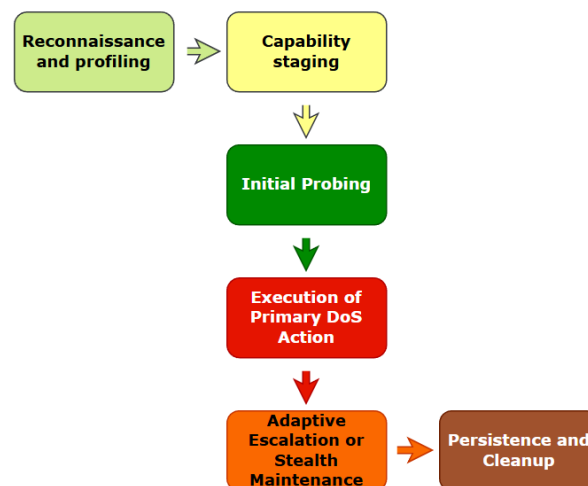


Figure 8. Denial of Service Attack Process.

4.5.2. Targeted Systems and Protocols

Continuing from the attack processes, a small set of radio and networked systems concentrates maritime availability risk because many operations depend on them simultaneously. GNSS is the most critical single vector for availability attacks, as jamming and spoofing directly deny or corrupt positioning and timing and cascade failures into integrated bridge systems and time dependent services [23,68]. VHF-based links, including AIS and VDES, are also exposed to local RF interference or protocol aware disruption, degrading collision avoidance and situational awareness [27,63].

Shipboard networks such as Wi-Fi, satellite backhaul, Long-Term Evolution (LTE), and emerging 5G links are vulnerable to classical network DoS and to physical layer or synchronization attacks that can be stealthy and hard to attribute [69,70]. Vessel Traffic Services and port IT infrastructure are attractive shore-based targets for volumetric DoS because disruption yields broad logistic and economic effects [65]. Finally, bridge components such as ECDIS, ARPA radar fusion, and Voyage Data Recorders are indirect victims: availability loss in upstream feeds or networked services can render these systems unavailable or unreliable, which in practice has safety-critical consequences [52,74].

4.5.3. Defense Measures

Effective mitigation of DoS may use layered defenses that address RF, network, and operational vectors concurrently. To enhance signal availability and resilience to DoS, systems should incorporate multi-constellation receivers capable of tracking signals from GPS, Galileo, GLONASS, and other satellite networks. Antenna diversity and directional antenna configurations can mitigate localized interference by spatially filtering unwanted signals. Hardware-based countermeasures such as spread spectrum techniques and anti-jamming front ends further reduce susceptibility to intentional disruption. Continuous

monitoring of NMEA output and receiver telemetry enables early detection of anomalies indicative of interference or spoofing, facilitating timely isolation and response [23,36,37,73]. For VHF and AIS systems, tools such as spectrum monitoring and direction finding help detect where interference is coming from. Smart antennas (using beamforming or adaptive reception) can block out the noise and focus on real signals, making it easier for operators to find and avoid jamming sources [48,62].

To harden networks and shore services, standard DoS controls such as network segmentation, rate limiting and filtering, hardened management interfaces, DoS scrubbing for critical shore endpoints, and secure device update and authentication practices to prevent botnet formation from compromised maritime IoT against maritime applications are imperative [69,71]. Physical layer and synchronization defenses require attention to receiver design and protocol resilience, for example secure synchronization and detection of anomalous timing behavior in cellular and satellite modems [70,73]. Finally, operational mitigations are essential: establish degraded mode navigation procedures that rely on radar and visual fixes, run incident exercises, report interference events to authorities, and maintain crosschecked manual processes to preserve safety when automated systems lose availability [65,66].

4.6. Elevation of Privilege

Elevation of privilege describes when an attacker moves from a low-privileged or unauthenticated position to a higher-privileged state on an SDR host, hypervisor, ship-board controller, or SDR-connected IT/OT component. In maritime settings this capability is particularly dangerous because privileged access to bridge systems, gateways, radios, or update mechanisms enables persistent control that can lead to manipulation of navigation, cargo and communication functions, including the ability to defeat forensic traces during incident investigation by wiping out logs [52,75]. Attackers are motivated to escalate privileges to gain persistence, tamper with device firmware or waveforms and hide their actions behind legitimate system accounts, all of which magnify the safety and operational impacts of vessels and their environments.

4.6.1. Description and Attack Methodology

Attackers usually begin with low-privilege access and then escalate in stages. They first gather information about exposed services and weak credentials, then exploit software or firmware flaws to execute exploits on a device, and finally gain administrative control that enables them to move to other systems [52,75]. The numbered steps that follow unpack this progression and show where defenses such as secure boot, runtime attestation, segmentation, and patching can stop the attack chain [60].

1. **Initial access:** This involves the use of low-privilege vectors such as exposed management ports, weak credentials, unsecured Wi-Fi, compromised maritime IoT devices, exploited radio modems, topology, and service information to gain access to a naval system, network, application, account, et cetera [69].
2. **Privilege Escalation:** Leveraging on gaining access to a naval system, an attacker may exploit application logic or firmware flaws in AIS handlers, gateway translators, NMEA parsers, radars, or SDR firmware to execute code or obtain elevated privileges on the host process [52,75]. The following are examples of privileged escalation actions that are usually performed.
 - (i) Time replay, jamming, or spoofing attacks might be employed to disable access controls and re-execute time-based access tokens, thereby gaining elevated privileges [60].

- (ii) Local privilege escalation may involve abusing misconfigured operating system services or insecure update mechanisms to gain root [69].
 - (iii) Lateral movement is achieved by the attacker switching across systems, networks, and application accounts after gaining access to one [65,75].
3. **Persistence:** This includes installing a rootkit or a backdoor in embedded SDR or a critical device, signed or unsigned waveform payloads, malicious firmware, or creating privileged service accounts that survive reboots and updates [52].
 4. **Defense evasion:** Attackers may abuse privileges to alter logs, disable monitoring, or tamper with telemetry to reduce detection and attribution. [52,66].

Each step in the attack chain, as shown in Figure 9, offers a chance to stop or slow down the attacker. For example, strong passwords and secure login methods can block initial access. Secure boot and runtime checks help protect devices from tampered firmware. Network segmentation and regular patching can limit how far an attacker can penetrate systems. Time-based authentication can stop replay attacks, while spread spectrum and frequency hopping make jamming harder. Using GNSS receivers with multiple antennas and satellite systems helps detect and resist spoofing.

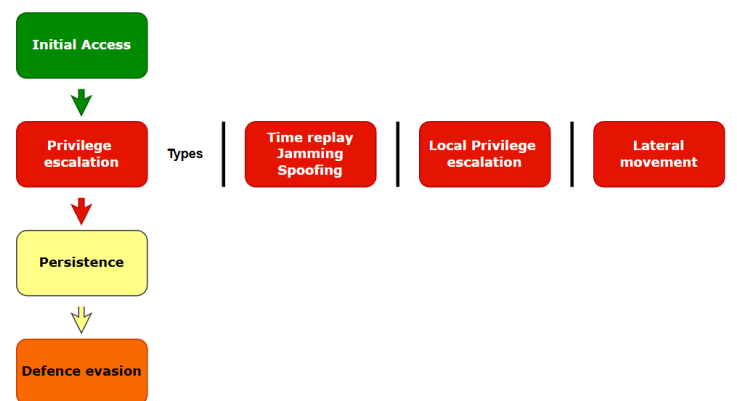


Figure 9. Elevation of Privilege Attack Process.

4.6.2. Targeted Systems and Protocols

Attackers often target maritime systems where software, radios, and networks connect. This includes embedded SDR platforms, which can be hijacked by tampering with waveform loaders or firmware. If attackers break out of containerized applications or hypervisors, they can control multiple virtual systems. Shipboard LANs, maritime IoT devices, and gateway units, especially those translating NMEA protocols are common entry points when poorly secured. Devices like chartplotters, ECDIS endpoints, satellite and cellular modems, and VDR ingestion services are also vulnerable if exposed or misconfigured [52,60].

Once inside, attackers use replay, jamming, or spoofing to bypass controls, especially in AIS, GNSS, and management protocols. They may exploit firmware bugs or weak updates to gain root access. From there, they move laterally across ship systems or into shore-based services, especially if cloud synchronizes the vessel without strong checks. To prevent this, defenses such as secure boot, run-time attestation, timestamped authentication, spread spectrum, and multi-antenna GNSS validation are essential across all layers, from SDR and IoT applications to software-defined networking [66,75]. The following section discusses more on the defensive measures further.

4.6.3. Defense Measures

Effective defense against privilege escalation in maritime systems requires a coordinated approach across embedded devices, networks, and operational layers. At the device level, implementing secure boot, firmware signing, and cryptographic validation of software updates ensures that only trusted code runs on SDRs, modems, and IoT components. Runtime attestation further protects against tampering by continuously verifying the integrity of real-time operating systems (RTOS), waveform memory, and hypervisor containers [76]. To further minimize exposure, systems should follow the principle of least privilege, enforcing role-based access control (RBAC) across onboard tools, cloud services, and API interfaces, while management protocols should adopt a default-deny posture. Continuing, patch and configuration management play a crucial role in addressing vulnerabilities in Linux kernels, embedded operating systems, SDN controllers, container engines, and drivers while also removing default credentials and disabling unused services [60,69].

In addition, network segmentation through Virtual Local Area Networks (VLANs), microsegmentation, or air-gapping helps isolate operational technology, navigation, and gateway systems, while SDN-based firewalls restrict lateral movement. Continuous monitoring using endpoint detection and response (EDR) and intrusion detection systems (IDS) enables early detection of privilege misuse, complemented by tamper-evident logging of administrative activities on chartplotters, ECDIS, and VDRs. Protecting AIS and GNSS from spoofing and replay with timestamped authentication, spread-spectrum modulation, and multi-antenna validation enhances signal-level trust. Finally, maintaining operational resilience requires regular crew training, incident response drills, red teaming, and vendor security vetting in alignment with maritime cybersecurity advisories [65,66,75,77].

5. Results and Discussion

The systematic review of 84 scholarly publications led to the identification of 44 distinct threats targeting Maritime Software-Defined Radio systems. Each identified threat was mapped to the STRIDE threat modeling framework to characterize it, including its security implications. The quantitative mapping revealed 23 Spoofing, 36 Tampering, 30 Repudiation, 24 Information Disclosure, 33 Denial of Service, and 28 Elevation of Privilege instances, as illustrated in Table 2. Also, in Table 2, S, T, R, ID, DoS, and EoP represent spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, respectively, with each check mark (✓) representing an instance of attack.

Beyond the distribution of STRIDE categories, the survey also revealed that most of the 44 threats, particularly technical attacks such as GPS and AIS spoofing, jamming, protocol exploitation, malware insertion, and buffer overflow exploits, are evaluated primarily through a combination of both empirical and simulation studies. In contrast, a smaller subset of threats, including eavesdropping, traffic sniffing, insider threats, social engineering, and phishing, is supported more by evidence from real incidents, user studies, or captured maritime network traffic. A further subset of emerging threats, such as spectrum data poisoning, frequency change attacks, AIS cloaking, rogue waveform upload, and bogus virtual aids-to-navigation, remains predominantly explored in simulation and emulation environments, underscoring the need for additional validation in operational maritime settings.

Overview and Discussion of Identified Threats

From the quantitative mapping, tampering emerged as the most dominant threat category, with 36 distinct instances identified across the reviewed studies. These attacks primarily target the integrity of SDR components, firmware, and signal processing pipelines. Examples such as firmware modification, malicious reconfiguration, rogue waveform upload, and hardware injection demonstrate how hackers can manipulate SDR behavior

at its core. The prevalence of tampering-based threats reinforces the importance of signal integrity verification, authenticated updates, SDR access controls, firmware integrity checks, compliance with IMO guidelines, and real-time cross-instrument monitoring. As SDRs rely heavily on software-defined architectures, even minor modifications to configuration files or code modules can lead to severe operational disruptions or enable persistent adversarial control. This finding suggests that the maritime domain must adopt robust supply chain security practices and trusted execution environments to ensure end-to-end device integrity.

Table 2. STRIDE Classification of Maritime SDR Threats.

Threats	Papers	S	T	R	ID	DoS	EoP
GPS Spoofing	[24,25,31,72]	✓	✓	✓		✓	
AIS Spoofing (Ghost Vessel)	[24–27]	✓	✓	✓		✓	
VHF/DSC Spoofing	[27,28,35,78,79]	✓	✓	✓		✓	
GPS Time Spoofing	[29,33,51]	✓	✓	✓		✓	✓
ECU Spoofing	[51,59,60]	✓	✓	✓		✓	✓
Sensor Spoofing	[31,51,60]	✓	✓	✓		✓	✓
Radar Spoofing	[65,66]	✓	✓	✓		✓	✓
Device Cloning	[26,27,60]	✓	✓	✓	✓	✓	✓
Message Injection	[30,44,45]		✓	✓	✓	✓	✓
Eavesdropping	[46,47,49,70]			✓	✓		✓
Traffic Analysis	[30,46,55]			✓	✓		✓
Sniffing	[47,57,71]			✓	✓		✓
Unauthorized Demodulation	[47,67]			✓	✓		✓
Side Channel Attack	[46,48]			✓	✓	✓	✓
Replay Attack	[44,45,55]		✓	✓	✓		✓
Jamming	[51,54,56]					✓	✓
Unauthorized Access	[38,41,43,45]		✓	✓	✓	✓	✓
Frame Exploitation	[47,55]		✓	✓	✓	✓	✓
Firmware Modification	[34,44,45]		✓	✓	✓	✓	✓
AIS Identity Manipulation	[27,30,36]	✓	✓	✓			
Authentication Bypass	[30,36,45,73]	✓	✓	✓	✓		✓
Lateral Movement	[57,58]	✓	✓		✓	✓	✓
Insider Threats	[58,61]	✓	✓	✓	✓	✓	
Spectrum Data Poisoning	[54,68,69]	✓	✓			✓	
Frequency Change Attack	[55,71,73]	✓	✓			✓	
De-authentication	[47,53,55,57,74]	✓	✓	✓			
DoS	[52,53]	✓	✓			✓	
Flooding Attack	[30,45,55]		✓			✓	
Signal, Protocol and Software Hijacking	[38,53,57,67]	✓	✓	✓	✓	✓	✓
Protocol Exploitation	[45,53,54]	✓	✓		✓	✓	✓
Signal Deception (Masking)	[37,51,52]	✓	✓			✓	
Time Manipulation Attack	[28,29,33]	✓	✓			✓	✓
Buffer Overflow	[38,45,67]		✓		✓	✓	✓
Fault-Based Attack	[45,72]		✓		✓	✓	✓
Hardware Injection	[38,41,46]		✓		✓		✓
AIS Cloaking	[27,30,45]		✓	✓		✓	
Malicious Reconfiguration	[67,72]	✓	✓	✓	✓	✓	✓
Rogue Waveform Upload Attack	[38,41,72]		✓	✓	✓	✓	✓
Social Engineering	[61,62]	✓	✓	✓	✓	✓	✓
Bogus Virtual Aids-to-Navigation (AtoN)	[27,30]	✓	✓	✓		✓	
Software (Malware) Insertion	[38,41]		✓	✓	✓	✓	✓
Phishing	[76,77]				✓		
Message Deletion	[44,45]		✓	✓		✓	
Total (44)	44	23	36	30	24	33	28

Following closely, denial of service attacks appeared in 33 instances, reflecting the high susceptibility of maritime SDRs to availability-related disruptions. Attacks such as jamming, flooding, de-authentication, and signal hijacking demonstrate how threat actors

can exploit the open and shared maritime radio spectrum to degrade or completely deny service availability. Since maritime communication depends heavily on continuous data exchange for navigation, distress signaling, cargo management, and situational awareness, such disruptions pose direct safety and economic implications. The results emphasize the urgent need for adaptive anti-jamming strategies, dynamic spectrum management, and redundancy mechanisms to maintain communication reliability under hostile conditions.

Repudiation threats (30 occurrences) represent another major category of concern, particularly in systems where accountability and traceability are weak or nonexistent. Attacks such as message deletion, replay, and message injection exploit the absence of reliable logging and verification mechanisms in legacy maritime communication protocols. In the context of SDRs, where messages and waveforms can be easily generated or modified, repudiation undermines both forensic analysis and system trustworthiness. Strengthening audit trails, cryptographic signatures, and time-stamping mechanisms would therefore be essential to improving non-repudiation and ensuring that critical communication events remain verifiable and tamper-evident.

Spoofing attacks remain one of the most well-documented and impactful categories. Threats such as GPS spoofing, AIS identity manipulation, radar deception, and bogus virtual AtoN creation demonstrate how adversaries can fabricate or falsify signals to mislead receivers. These attacks exploit the lack of authentication and encryption in many maritime radio protocols, resulting in severe navigational and operational risks. The widespread occurrence of spoofing attacks reflects the maritime sector's reliance on trust-based and unencrypted signaling standards. Consequently, introducing cryptographic authentication and physical-layer verification techniques such as signal fingerprinting or Doppler-based validation would significantly enhance the authenticity and reliability of transmitted signals.

Information Disclosure appeared in 24 instances, highlighting the persistent challenge of maintaining data confidentiality in open maritime environments. Attacks like eavesdropping, sniffing, traffic analysis, and side-channel exploitation illustrate how cybercriminals can passively intercept and infer sensitive information from radio transmissions. Because most maritime systems broadcast unencrypted data over open channels, they inherently enable cybercriminals to monitor operational movements, vessel identifiers, and even onboard network traffic. This emphasizes the need for lightweight encryption protocols and privacy-preserving communication frameworks tailored to bandwidth-constrained and latency-sensitive maritime networks.

Elevation of Privilege threats demonstrate the potential for attackers to gain unauthorized access and control within SDR ecosystems. Attacks such as authentication bypass, lateral movement, software hijacking, and malicious reconfiguration exploit weak access controls and poor isolation between SDR software layers. Once elevated privileges are obtained, attackers can modify operational parameters, inject malicious code, and pivot across connected systems. These findings highlight the necessity of implementing zero-trust architectures, role-based access control, and hardware-backed security modules to contain privilege escalation and limit the blast radius of potential compromises.

Collectively, the STRIDE analysis reveals that maritime SDR threats are multidimensional and interdependent cutting across both cyber and RF domains. The observed attack distribution suggests that while traditional issues such as spoofing and DoS remain significant, emerging threats increasingly target SDR software reconfiguration, control mechanisms, and firmware integrity. This evolution reflects a shift from purely communication-based disruptions toward more sophisticated and persistent compromise attempts that exploit the programmable essence of SDRs. Addressing these challenges requires a holistic defense strategy that integrates secure software design, resilient communication protocols, spectrum

monitoring, and continuous threat intelligence tailored to maritime operational environments. Ultimately, even though SDR security research is still in its early stages, the findings highlight the urgent need for the maritime industry to transition from reactive defense to proactive security engineering, ensuring that SDR-enabled systems remain trustworthy, resilient, and comply with evolving cybersecurity standards. Following this is Figure 10, which shows cyberattacks organized across five attack surfaces: device, software, network, message, and user surface, with each highlighting some specific attacks that exploit it.

The results shown in Figure 10 present a view of some threats facing maritime SDRs through the STRIDE framework. By grouping attacks across device, software, network, message, and user levels, the classification reveals that maritime SDR ecosystems face interconnected risks rather than isolated weaknesses. Each layer supports or influences the next, meaning a single compromise can cascade through the entire communication chain.

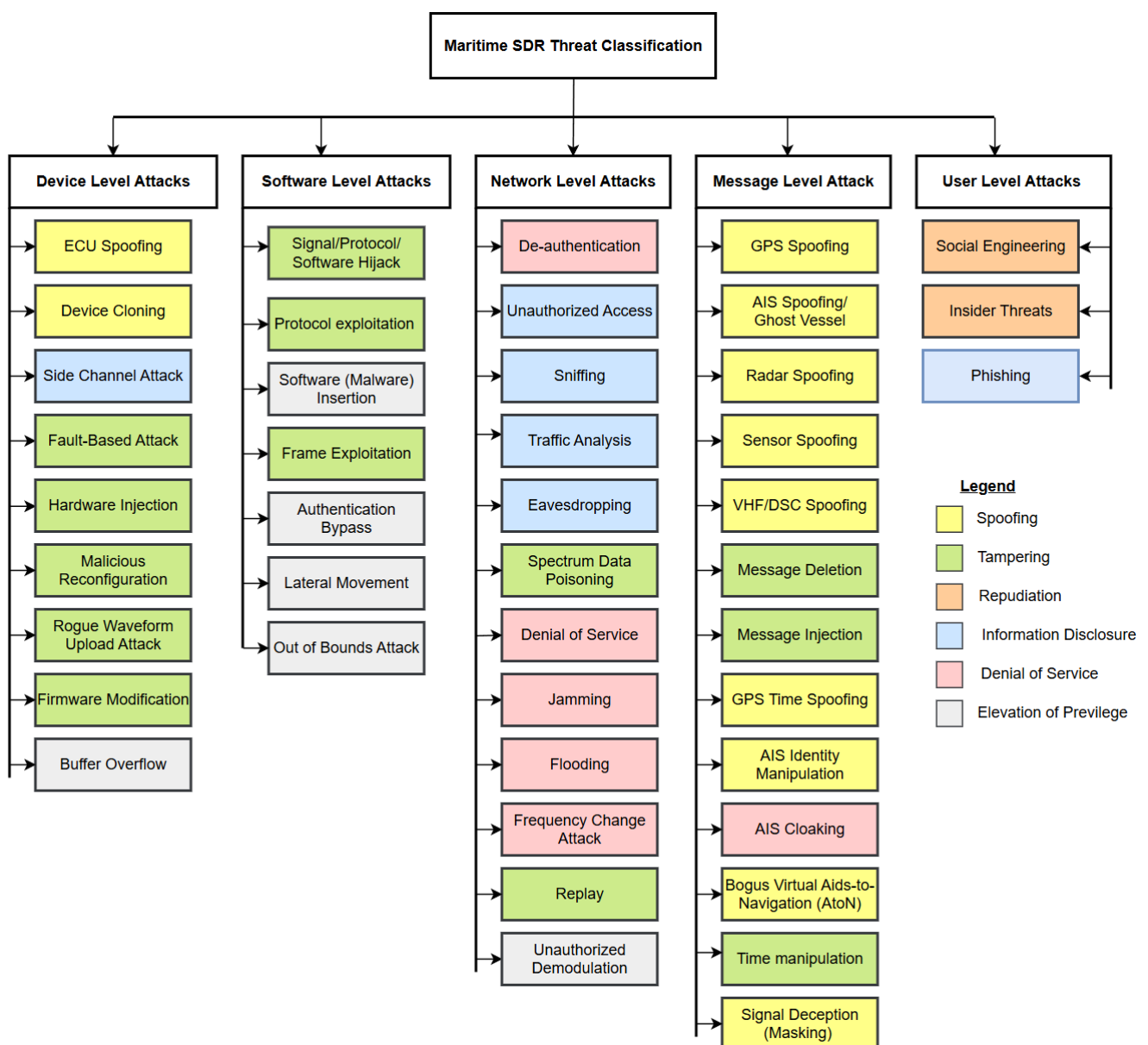


Figure 10. Attack Surface and STRIDE Classification of Maritime SDR Threats.

At the device level, most attacks target the hardware and firmware that form the foundation of SDR operation. ECU spoofing, device cloning, and hardware injection show

how adversaries exploit the programmable nature of SDRs to alter or mimic legitimate devices. Such tampering can modify signal behavior at its source, making it difficult to detect at higher levels. These findings highlight the need for secure hardware design, including authenticated firmware updates and hardware attestation mechanisms, to ensure trust in physical components.

The software level focuses on how attackers manipulate SDR control code or protocols. Threats such as protocol hijacking, malware insertion, and authentication bypass reveal that poorly protected software modules can be turned into attack vectors. Because SDR software directly controls signal generation and modulation, any compromise at this layer can change how the entire system communicates. Strong software validation, secure coding, and continuous integrity monitoring are therefore critical to protect this level.

At the network level, attacks primarily affect communication availability and confidentiality. De-authentication, flooding, and jamming fall under denial of service, while eavesdropping and traffic analysis threaten information disclosure. These attacks exploit the openness of maritime communication channels and can disrupt data exchange between vessels and control centers. Defending this layer requires adaptive spectrum management, encryption, and resilient synchronization protocols to maintain reliable links even under interference.

The message level represents the most visible form of threat to maritime operations. Attacks such as GPS spoofing, AIS ghost vessel creation, and message injection manipulate the content of transmitted signals, leading to false navigational data or deceptive maritime awareness. Because these messages directly inform vessel decisions, their alteration can have severe safety impacts. Robust message authentication, timestamp validation, and multi-source data cross-checking can help reduce these risks.

Finally, at the user level, the results show that human factors remain a significant vulnerability. Social engineering, phishing, and insider threats can undermine even technically secure systems. These attacks rely on deception or misuse of legitimate access privileges, emphasizing the importance of training, access control, and accountability in maritime organizations.

Together, these layers form an integrated view of SDR security. Spoofing and tampering are the most common threats across levels, reflecting ongoing challenges in ensuring data integrity and authenticity. Denial of service and information disclosure attacks further highlight the need for resilient communication designs. Overall, the classification demonstrates that maritime SDR protection requires a multi-layered defense strategy that combines secure hardware, verified software, adaptive networking, authenticated signaling, and user awareness. By aligning these elements, the maritime sector can strengthen both operational reliability and cyber resilience as SDR technology continues to evolve.

Table 3 shows that high-severity maritime SDR threats cluster around attacks that directly manipulate core navigation, identification, and control functions, rather than purely passive RF abuses. In this context, high/medium/low severity describe how serious the consequences of an attack are. High-severity attacks can directly endanger the vessel's safety, navigation, or control. Medium-severity attacks degrade operations, reliability, or situational awareness, but usually with some remaining fallback or recovery options, and low-severity attacks have limited immediate impact (for example, mainly reconnaissance or minor disruption) but may still support or enable more serious attacks later. Continuing with the analysis of Table 3, GPS and AIS spoofing, ECU and sensor spoofing, radar spoofing, device cloning, firmware modification, authentication bypass, unauthorized access, lateral movement, insider threats, and generic DoS are all rated high severity because they can mislead vessel positioning, distort traffic pictures, alter propulsion behavior, and ultimately jeopardize the safety of navigation and ship control. Even when

an attack type appears rarely, its operational impact ranges from loss of navigation to disruption of communications, showing that low-frequency but high-consequence incidents still pose a serious risk to maritime operations.

Table 3. STRIDE Classification of Maritime SDR Threats with Frequency, Severity and Operational Impact [24–31,33–38,41,43–49,51–62,65–74,76–93].

Threats	Frequency	Severity	Operational Impact
GPS Spoofing	4	High	Navigation deviation and collision risk
AIS Spoofing (Ghost Vessel)	4	High	False traffic and route diversion
VHF/DSC Spoofing	4	Medium	Misleading distress calls and crew confusion
GPS Time Spoofing	5	High	Safety-critical timing errors
ECU Spoofing	5	High	Engine/propulsion manipulation
Sensor Spoofing	5	High	False readings and poor situational awareness
Radar Spoofing	5	High	Phantom targets and mis-navigation
Device Cloning	6	High	Identity theft and persistent access
Message Injection	5	Medium	False commands and system compromise
Eavesdropping	3	Low	Confidentiality loss and intelligence gathering
Traffic Analysis	3	Low	Operational pattern exposure
Sniffing	3	Low	Sensitive data leakage
Unauthorized Demodulation	3	Low	Signal interception and privacy breach
Side Channel Attack	4	Medium	Key extraction and system compromise
Replay Attack	4	Medium	Reuse of valid signals and receiver confusion
Jamming	2	High	Communication denial and navigation loss
Unauthorized Access	5	High	System takeover and persistent compromise
Frame Exploitation	5	Medium	Protocol abuse and data corruption
Firmware Modification	5	High	Persistent malware and device bricking
AIS Identity Manipulation	3	High	Vessel misidentification and traffic disruption
Authentication Bypass	5	High	Unauthorized control and trust breakdown
Lateral Movement	5	High	Network-wide compromise
Insider Threats	5	High	Privileged misuse and sabotage
Spectrum Data Poisoning	3	Medium	ML model corruption and degraded detection
Frequency Change Attack	3	Medium	Loss of connectivity and service disruption
De-authentication	3	Medium	Forced disconnects and denial of service
DoS	3	High	Service outage, operational halt
Flooding Attack	2	Medium	Resource exhaustion
Signal, Protocol and Software Hijacking	6	High	Full system compromise
Protocol Exploitation	5	High	Protocol-level takeover
Signal Deception (Masking)	3	Medium	Hidden signals and mis-navigation
Time Manipulation Attack	4	High	System desynchronization
Buffer Overflow	4	High	Remote code execution
Fault-Based Attack	4	Medium	Hardware degradation and denial of service
Hardware Injection	3	High	Malicious hardware takeover
AIS Cloaking	3	Medium	Vessel invisibility and traffic disruption
Malicious Reconfiguration	6	Low	Persistent compromise and system instability
Rogue Waveform Upload Attack	5	High	SDR corruption and denial of service
Social Engineering	6	High	Crew deception and credential theft
Bogus Virtual Aids-to-Navigation (AtoN)	4	High	False navigation aids and collision risk
Software (Malware) Insertion	5	High	Persistent malware and system compromise
Phishing	1	High	Credential theft
Message Deletion	3	Medium	Loss of critical communication

At the same time, the table highlights how lower-severity but more stealthy activities, such as eavesdropping, traffic analysis, sniffing, and unauthorized demodulation, form a foundational layer for intelligence gathering and preparation of higher-impact attacks. Medium severity techniques such as replay attacks, frame exploitation, side-channel attacks,

spectrum data poisoning, frequency change attacks, deauthentication, flooding, and message injection bridge this gap by enabling protocol abuse, model corruption, and resource exhaustion that can degrade detection and facilitate subsequent privilege escalation or spoofing. Taken together, the distribution of frequency, severity, and operational impact in Table 3 supports the paper’s broader claim that maritime SDR threats are multi-stage and interdependent, with reconnaissance and low-severity compromises often serving as precursors to fewer but more dangerous attacks that can cause systemic disruption across shipboard and shore to side systems.

Aside from the frequency, severity and operational impacts, another factor that increases the risk of SDR attacks is the open nature of it and how it can easily be obtained by cybercriminals. SDR hardware is now so inexpensive and widely available that less technically capable criminals can obtain radio-frequency toolsets with minimal cost and effort. Devices such as the RTL-SDR, HackRF One, LimeSDR, and bladeRF can be ordered from common online marketplaces, shipped worldwide, and operated using freely available open-source software, eliminating many of the traditional financial and expertise barriers to RF exploitation. Once acquired, these platforms allow adversaries to synthesize, capture, and manipulate signals across key maritime bands, enabling practical spoofing, jamming, replay, and protocol manipulation attacks against navigation and communication systems without the need for specialized laboratory equipment or regulated infrastructure. Below are specifications of some SDR platforms demonstrating their capabilities and types of attacks they can be used to perform in Table 4 [49,59,68,71,72,94–99].

Table 4. Specification Comparison of SDR Hardware Platforms.

Specification	RTL-SDR	HackRF One	LimeSDR	BladeRF
Freq Range	22 MHz–2.2 GHz	1 MHz–6 GHz	100 kHz–3.8 GHz	300 MHz–3.8 GHz
RF Bandwidth	3.2 MHz	20 MHz	61.44 MHz	40 MHz
Transmitter Channels	1	1	2	1
Receivers	1	1	2	1
Duplex	N/A	Half	Full	Full
Interface	USB 2.0	USB 2.0	USB 3.0	USB 3.0
Chipset	RTL2832U	MAX5864	LMS7002M	LMS6002M
Open Source	No	Full	Full	Schematic and Firmware
Transmit Power	N/A	−10 dBm+	0–10 dBm	6 dBm
Price	\$30–40	\$320	\$349.95	\$420–1600

6. SDR Research Challenges

SDR research is currently facing several challenges, ranging from technical, security, operational, regulatory, interoperability, hardware limitations, and spectrum interference in open real-world experiments. Researchers studying SDRs, especially in the maritime radio domains, must deal with limited computing resources, complex signal environments, security risks, and a lack of common testing and regulation standards. Table 5 summarizes some of these challenges.

Solving these challenges requires collaboration across engineering, cybersecurity, and policy disciplines. Researchers are now focusing on secure architectures, reliable hardware designs, realistic test environments, privacy-aware data handling, and AI integration. Overcoming these barriers will ensure that SDRs continue to grow as trustworthy tools in both civilian and military applications.

Table 5. SDR Research Challenges Across Technical Domains.

Domains	Paper(s)	Key Issue(s)
Hardware	[1,49,100]	Limited processing power
Software and Firmware Security	[39,57,58]	Security weaknesses in software-defined infrastructures
RF Front-End Stability	[1,49]	Signal distortion and performance loss
Channel and Environment Testing	[2,101,102]	Laboratory tests fail to reflect real-world signal environments
Spectrum and Interference Management	[57,102]	Shared spectrum and interference risks
Data Governance and Privacy	[39]	Handling sensitive signal data without violating privacy
Standardization and Benchmarking	[49]	Lack of evaluation frameworks and benchmarks
Regulatory and Ethical Testing Limits	[57,102]	Legal and safety barriers on maritime SDR deployment
AI and Machine Learning Integration	[2,49]	Limited data and model reliability
Interoperability and Vendor Ecosystem	[1,2,58,103]	Device compatibility and Software update issues

7. Research Gaps and Future Directions

While the reviewed literature shows significant progression in understanding vulnerabilities of maritime Software-Defined Radios, it also reveals blind spots in both technical safeguards and operational preparedness. Many studies focus on proof-of-concept attacks or laboratory-based defensive mechanisms [28,36,72], but fewer address the complexities of shipboard integration, forensic readiness, and international enforcement [23,79]. Similarly, research into virtualized SDR environments emphasizes performance evaluation while overlooking supply-chain assurance and secure waveform provenance [40,51]. As maritime SDRs become increasingly embedded in navigation, safety, and port operations, these gaps become more consequential, exposing vessels and coastal infrastructures to sophisticated cyber–RF threats [31,61]. This section identifies pressing research deficiencies highlighted across existing work, explaining their implications for maritime cybersecurity and incident response, and proposes future research directions that can strengthen resilience at both technical and organizational levels. The goal is to provide a roadmap for researchers, practitioners, and policymakers seeking to close the gap between experimental findings and operational maritime security practice.

7.1. Regulatory and Standardization Challenges

Despite the presence of IMO, ITU, NIST 800-82, ISA/IEC 62443, DNV RP-0496, and AIS/VDES spectrum standards, none of these instruments defines SDR-specific security requirements for maritime RF systems. Existing regulations focus on high-level cyber risk management and generic OT security but remain largely technology agnostic with respect to programmable radios, dynamic waveforms, and RF layer threat modeling [89,90]. This creates an implementation gap where SDR platforms can be deployed in safety-critical roles without clear expectations for authentication, spectrum monitoring, or secure firmware lifecycle management.

Current AIS, VHF/DSC, NMEA 2000 and GNSS usage guidelines also lack binding provisions for message origin authentication, integrity protection, or non-repudiation across SDR enabled implementations [11,12,16,24]. As a result, spoofing, tampering, information disclosure and repudiation attacks demonstrated in the literature can be reproduced in real environments without violating any explicit SDR-security clauses. Future research should, therefore, (i) propose SDR aware security profiles that can be integrated into IMO cyber risk management guidance and national maritime directives; (ii) develop extensions to ITU-R M.1371, VDES and NMEA 2000 that specify cryptographic, logging and forensic requirements for SDR-based implementations; and (iii) explore how attestation, secure boot

and code signing requirements for maritime SDRs can be reflected in class rules and flag state inspections.

7.2. SDR Governance, Certification and Compliance

The survey highlights a lack of certification schemes and conformity assessment procedures tailored to maritime SDR platforms, even though the devices increasingly underpin GNSS, AIS, VDES, radar, and gateway functions [23,34,81,82,104]. Today, equipment testing focuses on RF performance and functional compliance, while security aspects such as spoofing resistance, secure update channels, or resilience to firmware tampering are rarely part of mandatory type approval policies. This absence of SDR-focused certification complicates enforcement: ship operators can meet existing cyber requirements on paper while running radios that are trivially reconfigurable by attackers.

Future work should design repeatable security evaluation frameworks and test profiles for maritime SDRs, including conformance tests for STRIDE-mapped threats (spoofing, tampering, DoS, elevation of privilege, information disclosure, and repudiation) and forensics capabilities. An important direction is to study how such frameworks could align with existing OT/ICS standards (e.g., IEC 62443 zones and conduits, NIST CSF) so that regulators, classification societies, and vendors can share a common language for SDR assurance and compliance.

7.3. Technical Gaps at Device and Software Layers

The review shows that most work on SDR tampering, firmware modification, and malicious waveform upload remains at the proof-of-concept level, with few studies addressing long term platform hardening in operational fleets. Trusted execution environments and supply chain provenance for SDR hardware and firmware are only briefly mentioned in the literature [40,53,105,106], despite well documented risks from malicious updates and rogue waveforms. Research is needed on lightweight attestation protocols, secure provisioning and update pipelines, and on device monitoring that are feasible for constrained maritime installations and can be audited against regulatory expectations.

Similarly, most threat modeling works assume single vendor SDR stacks, whereas real ships use heterogeneous hardware, virtualized radio functions, and third party applications [70,105]. This heterogeneity introduces new attack surfaces (e.g., hypervisor escape, container breakout, and API abuse) that are not yet systematically modeled under STRIDE for maritime scenarios. Future work should extend existing frameworks to cover multi-tenant, virtualized SDR deployments on board and at shore-side control centers, including secure orchestration and isolation mechanisms.

7.4. Gaps in Protocol, System and Data Perspectives

The analysis identifies persistent weaknesses in AIS, VHF/DSC, NMEA 2000 and GNSS authentication and integrity, but most proposed defenses are not evaluated in realistic, large scale maritime environments [24,26,31,35]. For instance, protected AIS schemes, GNSS spoofing detectors, and VDES authentication concepts are often validated only in lab settings or small trials, leaving open questions about interoperability, backward compatibility, bandwidth overhead, and regulatory acceptability. Future research should therefore focus on field trials and large-scale simulation campaigns that quantify operational impact, failure modes, and migration paths for authenticated signalling in mixed legacy/SDR fleets.

There is also a notable lack of longitudinal, open datasets capturing SDR-driven threats across different sea regions, traffic densities, and operational profiles [70,72]. Many studies rely on short experiments, synthetic traffic, or single-scenario case studies, which limits the robustness of detection algorithms and the ability to benchmark competing defenses. Developing privacy-aware, shareable datasets and common evaluation metrics for

spoofing, jamming, message injection and elevation-of-privilege scenarios would support reproducible research and inform both technical standards and regulatory risk assessments.

7.5. Gaps in Satellite Systems

Another critical gap lies in the resilience of satellite and terrestrial communication systems used in maritime operations, including GNSS, satcom, and cellular links. While GNSS spoofing and jamming detectors have been proposed, most are tested only in controlled environments and lack validation under real sea conditions, where multipath, antenna placement, and vessel dynamics complicate detection [23,29]. Similarly, vulnerabilities in satellite terminals, ground gateways, and their firmware remain underexplored despite their role as lifelines for long-range communication, leaving threat-modeling methods for satcom incidents immature [79]. At the port-to-ship interface, increasing reliance on 4G/5G introduces new attack surfaces such as synchronization jamming, rogue base stations, and protocol manipulation, yet the literature provides little operational guidance for hardening and risk assessment [70]. Addressing these gaps requires field-validated GNSS integrity detection, systematic auditing of satcom protocols and firmware, and tailored defenses and threat models for maritime cellular use to ensure resilient end-to-end communications.

A deeper challenge is that most proposed GNSS, satcom, and cellular defenses are evaluated in isolation, without considering the tightly coupled nature of modern maritime communication architectures. Redundancy schemes often assume that failure or compromise in one channel (for example, GNSS) can be mitigated by falling back to others (such as AIS, radar, or cellular backhaul), yet correlated attacks across multiple links are rarely modeled. Future research should therefore examine coordinated, multi-vector threat scenarios in which adversaries simultaneously exploit GNSS, satcom control planes, and coastal cellular infrastructure to degrade situational awareness and command-and-control. This requires cross-layer testbeds that integrate RF propagation, networking behavior, and bridge decision-making, enabling realistic assessment of how communication degradation propagates into navigation errors, delayed distress signalling, or loss of cargo and port logistics visibility.

In addition, there is little work on how resilience requirements for these communication systems can be operationalized through configuration baselines, monitoring practices, and incident-response procedures on board. Existing studies tend to describe detection algorithms or protocol hardening at a conceptual level, but provide limited guidance on thresholds, alarm handling, or decision support for watchstanders and shore-based security teams. Future work should develop measurable resilience indicators for maritime GNSS, satcom, and 4G/5G links, specify minimum logging and anomaly-detection capabilities for shipborne and shore-side equipment, and design playbooks that integrate RF anomaly handling into established bridge and port procedures. This would help ensure that communication resilience is treated as a managed, auditable aspect of maritime operations and safety management systems, rather than an implicit by-product of technology choice.

7.6. Security Gaps with NMEA 2000 Equipment, Network and Software Applications

Research gaps also exist in the security of NMEA 2000 equipment, networks, and software applications. Most devices on the NMEA 2000 bus were designed for closed, trusted environments and lack secure boot, firmware signing, or tamper resistance, making them vulnerable to cloning, unauthorized reprogramming, or hardware substitution attacks [27,80]. In practice, firmware updates are often performed via vendor-specific tools or removable media without strong authentication or attestation, which complicates provenance tracking and makes it difficult for operators to verify that critical sensors and controllers are running legitimate code. Future work should therefore investigate lightweight

hardware roots of trust, secure update channels, and lifecycle management schemes that are compatible with constrained maritime devices and extended maintenance cycles.

At the network layer, NMEA 2000 inherits weaknesses from CAN, including broadcast messaging without authentication, weak origin attribution, and susceptibility to spoofing and flooding, yet there is limited work on intrusion detection tailored to maritime traffic patterns and PGN semantics [78]. Existing IDS concepts for automotive CAN cannot be directly transferred because vessel topologies, message mixes, and safety requirements differ substantially from road vehicles. There is a need for models that learn normal PGN usage under varying operating modes (for example, harbour manoeuvring versus open-sea cruising) and can detect subtle manipulations that may precede more disruptive attacks, while avoiding alarm fatigue for bridge crews.

At the application level, vulnerabilities in chart plotters, gateways, and parsing libraries expose systems to input validation flaws, memory corruption, and message injection attacks, but systematic threat audits of NMEA 2000 software stacks remain scarce [52]. Many of these components act as protocol translators between NMEA 2000, Ethernet, and cloud services, meaning that compromised PGNs can become entry points into broader OT and IT environments. Future research must therefore combine secure coding practices, fuzz testing, and formal specification of PGN handling with architecture-level analyses that map how compromised NMEA 2000 applications could enable cross-domain lateral movement. Collectively, these efforts should feed into NMEA 2000-specific threat-modeling and certification frameworks, allowing regulators, classification societies, and vendors to converge on auditable security baselines for devices, networks, and software in integrated bridge and automation systems.

7.7. Forensic Readiness and Human Organizational Factors

The survey notes that, although spoofing, jamming and replay attacks are well documented, there is almost no work on standardized forensic procedures for SDR incidents in the maritime domain [28,31]. Questions such as what RF artefacts to capture, how to time-stamp and store IQ samples, and how to correlate them with bridge, engineering and network logs for evidentiary purposes remain largely unanswered. In practice, there is no common guidance on retention periods, sampling rates, or minimum metadata (for example, antenna configuration, receiver gain settings, or geolocation context) needed to make RF records admissible and interpretable across jurisdictions. Future work should define SDR-specific forensic readiness frameworks and logging requirements that can be referenced by IMO guidance, flag-state regulations, and class rules, and should also examine secure storage, chain-of-custody models, and privacy considerations for high-volume RF data. Establishing such norms would enable reliable attribution, consistent incident reconstruction, and legally robust follow-up after RF-layer incidents, rather than treating each investigation as an ad-hoc exercise.

Finally, existing literature gives limited attention to crew training, operational doctrine, and human-in-the-loop detection regarding SDR-enabled threats, even though many successful attacks exploit procedural gaps and low awareness. Most work assumes that anomaly detection outputs will be correctly interpreted and acted upon, without studying how bridge teams, VTS operators, and shore-based security centres actually perceive and respond to RF anomalies under time pressure. There is a need for empirical studies on how operators integrate RF cues with visual observations and navigation data, how incident response playbooks should embed SDR-specific steps (for example, switching antennas, cross checking independent sensors, and capturing IQ traces), and how simulator-based training can improve recognition of spoofing, jamming and deceptive messaging on the bridge. Future research should also examine how to encode these human and organiza-

tional considerations into regulatory guidance and company safety management systems, for example, through minimum competency requirements, standardized drills, and integration of RF threat scenarios into bridge resource management so that the sector moves from purely technical mitigation towards holistic resilience.

8. Conclusions

Maritime SDR systems face a concentrated set of technically diverse risks. The review documents 44 distinct threat types: tampering (36 instances), denial of service (33), elevation of privilege (28), repudiation (30), spoofing (23), and information disclosure (24), showing that attacks rarely affect a single layer in isolation but instead propagate across devices, protocols, software, and operators. High-severity scenarios arise when adversaries use low-cost SDR hardware to conduct GNSS and AIS spoofing, configuration tampering, and targeted jamming of navigation and safety-critical channels, which can directly affect vessel positioning, collision avoidance, distress signaling, and ship-to-shore coordination.

From a risk management perspective, the findings indicate that some systemic vulnerabilities are created by some factors, such as unauthenticated and unencrypted legacy maritime protocols, the widespread availability of capable but inexpensive SDR platforms, and the absence of SDR-specific security obligations in current maritime cyber and spectrum regulations. Quantitatively, this supports prioritizing defenses that (i) harden SDR hardware and firmware through secure boot, code signing, and remote attestation; (ii) introduce cryptographic authentication, integrity protection, and non-repudiation into GNSS-dependent and AIS/DSC/NMEA 2000 communications; (iii) deploy multi-sensor fusion and continuous spectrum monitoring to detect spoofing and jamming early; and (iv) institutionalize SDR-focused training and incident response within safety management systems so that the most severe and frequent threat classes are addressed first.

Operationally, this implies that maritime authorities, associations, shipowners, and operators are responsible for integrating these technical controls into safety management systems through configuration baselines, network segmentation, anomaly detection, and incident response playbooks that explicitly cover SDR-enabled threats. They should also invest in crew training and simulator based exercises that prepare operators to recognize and respond to spoofing, jamming, and deceptive RF behavior. Finally, the research community should focus on field-validated detection techniques, longitudinal datasets, SDR-aware forensic methods, and human centered studies that can be translated into practical guidance for the above stakeholders. By aligning regulatory, technical, and operational efforts around the most critical vulnerabilities identified in this review, the maritime sector can move from reactive responses to proactive, system wide SDR resilience.

Author Contributions: Conceptualization, E.M. and A.F.A.; methodology, E.M. and P.L.; validation, P.L.; formal analysis, C.V. and A.F.A.; resources, E.M. and P.L.; data curation, E.M.; writing original draft, E.M.; review and editing, C.V. and A.F.A.; visualization, E.M.; project administration, C.V.; supervision, C.V. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are openly available in Google Scholar.

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

References

1. Sims, H. Software Defined Radios—Architectures, Systems and Functions. In Proceedings of the Scientific Ballooning Technologies Workshop 2017, Minneapolis, MN, USA, 16–18 May 2017. Available online: <https://ntrs.nasa.gov/api/citations/20170008046/downloads/20170008046.pdf> (accessed on 6 April 2024).
2. Niknami, N.; Srinivasan, A.; St. Germain, K.; Wu, J. Maritime Communications—Current State and the Future Potential with SDN and SDR. *Network* **2023**, *3*, 563–584. Available online: <https://www.mdpi.com/2673-8732/3/4/25> (accessed on 8 October 2024). [CrossRef]
3. UNCTAD. *Review of Maritime Transport 2024 Overview*; United Nations Conference on Trade and Development: Geneva, Switzerland, 2024. Available online: <https://unctad.org/publication/review-maritime-transport-2024> (accessed on 6 April 2024).
4. United Nations Conference on Trade and Development (UNCTAD). *Review of Maritime Transport 2024; RMT 2024—Chapter II: World Shipping Fleet and Services*. 2024. Available online: https://unctad.org/system/files/official-document/rmt2024ch2_en.pdf (accessed on 6 April 2024).
5. United Nations Conference on Trade and Development (UNCTAD). *Review of Maritime Transport 2024. RMT 2024—Chapter I: International Maritime Trade*. 2024. Available online: https://unctad.org/system/files/official-document/rmt2024ch1_en.pdf (accessed on 6 April 2024).
6. Fitton, J.; Haghighat, A. A Review on Essentials and Technical Challenges of Software Defined Radio. In *Proceedings of the MILCOM 2002, Anaheim, CA, USA, 7–10 October 2002*; IEEE: New York, NY, USA, 2002; Volume 1, pp. 377–382. [CrossRef]
7. International Maritime Organization (IMO). *Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems (Adopted 16 June 2017)*; IMO: London, UK, 2017. Available online: <https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx> (accessed on 6 April 2024).
8. International Maritime Organization (IMO). *MSC-FAL.1/Circ.3/Rev.3: Guidelines on Maritime Cyber Risk Management (Approved 2025)*; Referenced in Republic of the Marshall Islands Marine Guideline 2-11-16, August 2025; IMO: London, UK, 2025. Available online: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> (accessed on 5 October 2024).
9. BIMCO; Class NK; Columbia Shipmanagement Cyprus; Chamber of Shipping of America; Cygnus Technologies; Digital Container Shipping Association (DCSA); INTERMANAGER; International Association of Dry Cargo Shipowners (INTERCARGO); International Association of Independent Tanker Owners (INTERTANKO); International Chamber of Shipping (ICS); et al. *The Guidelines on Cyber Security Onboard Ships*, Version 5; BIMCO/ICS: Copenhagen, Denmark, 2024. Available online: https://www.bimco.org/media/s4ddrsfe/2024-11-14-guidelines_on_cyber_security-v5-final.pdf (accessed on 6 April 2024).
10. United States Coast Guard (USCG). *Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities (26 February 2020)*; USCG: Washington, DC, USA, 2020. Available online: https://www.maritimesecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_cyber_security-v5-final.pdf (accessed on 6 April 2024).
11. United States Maritime Administration (MARAD). *MSCI Advisory 2023-013: Various GPS Interference & AIS Spoofing*; MARAD: Washington, DC, USA, 2023. Available online: <https://www.maritime.dot.gov/msci/2023-013-various-gps-interference-ais-spoofing> (accessed on 6 April 2024).
12. National Institute of Standards and Technology (NIST). *SP 800-82 Rev.3: Guide to Operational Technology (OT) Security*; NIST: Gaithersburg, MD, USA, 2023. Available online: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf> (accessed on 6 April 2024).
13. ISA/IEC 62443; Security of Industrial Automation and Control Systems—Quick Start Guide. ISA Global Cybersecurity Alliance (ISAGCA): Research Triangle Park, NC, USA, 2023. Available online: <https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf> (accessed on 6 April 2024).
14. Det Norske Veritas (DNV). *DNVGL-RP-0496: Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*; DNV: Oslo, Norway, 2016. Available online: <https://www.dnv.com/siteassets/images/pdf-documents/dnv-gl-rp-0496.pdf> (accessed on 6 April 2024).
15. International Telecommunication Union—Radiocommunication Sector (ITU-R). *Recommendation M.1371-5: Technical Characteristics for an AIS Using TDMA in the VHF Maritime Mobile Band*; ITU: Geneva, Switzerland, 2014. Available online: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-1!!PDF-E.pdf (accessed on 6 April 2024).
16. International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA). *Guideline 1082—An Overview of AIS, Edition 2.0*; IALA: Saint-Germain-en-Laye, France, 2016. Available online: https://navcen.uscg.gov/sites/default/files/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf (accessed on 6 April 2024).
17. Mauri, L.; Damiani, E. Modeling Threats to AI-ML Systems Using STRIDE. *Sensors* **2022**, *22*, 6662. Available online: <https://www.mdpi.com/1424-8220/22/17/6662> (accessed on 6 April 2024). [CrossRef]
18. Amro, A.; Gkioulos, V.; Katsikas, S. Assessing Cyber Risk in Cyber-Physical Systems Using the ATT&CK Framework. *ACM Trans. Priv. Secur.* **2023**, *26*, 22. [CrossRef]
19. Jiang, Y.; Zhang, H.; Li, X.; Chen, Y. MITRE ATT&CK Applications in Cybersecurity and the Way Forward. *arXiv* **2025**, arXiv:2502.10825. Available online: <https://arxiv.org/abs/2502.10825> (accessed on 6 April 2024). [CrossRef]

20. Ear, E.; Bailey, B. Towards Principled Risk Scores for Space Cyber Risk Management. *arXiv* **2024**, arXiv:2402.02635. Available online: <https://arxiv.org/abs/2402.02635> (accessed on 6 April 2024). [CrossRef]
21. Bhusal, G.; Shrestha, B. The Role of PASTA in Addressing Future Trends in Regulatory Compliance. *Int. J. Innov. Sci. Res. Technol.* **2024**, *9*, 241–248. Available online: <https://ijisrt.com/assets/upload/files/IJISRT24AUG241.pdf> (accessed on 6 April 2024).
22. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n71. Available online: <https://www.bmj.com/content/372/bmj.n71> (accessed on 6 April 2024). [CrossRef]
23. Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. *J. Mar. Sci. Eng.* **2023**, *11*, 928. [CrossRef]
24. Balduzzi, M.; Pasta, A.; Wilhoit, K. A Security Evaluation of AIS (Automatic Identification System). In Proceedings of the Annual Computer Security Applications Conference (ACSAC'14), New Orleans, LA, USA, 8–12 December 2014. [CrossRef]
25. Ramalinda, D.; Raharja, A. Vulnerabilities and Threats to AIS Security Systems. *J. Comput. Sci. Adv.* **2024**, *2*, 176–182. Available online: <https://pdfs.semanticscholar.org/7892/a2385a4475748d9155069c0447fb18668b57.pdf> (accessed on 6 April 2024). [CrossRef]
26. Lindback, A.; Javid, Y.; Gurtov, A. Demonstration of Digital Selective Call Spoofing. In Proceedings of the 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Tbilisi, Georgia, 24–27 June 2024; pp. 211–217. Available online: <https://ieeexplore.ieee.org/document/10646264> (accessed on 6 July 2024).
27. Kessler, G.C. Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. *Transnav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 279–286. Available online: https://www.transnav.eu/Article_Protected_AIS_A_Demonstration_Kessler,56,1016.html (accessed on 6 April 2024). [CrossRef]
28. Jetto, J.; Gandhiraj, R.; Sundaram, G.A.S.; Soman, K.P. Software-Defined Radio-Based GPS Spoofing Attack Model on Road Navigation System. In *Soft Computing and Signal Processing*; Springer: Singapore, 2021; Volume 1340, pp. 339–350. Available online: https://link.springer.com/chapter/10.1007/978-981-16-1249-7_32 (accessed on 6 April 2024).
29. Feng, Y.; Huang, W.; Wang, S.; Zhang, Y.; Jiang, S.; Cao, Z. Anti-Clone: A Lightweight Approach for RFID Cloning Attacks Detection. In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2022)*; Springer: Cham, Switzerland, 2023; Volume 461, pp. 75–90. Available online: https://eudl.eu/doi/10.1007/978-3-031-24386-8_5 (accessed on 6 April 2024).
30. Singh, A.; Kumar, A.; Kumar, R. A Novel Framework for Maritime Cybersecurity Using Blockchain and GNSS Spoofing Detection. *Mathematics* **2022**, *10*, 4097. [CrossRef]
31. Androjna, A.; Čuš, M.; Božič, M.; Perkovič, M. AIS Data Vulnerability Indicated by a Spoofing Case Study. *Appl. Sci.* **2021**, *11*, 5015. [CrossRef]
32. Cho, S.; Lee, J.; Kim, H. NAVTEX Message Authentication and Spoofing Detection in Maritime Safety Communications. *J. Mar. Sci. Eng.* **2025**, *13*, 1657. Available online: <https://www.mdpi.com/2077-1312/13/9/1657> (accessed on 6 July 2024). [CrossRef]
33. Gao, Y.; Zhang, Y.; Wang, H.; Li, J. Satellite Communication Security in Maritime Systems: Spoofing and Jamming Threats. *IEEE Sens. J.* **2020**, *20*, 13456–13465. Available online: <https://ieeexplore.ieee.org/document/9120284> (accessed on 6 July 2024).
34. TRITON Project. Maritime Cybersecurity Demonstration: SDR-Based Spoofing of Radar and VHF Systems. In Proceedings of the IEEE Maritime Security Workshop, The Hague, The Netherlands, 24–26 September 2014; IEEE: New York, NY, USA, 2014. Available online: <https://ieeexplore.ieee.org/document/6975613> (accessed on 6 July 2024).
35. Stewart, A.; Rice, E.; Safonov, P. Digital Authentication Strategies for the Automated Identification System. In Proceedings of the Midwest Instruction and Computing Symposium (MICS), Duluth, MN, USA, 6–7 April 2018. Available online: https://micsymposium.org/mics2018/proceedings/MICS_2018_paper_64.pdf (accessed on 6 July 2024).
36. Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* **2024**, *24*, 4210. [CrossRef]
37. Xiao, S.; Park, J.-M.; Ye, Y. Tamper Resistance for Software Defined Radio Software. In Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC), Seattle, WA, USA, 20–24 July 2009. [CrossRef]
38. SPARTA Aerospace. *Compromise Software Defined Radio — Technique IA-0002*; SPARTA Cyber Alliance: El Segundo, CA, USA, 2022. Available online: <https://sparta.aerospace.org/technique/IA-0002/> (accessed on 24 October 2024).
39. Hitefield, S.D. A Defense-In-Depth Security Architecture for Software Defined Radio Systems. Ph.D. Thesis, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, 2019. Available online: <https://vtechworks.lib.vt.edu/handle/10919/93968> (accessed on 1 August 2024).
40. Tan, S.H.M.; Yeo, C.K. GPS Location Spoofing and FM Broadcast Intrusion Using Software-Defined Radio. *J. Inf. Technol. Res.* **2020**, *12*, 104–117. Available online: <https://www.igi-global.com/article/gps-location-spoofing-and-fm-broadcast-intrusion-using-software-defined-radio/265152> (accessed on 1 August 2024). [CrossRef]
41. Meng, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sens.* **2022**, *14*, 4826. [CrossRef]
42. 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. *J. Navig.* **2022**, *75*, 333–345. [CrossRef]

43. Javid, Y.; Lindbäck, A. Demonstration of Digital Selective Call Spoofing. Bachelor's Thesis, Linköping University, Linköping, Sweden, 2023. Available online: <https://liu.diva-portal.org/smash/get/diva2:1791530/FULLTEXT01.pdf> (accessed on 2 July 2024).
44. Perkovič, M.; Androjna, A. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Trans. Marit. Sci.* **2021**, *10*, 173–181. [CrossRef]
45. Kauranen, A. Finland Detects Satellite Navigation Jamming and Spoofing in Baltic Sea. *Reuters*, 31 October 2024. Available online: <https://www.reuters.com/world/europe/finland-detects-satellite-navigation-jamming-spoofing-baltic-sea-2024-10-31> (accessed on 2 July 2024).
46. Wimpenny, G.; Lázaro, F.; Šafář, J.; Raulefs, R. A Pragmatic Approach to VDES Authentication. *J. Inst. Navig.* **2025**, *72*, navi.681. [CrossRef]
47. Wesson, K.D.; Gross, J.N.; Humphreys, T.E.; Evans, B.L. GNSS Signal Authentication via Power and Distortion Monitoring. *Navigation* **2017**, *64*, 51–66. Available online: <https://ieeexplore.ieee.org/document/8082785> (accessed on 6 July 2024). [CrossRef]
48. Pérez Marcos, M.; Marcos, C.; Díaz, D.; Fietz, K.; Forcada, A.; Ford, A.; García-Charton, J.A.; Goñi, R.; Lenfant, P.; Mallol, S.; et al. Reviewing the Ecosystem Services, Societal Goods, and Benefits of Marine Protected Areas. *Front. Mar. Sci.* **2021**, *8*, 613819. [CrossRef]
49. Akeela, R.; Dezfouli, B. Software-Defined Radios: Architecture, State-of-the-Art, and Challenges. *arXiv* **2018**, arXiv:1804.06564. Available online: <https://arxiv.org/abs/1804.06564> (accessed on 6 July 2024). [CrossRef]
50. Humphreys, T.E.; Shepard, D.P.; Bhatti, J.A.; Fansler, A.A. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. In Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012; pp. 3591–3605. Available online: <https://www.ion.org/publications/abstract.cfm?articleID=10534> (accessed on 6 July 2024).
51. Bezerra, G.M.G.; de Oliveira, N.R.; Ferreira, T.N.; Mattos, D.M.F. A Comprehensive Evaluation of Software-Defined Radio Performance in Virtualized Environments for Radio Access Networks. *Ann. Telecommun.* **2024**, *79*, 523–535. [CrossRef]
52. Rahman, M.A.; Islam, M.S.; Hossain, M.A.; Kaiser, M.S. Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience. *IEEE Access* **2022**, *10*, 29493–29505. [CrossRef]
53. Le Roy, F.; Quiniou, T.; Mansour, A.; Lababidi, R.; Le Jeune, D. RFID Eavesdropping Using SDR Platforms. In *Applications in Electronics Permeating Industry, Environment and Society*; De Gloria, A., Ed.; Lecture Notes in Electrical Engineering; Springer: Cham, Switzerland, 2017; Volume 429, pp. 208–214. [CrossRef]
54. Forsberg, J. Cybersecurity of Maritime Communication Systems: Spoofing Attacks Against AIS and DSC. Master's Thesis, Linköping University, Department of Computer and Information Science, Linköping, Sweden, 2022. Available online: <https://liu.diva-portal.org/smash/record.jsf?pid=diva2:1705102> (accessed on 24 October 2025).
55. Thomas, A. AIS Manipulation Motivations in the Maritime Domain. Working Paper, California State University Maritime Academy, Department of Global Studies and Maritime Affairs, Vallejo, CA, USA, 2022. Available online: https://www.wpsanet.org/papers/docs/Thomas_Aurora_AIS_spoofing.pdf (accessed on 24 October 2025).
56. Wu, Z.; Zhang, Y.; Yang, Y.; Liang, C.; Liu, R. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* **2020**, *8*, 165444–165496. Available online: <https://ieeexplore.ieee.org/document/9187240> (accessed on 6 July 2024). [CrossRef]
57. Forsberg, K. *Cybersecurity Considerations in Autonomous Ships*; NATO CCDCOE Publications: Tallinn, Estonia, 2022. Available online: https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous-Ships.pdf (accessed on 24 October 2025).
58. Li, M.; Zhou, J.; Chattopadhyay, S.; Goh, M. Maritime Cybersecurity: A Comprehensive Review. *arXiv* **2024**, arXiv:2409.11417. Available online: <https://arxiv.org/abs/2409.11417> (accessed on 6 July 2024).
59. Sanchez, I.; Baldini, G.; Shaw, D.; Giuliani, R. Experimental Passive Eavesdropping of DECT Voice Communications through Low-Cost SDRs. *Secur. Commun. Netw.* **2015**, *8*, 403–417. [CrossRef]
60. Mjølunes, S.F.; Olimid, R.F. Experimental Assessment of Private Information Disclosure in LTE Mobile Networks. In Proceedings of the 14th International Conference on Security and Cryptography (SECURITY 2017), Madrid, Spain, 24–26 July 2017; pp. 507–512. Available online: <https://www.scitepress.org/Papers/2017/64623/index.html> (accessed on 24 October 2025).
61. Guri, M. RAMBO: Leaking Secrets from Air-Gap Computers by Spelling Covert Radio Signals from Computer RAM. *arXiv* **2024**, arXiv:2409.02292. Available online: <https://arxiv.org/abs/2409.02292> (accessed on 6 July 2024). [CrossRef]
62. Baron-Hyppolite, A.; Santos, J.F.; DaSilva, L.; Kibilda, J. Eavesdropper Avoidance through Adaptive Beam Management in SDR-Based MmWave Communications. In Proceedings of the 2024 19th International Symposium on Wireless Communication Systems (ISWCS), Rio de Janeiro, Brazil, 14–17 July 2024; pp. 1–6. Available online: <https://vtechworks.lib.vt.edu/bitstreams/767d266d-f4c3-49d1-9fca-1e4df1a4db52/download> (accessed on 24 October 2025).
63. Lázaro, F.; Raulefs, R.; Bartz, H.; Jerkovits, T. VDES R-Mode: Vulnerability Analysis and Mitigation Concepts. *Int. J. Satell. Commun. Netw.* **2021**, *39*, 123–135. [CrossRef]

64. Bernabé, J.; Hernández-Ramos, J.L.; Skarmeta, A.F. Cybersecurity Challenges in the Maritime Sector: A Systematic Review. *Sensors* **2023**, *23*, 1234. [\[CrossRef\]](#)
65. Clavijo Mesa, M.V.; Patino-Rodriguez, C.E.; Guevara Carazas, F.J. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information* **2024**, *15*, 710. [\[CrossRef\]](#)
66. USCG Navigation Center; RNT Foundation. Maritime GNSS Interference Reports and GPS Trouble Submissions. USCG CGMIX Incident Portal and RNT Foundation GPS Issue Reports. 2024. Available online: <https://www.navcen.uscg.gov/guide-tool> (accessed on 26 October 2025).
67. Rügamer, S.; Kowalewski, D. Jamming and Spoofing of GNSS Signals—An Underestimated Risk?! In Proceedings of the FIG Working Week 2015, Sofia, Bulgaria, 17–21 May 2015. Available online: https://fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf (accessed on 26 October 2025).
68. Miljanovic, S.; Ardizzon, F.; Crosara, L.; Laurenti, N.; Canzian, L.; Lovisotto, E.; Montini, N.; Pozzobon, O.; Ioannides, R.T. Experimental Testing and Impact Analysis of Jamming and Spoofing Attacks on Professional GNSS Receivers. In Proceedings of the ICL-GNSS 2022, Tampere, Finland, 7–9 June 2022; CEUR Workshop Proceedings, Volume 3183. Available online: <https://ceur-ws.org/Vol-3183/paper9.pdf> (accessed on 26 October 2025).
69. Rao, R.M.; Ha, S.; Marojevic, V.; Reed, J.H. LTE PHY Layer Vulnerability Analysis and Testing Using Open Source SDR Tools. In Proceedings of the MILCOM 2017—IEEE Military Communications Conference, Baltimore, MD, USA, 23–25 October 2017; pp. 744–749. [\[CrossRef\]](#)
70. Alaimo, R.; Corallo, R.; Schilleci, S.; Dino, A.; Mangione, S.; Tinnirello, I.; Garlisi, D. Undercover Disruption: Stealth Jamming Attacks on 5G Synchronization Stages. In Proceedings of the CyReS 2024, Joint National Conference on Cybersecurity, Bologna, Italy, 3–8 February 2024; CEUR Workshop Proceedings, Volume 3962, pp. 35–46. Available online: <https://ceur-ws.org/Vol-3962/paper5.pdf> (accessed on 26 October 2025).
71. OTW, M. *Network Basics for Hackers: How Networks Work and How They Break*; Independently Published: Seattle, WA, USA, 2023; ISBN 9798373290043.
72. Zidane, Y.; Silva, J.S.; Tavares, G. Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study. *Drones* **2024**, *8*, 743. [\[CrossRef\]](#)
73. Mihaylova, D. An Overview of Methods of Reducing the Effect of Jamming Attacks at the Physical Layer. In Proceedings of the FABULOUS 2019—Future Access Enablers for Ubiquitous and Intelligent Infrastructures, Sofia, Bulgaria, 28–29 November 2019; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 283, pp. 271–284. Available online: https://link.springer.com/chapter/10.1007/978-3-030-23976-3_24 (accessed on 26 October 2025).
74. DiRenzo, J.; Goward, D.A.; Roberts, F.S. The Little-known Challenge of Maritime Cyber Security. In Proceedings of the IISA 2015—6th International Conference on Information, Intelligence, Systems and Applications, Corfu, Greece, 6–8 July 2015. Available online: <http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf> (accessed on 24 October 2025).
75. Jo, Y.; Choi, O.; You, J.; Cha, Y.; Lee, D.H. Cyberattack Models for Ship Equipment Based on the MITRE ATTACK Framework. *Sensors* **2022**, *22*, 1860. [\[CrossRef\]](#) [\[PubMed\]](#)
76. Tuncay, A.; Oğuz, Y.; Kantarci, B. Runtime Attestation and Anomaly Detection for SDR Firmware Integrity. *Ad Hoc Netw.* **2020**, *102*, 102116. [\[CrossRef\]](#)
77. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Guidelines for Cyber Risk Management in Shipboard Operational Technology Systems. *Transnav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 123–130. Available online: https://www.transnav.eu/Article_Guidelines_for_Cyber_Risk_Kavallieratos,54,1007.html (accessed on 24 October 2025).
78. Rogers, M.; Weigand, P.; Happa, J.; Rasmussen, K. Detecting CAN Attacks on J1939 and NMEA 2000 Networks. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 2406–2420. [\[CrossRef\]](#)
79. Keskin, O.F.; Lubja, K.; Bahsi, H.; Tatar, U. Systematic Cyber Threat Modeling for Maritime Operations: Attack Trees for Shipboard Systems. *J. Mar. Sci. Eng.* **2025**, *13*, 645. [\[CrossRef\]](#)
80. Quigley, C.; Sumpner, P. Making Marine Applications Based on NMEA 2000 Robust to Cyberattacks. In Proceedings of the CiA CAN Conference, Baden-Baden, Germany, 14–15 May 2024. Available online: https://www.can-cia.org/fileadmin/cia/documents/proceedings/2024_quigley.pdf (accessed on 24 October 2025).
81. Rastogi, N.; Hendler, J.; Ghosh, S. Explaining RADAR Features for Detecting Spoofing Attacks in Connected Autonomous Vehicles. *arXiv* **2022**, arXiv:2203.00150. Available online: <https://arxiv.org/abs/2203.00150> (accessed on 6 July 2024). [\[CrossRef\]](#)
82. Calatrava, H.; Tang, S.; Closas, P. Advances in Anti-Deception Jamming Strategies for Radar Systems: A Survey. *arXiv* **2025**, arXiv:2503.00285. Available online: <https://arxiv.org/abs/2503.00285> (accessed on 6 July 2024). [\[CrossRef\]](#)
83. Strohmeier, M.; Lenders, V.; Martinovic, I. Security of ADS-B: State of the Art and Beyond. *arXiv* **2013**, arXiv:1307.3664. Available online: <https://arxiv.org/abs/1307.3664> (accessed on 6 July 2024).

84. Baldini, G.; Sturman, T.; Biswas, A.R.; Leschhorn, R.; Gódor, G.; Street, M. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 355–379. Available online: <https://publications.jrc.ec.europa.eu/repository/handle/JRC59611> (accessed on 11 November 2025). [CrossRef]
85. Martinez Bolivar, I.M.; Nouvel, F.; Philippe, T. On the Performance Evaluation of LoRaWAN under Jamming. In Proceedings of the 12th Wireless and Mobile Networking Conference (WMNC), Paris, France, 11–13 September 2019; pp. 1–6. Available online: https://www.researchgate.net/publication/336170683_On_the_performance_evaluation_of_LoRaWAN_under_Jamming (accessed on 11 November 2025).
86. Bybyk, R.; Opirskyy, I.; McIntosh, M. SDR Receivers as a New Challenge to Cybersecurity Wireless Technology. In Proceedings of the CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, Ukraine, 21–22 October 2021; pp. 108–119. Available online: <https://ceur-ws.org/Vol-3188/paper11.pdf> (accessed on 11 November 2025).
87. Demeslay, C.; Gautier, R.; Rostaing, P.; Despina-Stoian, C. A Synchronization Front-End for LoRa Self-Jamming Operation on SDR Platforms. In Proceedings of the 15th International Conference on Communications (COMM), Bucharest, Romania, 3–4 October 2024; pp. 1–9.
88. Kaidenko, A.; Roskoshnyi, V. *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)*; INTERTANKO: London, UK, 2019. Available online: <https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf> (accessed on 11 November 2025).
89. Dimakopoulou, A.; Rantos, K. Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *J. Mar. Sci. Eng.* **2024**, *12*, 919. Available online: <https://www.mdpi.com/2077-1312/12/6/919> (accessed on 11 November 2025). [CrossRef]
90. Tam, K.; Hopcraft, R.; Moara-Nkwe, K.; Misis, J.P.; Andrews, W.; Harish, A.V.; Giménez, P.; Crichton, T.; Jones, K. Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. *J. Transp. Technol.* **2021**, *12*, 1–27. Available online: <https://www.scirp.org/journal/paperinformation.aspx?paperid=113658> (accessed on 11 November 2025). [CrossRef]
91. Shi, Y.; Erpek, T.; Sagduyu, Y.E.; Li, J.H. Spectrum Data Poisoning with Adversarial Deep Learning. *arXiv* **2019**, arXiv:1901.09247. Available online: <https://arxiv.org/abs/1901.09247> (accessed on 6 July 2024). [CrossRef]
92. Dossa, A.; Amhoud, E.M. Impact of Reactive Jamming Attacks on LoRaWAN: A Theoretical and Experimental Study. *arXiv* **2025**, arXiv:2501.18339. Available online: <https://arxiv.org/abs/2501.18339> (accessed on 6 July 2024).
93. Alves, R.P.; Silva, L.; Costa, M.; Souza, F. Experimental Comparison of 5G SDR Platforms: SrsRAN vs OpenAirInterface. *arXiv* **2024**, arXiv:2406.01485. Available online: <https://arxiv.org/abs/2406.01485> (accessed on 6 July 2024).
94. Li, K.; Yu, X.; Zhang, H.; Wu, L.; Du, X.; Ratazzi, P.; Guizani, M. Security Mechanisms to Defend Against New Attacks on Software-Defined Radio. In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. Available online: <https://ieeexplore.ieee.org/document/8422782> (accessed on 11 November 2025).
95. da Silva, F.A.B.; Moura, D.F.C.; Galdino, J.F. Classes of Attacks for Tactical Software-Defined Radios. *Int. J. Embed. Real-Time Commun. Syst.* **2012**, *3*, 57–82. Available online: <https://www.igi-global.com/article/classes-attacks-tactical-software-defined/74344> (accessed on 3 July 2025). [CrossRef]
96. Bao, T.; Tambe, M.; Wang, C. (Eds.) *Cyber Deception: Techniques, Strategies, and Human Aspects*; Springer: Cham, Switzerland, 2023; Volume 89. Available online: <https://link.springer.com/book/10.1007/978-3-031-16613-6> (accessed on 3 July 2025).
97. 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. [CrossRef]
98. Senarak, C. Port Cyberattacks from 2011 to 2023: A Literature Review and Discussion of Selected Cases. *Marit. Econ. Logist.* **2023**. Available online: <https://link.springer.com/article/10.1057/s41278-023-00276-8> (accessed on 6 July 2024). [CrossRef]
99. Vanitha, S.; Selvaa, M. GPS Spoofing Threats to Autonomous Maritime Drones. In *Advances in Cybersecurity and Signal Processing*; Springer: Cham, Switzerland, 2024; pp. 215–230.
100. Malatest, B. SDR Gateways for Sensor Avionics Systems. In *Aerospace Manufacturing and Design*; Per Vices Corporation: Toronto, ON, Canada, 2024; pp. 45–52. Available online: <https://www.aerospacemanufacturinganddesign.com/news/sdr-gateways-for-sensor-avionics-systems/> (accessed on 29 October 2025).
101. Marriwala, N.; Sahu, O.P.; Khullar, R.; Vohra, A. Software Defined Radio (SDR) 4-bit QAM Modem Using LabVIEW for Gaussian Channel. *Wirel. Commun.* **2011**, *3*, 206–212. Available online: <https://www.citresearch.org/dl/index.php/wc/article/view/WC032011014> (accessed on 29 October 2025).
102. Ulversoy, T. Software Defined Radio: Challenges and Opportunities. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 531–550. Available online: <https://ieeexplore.ieee.org/document/5452208> (accessed on 29 October 2025). [CrossRef]
103. Sadiku, M.N.O.; Akujuobi, C.M. Software-Defined Radio: A Brief Overview. *IEEE Potentials* **2004**, *23*, 14–15. Available online: <https://ieeexplore.ieee.org/document/1352161> (accessed on 29 October 2025). [CrossRef]
104. Dillinger, M.; Madani, K.; Alonistioti, N. *Software Defined Radio: Architectures, Systems and Functions*; John Wiley & Sons: Chichester, UK, 2005.

105. Tuttlebee, W.H.W. *Software Defined Radio: Enabling Technologies*; John Wiley & Sons: Chichester, UK, 2002.
106. Grayver, E. *Implementing Software Defined Radio*; Springer Science & Business Media: New York, NY, USA, 2012. Available online: <https://link.springer.com/book/10.1007/978-1-4614-1400-1> (accessed on 29 October 2025).

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