

Systematic Review

Safety and Security of Maritime Communication Systems: A Comprehensive Literature Review and Bibliometric Analysis

Paško Ivančić *, Zaloa Sanchez Varela *, Vice Milin and Ivan Peronja

Faculty of Maritime Studies, University of Split, 21000 Split, Croatia; vmilin@pfst.hr (V.M.); iperonja@pfst.hr (I.P.)

* Correspondence: pivancic@pfst.hr (P.I.); zsanchezv@pfst.hr (Z.S.V.)

Abstract

Maritime communication systems are among the most important infrastructure of global maritime safety and security. They consist of very high frequency (VHF) radio, the Global Maritime Distress and Safety System (GMDSS), contemporary satellite nets, Automatic Identification System (AIS) networks, and the emerging VHF Data Exchange System (VDES). These systems are essential for distress signaling, navigational coordination, and vessel traffic management. As maritime operations are experiencing accelerated digitalisation, the safety and security dimensions of maritime communication systems have attracted substantial and growing scientific attention. This study presents a comprehensive literature review and bibliometric analysis of the safety and security of maritime communication systems. Guided by the PRISMA 2020 guidelines and Systematic Literature Review (SLR) methodology, a structured search was conducted across three major scientific databases: Scopus, Web of Science (WoS), and IEEE Xplore. Starting from a raw pool of 6648 records retrieved between 2000 and 2026, the dataset was reduced through successive filtering to a final body of 68 high-relevance publications. Bibliometric analysis reveals a significant upward publication trend from 2015 onwards, with a marked acceleration after 2019. Thematic analysis identifies seven principal research clusters: GMDSS modernisation, AIS safety and security, VDES and VHF next-generation systems, maritime cybersecurity, satellite communications, risk assessment frameworks, and emerging technologies, including artificial intelligence and autonomous vessel communications. The review identifies significant research gaps, including the absence of integrated cross-system risk frameworks, insufficient attention to human factors in cybersecurity, limited studies addressing emerging regulatory, legal governance components and a brief analysis of the maritime communications market. This study provides a structured foundation for future research and policy development in maritime communication security.

Keywords: maritime communication systems; GMDSS; AIS; VDES; maritime safety and security; PRISMA; literature review; bibliometric analysis



Academic Editor: Zhipeng Wu

Received: 23 April 2026

Revised: 17 June 2026

Accepted: 23 June 2026

Published: 25 June 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.

1. Introduction

Maritime communication systems represent one of the most critical and complex technological infrastructures that support global maritime operations. Their primary function is to ensure reliable exchange of information between vessels, between vessels and shore-based authorities, and between vessels and satellite infrastructure. This includes a variety of operational scenarios: from routine navigational coordination and vessel traffic management to emergency distress alerting, search and rescue (SAR) coordination, and port state control (PSC) reporting. The importance of these systems is given at the

highest international level through the International Convention for the Safety of Life at Sea (SOLAS), which mandates specific communication equipment and operational requirements for all vessels engaged in international voyages [1].

The technological architecture of maritime communication systems has evolved substantially over the past four decades. The Global Maritime Distress and Safety System (GMDSS), introduced in 1999 as a replacement for the Morse code-based distress system, established the modern regulatory and technical baseline for maritime communications. GMDSS integrates multiple radio frequency bands, including medium frequency (MF), high frequency (HF), and VHF radio. Satellite communication services provided by Inmarsat and the COSPAS-SARSAT system create a layered architecture for global distress coverage [2,3]. Automatic Identification System (AIS) emerged in the early 2000s as a mandatory safety tool for vessel identification and traffic monitoring, operating on dedicated VHF channels. More recently, the VHF Data Exchange System (VDES) has been standardised as a next-generation maritime communication platform. It is offering substantially greater data throughput than AIS while maintaining backward compatibility with existing VHF maritime infrastructure [4,5].

Despite this, maritime communication systems face increasingly complex safety and security challenges. From a safety perspective, the reliability, coverage, and resilience of communication infrastructure directly determine outcomes in maritime emergencies. Equipment failures, propagation anomalies, and inadequate operator competence have been implicated in maritime accidents where distress signals were not transmitted or received in time [6,7]. From a security perspective, the digitalisation of maritime operations has introduced a broad attack surface susceptible to cyber threats, including GPS spoofing, AIS data falsification, jamming of radio communications, and network intrusion targeting onboard communication and navigation systems [8,9]. The convergence of operational technology (OT) and information technology (IT) aboard modern vessels has fundamentally altered the threats, causing the redesign of security frameworks that were originally designed for isolated, analogue systems.

Academic interest in the safety and security of maritime communication systems has grown substantially in recent years, reflecting both the operational significance of these threats and the increasing digitalisation of the maritime sector. However, the literature remains fragmented across several distinct subdomains, including GMDSS research, AIS security studies, cybersecurity frameworks, VDES technical development, and satellite communication architectures, with limited cross-domain synthesis. To date, no comprehensive systematic literature review has been published that integrates these exact terms under a unified bibliometric and thematic framework. This study addresses that gap by conducting a structured, PRISMA 2020-guided review and bibliometric analysis of research on the safety and security of maritime communication systems published between 2000 and 2026 [10].

The research objectives of this study are multiple: (i) to systematically identify, screen, and synthesise the scientific literature on the safety and security of maritime communication systems using SLR methodology; (ii) to conduct a comprehensive bibliometric analysis mapping publication trends, geographic distributions, authorship patterns, source distributions, and keyword structures within this research domain; and (iii) to develop a structured thematic synthesis of the identified literature, identifying the principal research clusters, methodological approaches, and research gaps that should guide future scholarly and policy efforts.

This paper is organised into five sections. Section 1 introduces the study context, motivation, and research objectives, and includes a subsection on the history and conceptual development of maritime communication systems and their safety and security compo-

nents. Section 2 details the methodological framework, including the PRISMA search and screening procedure, database selection, inclusion and exclusion criteria, and bibliometric methodology. Section 3 presents the core results, consisting of both the bibliometric analysis with all supporting figures and a structured thematic literature review organised by the seven identified research clusters. Section 4 presents a discussion of the principal findings, identifies research gaps, and outlines directions for future research. This section also gives a brief insight into the maritime communications market. Section 5 is a conclusion where the final words and concluding remarks are given.

1.1. Historical Development of Maritime Communication Systems

Before the introduction of radio communications, maritime distress relied entirely on visual and acoustic signaling: flags, flares, bells, and whistles. The introduction of wireless telegraphy at the turn of the twentieth century, largely attributed to Guglielmo Marconi, transformed maritime safety by enabling long-range communication between vessels and shore stations. The sinking of the RMS Titanic in 1912 brought international regulations, which led to the first International Convention for the Safety of Life at Sea in 1914, thus establishing mandatory wireless equipment requirements for certain vessel classes.

The following decades brought the systematic development of internationally coordinated maritime radio communication frameworks. The International Telecommunication Union (ITU) established dedicated maritime frequency allocations, and SOLAS revisions progressively expanded and standardised communication equipment requirements. The Morse code-based distress system, focused on the internationally recognised SOS signal on 500 kHz, remained the primary maritime distress mechanism for most of the twentieth century. However, this system had significant limitations: it required continuous manual watchkeeping on dedicated frequencies and depended on trained radio officers whose presence aboard commercial vessels was declining from the 1980s onwards [11].

The GMDSS represented the most fundamental transformation in maritime communication architecture since the introduction of radio itself. Developed under the guidance of the International Maritime Organization (IMO) and the ITU, the GMDSS was based on the principle of automated distress alerting, replacing manual watch-keeping with digital selective calling (DSC) on VHF Channel 70, MF 2187.5 kHz, and HF frequencies, supported by satellite alerting through Inmarsat and COSPAS-SARSAT [1,6]. Full implementation of the GMDSS was completed globally in 1999, and ongoing modernisation efforts have integrated emerging communication technologies, including broadband satellite services and VDES, into the GMDSS framework [2,3,7].

The parallel development of AIS from the 1990s onwards added a new dimension to maritime communication infrastructure. Originally conceived as a collision-avoidance and vessel-monitoring tool, AIS rapidly became embedded in port state control, maritime domain awareness, and environmental monitoring applications [12,13]. The AIS operates on VHF maritime mobile band channels 87B and 88B, broadcasting vessel identification, position, course, speed, and voyage data to all receivers within range. Its open, unauthenticated broadcast architecture subsequently emerged as a significant security vulnerability susceptible to spoofing, data injection, and signal jamming [14–16].

1.2. Safety and Security Domains of Maritime Communication Systems

The safety and security of maritime communication systems must be understood as distinct but deeply interrelated analytical domains. Safety, in this context, refers to the reliability, availability, and operability of communication systems in fulfilling their designated functions, particularly under environmental or operational conditions. Security, by contrast, refers to the protection of communication systems and their associated data

from deliberate interference, unauthorised access, and malicious manipulation. While traditional maritime safety research has addressed communication system failures primarily as technical or human factor problems, the growing cybersecurity threat landscape requires an integrated perspective that treats intentional threats as a significant component of overall system risk [8,9,17,18].

The safety dimensions of maritime communication systems consist of several critical aspects. Equipment reliability and environmental robustness are main, as communication systems must operate effectively across extreme conditions of temperature, humidity, vibration, and electromagnetic interference characteristic of the maritime environment. Operator competence represents another critical safety dimension, as the correct use of GMDSS equipment, including DSC controllers, satellite terminals, and AIS transponders, requires specific training and certification under the Standards of Training, Certification and Watchkeeping for Seafarers (STCW) Convention [2,4]. Coverage gaps in both terrestrial VHF and satellite communication services present additional safety risks, particularly in high-latitude polar regions where the geostationary satellite signal is limited [3].

The security dimensions of maritime communication systems have expanded dramatically with digitalisation. Cyberattacks targeting maritime communication infrastructure range from jamming and spoofing of AIS and GPS signals to intrusion campaigns targeting shipboard networks, Electronic Chart Display and Information Systems (ECDIS), and satellite communication terminals [17–20]. The IMO Maritime Cyber Risk Management resolution (MSC-FAL.1/Circ.3) and the associated BIMCO guidelines have established the international regulatory baseline for maritime cybersecurity, but implementation across the global fleet remains challenging [14,21,22].

2. Materials and Methods

This study uses a hybrid methodological framework combining the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines with Systematic Literature Review (SLR) methodology. This combined approach was selected on the basis of its mainstream adoption in maritime research and its capacity to ensure transparency, reproducibility, and rigour in the literature identification and screening process [23,24]. The PRISMA framework provides the procedural structure for literature identification and screening, while the SLR methodology informs the analytical framework for thematic synthesis and bibliometric evaluation. The frequent application of PRISMA and SLR methodologies in recent maritime science literature further validates this choice, as evidenced by a growing body of maritime systematic reviews addressing topics including port-related emissions [25], Port State Control inspection analysis [26], battery-powered ro-pax ferries [27], maritime signaling communication technologies [28], ship maneuvering in constrained waters [29], seafarer education and autonomous shipping [30], navigational safety hazards from offshore wind farms [31], maritime route optimisation [32], and maritime traffic complexity [33].

2.1. Literature Search Methodology

The literature search was conducted across three major scientific databases: Scopus, Web of Science (WoS), and IEEE Xplore. These databases were selected on the basis of their comprehensive coverage of the engineering, technology, and maritime science literature relevant to the subject domain. The primary search keyword employed was “maritime communication systems,” applied to the title, abstract, and keyword fields of all three databases. This deliberately broad search strategy was adopted to maximise output and minimise the risk of excluding relevant literature that may not employ safety or security terminology in primary metadata fields. The scope of the search was defined as January 2000 to

April 2026, the period following the full implementation of the GMDSS (1999) and covering the emergence of AIS, VDES, and maritime cybersecurity as research domains. The database search returned a total of 6648 records: Scopus (n = 4648), WoS (n = 1000), and IEEE Xplore (n = 1000). The search was conducted in April 2026, with all three databases queried using identical search parameters.

To support full reproducibility, the database-specific query strings are reported here. Scopus: TITLE-ABS-KEY (maritime AND communication AND systems), with the publication-year limit 2000–2026. Web of Science Core Collection: TS = (maritime AND communication AND systems), where the Topic (TS) field searches title, abstract, author keywords, and Keywords Plus, with timespan 2000–2026. IEEE Xplore: (“All Metadata”: maritime communication systems), with publication year restricted to 2000–2026. The same broad three-term anchor was applied consistently across the three databases, and each query was executed once on 14 April 2026. The raw exports underlying these counts are provided as Supplementary Material File S1.

The choice to anchor identification on the three generic terms maritime, communication, and systems, rather than on an exhaustive disjunction of technology-specific terms (for example, AIS, GNSS, SATCOM, VDES, or cybersecurity), reflects a deliberate trade-off between recall and precision. Because the three terms were combined with the Boolean operator AND across the title, abstract, and keyword fields, rather than matched as an exact phrase, a record qualified whenever the three concepts co-occurred anywhere in its indexed metadata; this retained a broad and heterogeneous identification pool (6648 records) rather than a narrowly phrase-matched one. Coverage of the specific technological subdomains was then secured downstream at the relevance-filtering stage (Stage 3), where an expansive synonym set encompassing AIS, VDES, satellite, VHF, radio, wireless, network, jamming, spoofing, and related terms was applied; these subdomains are consequently well represented in the final corpus, each forming a distinct thematic cluster in the results (Section 3.2). A single, very broad disjunctive identification query was avoided because it would have inflated the raw pool with large volumes of off-topic engineering literature while still relying on the same downstream filter for precision. The residual recall limitation of this anchored strategy is acknowledged explicitly in Section 4.

The retrieved records were processed through a structured four-stage screening procedure guided by the PRISMA 2020 guidelines presented in Figure 1. In the first stage, all records were subjected to a year filter, removing 571 records published before 2000, yielding 6077 records. In the second stage, duplicate removal was performed using a two-pass deduplication procedure: first by normalised DOI matching (removing 1222 duplicates), then by normalised title matching (removing a further 217 duplicates), yielding 4638 unique records. In the third stage, relevance filtering was applied to identify records pertaining to the safety and/or security of maritime communication systems. This was operationalised through a rule-based text matching algorithm applied to titles, abstracts, and keyword fields, requiring the co-presence of terms from three semantic categories: (a) safety/security terms (including safety, security, cybersecurity, risk assessment, vulnerability, jamming, spoofing, authentication, encryption, distress, GMDSS, and related terms); (b) communication terms (including communication, VHF, AIS, VDES, satellite, radio, wireless, network, broadband, and related terms); and (c) maritime terms (including maritime, marine, vessel, ship, shipping, nautical, offshore, port, and related terms).

This procedure reduced the dataset to 2035 relevant records (2603 records were excluded as not relevant). In the fourth stage, a relevance scoring algorithm was applied to the 2035 records to identify the highest-quality, most relevant publications for final inclusion. The scoring algorithm assigned each record a weighted sum of four components: (i) the count of high-value domain-specific terms, weighted $\times 2$ for occurrences in the title and

$\times 1$ for occurrences in the abstract and keyword fields; (ii) citation counts, transformed as $\log(1 + \text{citations})$ and min–max normalised, weighted $\times 3$; (iii) publication recency, taken as the min–max normalised publication year, weighted $\times 2$; and (iv) a document-type bonus of +1.5 for review and survey articles. Records with missing citation counts were treated as zero, and missing abstracts or keywords were handled as empty strings. The complete high-value term dictionary, component weights, normalisation, and the resulting per-record scores are provided, together with the full Python pipeline and the scored dataset, as Supplementary Material File S1. The highest-ranked candidates were then screened by two reviewers working as a team, balanced for thematic coverage across the seven identified research clusters, and subjected to a final quality appraisal by the supervising co-author, yielding a final body of 68 publications.

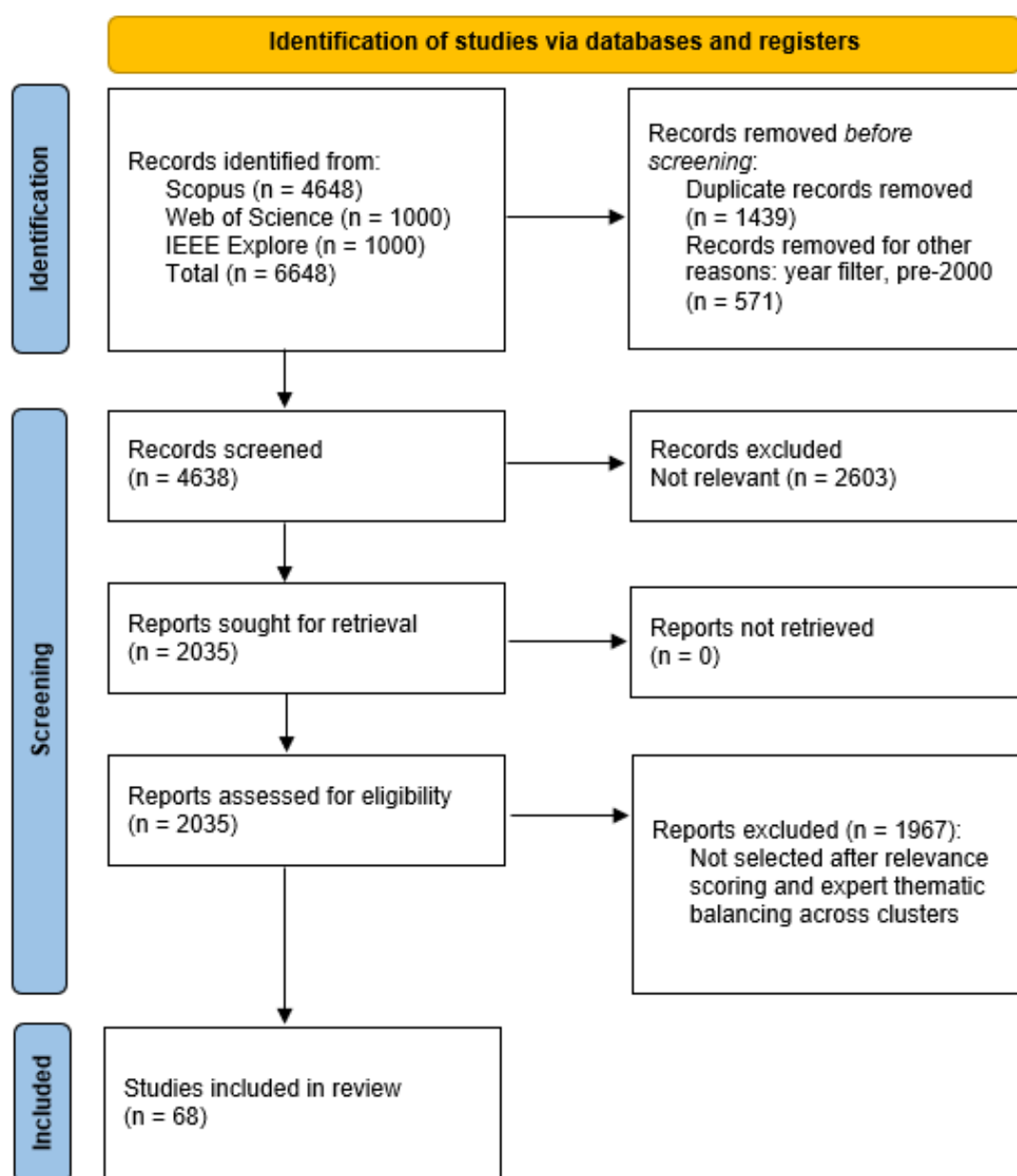


Figure 1. PRISMA 2020 flow diagram illustrating the literature retrieval and screening process. Screening comprises automated metadata processing (year filter, two-pass deduplication, and the rule-based relevance filter) that yields the 2035 relevant records, followed by scoring-based prioritisation and a final expert eligibility and thematic-curation step that yields the 68 included papers.

Table 1 below gives insights into the inclusion and exclusion criteria of the searched literature during the eligibility step, according to the PRISMA 2020 guidelines.

Table 1. Inclusion and exclusion criteria applied during the eligibility assessment stage.

Criterion	Inclusion	Exclusion
Time period	2000–2026	Pre-2000 publications
Language	English language only	Non-English publications
Subject domain	Safety and/or security of maritime communication systems	Maritime research unrelated to communications; communication research unrelated to maritime operations
Document type	Journal articles, conference papers, review articles, books, book chapters, theses	Editorials, errata, retracted papers, brief correspondence
Database source	Scopus, WoS, IEEE Xplore	Non-indexed sources, grey literature
Accessibility	Full-text available or sufficient abstract information	Records with no abstract and no accessible full text

2.2. Bibliometric Analysis Methodology

Bibliometric analysis was conducted on the full relevant pool of 2035 records as well as on the final 68 selected papers, depending on the indicator. Annual publication trend analysis and source distribution analysis were performed on the full relevant pool to provide an accurate representation of research activity in the domain. Document type analysis, geographic distribution, keyword analysis, citation analysis, and authorship pattern analysis were performed on the final 68 selected papers to characterise the highest-relevance subset in detail. All data processing and visualisation were performed using Python 3 with the Pandas (version 3.0.2), Numpy (version 2.4.0), and Matplotlib (version 3.10.8) libraries. The Matplotlib library is a widely used Python library for data visualization and is among the most popular in scientific research. No commercial bibliometric software was used.

3. Results

3.1. Bibliometric Analysis

The annual publication trend for the full relevant pool of 2035 records from 2000 to 2026 is illustrated in Figure 2. The data reveal a clear and sustained growth trajectory in research on the safety and security of maritime communication systems over the past two and a half decades. Publication volumes remained comparatively modest between 2000 and 2012, broadly in the range of a few dozen records per year. A notable change is seen around 2015, with growing industry and regulatory awareness of maritime cybersecurity risks following cyber incidents in transportation sectors and the publication of BIMCO cybersecurity guidelines in 2016. Publications increased from 55 records in 2015 to 84 in 2019, and accelerated further during the 2020–2025 period, with the annual number reaching 176 records in 2023, 235 in 2024, and 418 in 2025. This dramatic recent growth reflects the convergence of several developments: the IMO MSC-FAL.1/Circ.3 resolution on cyber risk management (2017), the accelerated digitalisation of vessels. Advances of VDES research following IMO standardisation, and heightened awareness of AIS security vulnerabilities, also contribute to this. The data for 2026 are partial, representing only the first four months of the year.

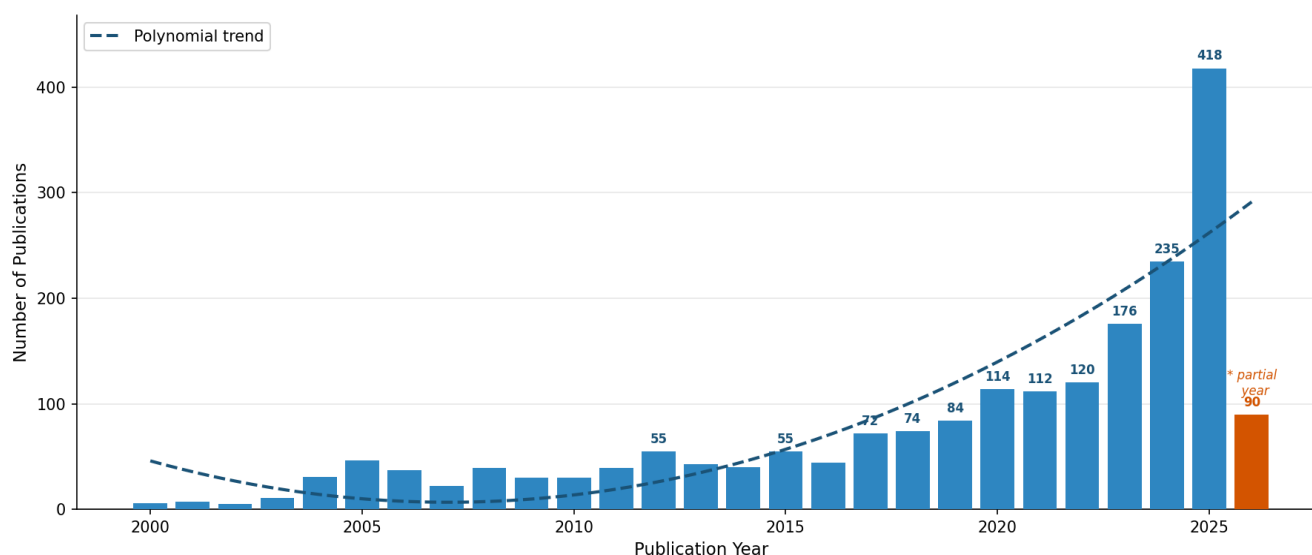


Figure 2. Annual publication trend in the safety and security of maritime communication systems (2000–2026), relevant pool ($n = 2035$). The dashed line represents a second-order polynomial trend. * 2026 data are partial (January–April only).

The document type distribution of the 68 final selected papers is presented in Figure 3. Journal articles constitute the largest category, accounting for 57.4% ($n = 39$) of the corpus, reflecting the maturity of several sub-domains within the field. Conference papers represent 26.5% ($n = 18$), consistent with the active role of IEEE-sponsored conferences and maritime safety symposia in disseminating early-stage research. Review articles account for 13.2% ($n = 9$), reflecting growing scholarly interest in synthesising the rapidly expanding literature, particularly in maritime cybersecurity. Books and book chapters together constitute 2.9% ($n = 2$) of the corpus, primarily comprising technical handbooks on marine radio communication [10]. The relatively high proportion of review articles is noteworthy and suggests an emerging consensus that the field requires integrative scholarly synthesis, further supporting the motivation for the present study.

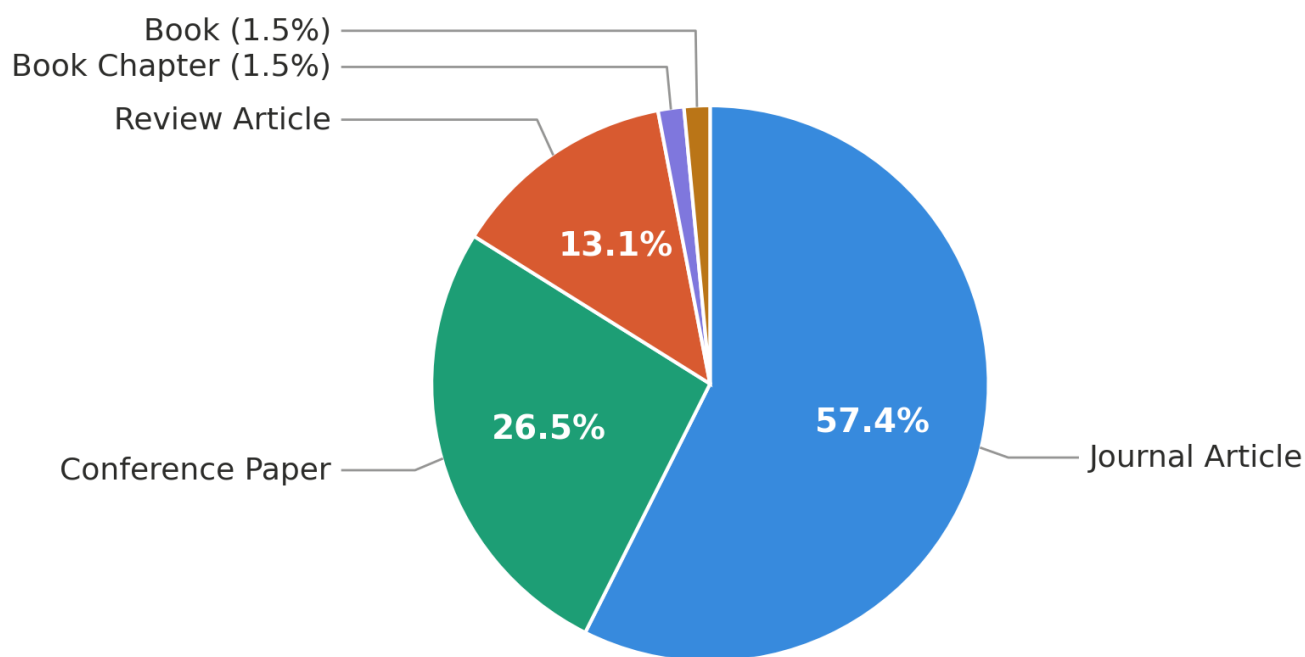


Figure 3. Document type distribution of the final selected papers ($n = 68$).

The distribution of publications across sources within the full relevant pool ($n = 2035$) is illustrated in Figure 4. All source names were first normalised to merge capitalisation and labelling variants of the same venue (for example, differing capitalisations and abbreviated index forms) prior to counting. After this consolidation, the Journal of Marine Science and Engineering (JMSE), published by MDPI, is the leading maritime-specific source with 45 publications, highlighting its role as a principal venue for interdisciplinary maritime research. The Proceedings of SPIE follow with 36 publications, capturing optical and sensor communications research with maritime applications. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, contributes 29 publications, and IEEE Access 28, reflecting the strong engineering and information-security orientation of the field. IEEE Transactions on Intelligent Transportation Systems (26 publications), Ocean Engineering (Elsevier, 25), and the IEEE Internet of Things Journal (25) round out the leading sources, together reflecting the dual engineering and safety-science character of the field.

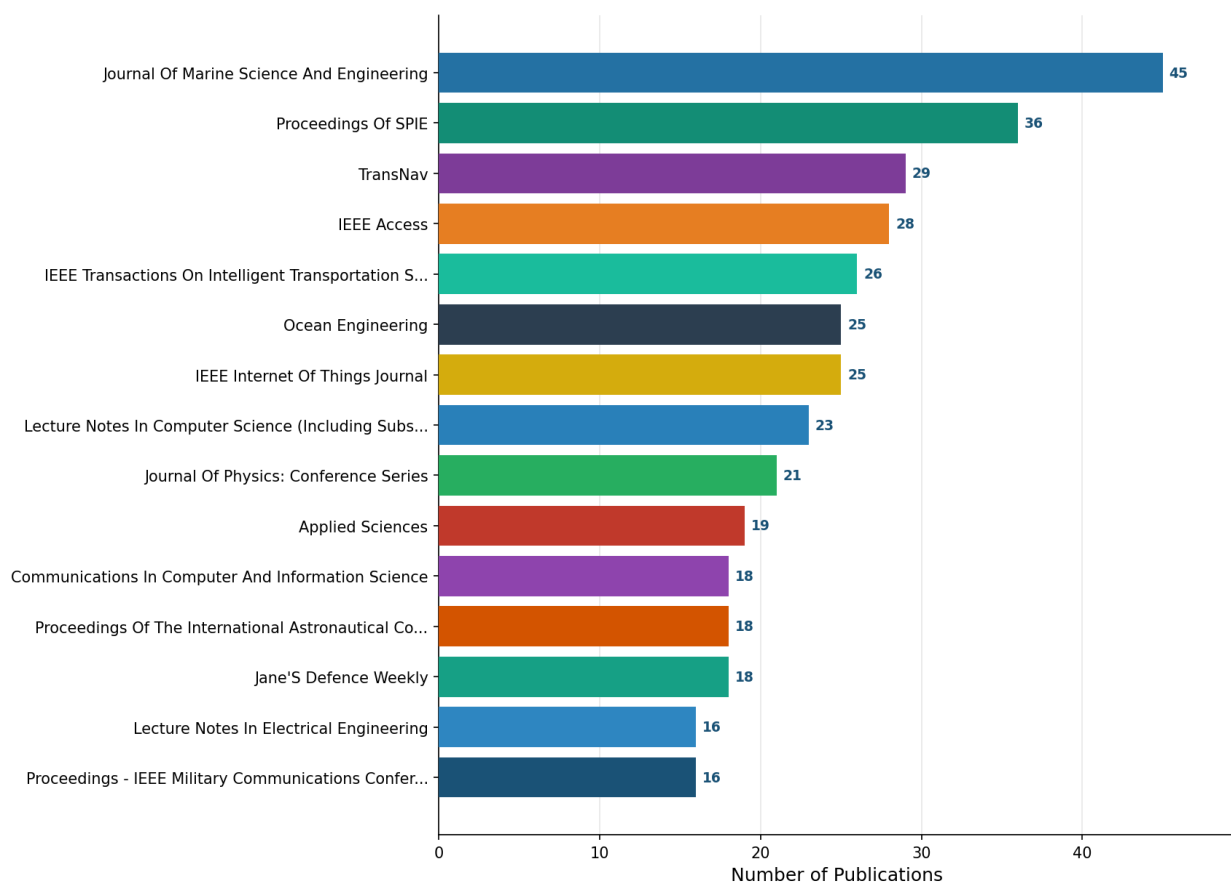


Figure 4. Top 15 publication sources in the relevant pool ($n = 2035$), after normalisation of source-name variants.

The geographic distribution of research output based on author affiliations in the final 68 selected papers is shown in Figure 5. The United Kingdom leads with 7 papers, driven by contributions from institutions active in VDES authentication, AIS security, and maritime cyber risk assessment, including work associated with the General Lighthouse Authorities and academic partners. China follows with 6 papers, with contributions spanning VDES physical layer research, BeiDou satellite communications, and maritime communication resource management. Germany contributes 4 papers, primarily through DLR (German Aerospace Center) research on VDES and GMDSS signal analysis. Spain, South Korea, Norway, Turkey, and Poland each contribute between 2 and 3 papers. The

geographic distribution reflects the concentration of maritime communication research in established maritime nations and countries with significant maritime technology industries. The relatively limited representation of developing maritime nations suggests a research capacity gap that warrants attention from international maritime organisations.

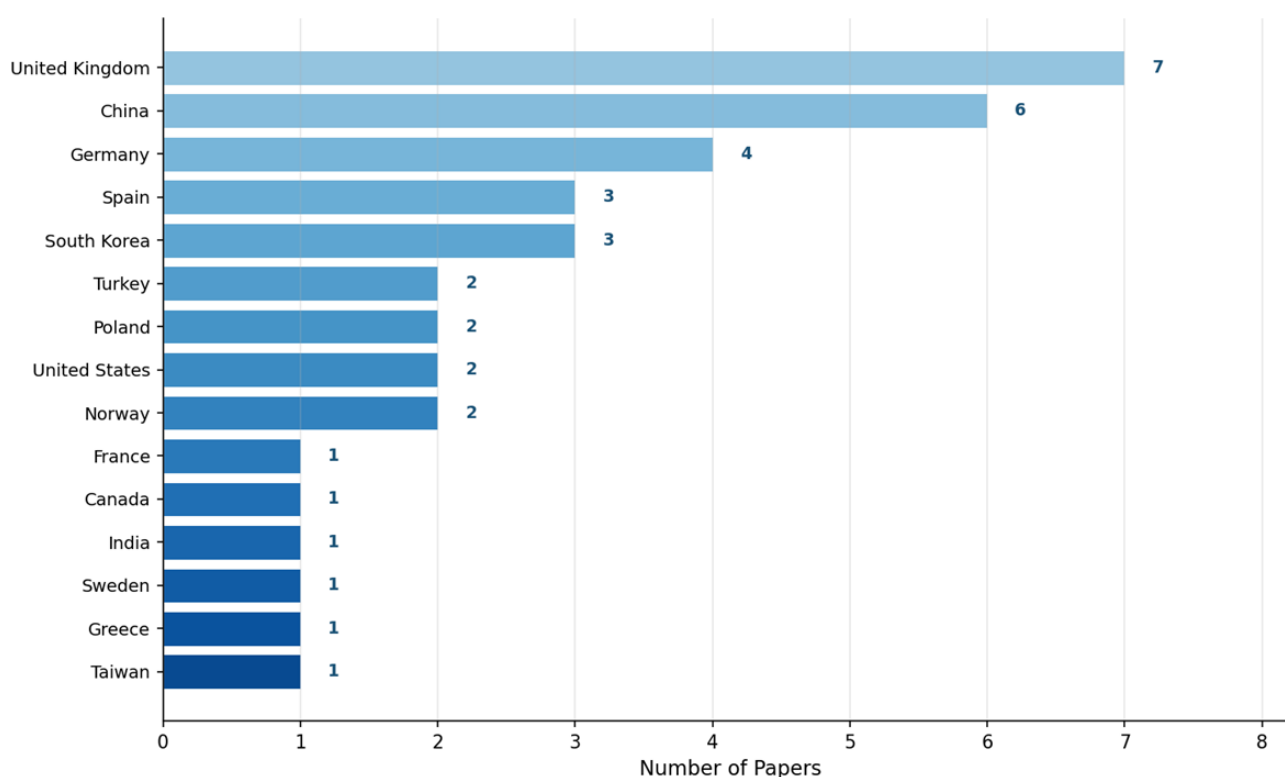


Figure 5. Geographic distribution of publications by author country affiliation (final 68 papers).

The top 20 author keywords from the final 68 selected papers are presented in Figure 6. VDES emerges as the most frequent keyword with 14 occurrences, reflecting the substantial proportion of the corpus dedicated to the development, evaluation, and security of this next-generation maritime communication standard. Cybersecurity ($n = 8$) and maritime cybersecurity ($n = 6$) together constitute the second most prominent keyword cluster, confirming the centrality of security concerns in the most relevant recent literature. GMDSS ($n = 5$) and maritime communication ($n = 5$) reflect foundational thematic anchors. AIS ($n = 3$) and e-navigation ($n = 3$) highlight the operational and digital transformation dimensions of the field. Notably, emerging technological keywords, including quantum cryptography ($n = 2$), machine learning ($n = 2$), and R-Mode ($n = 2$) signal the frontier directions in maritime communication security research.

Figure 7 presents the database provenance of records at both the relevant-pool stage ($n = 2035$) and the final-selection stage ($n = 68$). Because the three databases overlap substantially, the figure reports the number of records indexed in each database, where a record indexed in more than one database is counted in each; the bars therefore sum to more than the stage totals. In the relevant pool, 1460 records are indexed in Scopus, 410 in WoS, and 304 in IEEE Xplore, reflecting the broader indexing scope of Scopus relative to WoS and the specialised engineering focus of IEEE Xplore. Among the final corpus, 62 of the 68 papers are indexed in Scopus, 36 in WoS, and 5 in IEEE Xplore. The strong Scopus presence at both stages is consistent with Scopus contributing the largest share of raw records (4648 of 6648), while the substantial WoS presence in the final corpus reflects the citation-impact component of the scoring procedure, as WoS-indexed papers in this domain tend to carry higher citation counts.

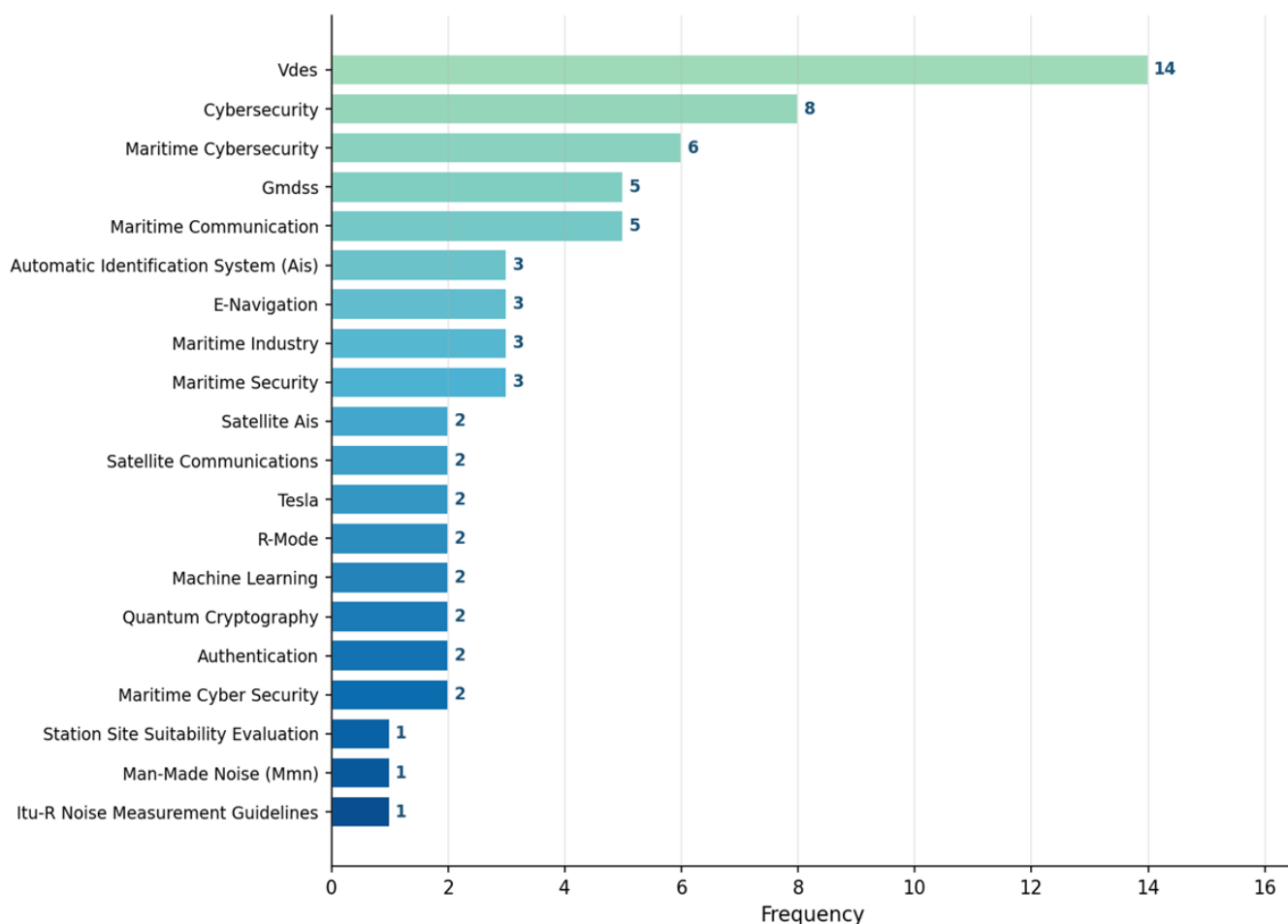
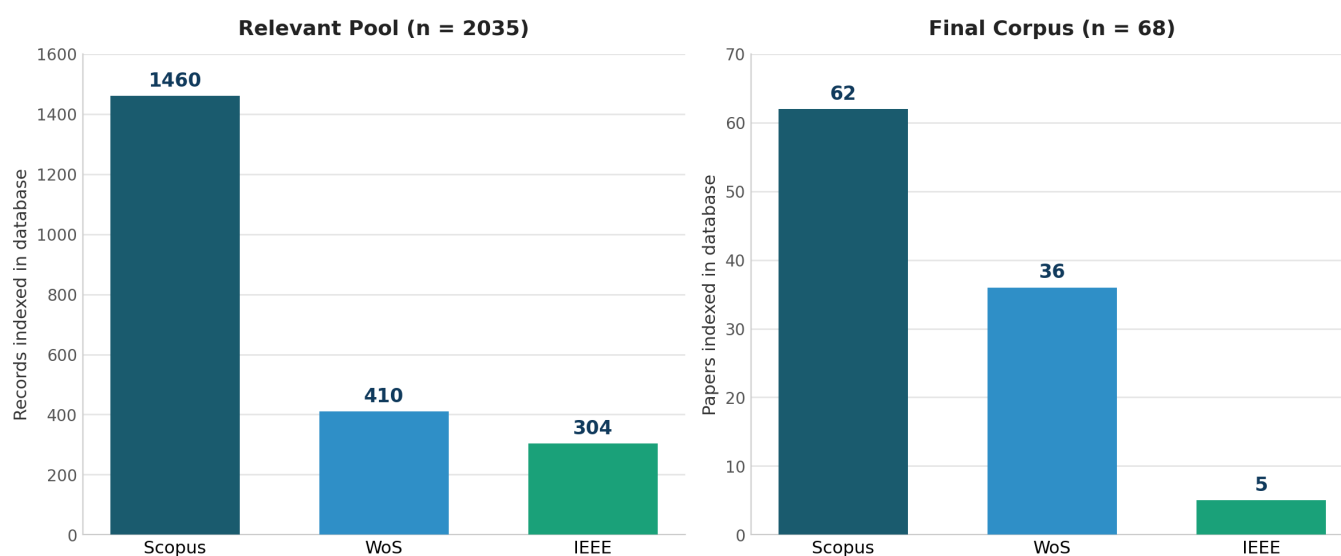


Figure 6. Top 20 author keywords in the final selected papers ($n = 68$). Keyword labels were normalised before counting to merge case and abbreviation variants (for example, “cyber security”/“cybersecurity” and “VHF Data Exchange System”/“VDES”); the same normalisation underlies the keyword co-occurrence analysis in Supplementary Material File S1.



Databases overlap: a record indexed in more than one database is counted in each.

Figure 7. Database provenance of records at the relevant-pool ($n = 2035$) and final-corpus ($n = 68$) stages, shown as the number of records indexed in each database. Because the databases overlap, a record indexed in more than one database is counted in each, so bars sum to more than the stage totals.

The thematic structure of the final 68 papers, organised into seven research clusters, is illustrated in Figure 8. The VDES/VHF/NAVDAT cluster is the largest, comprising 26.6% ($n = 18$) of the corpus, reflecting the prominence of next-generation communication system development in the current research landscape. Maritime cybersecurity constitutes 23.5% ($n = 16$), confirming it as the fastest-growing research cluster in the domain. Risk assessment, surveys, and comprehensive overviews account for 13.2% ($n = 9$), as does the GMDSS cluster ($n = 9$, 13.2%). AIS safety and security represents 11.8% ($n = 8$), while emerging topics ($n = 6$, 8.8%) and satellite communications ($n = 2$, 2.9%) complete the thematic picture.

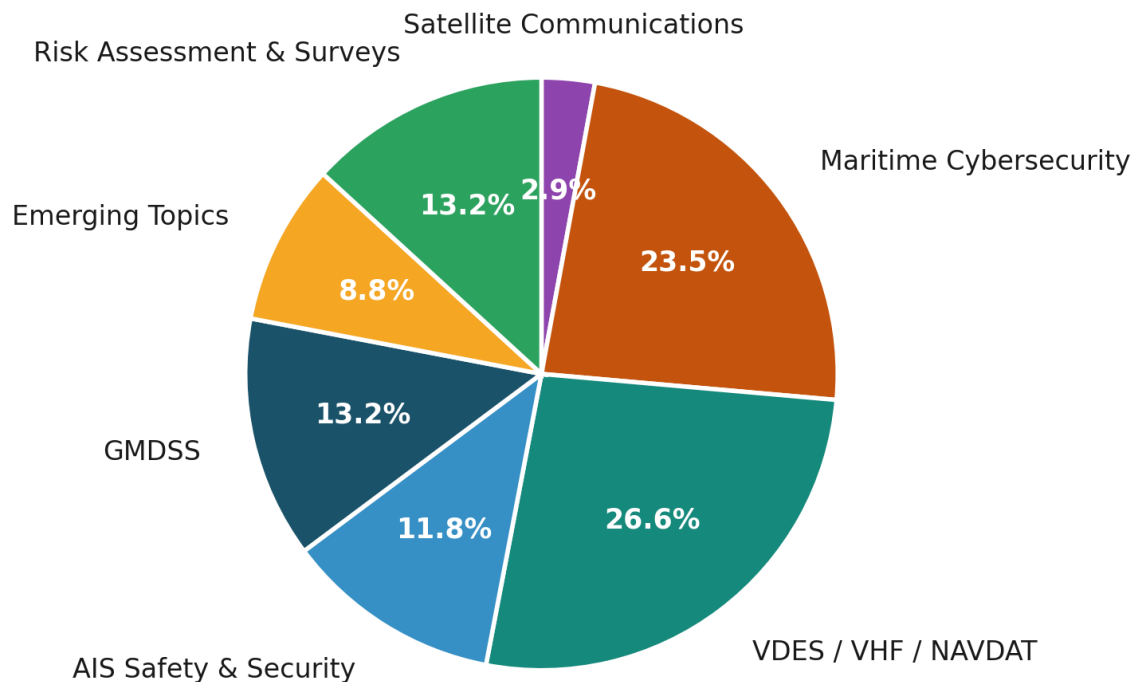


Figure 8. Thematic cluster distribution of the final selected papers ($n = 68$).

The citation distribution of the top 15 most cited papers in the final corpus is presented in Figure 9. The most highly cited paper is the comprehensive survey by Alqurashi et al. [34] on enabling technologies, opportunities, and challenges in maritime communications ($n = 227$ citations), published in the IEEE Internet of Things Journal in 2023, reflecting the broad disciplinary interest in this synthesis work. The AIS review by Robards et al. [12] ($n = 169$) and the foundational space-based AIS study by Eriksen et al. [13] ($n = 118$) represent the most cited AIS-related contributions. The VDES survey by Lázaro et al. [35] ($n = 70$) is the most cited VDES paper, while maritime cyber risk assessment studies by Svilicic et al. [20] ($n = 63$) and Androjna et al. [36] ($n = 61$) lead the cybersecurity cluster. The citation analysis confirms that the most influential contributions in the domain are survey and review articles, foundational AIS studies, and early maritime cybersecurity frameworks, consistent with the relatively recent emergence of VDES and advanced cybersecurity as active research frontiers.

The distribution of the number of authors per paper in the final 68 selected papers is shown in Figure 10. The mean number of authors per paper is 3.6, with a standard deviation of 1.79. Single-author papers account for approximately 10% of the corpus, while papers with two to four authors represent the dominant collaboration mode, collectively accounting for approximately 60% of publications. Papers with five or more authors constitute approximately 30% of the corpus, reflecting the multi-disciplinary character of research at the intersection of communication engineering, cybersecurity, and maritime operations. The

collaboration pattern is consistent with the broader trend in applied engineering research, where small, focused teams are the dominant publication unit but large interdisciplinary collaborations are increasingly common in cyber-physical systems research.

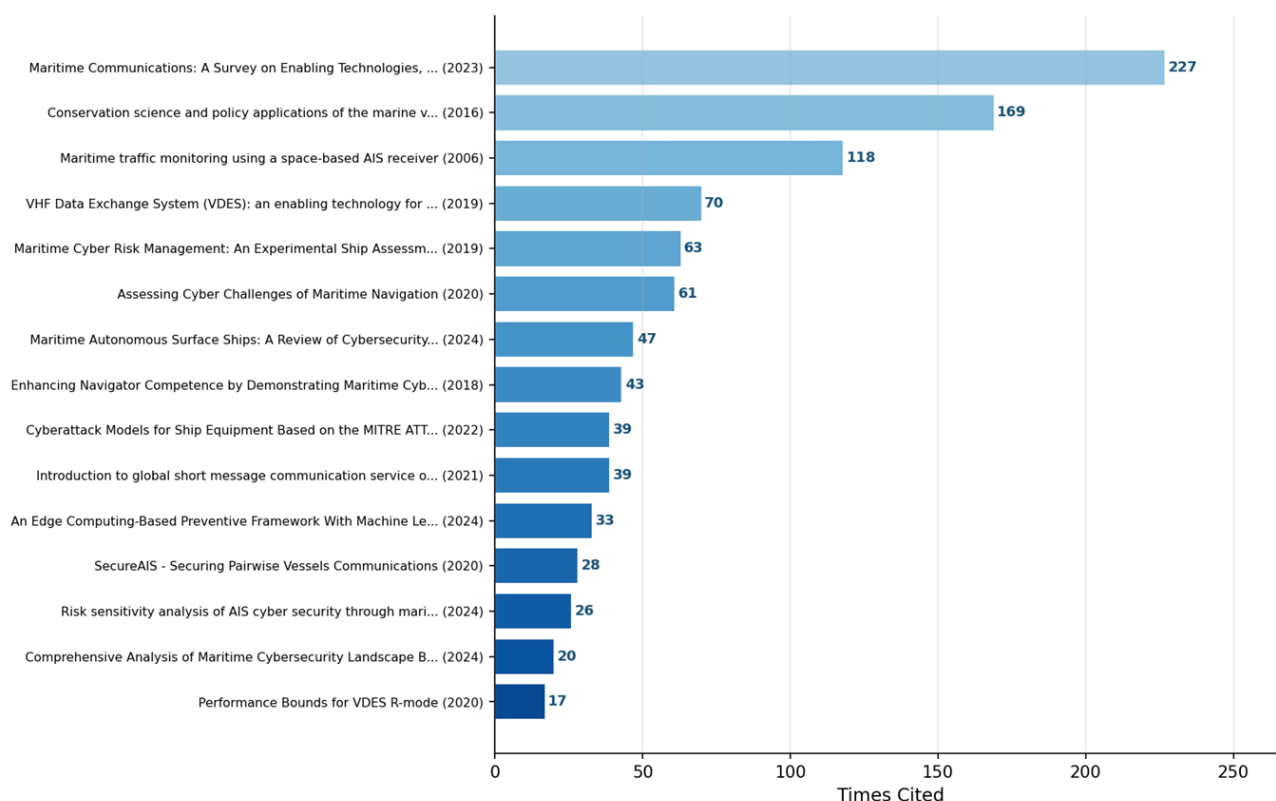


Figure 9. Top 15 most cited papers in the final selected corpus (n = 68). Citation counts are the per-database “cited by” values recorded in the database exports (Scopus, Web of Science, and IEEE Xplore), extracted on 14 April 2026.

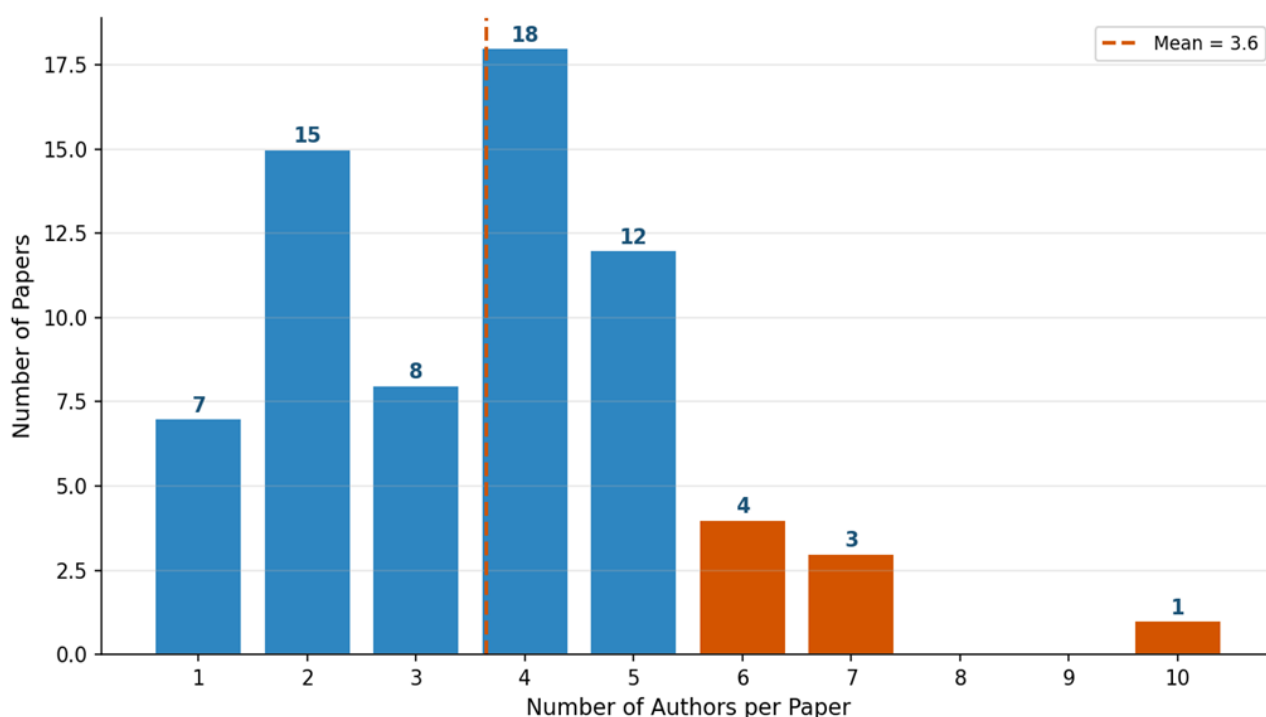


Figure 10. Author collaboration pattern—number of authors per paper (n = 68).

3.2. Thematic Literature Review

The following subsections present a structured thematic synthesis of the 68 selected papers. Selected papers are organized according to the seven research clusters identified in the bibliometric analysis. For each cluster, the principal findings, methodological approaches, and key contributions of the reviewed literature are synthesised and evaluated. Throughout this synthesis, “safety” refers to the protection of communication functions against accidental failure, interference, and operational hazards (for example, distress alerting, signal integrity, and coverage), whereas “security” refers to protection against deliberate adversarial action (for example, jamming, spoofing, intrusion, and data manipulation). Many of the reviewed works address both dimensions; in such cases the paper is assigned to the cluster reflecting its primary contribution, and its secondary safety or security aspects are noted in the narrative.

3.2.1. GMDSS: Modernisation, Equipment, and Training

The GMDSS cluster includes nine publications addressing the technical, operational, and regulatory dimensions of the GMDSS. Modernising GMDSS has been a key focus of this research, as the system was designed in the late 1980s. It needs major updates to meet modern maritime needs. Ilcev [1,3,7] has produced a series of technically detailed analyses that examine the current GMDSS architecture, its functional limitations, and proposals for incorporating modern broadband satellite services, including Low Earth Orbit (LEO) satellite constellations such as Iridium, Globalstar, and OneWeb, into the GMDSS framework. These studies argue that the current GMDSS satellite component, dominated by Inmarsat Medium Earth Orbit (MEO) services, offers insufficient polar coverage and bandwidth for modern maritime operational requirements, and that regulatory reform of the ITU Radio Regulations is necessary to accommodate new service providers [3].

The equipment and operational dimensions of GMDSS have been examined by Valcic et al. [4,6,37], whose studies address both the technical performance of GMDSS equipment under realistic operational conditions and the evolving regulatory framework governing GMDSS modernisation within the IMO. The study by Valcic et al. [4] presents a survey-based analysis of GMDSS equipment usage patterns and seafarer experience, finding significant variation in equipment familiarity and operational competence across vessel types and flag states, with particular deficiencies identified in the use of MF/HF DSC equipment and Inmarsat satellite terminals. The interface between GMDSS and emerging e-navigation concepts is addressed by Koshevyy and Shishkin [8], who propose enhanced VHF and MF/HF DSC interfaces within the e-navigation framework, emphasising the need for seamless integration of digital communication and navigation data streams aboard ship.

Two key studies examine GMDSS training and compliance. Rey-Charlo et al. [2] analyse Paris Memorandum of Understanding (MoU) inspection data and find GMDSS faults are common and mainly due to poor training rather than technical issues. This study is complemented by Rey-Charlo et al. [9], which examines detained vessels under Paris MoU specifically for GMDSS non-compliance, providing a quantitative evidence base for the operational safety implications of inadequate GMDSS implementation. The environmental and physical performance of GMDSS distress signal reception is examined by Uljasz [5], who analyses the influence of environmental noise power on the probability of successfully receiving GMDSS alarm signal. This research provides a quantitative assessment of the coverage reliability implications of ambient electromagnetic noise in maritime environments.

3.2.2. AIS Safety and Security

The AIS safety and security cluster contains eight publications addressing the operational capabilities, security vulnerabilities, and defensive measures associated with the AIS. AIS security has emerged as one of the most actively researched topics in maritime communication security, driven by the widespread documentation of AIS spoofing, data falsification, and signal manipulation in both academic and operational contexts. The foundational security concern with AIS is its open, unauthenticated broadcast architecture: any vessel or shore-based station can inject falsified AIS messages into the maritime common operating picture without detection under the current standard [38].

Soner et al. [14] present a comprehensive risk sensitivity analysis of AIS cybersecurity, mapping AIS vulnerabilities against the evolving maritime cyber regulatory framework, including IMO MSC-FAL.1/Circ.3 and flag state cyber regulations. Their analysis identifies AIS spoofing and GPS spoofing (which produces cascading false position data in AIS transponders) as the highest-risk attack vectors, and critiques the slow pace of regulatory response relative to the documented threat. Androjna and Perkovic [16] address the growing problem of deliberate AIS data falsification, examining the technical mechanisms of AIS data manipulation and discussing the timeframe within which trust in AIS data may become untenable without authentication mechanisms. This work is complemented by Louart et al. [15], who propose a machine learning-based approach for detecting AIS identity spoofing by analysing statistical anomalies in the kinematic data of vessel trajectories, demonstrating effective spoofing detection performance on real AIS datasets.

The authentication problem for AIS is addressed at a fundamental cryptographic level by Wimpenny et al. [38], who propose a public key infrastructure (PKI) based authentication scheme for both AIS and VDES messages. A complementary approach is presented by Aziz et al. [39], who develop a cryptographic protocol for securing pairwise AIS communications between vessels without reliance on a centralised infrastructure. This technically rigorous contribution argues that VDES, as the emerging successor to AIS, provides the opportunity to introduce authentication as a native feature of the standard, using digital signatures appended to VDE messages. The security of AIS-based satellite services is examined by Proud et al. [40], who assess the cybersecurity implications of AIS-based mobile satellite service, noting that the global reach of satellite AIS amplifies both the utility and the attack surface of AIS infrastructure. The foundational contribution of Eriksen et al. [13] on space-based AIS reception, while primarily technical, established the monitoring architecture that underpins current maritime domain awareness and remains the most cited paper in the AIS sub-domain.

The conservation science applications of AIS, reviewed by Robards et al. [12], provide an important contextualisation of the safety implications of AIS data reliability for non-navigational applications, including vessel strike risk to marine mammals, marine protected area monitoring, and fisheries management. The integration of AIS data with ship simulators for maritime safety training and research is examined by Rahmawati et al. [41], who conduct a systematic literature review identifying the principal methodologies and applications of this combined approach. This review highlights the consequences of AIS data integrity failures across multiple domains that now depend on AIS as a primary data source. The low-cost AIS receiver prototype presented by Cabrera et al. [42] addresses the hardware accessibility dimension of AIS infrastructure, demonstrating that cost-effective AIS reception is technically feasible with commercial off-the-shelf components, with implications for the development of AIS monitoring networks in resource-constrained port state environments.

3.2.3. VDES, VHF, and Next-Generation Maritime Communication Systems

The VDES, VHF, and next-generation communication systems cluster is the largest in the corpus, comprising 18 publications. They range from physical layer design, system performance analysis, authentication and security, satellite integration, to application development. VDES, standardised by the ITU as a next-generation maritime communication system operating in the VHF maritime mobile band, represents the most significant development in maritime communication architecture since GMDSS. It offers data throughput orders of magnitude greater than AIS while maintaining backward compatibility with existing maritime VHF infrastructure [35].

The physical layer design and performance of VDES are addressed in several technically detailed contributions. Raulefs et al. [43] present foundational work on the physical layer design of the VHF Data Exchange (VDE) link, addressing modulation scheme selection, channel coding, and performance under the maritime VHF propagation channel. Lázaro et al. [35] provide a comprehensive systems-level overview of VDES as an enabling technology for maritime communications, synthesising the standard's architecture, frequency allocation, data rates, and application scenarios. Valcic et al. [37] present an OFDM-based VHF maritime communication system model for data exchange, demonstrating the feasibility of high-data-rate transmission over maritime VHF channels using OFDM techniques. The performance of the VDES R-Mode is analysed by Safár et al. [44] and by Lázaro et al. [45], with the latter providing a vulnerability analysis and mitigation concepts for R-Mode security threats.

The satellite component of VDES is addressed in several important contributions. Bradbury et al. [46] present the NorSat-2 satellite mission as an enabling platform for VDES space component development, describing its payload design and in-orbit performance. Quintana-Díaz et al. [47] report in-orbit interference measurements in the VDES band from NorSat-2, providing empirical data on the electromagnetic compatibility environment for satellite VDES operations. The authentication and security of VDES are addressed by Wimpenny et al. [24,38], with the latter presenting a pragmatic authentication framework for VDES that balances cryptographic security with the bandwidth and latency constraints of the VHF maritime channel. Lázaro et al. [45] address VDES R-Mode vulnerability specifically, presenting a structured vulnerability analysis and proposing mitigation concepts at both the physical and protocol layers.

The historical context and technological pedigree of VDES are provided by Bauk [48], who reviews NAVDAT and VDES as upgrades of maritime communication systems, tracing the evolution from legacy maritime data systems to the current VDES standard. Golaya and Yogeswaran [49] offer a broad historical perspective on maritime communication evolution, contextualising VDES within the complete arc from flag signaling to digital communication. The application of VDES to fisheries and smart maritime sectors is explored by Wu et al. [50], who examine the application prospects and challenges of VDES in smart fisheries, identifying significant opportunities for vessel monitoring, catch reporting, and fisheries management applications. Rong et al. [23], Sung et al. [51], Bronk et al. [52], and Wu and Song [53] address specific technical aspects of VDES including multiple access protocols, MIMO-aided resource scheduling, terrestrial component simulation, and data gateway implementation. Molina et al. [54] provide a comprehensive overview of the VDES physical layer covering modulation, coding, and channel characteristics. Kim [55] presents a hardware implementation perspective through SIMULINK modelling and FPGA realisation of a turbo decoder for VDES receivers. Alissa et al. [56] demonstrate the application of VDES for distributing adapted NRTK correction data to vessels, illustrating the navigation safety benefits of higher-bandwidth VDES data services.

3.2.4. Maritime Cybersecurity

The maritime cybersecurity cluster comprises 16 publications. It addresses the rapidly evolving field of cyber threats, defensive frameworks, training environments, and governance structures relevant to maritime communication and navigation systems. This cluster has seen the most rapid growth in publication volume of any in the domain, reflecting the heightened attention of the maritime industry, regulators, and academic community to cyber risk following a series of high-profile incidents including the Maersk NotPetya attack (2017), the COSCO ransomware incident (2018), and multiple GPS spoofing campaigns in the Black Sea and Middle East.

Comprehensive analyses of the maritime cybersecurity domain are provided by Dimakopoulou and Rantos [17], who present a structured analysis based on the NIST Cybersecurity Framework (CSF) v2.0, mapping maritime cybersecurity vulnerabilities, existing controls, and gaps across the identify, protect, detect, respond, and recover functions. Martínez et al. [18] contribute a systematic analysis of maritime cybersecurity from an information security management perspective. They address the specific challenges of applying ISO 27001 [57] and IEC 62443 [58] frameworks to the maritime operational technology environment. Jo et al. [18] present cyberattack models for ship equipment based on the MITRE ATT&CK framework and provide a structured taxonomy of attack techniques, tactics, and procedures applicable to shipboard communication and navigation systems, including ECDIS, AIS transponders, and satellite communication terminals.

Maritime cyber risk assessment at the ship level is addressed by Svilicic et al. [20], whose experimental ship-based assessment represents one of the first published empirical evaluations of cyber vulnerabilities aboard an operational vessel, documenting significant unprotected network exposures in satellite communication terminals, ECDIS, and automation systems. Androjna et al. [36] provide a broader assessment of cyber challenges to maritime navigation, examining the threat landscape from a navigational safety perspective and evaluating the adequacy of existing regulatory frameworks. The emerging field of maritime security operations centres is examined by Nasr et al. [59], who conduct a systematic literature review of M-SOC concepts, identifying research and proposing a framework for shore-based maritime cyber monitoring and incident response.

Artificial intelligence applications in maritime cybersecurity are addressed by Miller et al. [60] and Cichocki [61], with the former providing a systematic review of AI-driven threat detection and risk mitigation strategies, and the latter examining the dual-use nature of AI in maritime cyber operations. Tabish and Chaur-Luh [62] review cybersecurity challenges, countermeasures, and future perspectives specifically for Maritime Autonomous Surface Ships (MASS), a rapidly growing research area given the projected expansion of autonomous vessel operations. Kim et al. [63] present a cutting-edge contribution applying variational quantum anomaly detection to maritime network intrusion detection, signaling the nascent exploration of quantum computing applications in maritime cybersecurity. Cybersecurity training and competence are addressed by Potamos et al. [64], who develop a maritime cyber range training environment, Hareide et al. [22], who examine approaches to demonstrating maritime cybersecurity to navigators, and Nikolov [65], who presents a maritime cybersecurity virtual training environment. The HarborLang framework presented by Malakhova et al. [66] provides a domain-specific language for cyber threat simulation and assessment in maritime operational environments, enabling structured modelling of attack scenarios against shipboard communication and navigation systems. Ruhland et al. [67] address embedded authentication mechanisms specifically designed for maritime bridge networks, proposing lightweight cryptographic solutions suitable for the constrained computing environments typical of shipboard OT systems. The development of maritime cyber safety culture is addressed by Hopcraft et al. [21].

3.2.5. Satellite Communications

Satellite communications represent a critical layer of maritime communication infrastructure, providing global coverage for vessel tracking, data services, and distress alerting beyond the range of terrestrial VHF systems. Two papers in the final corpus specifically address advanced satellite communication technologies with direct maritime security and safety relevance. Li et al. [68] present the BeiDou-3 Global Short Message Communication (GSMC) service, a unique capability of the Chinese BeiDou Navigation Satellite System that enables two-way short message communication with global coverage at no charge to users, with significant implications for maritime distress and safety communications in regions not covered by existing Inmarsat and COSPAS-SARSAT infrastructure. Lin [69] examines a UAV-assisted secure maritime communication system incorporating dynamic quantum relaying and satellite collaboration, representing a forward-looking integration of unmanned aerial vehicle relay platforms, quantum communication security, and satellite connectivity for maritime applications in contested or infrastructure-limited environments.

3.2.6. Risk Assessment and Comprehensive Surveys

The risk assessment and survey cluster includes nine publications providing either structured risk assessment frameworks for maritime communication systems or comprehensive disciplinary overviews. The survey by Alqurashi et al. [34] is the most significant contribution in this cluster, providing a thorough examination of enabling technologies, opportunities, and challenges across the full spectrum of maritime communication systems, including cellular (LTE/5G), satellite, cognitive radio, free-space optical, and VHF/UHF systems, with explicit attention to the security and reliability dimensions of each technology class. The handbook by Lees and Williamson [11] provides the most comprehensive reference work in the corpus, covering the complete operational and technical landscape of marine radio communication within the GMDSS framework.

Valcic et al. [70] provide a structured comparative analysis of existing maritime communication systems for data exchange, systematically evaluating the advantages and limitations of AIS, VDES, Inmarsat, Iridium, and other systems against a defined set of safety and operational criteria. Powell [71] surveys comprehensive approaches to enhancing maritime wireless networks, addressing quality of service, interference management, and security enhancement across multiple communication layers. The survey by Algarni et al. [72] examines edge computing-based preventive frameworks integrating machine learning for anomaly detection and risk management in maritime wireless communications, bridging the domains of network edge computing, machine learning, and maritime communication security. Jin et al. [73] address the legal and governance dimensions of maritime cyber operations, examining the international legal framework governing state and non-state cyber activities in maritime contexts, including questions of jurisdiction, attribution, and proportional response. Mfodwo et al. [74] present a threat modelling analysis of maritime software-defined radios, an emerging architectural paradigm for flexible maritime communication that introduces new security considerations.

3.2.7. Emerging Topics

The emerging topics cluster includes six publications addressing frontier research directions in maritime communication safety and security. López-Díaz et al. [75] present a viability and performance analysis of a maritime communication network operating on the medium frequency (MF) band, demonstrating that MF networks can provide reliable data communication within coastal zones and provide a technical basis for MF as a backup maritime communication layer in GMDSS modernisation scenarios. Korcz [76] examines

the regulatory and technical issues of maritime radiocommunication addressed at the World Radiocommunication Conference 2019 (WRC-19), providing a policy-level analysis of spectrum management decisions with long-term implications for maritime communication system development. He and Li [77] examine the paradigm shift in maritime safety communication from a coast station perspective, analysing the optimisation of coast station service layouts in the context of evolving communication technology.

Boretti [78] explores the expanding role of unmanned surface vehicles (USVs) in maritime security, examining the communication system requirements of autonomous vessel operations and the security implications of reliance on wireless communication for autonomous vessel command and control. Rong [79] presents a reinforcement learning framework for maritime communication system optimisation, demonstrating the potential of deep reinforcement learning to dynamically optimise communication resource allocation across heterogeneous maritime networks. Peng et al. [80] provide a bibliometric analysis specifically focused on maritime cybersecurity research, offering a meta-analytic perspective on the structure and evolution of the cybersecurity sub-domain.

4. Discussion

The bibliometric and thematic analysis presented in this study reveals a research domain characterised by rapid growth, increasing thematic diversity, and an evolving focus from technical performance evaluation toward integrated safety and security frameworks. Several key findings are presented in this discussion.

First, the dramatic acceleration of publication volume from 2019 onwards is indicative of a field responding to urgent operational and regulatory stimuli. The convergence of IMO cyber risk management requirements, high-profile maritime cyber incidents, and the accelerated digitalisation of vessel systems has transformed maritime communication security from a niche concern of maritime technology researchers into a mainstream interdisciplinary research priority. The growth of the cybersecurity cluster from near-zero publications before 2015 to the second-largest cluster in the current corpus underscores this transformation.

Second, the dominance of VDES in the keyword analysis and thematic distribution reflects the strategic importance of this technology for the future of maritime communication infrastructure. VDES is simultaneously a technical development project, a regulatory challenge, and a security design opportunity: the decisions made now regarding VDES authentication, interference resilience, and system architecture will shape the security of maritime communications for decades. The substantial research investment in VDES physical layer, satellite integration, and authentication highlights the need for equally rigorous research on VDES implementation security, spectrum management, and interoperability with legacy GMDSSs.

Third, the geographic concentration of research output in a small number of countries, notably the United Kingdom, China, Germany, Spain, and South Korea, raises questions about the global representativeness of the research base. Maritime communication security challenges are faced by all maritime nations, but the research agenda appears to be shaped disproportionately by nations with significant maritime technology industries and academic research infrastructure. This may result in research priorities that do not adequately reflect the communication infrastructure challenges of developing maritime nations, particularly regarding GMDSS coverage gaps, training deficiencies, and PSC enforcement capacity.

The thematic analysis identifies several significant research gaps that should guide future scholarly efforts:

- Integrated cross-system risk frameworks. The existing literature addresses the safety and security of individual maritime communication systems such as GMDSS, AIS,

VDES, and satellite terminals, but mainly in isolation. There is a notable absence of integrated risk frameworks that evaluate the cumulative and interdependent failure modes across the full maritime communication architecture. A vessel in distress may simultaneously experience GMDSS equipment failure, AIS spoofing, and satellite communication degradation; understanding the compounded risk of such scenarios requires a systems-of-systems analytical approach not yet present in the literature.

- Human factors in maritime cybersecurity. While technical vulnerability analyses are well represented, the human factors dimension of maritime cybersecurity, including crew cyber awareness, social engineering susceptibility, operational security behaviour, and the human–machine interface implications of cybersecurity tools, is under-researched. Studies by Hareide et al. [22] and Hopcraft et al. [21] represent important contributions, but the field lacks the structured empirical research base on human factors in maritime cyber incidents comparable to that available in aviation or healthcare cybersecurity.
- Legal and governance frameworks. The legal dimensions of maritime communication security, including jurisdictional questions in cyber incident response, the application of international maritime law to cyber operations targeting maritime infrastructure, and the liability implications of communication system security failures, remain significantly under-researched. Jin et al. [73] represent a pioneering contribution, but the intersection of maritime law, international cybersecurity law, and communication system governance requires substantially more scholarly attention.
- Polar and remote area communication security. With increasing maritime activity in Arctic and Antarctic waters, the specific communication security and reliability challenges of polar maritime operations, including limited satellite coverage from geostationary orbits, HF propagation anomalies, and the absence of terrestrial VHF infrastructure, are largely unaddressed in the current literature. The GMDSS modernisation cluster identifies coverage gaps as a technical challenge, but the security implications of these gaps have not been systematically examined.
- Autonomous vessel communication security. While Boretti [78] and Tabish and Chaur-Luh [62] address aspects of autonomous vessel cybersecurity, the specific communication security requirements of Maritime Autonomous Surface Ships (MASS) in operational service represent a frontier research area. MASS rely entirely on wireless communication for remote monitoring, command and control, and collision avoidance, making communication security existentially critical for safe autonomous operations. The regulatory framework for MASS communication security is still nascent, and the academic literature has not yet produced the foundational security architecture research that this domain urgently requires.

Table 2 below gives a brief summary of the most relevant key publications selected.

Additionally, the findings of this review are directly relevant to the commercial maritime communications market, which is undergoing a substantial structural transformation. Industry analyses consistently indicate strong growth trajectories: the broader maritime communication systems market was valued at approximately USD 3.0–3.4 billion in 2024, with projections placing it at USD 4.3–5.4 billion by 2029 at compound annual growth rates of approximately 5–6% [81]. The satellite communications segment, which supports GMDSS, crew connectivity, and emerging broadband data services, is growing considerably faster, with estimates for 2025 ranging from USD 4.7 to over USD 7 billion depending on market scope, and forecasts indicating a doubling of revenues within the decade. This is driven by Low Earth Orbit (LEO) constellation deployment, VSAT broadband uptake, and the IMO's 2024 GMDSS modernisation, which opened satellite service certification to new providers [82]. Starlink's LEO services were reported to be installed on approximately

75,000 vessels by the end of 2024 [83]. The rapid growth of broadband connectivity aboard commercial vessels directly amplifies the cybersecurity exposure documented throughout this review, as crew members and onboard systems gain persistent internet access, increasing susceptibility to phishing, social engineering, and ransomware attack vectors [82]. These market figures are drawn from commercial consultancy reports [81–84] rather than peer-reviewed sources, and are reported here only to provide indicative industrial context for the research trends identified above; the specific values and growth rates should be interpreted with the methodological caution appropriate to proprietary market estimates.

The maritime cybersecurity market itself reflects this expanding threat surface. It was estimated at USD 3.2–3.7 billion in 2024, with projections to reach USD 9.0 billion or more by 2033 at a CAGR of approximately 12–13% [81]. Commercial shipping accounts for the largest market segment at approximately 40–42% of revenue share. This reflects the scale of digital integration in cargo tracking, fleet management, and satellite-linked navigation systems [84]. The network security segment, which includes the communication infrastructure analysed in this review, held approximately 33% of cybersecurity market revenue in 2024 [83]. These commercial dynamics reinforce a key implication of this review: the seven research gaps identified above are not merely academic concerns but correspond to concrete market failures and regulatory deficiencies with measurable economic consequences. The absence of integrated cross-system risk frameworks, insufficient human factors research, and the nascent state of autonomous vessel communication security represent areas where the growth of commercial investment has outpaced the availability of validated scientific knowledge. Accordingly, it should be considered a priority for funding organizations and global maritime regulatory bodies to ensure that the research agenda outlined in this study is aligned with the structural transformations taking place in the maritime communications market.

Several limitations of the review process should be acknowledged. First, the search was restricted to three databases (Scopus, Web of Science, and IEEE Xplore) and to English language, peer-reviewed and conference literature. Grey literature, standards, and non-indexed sources were therefore not systematically captured. Second, title/abstract screening and eligibility assessment were carried out by two reviewers working in a pair rather than as independent double-screening with formal mutual agreement; disagreements were resolved by discussion as they arose, and a final quality appraisal was performed by the supervising co-author. The review was not registered in PROSPERO or an equivalent register, and no separate published protocol was prepared. Third, candidate prioritisation relied on an automated rule-based relevance filter and a transparent weighted scoring algorithm (Supplementary Material File S1); while this makes the workflow fully reproducible, the term dictionary and weights were defined by the authors and inevitably embed design choices, and no formal sensitivity analysis of these parameters was undertaken. Fourth, the thematic synthesis into seven clusters was performed narratively on the basis of full-text reading; although the author-keyword co-occurrence structure of the corpus is broadly consistent with these clusters, the cluster boundaries remain a matter of expert judgement rather than algorithmic community detection (e.g., VOSviewer or CiteSpace). Fifth, identification relied on a three-term keyword anchor (maritime AND communication AND systems) applied to indexed metadata. Although this anchor was paired with a deliberately broad downstream relevance filter, studies that describe a specific technology, such as AIS, GNSS, SATCOM, VDES, or maritime cybersecurity, without any of the three anchor terms co-occurring in their title, abstract, or keywords would not have entered the identification pool, so some technology-specific literature indexed only under narrower terminology may be under-represented. The final corpus nonetheless spans all of these subdomains, which suggests that any such under-coverage is partial rather than systematic.

Table 2. Summary of selected key publications by thematic cluster, primary focus, methodology, and key findings. This table is a selective summary of representative publications chosen to illustrate each thematic cluster; it is not an exhaustive evidence table of all 68 included studies.

Ref.	Year	Cluster	Primary Focus	Method	Key Finding
[1]	2020	GMDSS	GMDSS modernisation	Technical review	LEO satellite integration needed for GMDSS upgrade
[2]	2023	GMDSS	PSC inspection data/training	Data analysis	GMDSS deficiencies linked to training inadequacies
[4]		GMDSS	Seafarers GMDSS usage	Survey	Significant operational competence gaps across vessel types
[14]	2024	AIS	AIS cybersecurity risk	Risk analysis	Spoofing and GPS falsification are identified as the highest risks
[16]	2024	AIS	AIS data falsification	Technical analysis	The current AIS architecture is unsustainable without authentication
[38]	2018	AIS/VDES	PKI authentication for AIS/VDES	Cryptographic design	PKI viable for VDES-native authentication implementation
[45]	2023	VDES	VDES R-Mode vulnerability	Vulnerability analysis	Multiple physical and protocol layer vulnerabilities identified
[35]	2019	VDES	VDES enabling technologies	System survey	VDES enables broadband maritime services with AIS compatibility
[64]	2021	Cyber	Maritime cyber range	Training environment design	Cyber range effective for maritime crew cyber training
[19]	2022	Cyber	Cyberattack models (MITRE)	Threat modelling	MITRE ATT&CK applicable to shipboard OT/IT environment
[17]	2024	Cyber	NIST CSF v2.0 analysis	Framework analysis	Significant gaps in the detection and response functions were identified
[18]	2024	Cyber	ISO 27001/IEC 62443	Security management	OT/IT convergence creates unique maritime security challenges
[34]	2023	Survey	Maritime comm. technologies survey	Comprehensive survey	Most cited: 227 citations; covers full technology spectrum
[20]	2019	Risk	Ship cyber risk experiment	Experimental assessment	Unprotected exposures found in SATCOM and ECDISs
[74]	2026	Emerging	SDR security threat modelling	Threat analysis	SDR introduces a significant new attack surface in maritime communications

5. Conclusions

This study has presented the first comprehensive PRISMA-guided systematic literature review and bibliometric analysis of research on the safety and security of maritime communication systems, drawing on a dataset of 68 high-relevance publications identified from a raw pool of 6648 records retrieved from Scopus, Web of Science, and IEEE Xplore for the period 2000–2026. The principal findings of the study can be summarised as follows.

Publication activity in this domain has grown exponentially since 2015 and has accelerated sharply since 2019, driven by the IMO cybersecurity regulatory requirements, high-profile maritime cyber incidents, VDES standardisation, and accelerated vessel digitalisation. The research is geographically concentrated in the United Kingdom, China, Germany, Spain, and South Korea, and is dominated by IEEE Access, the Journal of Marine Science and Engineering, and TransNav as principal publication venues. Seven thematic research clusters have been identified: GMDSS modernisation, AIS safety and security, VDES and next-generation VHF systems, maritime cybersecurity, satellite communications, risk assessment and comprehensive surveys, and emerging topics.

The thematic synthesis reveals that the most significant recent research developments are the emergence of VDES authentication frameworks as a central design challenge for next-generation maritime communications, the maturation of maritime cybersecurity as a structured research discipline with established frameworks (NIST CSF, MITRE ATT&CK, IMO MSC-FAL.1/Circ.3), and the growing application of artificial intelligence and machine learning to threat detection in maritime communication networks. Foundational research gaps include the absence of integrated cross-system risk frameworks, insufficient attention to human factors in maritime cybersecurity, limited research on legal and governance dimensions, and the nascent state of communication security research for autonomous vessel operations.

The results of this study provide a structured knowledge base for researchers, naval architects, maritime operators, and policymakers seeking to understand the current state of research and identify priority areas for future investment. The bibliometric dataset and thematic taxonomy developed here can serve as a reference framework for subsequent systematic reviews, meta-analyses, and research agenda-setting exercises in maritime communication safety and security.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/technologies14070390/s1>. File S1: Reproducible screening and relevance-scoring pipeline [10].

Author Contributions: Conceptualization, P.I., Z.S.V., V.M. and I.P.; methodology, P.I. and V.M.; software, V.M.; validation, Z.S.V.; formal analysis, P.I. and I.P.; investigation, P.I. and V.M.; resources, P.I.; data curation, V.M. and Z.S.V.; writing—original draft preparation, P.I., Z.S.V., V.M. and I.P.; writing—review and editing, P.I. and Z.S.V.; visualization, V.M.; supervision, Z.S.V. and I.P.; funding acquisition, P.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The three raw database exports (Scopus, Web of Science, and IEEE Xplore), the complete screening and relevance-scoring pipeline implemented in Python 3, the scoring parameter table, and the scored relevant-pool dataset are provided as Supplementary Material, enabling full reproduction of the record counts and the selection workflow reported in this study.

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

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
BIMCO	Baltic and International Maritime Council
COSPAS-SARSAT	Cosmicheskaya Sistyema Poiska Avarynykh Sudov—Search and Rescue Satellite-Aided Tracking
CSF	Cyber Security Framework
DSC	Digital Selective Call
ECDIS	Electronic Chart Display and Information System
GMDSS	Global Maritime Distress and Safety System
HF	High Frequency
IMO	International Maritime Organization
IT	Information Technology
ITU	International Telecommunication Union
LEO	Low Earth Orbit
MASS	Maritime Autonomous Surface Ships
MF	Medium Frequency
MoU	Memorandum of Understanding
M-SOC	Maritime Security Operations Center
NAVDAT	Navigation Data System
NIST	National Institute of Standards and Technology
OT	Operational Technology
PKI	Public Key Infrastructure
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PSC	Port State Control
R-Mode	Ranging Mode
SAR	Search and Rescue
SART	Search and Rescue Transponder
SDR	Software-Defined Radio
SLR	Systematic Literature Review
SOLAS	International Convention for the Safety of Life at Sea
STCW	Standards of Training, Certification and Watchkeeping for Seafarers
UHF	Ultra-High Frequency
USV	Unmanned Surface Vehicle
VDES	VHF Data Exchange System
VHF	Very High Frequency
WoS	Web of Science
WRC	World Radiocommunication Conference

References

1. IMO. SOLAS: *International Convention for the Safety of Life at Sea, 1974, as Amended*; International Maritime Organization: London, UK, 2024.
2. Rey-Charlo, R.E.; Cueto, J.L.; Piniella, F. Analyzing Port State Control Data to Explore Future Improvements to GMDSS Training. *J. Mar. Sci. Eng.* **2023**, *11*, 2379. [[CrossRef](#)]
3. Ilcev, D.S. Alternative Maritime Satellite Solutions for Enhanced GMDSS Network. *TransNav* **2022**, *16*, 361–370. [[CrossRef](#)]
4. Valcic, S.; Skrobonja, A.; Maglic, L.; Svilicic, B. GMDSS Equipment Usage: Seafarers' Experience. *J. Mar. Sci. Eng.* **2021**, *9*, 476. [[CrossRef](#)]
5. Uljasz, B. The Influence of Environmental Noise Power on the Probability of Receiving GMDSS Alarm Signals. *TransNav* **2025**, *19*, 33. [[CrossRef](#)]
6. Valcic, S.; Zuskin, S.; Brcic, D.; Sakan, D. An Overview of Recent Changes in the Global Maritime Distress and Safety System Regarding Maritime Mobile Satellite Service. *Naše More* **2019**, *66*, 170–176. [[CrossRef](#)]
7. Ilcev, D.S. Software Solutions for GMDSS Network and Equipment. *TransNav* **2022**, *16*, 487–496. [[CrossRef](#)]

8. Koshevyy, V.M.; Shishkin, O.V. Developments of Interface for VHF, MF/HF Communication Using DSC in GMDSS Services in the Framework of E-navigation Concept. *TransNav* **2021**, *15*, 555–561. [\[CrossRef\]](#)
9. Rey-Charlo, R.E.; Piniella, F.; Alcaide, J.I. Detained Vessels under Paris MoU: Implementation of GMDSS. In *Maritime Technology and Engineering 4*; CRC Press: Boca Raton, FL, USA, 2019. [\[CrossRef\]](#)
10. 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. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Lees, G.D.; Williamson, W.G. *Handbook for Marine Radio Communication*, 6th ed.; Routledge: London, UK, 2022. [\[CrossRef\]](#)
12. Robards, M.D.; Silber, G.K.; Adams, J.D.; Arroyo, J.; Lorenzini, D.; Schwehr, K.; Amos, J. Conservation Science and Policy Applications of the Marine Vessel Automatic Identification System (AIS)—A Review. *Bull. Mar. Sci.* **2016**, *92*, 75–103. [\[CrossRef\]](#)
13. Eriksen, T.; Høye, G.; Narheim, B.; Jenslokken, B.; Meland, B.J. Maritime Traffic Monitoring Using a Space-Based AIS Receiver. *Acta Astronaut.* **2006**, *58*, 537–549. [\[CrossRef\]](#)
14. Soner, O.; Kayisoglu, G.; Bolat, P.; Tam, K. Risk Sensitivity Analysis of AIS Cyber Security through Maritime Cyber Regulatory Frameworks. *Appl. Ocean Res.* **2024**, *143*, 103855. [\[CrossRef\]](#)
15. Louart, M.; Szkolnik, J.-J.; Boudraa, A.-O.; Le Lann, J.-C.; Le Jeune, D. An Approach to Detect Identity Spoofing in AIS Messages. *Expert Syst. Appl.* **2024**, *255*, 124257. [\[CrossRef\]](#)
16. Androjna, A.; Perkovic, M. AIS Data Falsification—How Long Will It Be Before We Can No Longer Trust AIS? In Proceedings of the MetroSea 2024, Split, Croatia, 4–6 November 2024. [\[CrossRef\]](#)
17. Dimakopoulou, A.; Rantos, K. Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *J. Mar. Sci. Eng.* **2024**, *12*, 919. [\[CrossRef\]](#)
18. Martínez, F.; Sánchez, L.E.; Santos-Olmo, A.; Rosado, D.G.; Fernández-Medina, E. Maritime Cybersecurity: Protecting Digital Seas. *Int. J. Inf. Secur.* **2024**, *23*, 1429–1457. [\[CrossRef\]](#)
19. Jo, Y.; Choi, O.; You, J.; Cha, Y.; Lee, D.H. Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors* **2022**, *22*, 1860. [\[CrossRef\]](#) [\[PubMed\]](#)
20. Svilicic, B.; Kamahara, J.; Rooks, M.; Yano, Y. Maritime Cyber Risk Management: An Experimental Ship Assessment. *J. Navig.* **2019**, *72*, 1108–1120. [\[CrossRef\]](#)
21. Hopcraft, R.; Tam, K.; Misas, J.D.P.; Moara-Nkwe, K.; Jones, K. Developing a Maritime Cyber Safety Culture: Improving Safety of Operations. *Mar. Technol. Rev.* **2023**, *5*, 258750. [\[CrossRef\]](#)
22. Hareide, O.S.; Josok, O.; Lund, M.S.; Ostnes, R.; Helkala, K. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *J. Navig.* **2018**, *71*, 1025–1039. [\[CrossRef\]](#)
23. Rong, S.; Wang, M. Multiple Access Protocol for Ad-hoc Networks in VHF Data Exchange System. In Proceedings of the IEEE CompComm 2018, Chengdu, China, 1–3 August 2018. [\[CrossRef\]](#)
24. Wimpenny, G.; Lázaro, F.; Šafař, J.; Raulefs, R. A Pragmatic Approach to VDES Authentication. *Navigation* **2025**, *72*, navi.681. [\[CrossRef\]](#)
25. Bojić, F.; Gudelj, A.; Bošnjak, R. Port-Related Shipping Gas Emissions—A Systematic Review of Research. *Appl. Sci.* **2022**, *12*, 3603. [\[CrossRef\]](#)
26. Boko, Z.; Skoko, I.; Sanchez Varela, Z.; Milin, V. Advancing Maritime Safety: A Literature Review on Machine Learning and Multi-Criteria Analysis in PSC Inspections. *J. Mar. Sci. Eng.* **2025**, *13*, 974. [\[CrossRef\]](#)
27. Glavinović, R.; Vukić, L.; Plazibat, V.; Račić, M. Methodological Approaches to Battery-Powered Ro-Pax Ferries in Domestic Shipping: A Systematic Review of Route-Based Case Studies. *J. Mar. Sci. Eng.* **2026**, *14*, 226. [\[CrossRef\]](#)
28. Karin, I.; Medvešek, I.G.; Šoda, J. Best-Suited Communication Technology for Maritime Signaling Facilities: A Literature Review. *Appl. Sci.* **2025**, *15*, 3452. [\[CrossRef\]](#)
29. Maljković, M.; Pavić, I.; Meštrović, T.; Perković, M. Ship Maneuvering in Shallow and Narrow Waters: Predictive Methods and Model Development Review. *J. Mar. Sci. Eng.* **2024**, *12*, 1450. [\[CrossRef\]](#)
30. Meštrović, T.; Pavić, I.; Maljković, M.; Androjna, A. Challenges for the Education and Training of Seafarers in the Context of Autonomous Shipping: Bibliometric Analysis and Systematic Literature Review. *Appl. Sci.* **2024**, *14*, 3173. [\[CrossRef\]](#)
31. Milin, V.; Skoko, I.; Lekšić, Ž.; Boko, Z. Navigational Safety Hazards Posed by Offshore Wind Farms: A Comprehensive Literature Review and Bibliometric Analysis. *J. Mar. Sci. Eng.* **2025**, *13*, 1330. [\[CrossRef\]](#)
32. Milin, V.; Stanivuk, T.; Skoko, I.; Bulić, T. Dijkstra and A* Algorithms for Algorithmic Optimization of Maritime Routes and Logistics of Offshore Wind Farms. *J. Mar. Sci. Eng.* **2025**, *13*, 1863. [\[CrossRef\]](#)
33. Milin, V.; Lalić, B.; Stanivuk, T.; Maleš, M. Understanding Maritime Traffic Complexity: A Comprehensive Concept Development Review. *Technologies* **2026**, *14*, 231. [\[CrossRef\]](#)
34. Alqurashi, F.S.; Trichili, A.; Saeed, N.; Ooi, B.S.; Alouini, M.-S. Maritime Communications: A Survey on Enabling Technologies, Opportunities, and Challenges. *IEEE Internet Things J.* **2023**, *10*, 3525–3558. [\[CrossRef\]](#)

35. Lázaro, F.; Raulefs, R.; Wang, W.; Clazzer, F.; Plass, S. VHF Data Exchange System (VDES): An Enabling Technology for Maritime Communications. *CEAS Space J.* **2019**, *11*, 55–67. [\[CrossRef\]](#)
36. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing Cyber Challenges of Maritime Navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [\[CrossRef\]](#)
37. Valcic, S.; Pogány, T.; Mrak, Z. A Model of OFDM Based Maritime VHF Communication System for Data Exchange. *Pol. Marit. Res.* **2018**, *25*, 42–50. [\[CrossRef\]](#)
38. Wimpenny, G.; Šafař, J.; Grant, A.; Bransby, M.; Ward, N. Public Key Authentication for AIS and the VHF Data Exchange System (VDES). In Proceedings of the ION GNSS+ 2018, Miami, FL, USA, 24–28 September 2018. [\[CrossRef\]](#)
39. Aziz, A.; Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. SecureAIS—Securing Pairwise Vessels Communications. In Proceedings of the IEEE CNS 2020, Avignon, France, 29 June–1 July 2020. [\[CrossRef\]](#)
40. Proud, R.; Browning, P.; Kocak, D.M. AIS-Based Mobile Satellite Service Expands Opportunities for Affordable Global Ocean Observing and Monitoring. In Proceedings of the OCEANS 2016, Monterey, CA, USA, 19–23 September 2016. [\[CrossRef\]](#)
41. Rahmawati, M.; Pitana, T.; Handani, D.W.; Siswanto, N. Utilization of AIS Data and Ship Simulator Integration in Maritime Safety: A Systematic Literature Review. *IOP Conf. Ser. Earth Environ. Sci.* **2025**, *1461*, 012049. [\[CrossRef\]](#)
42. Cabrera, F.; Molina, N.; Tichavska, M.; Arana, V. Design of a Low Cost Prototype of Automatic Identification System (AIS) Receiver. In Proceedings of the URSI AT-RASC 2015, Gran Canaria, Spain, 18–22 May 2015. [\[CrossRef\]](#)
43. Raulefs, R.; Stenbock, T.A.; Dammann, A.; Plass, S. Physical Layer Design towards VHF Data Exchange (VDE) Link. In Proceedings of the OCEANS 2015, Genova, Italy, 18–21 May 2015. [\[CrossRef\]](#)
44. Šafař, J.; Grant, A.; Williams, P.; Ward, N. Performance Bounds for VDES R-Mode. *J. Navig.* **2020**, *73*, 23–39. [\[CrossRef\]](#)
45. Lázaro, F.; Raulefs, R.; Bartz, H.; Jerkovits, T. VDES R-Mode: Vulnerability Analysis and Mitigation Concepts. *Int. J. Satell. Commun. Netw.* **2023**, *41*, 521–534. [\[CrossRef\]](#)
46. Bradbury, L.M.; Diaconu, D.; Laurin, S.M.; Beattie, A.M.; Ma, C.; Spydevold, I.S.; Haugli, H.C.; Zee, R.E.; Harr, J.; Udnæs, F. NorSat-2: Enabling Advanced Maritime Communication with VDES. *Acta Astronaut.* **2019**, *156*, 232–239. [\[CrossRef\]](#)
47. Quintana-Diaz, G.; Birkeland, R.; Loge, L.; Andersen, E.; Bolstad, A.; Ekman, T. In-Orbit Interference Measurements and Analysis in the VDES-Band with the NorSat-2 Satellite. In Proceedings of the IEEE Aerospace Conference 2022, Big Sky, MT, USA, 5–12 March 2022. [\[CrossRef\]](#)
48. Bauk, S.I. A Review of NAVDAT and VDES as Upgrades of Maritime Communication Systems. In *Maritime Technology and Engineering 4*; CRC Press: Boca Raton, FL, USA, 2019. [\[CrossRef\]](#)
49. Golaya, A.P.; Yogeswaran, N. Maritime Communication: From Flags to the VHF Data Exchange System (VDES). *J. Inst. Eng. India Ser. B* **2020**, *16*, 1–13. [\[CrossRef\]](#)
50. Wu, Z.L.; Xiong, M.S.; Cheng, T.F.; Dai, Y.; Zhang, S.M.; Fan, W.; Cui, W. Application Prospects and Challenges of VHF Data Exchange System (VDES) in Smart Fisheries. *J. Mar. Sci. Eng.* **2025**, *13*, 250. [\[CrossRef\]](#)
51. Sung, J.; Cho, S.; Jeon, W.; Park, K.; Ahn, S.J.; Kwon, K. MIMO-Aided Efficient Communication Resource Scheduling Scheme in VDES. *TIIS* **2022**, *16*, 2681–2697. [\[CrossRef\]](#)
52. Bronk, K.; Koncicki, P.; Lipka, A.; Rutkowski, D.; Wereszko, B. Simulation and Measurement Studies of the VDES System's Terrestrial Component. *Pol. Marit. Res.* **2019**, *26*, 124–133. [\[CrossRef\]](#)
53. Wu, T.; Song, Z. Design and Implementation of VDES Data Gateway Applied to Maritime Communication. In Proceedings of the ICEIEC 2023, Beijing, China, 29–30 July 2023. [\[CrossRef\]](#)
54. Molina, N.; Cabrera, F.; Araña, V.; Tichavska, M. An Overview About the Physical Layer of the VHF Data Exchange System (VDES). In *Advances in Artificial Intelligence*; Springer: Cham, Switzerland, 2020. [\[CrossRef\]](#)
55. Kim, J.H. SIMULINK Modeling and FPGA Implementation of Turbo Decoder for VDES Receiver. *J. Korea Inst. Inf. Commun. Eng.* **2025**, *50*, 489–497. [\[CrossRef\]](#)
56. Alissa, S.; Håkansson, M.; Rieck, C.; Dutta, U.; Nord, S.; Bergljung, P.; Bagge, A. Distribution of the Adapted-NRTK Correction Data via VDES for the Shipping Navigation Safety. In Proceedings of the ION GNSS+ 2021, St. Louis, MO, USA, 20–24 September 2021. [\[CrossRef\]](#)
57. ISO/IEC 27001:2013; Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO: Geneva, Switzerland, 2013.
58. IEC 62443-3-3:2013; Industrial Communication Networks—Network and System Security—Part 3-3: System Security Requirements and Security Levels. IEC: Geneva, Switzerland, 2013.
59. Nasr, A.N.; Vaarandi, R.; Zaitseva-Pärnaste, I.; Kujala, P. Maritime Security Operations Center (M-SOC): Systematic Literature Review, Research Gaps and Future Areas to Investigate. *TransNav* **2025**, *19*, 11. [\[CrossRef\]](#)
60. Miller, T.; Durlik, I.; Kostecka, E.; Sokolowska, S.; Kozłowska, M. Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies. *Electronics* **2025**, *14*, 1844. [\[CrossRef\]](#)
61. Cichocki, R. Artificial Intelligence in Maritime Cybersecurity: Dual-Use Applications for Defense and Offense in the Age of Digital Seas. *TransNav* **2025**, *19*, 34. [\[CrossRef\]](#)

62. Tabish, N.; Chaur-Luh, T. Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. *IEEE Access* **2024**, *12*, 17114–17136. [\[CrossRef\]](#)
63. Kim, M.; El Azaoui, A.; Park, J.H. VQAD-Sec: A Variational Quantum Anomaly Detection for Intrusion Detection in Maritime Networks. *HCIS* **2026**, *16*, 10. [\[CrossRef\]](#)
64. Potamos, G.; Peratikou, A.; Stavrou, S. Towards a Maritime Cyber Range Training Environment. In Proceedings of the IEEE CSR 2021, Dublin, Ireland, 28–30 June 2021. [\[CrossRef\]](#)
65. Nikolov, B. Approach to Developing a Maritime Cybersecurity Virtual Training Environment. *Eng. Technol. Rev.* **2024**, *2*, 220–225. [\[CrossRef\]](#)
66. Malakhova, D.; Hacks, S.; Alexeeva, A.; Pathe, T.R. HarborLang: Enhancing Maritime Operational Safety Through Cyber Threat Simulation and Assessment. In *Computer Security*; Springer: Cham, Switzerland, 2025. [\[CrossRef\]](#)
67. Ruhland, L.; Schmidt, M.; Bauer, J.; Padilla, E. Keeping the Baddies Out and the Bridge Calm: Embedded Authentication for Maritime Networks. In Proceedings of the IEEE ISNCC 2022, Shenzhen, China, 19–22 July 2022. [\[CrossRef\]](#)
68. Li, G.; Guo, S.R.; Lü, J.; Zhao, K.L.; He, Z.H. Introduction to Global Short Message Communication Service of BeiDou-3 Navigation Satellite System. *Adv. Space Res.* **2021**, *68*, 1301–1312. [\[CrossRef\]](#)
69. Lin, W. A UAV-Assisted Secure Maritime Communication System with Dynamic Quantum Relaying and Satellite Collaboration. *Procedia Comput. Sci.* **2025**, *266*, 1065–1072. [\[CrossRef\]](#)
70. Valcic, S.; Mrak, Z.; Gulic, M. Analysis of Advantages and Disadvantages of Existing Maritime Communication Systems for Data Exchange. *Pomor. Zb.* **2016**, *30*, 45–60. [\[CrossRef\]](#)
71. Powell, D.J. Comprehensive Approaches to Enhance Maritime Wireless Networks: A Survey. Ph.D. Thesis, University of Greenwich, London, UK, 2024. [\[CrossRef\]](#) [\[PubMed\]](#)
72. Algarni, A.; Acarer, T.; Ahmad, Z. An Edge Computing-Based Preventive Framework with Machine Learning Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications. *IEEE Access* **2024**, *12*, 49750–49767. [\[CrossRef\]](#)
73. Jin, Y.M.; Feng, Y.; Liu, C.M.; Li, S.B. Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations. *Front. Mar. Sci.* **2025**, *12*, 1616906. [\[CrossRef\]](#)
74. Mfodwo, E.; Lanka, P.; Aydogan, A.F.; Varol, C. Uncovering the Security Landscape of Maritime Software-Defined Radios: A Threat Modeling Perspective. *Appl. Sci.* **2026**, *16*, 813. [\[CrossRef\]](#)
75. López-Díaz, A.I.; Gutiérrez, M.A.; Piris, A.O.; Díaz-Ruiz-Navamuel, E. Viability and Performance Analysis, at a Physical Level, of a Maritime Communication Network on Medium Frequency. *J. Mar. Sci. Eng.* **2021**, *9*, 970. [\[CrossRef\]](#)
76. Korcz, K. The Issues of Maritime Radiocommunication on the WRC-19. *TransNav* **2019**, *13*, 631–636. [\[CrossRef\]](#)
77. He, H.; Li, Y. Paradigm Shift of the Maritime Safety Communication: Optimizing the Layout of Coast Station Services. In *International Conference on Marine Equipment & Technology and Sustainable Development. METSD 2023. Lecture Notes in Civil Engineering*; Springer: Singapore, 2023. [\[CrossRef\]](#)
78. Boretti, A. Navigating the Future: The Expanding Role of Unmanned Surface Vehicles in Maritime Security. *J. Mar. Sci. Appl.* **2025**, *18*, 1–23. [\[CrossRef\]](#)
79. Rong, B. Reinforcement Learning for Maritime Communications. *IEEE Wirel. Commun.* **2023**, *30*, 22–23. [\[CrossRef\]](#)
80. Peng, P.; Xie, X.W.; Claramunt, C.; Lu, F.; Gong, F.Z.; Yan, R. Bibliometric Analysis of Maritime Cybersecurity: Research Status, Focus, and Perspectives. *Transp. Res. Part E* **2025**, *195*, 103971. [\[CrossRef\]](#)
81. MarketsandMarkets. *Maritime Communication Market—Global Forecast to 2029*; MarketsandMarkets Research: Pune, India, 2024. Available online: <https://www.marketsandmarkets.com/Market-Reports/maritime-communication-market-137134882.html> (accessed on 15 April 2026).
82. Grand View Research. *Maritime Cybersecurity Market Size, Share & Trends Analysis Report, 2025–2033*; Grand View Research: San Francisco, CA, USA, 2025. Available online: <https://www.grandviewresearch.com/industry-analysis/maritime-cybersecurity-market-report> (accessed on 15 April 2026).
83. Valour Consultancy. *Maritime Satellite Connectivity Market: The Current State of Play and Predictions for 2025*; Valour Consultancy: London, UK, 2025. Available online: <https://valourconsultancy.com/maritime-satellite-connectivity-market-the-current-state-of-play-and-predictions-for-2025/> (accessed on 15 April 2026).
84. Mordor Intelligence. *Maritime Satellite Communication Market Size & Share Analysis—Growth Trends & Forecasts (2025–2030)*; Mordor Intelligence: Hyderabad, India, 2026. Available online: <https://www.mordorintelligence.com/industry-reports/maritime-satellite-communication-market> (accessed on 15 April 2026).

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.