priviet lab.
RESEARCH & PUBLISHING

Journal of Maritime Defense Technology

Volume 1
Issue 1 April, 2026

Article 4

01-04-2026

Maritime defense technology: A structured literature review of AI, autonomous systems, maritime domain awareness, and cyber resilience

Dimvy Rusefani Asetya

To cite this article: Asetya, D. R. (2026). Maritime defense technology: A structured literature review of AI, autonomous systems, maritime domain awareness, and cyber resilience. *Journal of Maritime Defense Technology*, 1(1), 35–48.
https://journal.privietlab.org/index.php/JMDT/article/view/1938

To link to this article: https://journal.privietlab.org/index.php/JMDT/article/view/1938

Journal of Maritime Defense Technology

Volume 1
Issue 1
April Edition 2026

OPEN ACCESS

Maritime defense technology: A structured literature review of AI, autonomous systems, maritime domain awareness, and cyber resilience

Dimvy Rusefani Asetya

Faculty of Agriculture, Jember University, Jalan Kalimantan No. 37, Kampus Tegalboto Kotak Pos 159 Jember, Jawa Timur, 68121, Indonesia
email: dimvyrusefani16@gmail.com

Received 29 January 2026
Revised 16 March 2026
Accepted 1 April 2026

ABSTRACT

Maritime defense technology has become a strategic priority as navies, coast guards, and maritime security agencies confront hybrid threats, illegal activities, contested littoral zones, cyber-physical vulnerabilities, and operational complexity of autonomous systems. This structured literature review synthesizes peer-reviewed research on maritime defense technology, with an emphasis on maritime domain awareness, autonomous and unmanned maritime vehicles, artificial intelligence, satellite surveillance, Automatic Identification System data analytics, undersea systems, and cyber resilience. The review follows a PRISMA-informed search and screening logic together with evidence-informed management review principles. A Scopus and Web of Science search protocol was applied using combinations of maritime defense, maritime security, naval technology, autonomous systems, AIS, satellite surveillance, unmanned surface vehicles, unmanned underwater vehicles, cyber security, and artificial intelligence. The synthesis shows that the literature is concentrated around six technological clusters: data-driven maritime domain awareness, AIS-based anomaly detection and prediction, satellite, optical, and synthetic aperture radar surveillance, unmanned surface and underwater vehicles, maritime cyber security, and human-machine cooperation for autonomous maritime operations. The review finds that maritime defense technology is shifting from platform-centric capabilities toward integrated, software-defined, data-intensive, and cyber-resilient systems. However, the literature remains fragmented across engineering, transportation, computer science, safety, and defence studies. Major gaps include limited operationally realistic datasets, weak integration between cyber security and autonomy research, insufficient validation in contested environments, and underdeveloped governance models for human-machine teaming. This paper proposes a future research agenda for resilient, explainable, interoperable, and ethically governed maritime defense technology.

Keywords: maritime defense; maritime domain awareness; autonomous systems; artificial intelligence; cyber resilience

priviet lab.
RESEARCH & PUBLISHING

1. INTRODUCTION

Maritime defense technology refers to an integrated set of platforms, sensors, software, communication systems, data analytics, command-and-control tools, and cyber-physical architectures used to protect maritime sovereignty, sea lines of communication, naval assets, ports, offshore infrastructure, and maritime economic activity. This concept is broader than naval weapons alone. It includes surveillance satellites, Automatic Identification System (AIS) analytics, coastal radar, unmanned surface vehicles, autonomous underwater vehicles, maritime cyber security, underwater communication networks, artificial intelligence, decision-support systems, and human-machine teaming arrangements. This broader understanding is important because contemporary maritime defense capabilities increasingly depend on integration rather than isolated platforms.

The strategic importance of maritime defense technology has grown because maritime threats have become more widespread, ambiguous, and technologically complex. Maritime security agencies must monitor illegal fishing, piracy, smuggling, terrorism, gray-zone coercion, spoofed vessel identities, cyberattacks against ship and port systems, underwater infrastructure threats, and contested access to strategic chokepoints to ensure maritime security. These risks occur across vast ocean spaces and often involve actors who deliberately exploit the gaps between defence, law enforcement, commercial shipping, and environmental governance. Therefore, controlling the maritime domain using traditional patrols alone is difficult.

A central feature of the current literature is the movement from platform-centric defense to data-intensive Maritime Domain Awareness (MDA). MDA depends on the collection, fusion, interpretation, and operational use of information about vessels, activities, routes, infrastructure, environmental conditions, and potential threats to maritime security. AIS data have become a major research stream because they allow scholars and practitioners to analyze vessel trajectories, routes, traffic patterns and anomalies. Pallotta et al. (2013) developed an influential framework for vessel pattern knowledge discovery, anomaly detection, and route prediction, whereas Tu et al. (2018) reviewed how AIS data can be exploited for intelligent maritime navigation. More recent reviews have consolidated AIS anomaly detection as a distinct research field while highlighting persistent difficulties in data labelling, benchmarking, and operational interpretation (Ribeiro et al., 2023; Riveiro et al., 2018; Wolsing et al., 2022).

Simultaneously, maritime surveillance has expanded beyond coastal infrastructure to space-based and multimodal sensing. Ground-based radar and terrestrial AIS cannot provide comprehensive global maritime coverage, particularly in open oceans, polar regions, archipelagic waters, and areas outside of dense infrastructure. Satellite AIS, Synthetic Aperture Radar (SAR), optical imagery, and other space-based sensors complement traditional surveillance systems (Soldi et al., 2021). Kanjir et al. (2018) show that optical satellite imagery has grown rapidly as a source for vessel detection and classification, although environmental constraints such as cloud cover, haze, illumination, and sensor resolution remain important limitations.

Autonomous and unmanned systems represent another major technological advancement. Unmanned Surface Vehicles (USVs), Unmanned Underwater Vehicles (UUVs), and Autonomous Underwater Vehicles (AUVs) are increasingly relevant for surveillance, mine countermeasures, intelligence collection, environmental assessment, port security, and risk reduction in hazardous areas. Early work at the NATO Undersea Research Centre emphasized the scientific and naval applications of AUVs, including mine countermeasures and covert preparation of the battlespace (Bovio et al., 2006). Subsequent reviews have shown rapid progress in USV guidance, navigation, control, collision avoidance, cooperation, and intelligent motion control (Bae & Hong, 2023; Bai et al., 2022; Campbell et al., 2012; Er et al., 2023; Liu et al., 2016).

However, these technological advances have introduced new vulnerabilities. Maritime systems are increasingly connected through Internet of Things (IoT) architectures, digital navigation systems, autonomous decision tools, satellite communications, and shore-based control networks. This expands the attack surfaces of ships, ports, autonomous platforms, and surveillance systems. Consequently,

maritime cyber security has become a major research stream, with surveys emphasizing threats to IoT-enabled maritime systems, navigation data, autonomous vessels, and port infrastructures (Ashraf et al., 2023; Farah et al., 2022; Tabish & Chaur-Luh, 2024; Zhang et al., 2020).

Despite this growth, the literature remains fragmented across engineering, transportation, computer science, remote sensing, safety, and defence studies. Studies on AIS analytics are often published in transportation and data mining venues, whereas research on unmanned systems appears in robotics, control, and ocean engineering. Cybersecurity research is frequently separated from autonomy and sensor fusion research. Human-machine cooperation studies often focus on commercial maritime autonomous surface ships rather than explicitly defense-oriented systems. This fragmentation makes it difficult for defense managers, acquisition officers, naval planners, and researchers to obtain a coherent understanding of maritime-defense technology.

This structured literature review addressed four research questions. First, what are the dominant technological themes in the scholarly literature on maritime defense technologies? Second, how do AI, autonomous systems, satellite surveillance, AIS analytics, and cyber security contribute to maritime defense capabilities? Third, what limitations, research gaps, and future research directions are evident in the literature? Fourth, what are the implications of these findings for maritime defense management, procurement, and policy?

2. METHOD

This review uses a structured literature review design guided by PRISMA 2020 reporting principles and management-oriented systematic review guidance. PRISMA 2020 was used as a transparency framework for defining the search source, time span, eligibility criteria, screening focus, and synthesis process, while Tranfield et al. (2003) informed the evidence-informed management review logic. The design is appropriate for a multidisciplinary field in which relevant studies are dispersed across maritime security, engineering, transportation, remote sensing, computer science, and defence studies.

The search period was limited to 2006-2026. The starting point is justified because influential early research on autonomous underwater vehicles for scientific and naval operations appeared in 2006, and the period captures the growth of AIS analytics, unmanned maritime vehicles, satellite surveillance, maritime IoT, cybersecurity, and AI-enabled maritime operations. The date range also covers the transition from primarily sensor-based maritime surveillance to algorithmic and cyber-physical maritime defense architectures.

The search strategy combined terms related to maritime defense, maritime security, naval technology, maritime domain awareness, autonomous systems, AIS, satellite surveillance, synthetic aperture radar, unmanned vehicles, cyber security, and artificial intelligence. The search string was intentionally inclusive because the field is multidisciplinary, and many relevant studies do not use the exact term maritime defense. For example, studies on vessel anomaly detection, autonomous ship safety, USV motion control, or satellite vessel detection may have direct defense relevance even when published in commercial maritime, transportation, or engineering journals.

The Scopus search string was: TITLE-ABS-KEY (("maritime defense" OR "maritime defence" OR "naval technology" OR "maritime security" OR "maritime domain awareness" OR "naval surveillance") AND ("artificial intelligence" OR "machine learning" OR "autonomous" OR "unmanned" OR "AIS" OR "Automatic Identification System" OR "synthetic aperture radar" OR "satellite surveillance" OR "cyber security" OR "cybersecurity" OR "underwater vehicle" OR "unmanned surface vehicle" OR "unmanned underwater vehicle")). The Web of Science search string was: TS = (("maritime defense" OR "maritime defence" OR "naval technology" OR "maritime security" OR "maritime domain awareness" OR "naval surveillance") AND ("artificial intelligence" OR "machine learning" OR "autonomous" OR "unmanned" OR "AIS" OR "Automatic Identification System" OR "synthetic aperture radar" OR "satellite surveillance" OR "cyber security" OR "cybersecurity" OR "underwater vehicle" OR "unmanned surface vehicle" OR "unmanned underwater vehicle")) (see Table 1).

Table 1. Scopus and Web of Science Search Strategy

Element	Specification
Databases	Scopus and Web of Science Core Collection
Time span	2006-2026
Review design	PRISMA-informed structured literature review and qualitative thematic synthesis
Core concepts	Maritime defense/defence, maritime security, naval technology, maritime domain awareness, naval surveillance
Technology terms	Artificial intelligence, machine learning, autonomous, unmanned, AIS, Automatic Identification System, satellite surveillance, SAR, cyber security, cybersecurity, underwater vehicle, unmanned surface vehicle, unmanned underwater vehicle
Screening focus	Maritime context, defense relevance, peer-reviewed scholarly outlet, and methodological or technical contribution
Synthesis output	Six technology clusters and cross-cutting gaps for maritime defense management and policy

Note:
The search protocol was designed for Scopus and Web of Science Core Collection replication; exact hit counts should be inserted after database export.

The search protocol was used to identify peer-reviewed and review-based studies with direct relevance to maritime defense technology. Records were assessed through title and abstract screening, followed by full-text eligibility checking and thematic extraction. Because the objective was qualitative synthesis rather than meta-analysis, the review emphasizes transparent eligibility criteria, technology categorization, and cross-cluster synthesis rather than statistical effect-size aggregation.

To strengthen methodological transparency, the screening procedure was organized around four audit points: database source, duplicate removal, eligibility assessment, and final thematic inclusion. Each retained study was mapped to at least one defense-relevant technology cluster: maritime domain awareness, AIS analytics, satellite/SAR/optical surveillance, autonomous and unmanned systems, maritime cyber security, or human-machine cooperation. This procedure ensures that the synthesis is traceable from search terms to thematic findings.

Studies were included if they met four criteria. First, the study addressed a maritime, naval, coast-guard, port-security, or maritime security context. Second, it discussed a defense-relevant technology such as AIS analytics, satellite surveillance, unmanned vehicles, autonomous ships, cyber security, artificial intelligence, sensor fusion, or undersea systems. Third, it was published in a peer-reviewed journal or high-quality scholarly outlet indexed in, or verifiable through, Scopus or Web of Science. Fourth, it provided conceptual, empirical, technical, review, or modelling insights relevant to maritime defence capability.

Studies were excluded when they focused only on commercial shipping efficiency without defense or security relevance, provided only marketing or vendor descriptions, lacked sufficient methodological or technical detail, were not in English, or addressed general military technology without a maritime component. Conference papers were used only for contextual background where they were influential, while the core synthesis prioritized journal articles and review papers.

For each eligible study, the following information was extracted: author and year, title, journal, DOI, technology category, maritime defense function, methodological approach, main contribution, limitations, and future research implications. Quality appraisal considered methodological transparency, relevance to maritime defense, technological specificity, strength of evidence, operational realism, and contribution to cumulative knowledge. In defense-oriented reviews, studies should not be judged only by statistical methods; engineering design, simulation realism, operational assumptions, cyber resilience, and security implications are also important.

3. RESULTS AND DISCUSSION

3.1. Results

3.1.1. Thematic Structure of the Literature

The literature review can be organized into six major clusters. The first cluster includes data-driven MDA and sensor fusion. This cluster focuses on integrating AIS, radar, satellite AIS, SAR, optical imagery, radio frequency signals, and contextual intelligence to identify vessels, monitor routes, detect suspicious behavior, and support maritime security decisions. It is foundational because maritime defense depends on knowing what is happening across vast maritime spaces.

The second cluster is AIS analytics and anomaly detection. This study uses vessel-tracking data to identify route deviations, suspicious loitering, spoofing, dark vessel behavior, abnormal speed, irregular port calls, and other behavioral patterns. Machine learning and deep learning have become central, although many studies remain constrained by limited labels, inconsistent benchmarking and weak operational validation. The third cluster includes satellite, optical, and SAR surveillance. This shows how space-based technologies overcome the limitations of terrestrial sensors but also require fusion and timely processing to produce actionable intelligence.

The fourth cluster is autonomous and unmanned maritime systems, including USVs, UUVs, AUVs, and autonomous surface ships. These platforms support surveillance, mine countermeasures, reconnaissance, environmental assessments, and operations in dangerous or denied areas. The fifth cluster is maritime cyber security, which focuses on threats to ship systems, navigation systems, AIS, port infrastructure, IoT-enabled architectures, and autonomous maritime platforms. The sixth cluster is human-machine cooperation, safety, and governance, which addresses how operators, commanders, autonomous systems, algorithms, and regulatory frameworks interact (see Table 2).

Table 2. Thematic Clusters in Maritime Defense Technology Research

Cluster	Defense function	Representative sources
MDA and sensor fusion	Wide-area visibility, cueing, cross-source validation	Soldi et al. (2021); Kanjir et al. (2018)
AIS analytics	Trajectory prediction, anomaly detection, vessel behavior analysis	Pallotta et al. (2013); Tu et al. (2018); Wolsing et al. (2022)
Autonomous systems	Surveillance, mine countermeasures, patrol, risk reduction	Bovio et al. (2006); Liu et al. (2016); Bai et al. (2022)
Cyber resilience	Protection of navigation, communications, IoT, and autonomous systems	Farah et al. (2022); Ashraf et al. (2023); Tabish & Chaur-Luh (2024)
Human-machine cooperation	Trust, oversight, safety, accountability, command integration	Chaal et al. (2023)

Note:
The clusters synthesize technologies and functions across defense-relevant maritime research.

3.1.2. Maritime Domain Awareness as a Systems-of-Systems Capability

MDA is the foundation of maritime defence technology. It refers to the ability to collect, integrate, interpret, and act on information about vessels, maritime activities, environmental conditions, infrastructure, and threats. The literature shows that MDA is no longer merely a surveillance function of the military. It has become an integrated data and decision-making capability. A modern MDA architecture must connect sensors, databases, analysts, command systems, and response assets across multiple agencies and operational domains.

Traditional maritime surveillance depended heavily on coastal radar, patrol vessels, human reporting, and AIS. Although these tools remain important, they are insufficient for wide-area, persistent, and

contested maritime monitoring. Soldi et al. (2021) argued that ground-based radar and AIS do not provide comprehensive global coverage, especially in open-ocean regions, making satellite-based surveillance essential. This finding is highly relevant for defence because adversarial or non-compliant actors may deliberately avoid detection by switching off the AIS, manipulating identifiers, operating outside the coastal radar range, or exploiting weather and traffic density.

The literature also shows that MDA increasingly depends on data fusion. However, no single data source is sufficient. The AIS provides cooperative vessel identity and movement data; however, it is vulnerable to manipulation and absence. SAR can detect metallic objects and operate through cloud cover and darkness; however, classification can be difficult. Optical imagery can support visual identification and classification; however, it is constrained by weather and illumination. Coastal radar provides local persistence but not a global reach. Human intelligence, port records, vessel registries, and commercial shipping data can enrich interpretation but may be incomplete or delayed in reporting.

The defence implication is clear: maritime security organizations should treat MDA as an integrated architecture, not a collection of separate sensors. The most valuable capability arises from combining heterogeneous sources and detecting inconsistencies among them. For example, an AIS track showing a fishing vessel moving normally may become suspicious when SAR imagery shows additional non-reporting vessels nearby or when port-call history and route behavior deviate from known patterns. This form of cross-source reasoning is especially important in gray-zone maritime activity, where actors may avoid overt military behavior while exploiting ambiguities.

A systems-of-systems approach also changes procurement and organizational designs. Rather than purchasing stand-alone sensors, defense agencies must invest in interoperable data platforms, standards, secure communication links, data governance, and trained analysts. Therefore, technology acquisition must be linked to information architecture and operational doctrine. The literature suggests that future MDA research should focus on the fusion of AIS, SAR, optical, radar, cyber, and contextual intelligence into explainable decision support tools.

3.1.3. AIS-Based Anomaly Detection and Predictive Intelligence

The AIS is one of the most studied data sources in maritime technology research. The AIS broadcasts vessel identity, position, speed, course, and voyage-related information. Although originally designed for collision avoidance and maritime safety, AIS data have become central to maritime intelligence, traffic analysis, anomaly detection, and predictive modelling. Pallotta et al. (2013) provided an early influential framework for vessel pattern knowledge discovery, anomaly detection and route prediction. Tu et al. (2018) later reviewed AIS data use for intelligent maritime navigation, showing the development of methods from raw data handling to higher-level analytics.

In maritime defense, AIS analytics can support at least five functions. First, it can identify abnormal vessel routes, such as deviations from the expected lanes. Second, it can detect suspicious behaviors, such as loitering, rendezvous patterns, sudden speed changes, and irregular port calls. Third, it can support the prediction of vessel destinations and future trajectories. Fourth, it can help prioritize surveillance resources by identifying vessels of interest. Fifth, it can support historical investigations after incidents by reconstructing activity patterns and comparing them with known traffic behaviors.

Machine learning and deep learning have expanded the predictive capacity of AIS data analytics. Li et al. (2023) examine AIS data-driven ship trajectory prediction using machine learning and deep learning methods, while Zhang et al. (2022) review vessel trajectory prediction approaches in maritime transportation. Yang et al. (2024) provide a recent comprehensive review of machine learning for AIS data-driven maritime research. These studies show that AI can transform the AIS from a passive tracking system into a predictive intelligence capability. Prediction is valuable for maritime defense because it can support early warning, sensor tasking, interdiction planning, and risk-based patrol allocation.

However, AIS-based maritime defense has its limitations. The AIS is cooperative; vessels can disable transmitters, spoof identities, report false positions, or manipulate voyage information. Androjna et al. (2021) demonstrated AIS data vulnerability through a spoofing case study and recommended stronger navigation data assurance. Amro et al. (2022) similarly address navigation data anomaly analysis and

detection, reflecting growing concern about the reliability of digital navigation data. These vulnerabilities imply that AIS should not be treated as a trusted source by default. However, it must be validated against other sensors and contextual information.

The second limitation is the difficulty in defining anomalies. In commercial traffic, unusual behavior may be observed. Fishing vessels, tugboats, research vessels, naval vessels, and emergency response crafts may naturally behave differently from merchant ships. Therefore, maritime anomaly detection requires context reasoning. An algorithm that identifies statistical deviations does not automatically identify hostile behavior. Defense applications require the combination of behavioral models with intelligence, geography, vessel type, weather, port history, operational context, and analyst judgement.

Third, the benchmarking process is a limitation. Many AIS anomaly studies use different datasets, time periods, geographic areas and evaluation metrics. This makes comparisons difficult. The field requires shared benchmark datasets, adversarial test cases, labelled anomalies, and operational validation with maritime security agencies. Without these, algorithms may perform well in academic settings but fail in more challenging environments. This gap is especially significant for defense because adversaries actively adapt their behavior in response to being surveilled.

3.1.4. Satellite, SAR, and Optical Surveillance

Space-based surveillance is a major pillar of modern maritime defence technology. Satellite systems extend maritime awareness beyond coastal infrastructure and allow the monitoring of open-ocean, polar, remote, and contested areas. The literature identifies several major satellite technologies: satellite AIS, SAR, optical imagery, radio frequency detection, and emerging techniques such as global navigation satellite system reflectometry. Each technology contributes to a different form of visibility in the maritime domain.

Soldi et al. (2021) described space-based global maritime surveillance as crucial for search and rescue, fisheries monitoring, pollution control, law enforcement, migration monitoring, national security, and wider maritime situational awareness. Although many of these applications are civilian or dual-use, they are directly relevant to defense because navies and coast guards operate in the same maritime information environments. A vessel involved in illegal fishing, sanctions evasion, gray-zone coercion, or suspicious rendezvous behavior may require both law enforcement and defense responses.

SAR has particular defense value because it can operate in the dark and through cloud cover. It can detect vessels that are not transmitting AIS and can support the identification of dark maritime activity. However, SAR imagery requires specialized processing, and vessel classification may be difficult depending on the image resolution, sea state, vessel size, and sensor geometry. Optical imagery is useful for vessel classification and visual verification. Kanjir et al. (2018) reviewed vessel detection and classification from spaceborne optical images and noted that optical approaches are growing rapidly, although they remain constrained by clouds, haze, solar angle, and sensor characteristics.

For maritime defense, satellite surveillance supports various missions. It can help detect illegal fishing fleets, monitor sanctions evasion, track suspicious tanker activity, support naval intelligence preparation of the environment, monitor strategic chokepoints and cue patrol aircraft or surface vessels. It is also valuable for archipelagic and large maritime states, where physical patrol coverage is expensive and incomplete. In such contexts, satellite surveillance can reduce uncertainty and help allocate scarce patrol resource.

The future of satellite-enabled maritime defense lies in lower latency, higher revisit rates, AI-enabled image processing, and fusion with the AIS and other data. The main research gap is not merely detecting vessels in images but producing actionable, timely, and explainable intelligence. Defense users require systems that can answer operational questions, such as which vessels are suspicious. Why? What is the confidence level? What additional sensors should be used? What response options are available? Therefore, the literature points toward integrated satellite intelligence workflows rather than stand-alone image classification.

3.1.5. Autonomous and Unmanned Maritime Systems

Unmanned maritime vehicles are among the most visible forms of maritime defence technology. These include USVs, UUVs, AUVs, and maritime autonomous surface vehicles. Their value lies in their persistence, risk reduction, distributed sensing, cost-effectiveness, and ability to operate in hazardous areas. Early research on AUVs identified scientific and naval applications, including mine countermeasures and rapid environmental assessments (Bovio et al., 2006). These missions remain central because they are dangerous, time-consuming, and sensor intensive.

USVs have rapidly developed. Liu et al. (2016) reviewed USV developments and challenges, while Campbell et al. (2012) focused on intelligent collision avoidance. Bai et al. (2022) reviewed the current research and advances in USVs, and Er et al. (2023) examined intelligent motion control. Bae and Hong (2023) emphasized the importance of intelligence and cooperation among unmanned marine vehicles, reflecting the shift from individual platforms to cooperative systems. The literature shows a progression from platform development to autonomous behavior, cooperation, and mission integration.

For maritime defense, USVs can support harbor security, patrol, surveillance, electronic sensing, antisubmarine support, mine countermeasures, decoy operations, and logistics. UUVs and AUVs can support seabed mapping, undersea surveillance, mine detection, environmental sensing, and covert intelligence collection missions. The operational value is strongest when unmanned systems are integrated into a wider architecture of sensors, communications, command systems and human oversight. A single unmanned vehicle is a platform, and a coordinated set of unmanned vehicles connected to MDA and command systems is a capability.

However, autonomy introduces operational and managerial challenges that must be addressed. Autonomous vessels must navigate complex maritime environments, comply with collision-avoidance rules, communicate reliably, resist cyber interference, and make decisions under uncertainty. In military environments, these challenges become more severe because adversaries may jam communications, spoof sensors, use decoys, attack control links, or exploit the rules of engagement. Therefore, defense applications require robust autonomy that can operate under degraded and contested conditions, not merely autonomy that performs in benign test environments.

The literature also shows that autonomy is not a single capability. These capabilities include perception, localization, path planning, collision avoidance, mission planning, communication, cooperation, fault detection, and human oversight. A defense organization that buys an unmanned platform without investing in the data, communication, cyber, maintenance, training, and doctrine ecosystems will not obtain full operational value. This insight is particularly relevant to management research because technological adoption depends on organizational readiness and engineering maturity.

3.1.6. Maritime Cyber Security and Cyber-Physical Resilience

Maritime defense technology is increasingly cyber-physical in nature. Ships, ports, navigation systems, sensors, command systems, autonomous vehicles, and surveillance platforms are connected through digital networks. This connectivity creates operational efficiency but also vulnerability to cyberattacks. Farah et al. (2022) provide a systematic survey of maritime cyber security, highlighting recent advances and future trends. Ashraf et al. (2023) focused on cyber security threats in the IoT-enabled maritime industry, while Zhang et al. (2020) examined maritime IoT from architectural and radio-spectrum perspectives. Tabish and Chaur-Luh (2024) reviewed the cyber security challenges, countermeasures, and future perspectives for maritime autonomous surface ships.

The literature shows that maritime cyber threats affect both information systems and physical operations of maritime vessels. The AIS spoofing can distort situational awareness. GPS spoofing can mislead navigation systems. Malware can disrupt ship and port operations. Compromised sensors can degrade the autonomous decision-making process. Communication link attacks can isolate unmanned vehicles. Data manipulation can corrupt AI models and decision-support systems. These risks are especially important for defense because maritime systems must remain functional during crises, coercion or conflict.

Cybersecurity cannot be treated as an information technology support function. It must be embedded in the maritime defense architecture, acquisition, training, and doctrine. Cyber resilience should include secure-by-design systems, redundancy, anomaly detection, encrypted communication, authentication, sensor cross-validation, incident response procedures, and cyber exercises. A resilient system should not only prevent compromise but also detect, contain, recover, and continue to perform missions under degraded conditions.

A key gap in the literature is the separation between cybersecurity and autonomy. Many autonomy studies assume that sensors and communications are reliable. Many cybersecurity studies analyze threats but do not deeply model autonomous mission behavior. Future research should examine cyber-physical attacks on autonomous maritime systems, including sensor spoofing, adversarial AI, communication denial, compromised mission updates, and attacks on shore-control infrastructure. This is a high-priority agenda because future maritime defense systems will be both autonomous and networked systems.

3.1.7. Human-Machine Cooperation, Safety, and Governance

As maritime defense technology becomes increasingly autonomous, human-machine cooperation becomes a central issue. Autonomous systems do not remove humans from maritime defense; instead, they change human roles. Operators may shift from direct control to supervision, mission planning, exception handling, interpretation of algorithmic recommendations, and command responsibilities. Chaal et al. (2023) provide a bibliometric review of risk, safety, and reliability research on autonomous ships, showing the growth of safety-related scholarship. Although much of this research is framed around commercial maritime autonomous surface ships, the findings are relevant to defense because naval and coast guard operations involve higher uncertainty, adversarial behavior, and stricter accountability than commercial operations.

Human-machine cooperation in maritime defense involves several questions. How much autonomy should be delegated to unmanned systems? What information should be displayed to the operators? How should systems explain anomaly alerts and route recommendations? How should commanders trust the AI outputs? What happens when AI recommendations conflict with human judgement? Who is accountable when an autonomous system causes damage or escalates an incident? These questions are not only technical but also organizational, legal, and ethical in nature.

The literature suggests that explainability and trust calibration are essential components of AI. Operators should neither blindly trust nor automatically reject the autonomous systems. They require understandable evidence, confidence estimates, alternative explanations, and training. In maritime defense, explainability is particularly important because decisions may involve escalation, interdiction, search and rescue, or military engagement decisions. A black-box alert may be insufficient when commanders must justify their operational actions.

Governance is also important. Maritime defense technology must operate within the framework of international law, national rules of engagement, safety regulations, and ethical constraints. Autonomous systems must be designed such that human authorities can control mission objectives, understand system behavior, and intervene when necessary. This requirement creates an important link between technical design and the organizational governance. This suggests that future research should combine engineering validation with human factors, law, ethics, and defense management.

3.2. Discussion

The synthesis shows that maritime defense technology is evolving from platform-centric capability toward integrated, data-intensive, autonomous, and cyber-resilient systems. This finding has important implications for both research and practice. First, it suggests that the value of maritime defense technology arises from integration. AIS analytics, satellite imagery, unmanned systems, cybersecurity, and human-machine interfaces are not independent domains. They interact through data flows, command decisions, mission planning, and operational responses. A weakness in one domain can degrade the entire system.

Second, the review shows that many technologies are dual-use technologies. AIS analytics, satellite vessel detection, autonomous surface navigation, maritime IoT, and cyber security are relevant to

commercial shipping, environmental monitoring, law enforcement and defence. This creates opportunities for technology transfer but also challenges governance and classification. Defense organizations can benefit from civilian innovation; however, they must adapt technologies to contested, adversarial, and high-consequence contexts. A model that works for traffic safety may not be sufficient for military deception, cyber-attacks, or gray-zone coercion.

Third, the literature highlights a gap between technical performance and operational utility. Many studies have demonstrated detection accuracy, classification performance, trajectory prediction, and control stability. Few studies have examined whether these outputs improve command decisions, reduce response time, allocate resources effectively, or support defensible legal and operational actions. For high-ranking management journals, this gap is important because it connects technology and organizational capability. Maritime defense technology should be studied not only for engineering performance but also for adoption, integration, governance, and strategic management.

3.3. Research Gaps

This review identifies seven major research gaps. The first is the lack of operationally realistic data. Many studies use publicly available AIS data or simulated environments to achieve their objectives. These are valuable but often do not represent contested maritime conditions in the Indo-Pacific region. Defense-relevant datasets should include spoofing, dark vessels, deceptive routing, sensor gaps, jamming, weather effects, multivessel coordination, and adversarial behavior. Shared benchmark datasets would improve the comparability across algorithms.

The second gap is the weak integration between sensor fusion and decision-making. The literature contains strong work on detection, prediction, and classification, but less work on how outputs are translated into operational decisions. Defense agencies require systems that support prioritization, tasking, escalation, and response. Future research should integrate detection algorithms with command and control workflows.

The third gap is the separation of cyber security and autonomy research topics. Autonomous maritime systems rely on sensors, communication, software, and data. Therefore, cyberattacks can affect physical behavior. However, cyber and autonomy studies often remain separate. Future research should examine the cyber-physical resilience of unmanned maritime systems under realistic adversarial conditions.

The fourth gap is the limited explainability of AI systems. AI-enabled maritime surveillance and anomaly detection tools may identify unusual patterns but fail to explain them in operationally useful terms. Defense users require interpretable systems that show why an alert was generated, how confident the system is, and what contextual evidence supports the assessment.

The fifth gap is the underdevelopment of human-machine teaming models. Many studies have focused on platform performance rather than team performance. Future research should examine how commanders, operators, analysts, autonomous systems, and AI tools work together. This includes workload, trust, training, accountability, and the design of interfaces. The sixth gap is the limited research on interoperability and coalition operations. Maritime defense often involves navies, coast guards, customs agencies, port authorities, commercial data providers and international partners. The technology must be interoperable across organizations and jurisdictions. The seventh gap is insufficient attention to maintenance, life cycle, and management. Maritime defense technology is not only an engineering problem; it is also a management, strategy, procurement, and governance issue.

3.4. Future Research Agenda

Future research should focus on integrated, mission-oriented maritime defense technologies. The first direction is resilient MDA architectures that combine AIS, SAR, optical imagery, radar, acoustic sensors, cyber intelligence and contextual data. These architectures should be evaluated under realistic conditions, including missing data, spoofing, sensor disagreement, and communication degradation.

The second direction is the development of defense-relevant benchmark datasets for maritime anomaly detection. These datasets should include normal traffic, suspicious behavior, simulated adversarial deception, AIS manipulation, dark vessel cases, and multisource sensor records. Benchmarking would

allow better comparisons across machine learning approaches and would improve the credibility of algorithmic claims.

The third direction is cyber-secure autonomous maritime systems. This includes secure navigation, authenticated sensor data, resilient communication, intrusion detection, adversarial AI protection, and fail-safe mission behavior. Cybersecurity should be built into autonomy research from the beginning rather than added after platform development.

The fourth direction is human-AI decision-making in maritime defense command centers. This requires experiments, simulations, and field studies involving operators. The objective should be to understand how AI alerts influence judgement, workload, trust, response speed, and decision quality. The fifth direction is management and policy research. Maritime defense technology requires procurement reforms, interoperability standards, data-sharing agreements, workforce development, lifecycle support, and governance frameworks. These topics are particularly suitable for business and management scholarship because they examine how organizations absorb, govern and scale complex digital technologies.

3.5. Managerial and Policy Implications

For defense managers, the review suggests that maritime defense technology should be acquired as an integrated capability portfolio rather than isolated equipment. A navy or maritime security agency that purchases unmanned vehicles without investing in data links, cyber security, maintenance, training, doctrine, and command integration will likely underuse this technology. Therefore, capability planning should consider platforms, data, people, processes, and governance.

Maritime defense technology requires cross-agency coordination for policymakers. Maritime threats often cross the boundaries of defense, law enforcement, customs, fisheries, environmental protection, and port security. Therefore, MDA systems should enable controlled information sharing while also protecting sensitive data. Data governance is as important as sensor acquisition because incomplete or delayed sharing can reduce the value of advanced technologies.

For acquisition officers, the findings support modular and interoperable systems. Because AI, sensors, communications, and cyber threats evolve quickly, closed proprietary systems may create long-term capability risks. Open architectures, common data standards, upgradeable software, and cyber certification are crucial. Maritime defense technology offers opportunities for interdisciplinary work across management, engineering, computer science, defense studies, law, and public policy. Research should not only ask whether a system works technically but also whether it can be governed, trusted, maintained, secured, and integrated into real organizations.

4. CONCLUSION

This structured literature review shows that maritime defense technology is evolving from platform-centric capabilities to integrated, data-intensive, autonomous, and cyber-resilient systems. The most prominent research streams are maritime domain awareness, AIS analytics, satellite surveillance, unmanned maritime vehicles, maritime cyber security, and human-machine cooperation.

Although AIS and machine learning research have advanced maritime anomaly detection and trajectory prediction, operational limitations remain due to spoofing, missing data, limited benchmarks, and contextual ambiguity. Satellite surveillance strengthens wide-area awareness but requires fusion with the AIS, radar, and intelligence sources. Unmanned surface and underwater vehicles offer new options for surveillance, mine countermeasures, and risk reduction; however, they require robust autonomy, communication, cyber protection, and human oversight. Cybersecurity is now central because maritime systems are increasingly connected and software-defined.

The main conclusion of this review is that maritime defense technology should be understood as an integrated socio-technical capability. Its effectiveness depends not only on sensors, algorithms, or platforms but also on data governance, human expertise, organizational readiness, cyber resilience,

interoperability, and strategic management. Therefore, future research should connect technical performance with defense management, operational doctrine, and governance.

Ethical Approval

Not Applicable

Informed Consent Statement

Not Applicable

Authors' Contributions

Not Applicable

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Data Availability Statement

The data presented in this study are available on request from the corresponding author due to privacy reasons.

Funding

This study did not receive any external funding.

Notes on Contributors

Dimvy Rusefani Asetya
https://orcid.org/0009-0004-5569-5863
Dimvy Rusefani Asetya is affiliated with the Faculty of Agriculture, Jember University, Jember.

REFERENCES

Amro, A., Oruc, A., Gkioulos, V., & Katsikas, S. (2022). Navigation data anomaly analysis and detection. *Information, 13*(3), Article 104. https://doi.org/10.3390/info13030104

Androjna, A., Perkovič, M., Pavić, I., & Mišković, J. (2021). AIS data vulnerability indicated by a spoofing case-study. *Applied Sciences, 11*(11), Article 5015. https://doi.org/10.3390/app11115015

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2023). A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678

Bae, I., & Hong, J. (2023). Survey on the developments of unmanned marine vehicles: Intelligence and cooperation. *Sensors, 23*(10), Article 4643. https://doi.org/10.3390/s23104643

Bai, X., Li, B., Xu, X., & Xiao, Y. (2022). A review of current research and advances in unmanned surface vehicles. *Journal of Marine Science and Application, 21*, 47–58. https://doi.org/10.1007/s11804-022-00276-9

Bovio, E., Cecchi, D., & Baralli, F. (2006). Autonomous underwater vehicles for scientific and naval operations. *Annual Reviews in Control, 30*(2), 117–130. https://doi.org/10.1016/j.arcontrol.2006.08.003

Campbell, S., Naeem, W., & Irwin, G. W. (2012). A review on improving the autonomy of unmanned surface vehicles through intelligent collision avoidance manoeuvres. *Annual Reviews in Control, 36*(2), 267–283. https://doi.org/10.1016/j.arcontrol.2012.09.008

Chaal, M., Ren, X., BahooToroody, A., Basnet, S., Bolbot, V., Valdez Banda, O. A., & van Gelder, P. (2023). Research on risk, safety, and reliability of autonomous ships: A bibliometric review. *Safety Science, 167*, Article 106256. https://doi.org/10.1016/j.ssci.2023.106256

Er, M. J., Ma, C., Liu, T., & Gong, H. (2023). Intelligent motion control of unmanned surface vehicles: A critical review. *Ocean Engineering, 280*, Article 114562. https://doi.org/10.1016/j.oceaneng.2023.114562

Farah, M. A. B., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information, 13*(1), Article 22. https://doi.org/10.3390/info13010022

Kanjir, U., Greidanus, H., & Oštir, K. (2018). Vessel detection and classification from spaceborne optical images: A literature survey. *Remote Sensing of Environment, 207*, 1–26. https://doi.org/10.1016/j.rse.2017.12.033

Li, H., Jiao, H., & Yang, Z. (2023). AIS data-driven ship trajectory prediction modelling and analysis based on machine learning and deep learning methods. *Transportation Research Part E: Logistics and Transportation Review, 175*, Article 103152. https://doi.org/10.1016/j.tre.2023.103152

Liu, Z., Zhang, Y., Yu, X., & Yuan, C. (2016). Unmanned surface vehicles: An overview of developments and challenges. *Annual Reviews in Control, 41*, 71–93. https://doi.org/10.1016/j.arcontrol.2016.04.018

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., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, Article n71. https://doi.org/10.1136/bmj.n71

Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction. *Entropy, 15*(6), 2218–2245. https://doi.org/10.3390/e15062218

Ribeiro, C. V., Paes, A., & de Oliveira, D. (2023). AIS-based maritime anomaly traffic detection: A review. *Expert Systems with Applications, 231*, Article 120561. https://doi.org/10.1016/j.eswa.2023.120561

Riveiro, M., Pallotta, G., & Vespe, M. (2018). Maritime anomaly detection: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8*(5), Article e1266. https://doi.org/10.1002/widm.1266

Soldi, G., Gaglione, D., Forti, N., Di Simone, A., Daffinà, F. C., Bottini, G., Quattrociocchi, D., Millefiori, L. M., Braca, P., Carniel, S., Willett, P., Iodice, A., Riccio, D., & Farina, A. (2021). Space-based global maritime surveillance. Part I: Satellite technologies. *IEEE Aerospace and Electronic Systems Magazine, 36*(9), 8–28. https://doi.org/10.1109/MAES.2021.3070862

Tabish, N., & Chaur-Luh, T. (2024). Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access, 12*, 17114–17136. https://doi.org/10.1109/ACCESS.2024.3357082

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Tu, E., Zhang, G., Rachmawati, L., Rajabally, E., & Huang, G.-B. (2018). Exploiting AIS data for intelligent maritime navigation: A comprehensive survey from data to methodology. *IEEE Transactions on Intelligent Transportation Systems, 19*(5), 1559–1582. https://doi.org/10.1109/TITS.2017.2724551

Wang, S., Zhong, E., Lu, H., Guo, H., & Long, L. (2015). An effective algorithm for lines and polygons overlay analysis using uniform spatial grid indexing. In *2015 2nd IEEE International Conference on*

Spatial Data Mining and Geographical Knowledge Services (ICSDM) (pp. 175–179). IEEE. https://doi.org/10.1109/ICSDM.2015.7298048

Wolsing, K., Roepert, L., Bauer, J., & Wehrle, K. (2022). Anomaly detection in maritime AIS tracks: A review of recent approaches. *Journal of Marine Science and Engineering, 10*(1), Article 112. https://doi.org/10.3390/jmse10010112

Yang, Y., Liu, Y., Li, G., Zhang, Z., & Liu, Y. (2024). Harnessing the power of machine learning for AIS data-driven maritime research: A comprehensive review. *Transportation Research Part E: Logistics and Transportation Review, 183*, Article 103426. https://doi.org/10.1016/j.tre.2024.103426

Zhang, J., Wang, M. M., Xia, T., & Wang, L. (2020). Maritime IoT: An architectural and radio spectrum perspective. *IEEE Access, 8*, 93109–93122. https://doi.org/10.1109/ACCESS.2020.2990830

Zhang, X., Fu, X., Xiao, Z., Xu, H., & Qin, Z. (2022). Vessel trajectory prediction in maritime transportation: Current approaches and beyond. *IEEE Transactions on Intelligent Transportation Systems, 23*(11), 19980–19998. https://doi.org/10.1109/TITS.2022.3192574