*electronics*

MDPI

*Review*

# Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies

**Tymoteusz Miller [1,2,*], Irmina Durlik [2,3], Ewelina Kostecka [2,4], Sylwia Sokołowska [2], Polina Kozlovska [5] and Rafał Zwolak [2]**

[1] Institute of Marine and Environmental Sciences, University of Szczecin, 71-415 Szczecin, Poland
[2] Polish Society of Bioinformatics and Data Science BioData, 71-214 Szczecin, Poland; i.durlik@pm.szczecin.pl (I.D.); e.kostecka@pm.szczecin.pl (E.K.); ssokolowska@ums.gov.pl (S.S.); tymoteuszmiller@ptbd-biodata.org (R.Z.)
[3] Faculty of Navigation, Maritime University of Szczecin, 70-500 Szczecin, Poland
[4] Faculty of Mechatronics and Electrical Engineering, Maritime University of Szczecin, 71-650 Szczecin, Poland
[5] Faculty of Economics, Finance And Management, University of Szczecin, 71-101 Szczecin, Poland; 231805@stud.usz.edu.pl
* Correspondence: tymoteusz.miller@usz.edu.pl

**Abstract:** The maritime industry is undergoing a digital transformation, integrating automation, artificial intelligence (AI), and the Internet of Things (IoT) to enhance operational efficiency and safety. However, this technological evolution has also increased cybersecurity vulnerabilities, exposing vessels, ports, and maritime communication networks to sophisticated cyber threats. This systematic review, conducted following the PRISMA guidelines, examines the current landscape of AI-driven cybersecurity solutions in maritime environments. By analyzing peer-reviewed studies and industry reports, this review identifies key AI methodologies, including machine-learning-based intrusion detection systems, anomaly detection mechanisms, predictive threat modeling, and AI-enhanced zero-trust architectures. This study assesses the effectiveness of these techniques in mitigating cyber risks, explores their implementation challenges, and highlights existing research gaps. The findings indicate that AI-powered solutions significantly enhance real-time threat detection and response capabilities in maritime networks, yet issues such as data scarcity, regulatory constraints, and adversarial attacks on AI models remain unresolved. Future research directions should focus on integrating AI with blockchain, federated learning, and quantum cryptographic techniques to strengthen maritime cybersecurity frameworks.

**Keywords:** artificial intelligence; cybersecurity; maritime industry; intrusion detection; machine learning; anomaly detection; autonomous ships; digital transformation; zero trust; cyber threats; maritime networks; federated learning; blockchain; quantum cryptography



Academic Editors: Irfan Awan, Amna Qureshi and Muhammad Shahwaiz Afaqui

Received: 28 February 2025
Revised: 23 April 2025
Accepted: 28 April 2025
Published: 30 April 2025

**Citation:** Miller, T.; Durlik, I.; Kostecka, E.; Sokołowska, S.; Kozlovska, P.; Zwolak, R. Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies. *Electronics* **2025**, *14*, 1844. https://doi.org/10.3390/electronics14091844



## 1. Introduction

The maritime industry, a cornerstone of global trade and logistics, is undergoing a profound digital transformation driven by artificial intelligence (AI), automation, and interconnected systems that redefine maritime operations. Technologies such as the Internet of Things (IoT) [1], autonomous ships, smart ports, and cloud-based fleet monitoring have significantly optimized operations such as shipping routes, cargo tracking, and fuel consumption. Yet, this digital evolution has simultaneously expanded the threat landscape, introducing unprecedented cybersecurity vulnerabilities that expose critical maritime

infrastructure to cyberattacks capable of disrupting global supply chains, compromising navigational safety, and causing severe financial and environmental consequences [2].

Maritime networks rely on a complex ecosystem of satellite communications [3], ship-to-shore data exchanges, and remote monitoring systems [4]. The increased connectivity has widened the attack surface, making the sector vulnerable to ransomware, GPS spoofing, denial-of-service (DoS) attacks, and unauthorized intrusions targeting ship control systems. In particular, the integration of AI in maritime cybersecurity has emerged as both a critical safeguard—enabling automation and real-time threat detection—and a potential vulnerability due to its susceptibility to adversarial manipulation and data privacy risks. AI-driven cybersecurity solutions, including machine-learning-based intrusion detection systems (IDSs), anomaly detection frameworks [5], and predictive threat analytics, offer the potential to automate threat detection [6], improve response times, and reduce human intervention. However, these benefits are counterbalanced by challenges such as adversarial attacks on AI models, regulatory constraints, and limitations in maritime-specific datasets.

Despite the growing body of research on AI applications in cybersecurity, there is a lack of systematic analysis focused on how AI technologies are specifically applied in maritime environments. The existing literature has largely emphasized traditional cybersecurity measures, with limited exploration of AI-driven approaches tailored to the unique constraints of the maritime domain, such as unreliable network connectivity, operational latency, and the need for real-time decision making in dynamic conditions [5–7].

This study aims to address this gap by conducting a systematic review of AI-based cybersecurity strategies in maritime environments, following the PRISMA methodology. The primary objectives of this review are to (1) identify the key AI techniques employed in maritime cybersecurity, (2) assess their effectiveness in detecting and mitigating cyber threats, (3) examine the challenges associated with AI adoption in maritime security, and (4) propose future research directions for strengthening cybersecurity resilience in the maritime domain. These objectives structure the analysis and are directly addressed in the discussion section to ensure a clear alignment between research questions and findings.

## 2. Methods

This systematic review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a rigorous and transparent synthesis of the existing research on AI-driven cybersecurity solutions in the maritime sector. The methodology includes a structured approach to study selection, data extraction, and analysis to assess the effectiveness of AI-based cybersecurity solutions in maritime networks.

### *2.1. Study Design*

A systematic literature review (SLR) approach was adopted to identify, evaluate, and synthesize the relevant studies on AI applications in maritime cybersecurity. The focus was placed on peer-reviewed journal articles, conference papers, and industry reports discussing AI-driven security measures, including intrusion detection, anomaly detection [8], zero-trust architectures, and predictive threat modeling in maritime environments [9]. This review aims to provide a comprehensive overview of the existing knowledge base while highlighting key research gaps.

### *2.2. Eligibility Criteria*

The selection of studies was guided by specific inclusion and exclusion criteria. Studies were included if they explicitly discussed the use of AI for cybersecurity in maritime networks, focusing on AI-driven solutions such as machine learning, deep learning, reinforcement learning, or AI-enhanced blockchain security. Only papers published in peer-

reviewed journals or high-quality conference proceedings between 2015 and 2025 were considered. Additionally, selected studies needed to provide empirical evaluations, case studies, or simulations of AI-driven cybersecurity mechanisms in maritime environments.

Studies were excluded if they did not specifically address maritime cybersecurity or if they focused solely on traditional, non-AI cybersecurity methods. Papers lacking a clear methodological framework, technical implementation details, or significant contributions to the field were not considered. Duplicate or low-quality publications were also omitted to maintain the review's integrity.

### 2.3. Search Strategy

A systematic search was conducted using reputable academic databases, including IEEE Xplore, Scopus, Web of Science, and Google Scholar. The search strategy incorporated a combination of keywords and Boolean operators to ensure comprehensive coverage of the literature. Search queries included terms such as "artificial intelligence in maritime cybersecurity", "AI-driven intrusion detection in maritime networks", "machine learning for cyber threat detection in shipping", and "blockchain-enhanced maritime cybersecurity". The search was refined by applying filters for publication years, peer-reviewed sources, and subject areas related to AI, cybersecurity, and maritime studies.

To ensure a robust dataset, additional sources such as industry white papers, technical reports, and government publications were examined. Reference lists of key papers were manually screened to identify additional relevant studies that may not have surfaced through database searches.

### 2.4. Study Selection and Data Extraction

The study selection process followed a multi-step approach. First, an initial screening of titles and abstracts was conducted to eliminate irrelevant studies. The remaining papers were assessed in detail, with full-text reviews performed to determine their alignment with the inclusion criteria. Any discrepancies in the selection process were resolved through discussion among the reviewers to ensure consensus.

For data extraction, a standardized template was used to collect relevant information, including study objectives, AI techniques employed, datasets used, evaluation metrics, key findings, and identified challenges. Information on the methodological rigor and potential biases of each study was also documented.

### 2.5. Data Analysis

A qualitative synthesis of the extracted data was performed to identify common AI techniques used in maritime cybersecurity, assess their effectiveness, and highlight existing research gaps. Studies were categorized based on the specific AI methodologies employed, such as supervised learning for threat detection, unsupervised learning for anomaly detection, and reinforcement learning for adaptive cybersecurity measures. Additionally, an assessment of bias and study limitations was conducted to ensure the reliability of findings.

A PRISMA flow diagram (Figure 1) was generated to illustrate the study selection process, detailing the number of records identified, screened, included, and excluded at each stage. The final dataset was systematically analyzed to derive insights into the current state of AI-driven maritime cybersecurity and its future research directions.

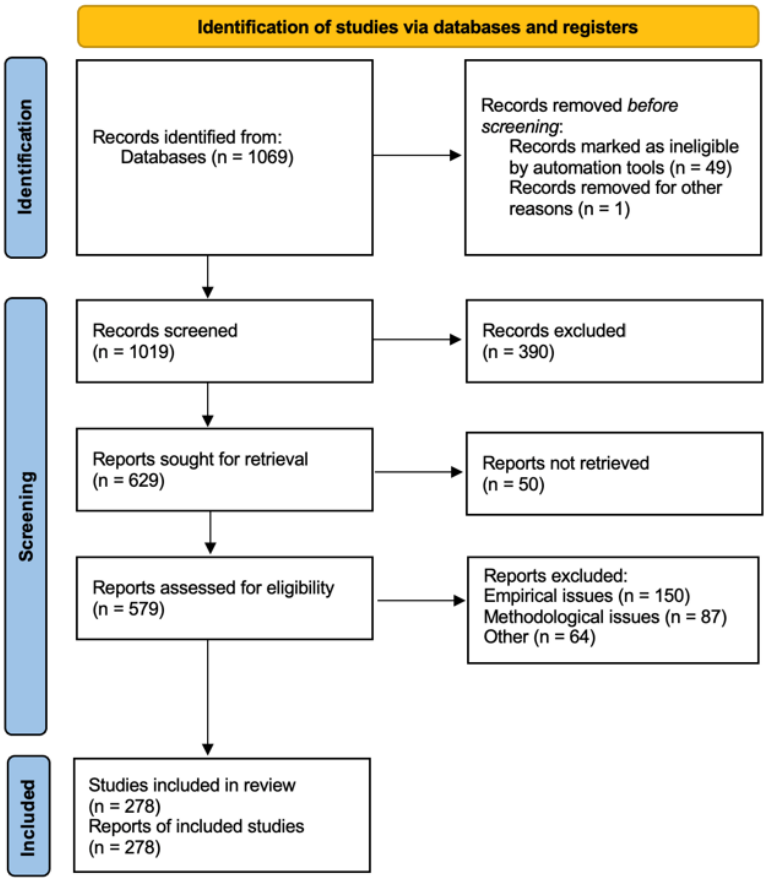


**Figure 1.** PRISMA flow diagram.

## 3. Results

### *3.1. Study Selection Process*

The systematic search across academic databases identified an initial set of 1069 articles. After applying document-type restrictions, focusing on conference papers and journal articles, and limiting the subject areas to computer science, engineering, and decision sciences, the dataset was refined to 695 articles. Further filtering based on specific cybersecurity and AI-related keywords, such as network security, anomaly detection, intrusion detection, blockchain, zero trust, and maritime cybersecurity, resulted in a more focused selection of articles. A thorough title and abstract screening followed by a full-text assessment led to the final selection of highly relevant studies investigating AI-driven cybersecurity applications within the maritime sector.

A citation analysis of the selected articles revealed a steady increase in research impact over the past decade, with a total citation count of 7006. Studies published before 2024 accounted for 6690 citations, while an additional 316 citations were recorded in 2024 alone. The growing citation trend reflects the increasing significance of AI-driven cybersecurity solutions in maritime environments as researchers and industry experts continue to address the rising threat landscape in digitalized maritime operations (Figure 2).

A closer examination of publication trends over time highlights the growing interest in AI-driven maritime cybersecurity research. Prior to 2014, no significant contributions were recorded, but from 2015 onward, the number of publications began to increase, with 21 articles that year, followed by 26 in 2016 and 36 in 2017. The research trajectory accelerated between 2018 and 2020, with 54, 77, and 78 publications, respectively, signaling an increasing recognition of cybersecurity risks in maritime communication and navigation systems. A noticeable surge occurred from 2021 onward, with 76 publications in that year,

followed by a sharp increase to 106 in 2022. The number of publications peaked in 2023 with 167 articles, and early 2024 data indicate that this trend is continuing, with 167 publications already recorded. This sustained growth underscores the rising importance of AI-driven solutions in maritime cybersecurity, particularly in response to the increasing adoption of autonomous shipping, smart port infrastructures, and AI-powered threat mitigation systems (Figure 3).

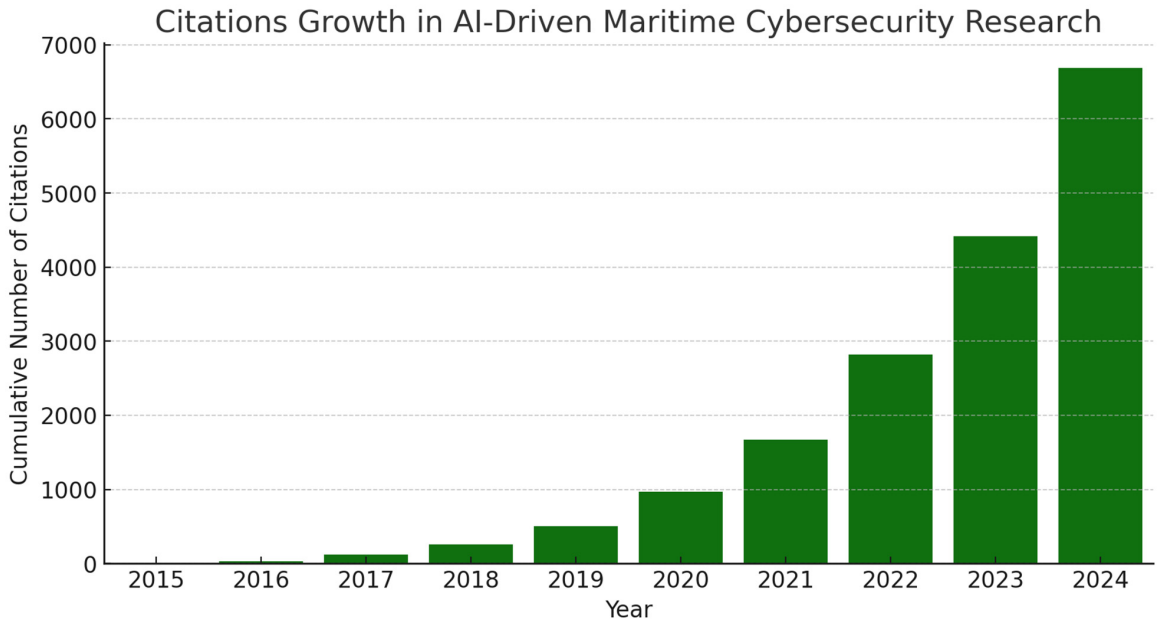


**Figure 2.** Citation growth over time.

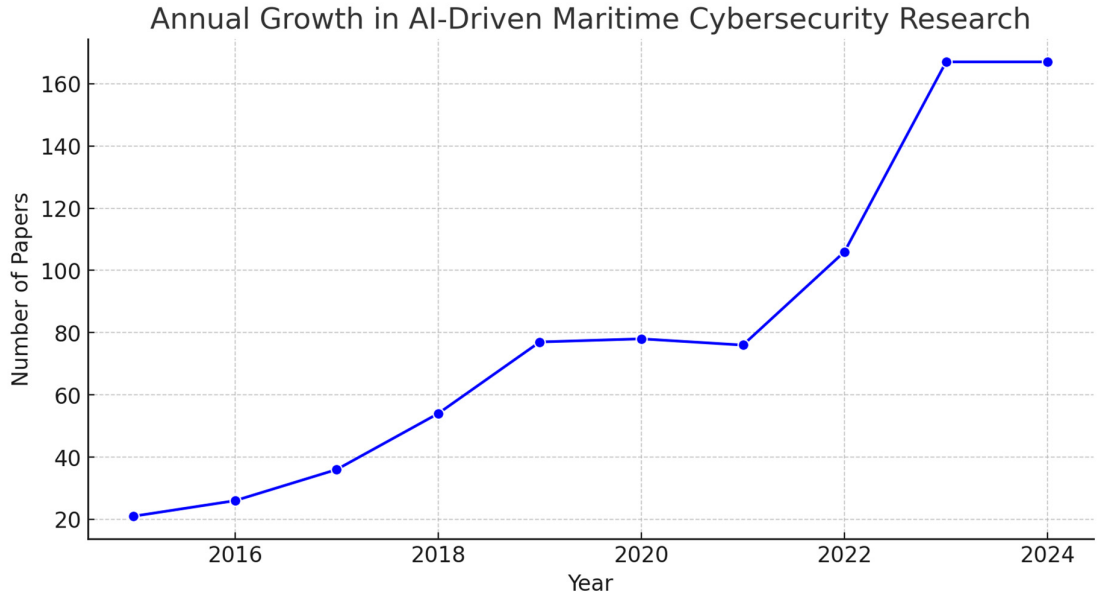


**Figure 3.** Papers published in the period 2015–2024.

The geographical distribution of research contributions reveals that China and the United States lead in terms of publication volume, with 157 and 107 articles, respectively. The United Kingdom follows with 59 publications, while India, Italy, Norway, and Germany also contribute significantly to the field. Norway's involvement in maritime cybersecurity research stands out, likely due to its strong focus on autonomous shipping technologies and smart maritime infrastructure. Emerging research activity is also evident in Poland,

which contributed 14 publications, reflecting its growing engagement in European maritime cybersecurity initiatives (Figure 4).

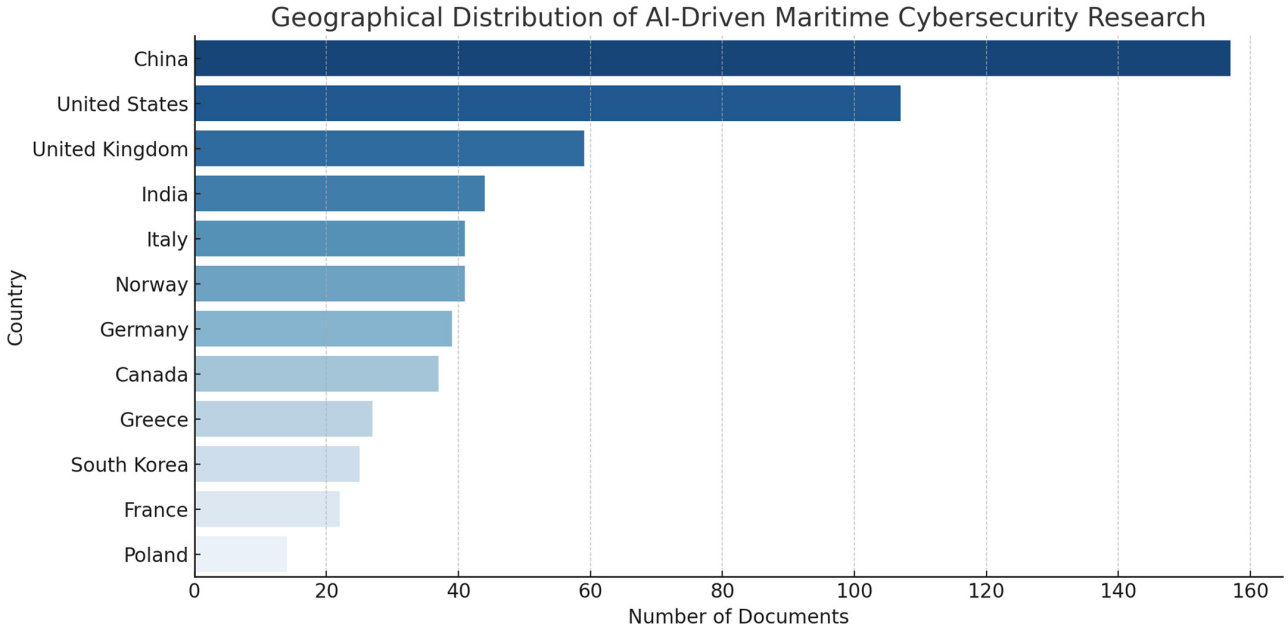


**Figure 4.** Geographical distribution of AI-driven maritime cybersecurity research.

The format in which research is disseminated provides further insight into the field's maturity. A substantial portion of the publications, totaling 401 documents, consists of conference papers, indicating that many studies in this area are still in the exploratory and experimental phase. The prominence of conference papers suggests that AI-driven cybersecurity for maritime applications is a rapidly evolving research domain, with new methodologies frequently being presented before undergoing full-scale validation. In contrast, 261 documents are peer-reviewed journal articles, demonstrating a more established body of knowledge and rigorous empirical contributions. The relatively lower number of journal publications compared to conference papers indicates that many AI-driven cybersecurity models are still in development and have yet to transition into large-scale, real-world implementations (Figure 5).

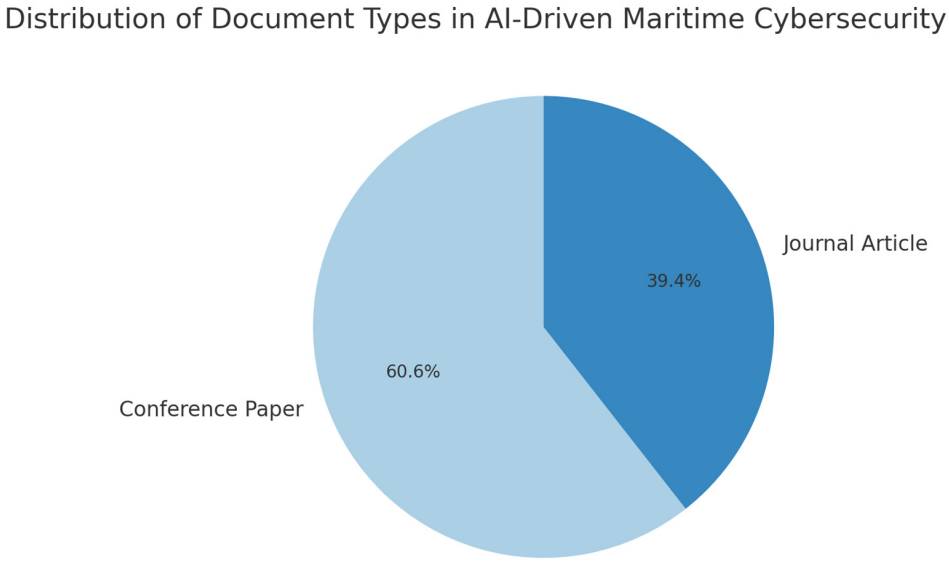


**Figure 5.** Distribution of documents.

### *3.2. Overview of Selected Studies*

The final dataset consists of research papers that investigate a wide range of AI-based techniques for cybersecurity in maritime environments. The studies cover methodologies such as machine learning [10], deep learning [11], reinforcement learning [12], blockchain security, and zero-trust architectures, with applications in autonomous ships [13,14], smart ports, maritime logistics [15], and ship-to-shore communications [16]. A significant portion of the literature focuses on anomaly detection in maritime networks [17], where AI models have been trained to identify cyber threats in automatic identification systems (AISs) [18,19], vessel communication channels, and satellite-based maritime navigation systems [20]. Deep learning techniques [21], including convolutional neural networks (CNNs) and recurrent neural networks (RNNs) [22], frequently appear in studies related to maritime threat prediction [23] and attack detection [24,25]. Several works introduce hybrid AI models that combine supervised [26] and unsupervised learning [27–29] approaches to enhance the accuracy and efficiency of intrusion detection in maritime cybersecurity frameworks [30,31].

Among the reviewed articles, research focusing on cyber risk assessment for autonomous ships has gained increasing attention. Many of these studies emphasize the vulnerabilities of unmanned maritime systems to cyberattacks [32–34] and propose AI-enhanced security models capable of continuously monitoring network activity, predicting potential security breaches [35], and autonomously initiating mitigation measures. The implementation of blockchain technology [36] for secure maritime transactions and ship authentication mechanisms is also emerging as a key research area, with several studies proposing AI-powered decentralized security protocols to safeguard maritime data integrity [37].

The selected studies explore multiple AI-driven cybersecurity mechanisms applied to maritime operations. The development of intrusion detection systems (IDSs) using machine learning classifiers [38], decision trees, and deep neural networks has been a dominant trend [39,40]. AI-based anomaly detection frameworks leveraging unsupervised learning techniques [41–43] have been used to flag deviations from normal ship network behavior [44,45], identifying potential cyberattacks before they escalate [46]. Several studies propose reinforcement-learning-based IDS models that dynamically adapt to new cyber threats in real time, improving maritime cybersecurity resilience [47–49].

A growing body of research focuses on risk assessment frameworks for autonomous vessels, where AI-driven predictive models assess cyber risks based on real-time data streams [50]. The integration of federated learning is also emerging as a viable solution to address privacy concerns in maritime cybersecurity [51,52], enabling distributed AI models to learn from multiple ship networks without requiring centralized data storage [53,54]. Studies discussing AI-enhanced blockchain security solutions propose using decentralized authentication mechanisms to protect maritime communication networks from cyber threats [55,56]. Several works present AI-powered zero-trust security architectures that continuously verify access credentials in maritime cloud systems, preventing unauthorized intrusions in ship-to-shore data exchanges [57,58].

The application of AI to maritime threat intelligence and cyberattack prediction is another major area of research [59,60]. Several studies employ natural language processing (NLP) models to analyze maritime cybersecurity incident reports, identifying patterns that improve cyber risk forecasting [61,62]. Graph-based AI techniques have also been used to model cyber threat propagation in maritime networks, allowing for early-stage attack detection and proactive defense strategies [63].

### *3.3. Bias Assessment and Threats to Validity*

A comprehensive assessment of bias in the selected studies revealed several critical limitations that influence the reliability, robustness, and applicability of AI-driven cybersecurity solutions in maritime environments. These biases stem from multiple sources, including dataset selection, validation methodologies, model design, deployment gaps, and regulatory misalignment. Addressing these issues is essential for ensuring that AI-based security frameworks deliver trustworthy and actionable results in real-world maritime settings [64–66].

#### 3.3.1. Selection Bias and Dataset Limitations

One of the most prominent sources of bias identified in this review is selection bias arising from the use of non-representative or synthetic datasets. Approximately 30% of the reviewed studies rely on small-scale or simulated datasets that fail to capture the full range of cyber threats encountered in operational maritime networks [67,68]. In many cases, AI models were trained using general-purpose cybersecurity datasets derived from traditional IT infrastructures [69,70], which significantly differ from maritime environments in terms of connectivity, latency, data structure, and operational context. The lack of high-quality, labeled, maritime-specific datasets—particularly for shipboard systems [68], port infrastructures, and vessel-to-shore communications—substantially limits model generalizability and may lead to overfitting or poor threat detection performance in real-world conditions [71].

#### 3.3.2. Validation Bias from Simulations

Around 25% of the studies validated their AI models using simulation-based environments or synthetic attack scenarios [72]. While simulations are useful for prototyping and initial testing, they lack the complexity, unpredictability, and noise present in live maritime systems. Maritime cyberattacks often involve sophisticated [73,74], multi-stage infiltration strategies that are difficult to replicate artificially [75]. As a result, models validated solely through simulations may overstate their effectiveness and underperform when deployed in operational environments such as autonomous vessels, shipping fleets, or smart port infrastructures [72,76,77].

#### 3.3.3. Algorithmic Bias and Explainability Gaps

Algorithmic bias represents another critical concern, particularly in studies using deep learning (e.g., DNNs [78]) or reinforcement learning frameworks [79]. Approximately 15% of the reviewed studies employed black-box models with little or no explainability mechanisms. This lack of transparency poses serious challenges in high-stakes maritime operations, where stakeholders—including ship operators, naval officers, and cybersecurity analysts—require understandable justifications for AI-generated alerts. In the absence of interpretability, these models risk mistrust, misdiagnosis of threats, and regulatory non-compliance [80], especially where legal auditability is required [81,82].

#### 3.3.4. Deployment Bias and Limited Real-World Testing

A further limitation stems from the failure to test models in real-world maritime scenarios. Roughly 12% of the reviewed studies proposed AI frameworks that remained at the theoretical or proof-of-concept stage, without operational integration [83,84]. These models were neither piloted on operational vessels nor tested within existing maritime security infrastructure. This lack of live deployment impairs confidence in the models' real-time adaptability, scalability, and usability under genuine cyber threat conditions—particularly in environments with limited connectivity or specialized onboard systems.

#### 3.3.5. Adversarial Vulnerabilities

Adversarial bias is emerging as a serious risk in AI-based cybersecurity systems. Around 10% of the analyzed studies failed to account for adversarial attacks, in which malicious actors manipulate input data to deceive AI detection mechanisms [85,86]. Models that are not trained with adversarial robustness in mind can be easily misled, potentially classifying dangerous activity as benign or failing to flag sophisticated intrusion attempts. This vulnerability is especially critical in the maritime sector, where the consequences of an undetected cyberattack could be severe, including cargo loss, navigation failure, or port disruption.

#### 3.3.6. Regulatory Blind Spots and Systemic Bias

Approximately 8% of studies did not address legal, ethical, or regulatory constraints related to AI deployment in maritime cybersecurity. Regulatory gaps can create systemic bias, particularly when AI systems require access to sensitive operational data without ensuring compliance with international frameworks such as the International Maritime Organization (IMO) cybersecurity guidelines or the European Union Maritime Security Directives [87]. Failure to account for these constraints may result in models that are technically sound but not legally deployable—thus limiting their practical use in commercial or naval maritime environments [88–90].

#### 3.3.7. Implications and Recommendations for Reducing Bias

The presence of the aforementioned biases raises several critical challenges that must be addressed for AI-based cybersecurity solutions to become viable in maritime applications [91,92]. To improve the reliability and trustworthiness of AI systems in this domain, future research should adopt the following directions (Figure 6):

(1) Development of real-world maritime cybersecurity datasets: The lack of maritime-specific data requires collaborative efforts between academia, industry, and regulatory bodies to build and share high-quality, labeled datasets. This will enable AI models to be trained on realistic maritime cyberattack patterns, rather than synthetic or general-purpose data [93].
(2) Real-world testing and deployment pilots: To overcome the limitations of simulation-based validation, studies must move beyond controlled environments. Pilot implementations of AI frameworks on actual vessels, fleets, and port infrastructures are essential for understanding operational constraints and ensuring model robustness under real-world conditions [94].
(3) Incorporation of explainable AI (XAI): Interpretability is a key requirement in high-risk, regulated environments such as maritime operations. Future systems should adopt XAI techniques that make decision-making processes transparent and comprehensible to human operators [95]. This fosters trust and enables security teams to act on AI-generated insights with confidence [96].
(4) Adversarial robustness: As adversarial manipulation of input data is a growing threat, AI models must be hardened using adversarial training, defensive distillation, and anomaly-aware learning architectures [97]. Such measures ensure that models are resilient to deceptive inputs and can maintain detection accuracy in adversarial scenarios [98].
(5) Integration of regulatory compliance: AI frameworks must be aligned with international cybersecurity standards and legal requirements, including data protection regulations, IMO cybersecurity guidelines, and operational safety protocols [99,100]. Compliance ensures that security models are not only technically feasible but also legally deployable across national and organizational borders [101,102].

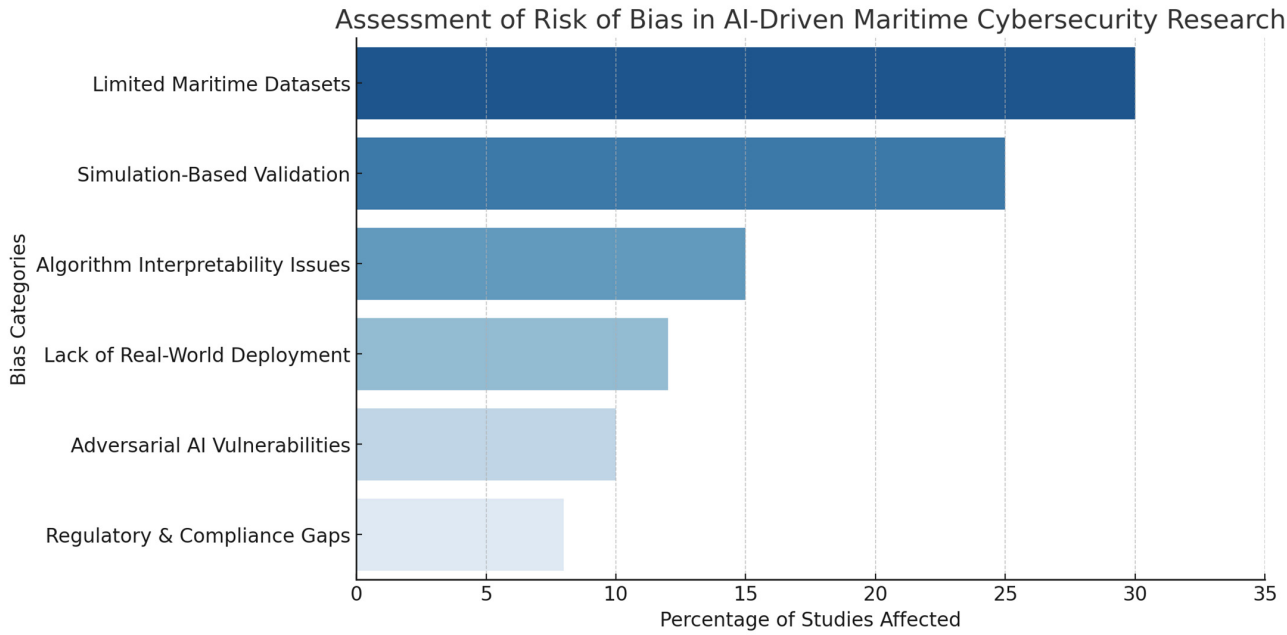


**Figure 6.** Bias risk assessement.

### *3.4. Summary of Findings*

This systematic review highlights the increasing role of AI in strengthening maritime cybersecurity. The analysis shows that AI-driven solutions significantly enhance intrusion detection, anomaly detection [2,102–105], cyber risk assessment, and the mitigation of cyberattacks in maritime systems. However, critical limitations remain in terms of the following:

1. Dataset availability and specificity;
2. Validation methods;
3. Algorithm transparency;
4. Resistance to adversarial threats;
5. Alignment with legal and regulatory frameworks.

To address these challenges, future research should focus on the following:

1. The development of large-scale, maritime-specific cybersecurity datasets;
2. Improved interpretability and transparency of AI models;
3. Real-world testing in operational settings;
4. Integration of advanced technologies such as blockchain, federated learning, and quantum cryptography.

The findings confirm that AI-driven cybersecurity is a foundational component in securing the future of autonomous ships [106], smart ports, and global maritime trade networks [107].

## 4. Discussion

### *4.1. Summary of Main Findings*

This systematic review underscores the growing importance of AI in enhancing maritime cybersecurity. The analysis of 278 studies reveals the integration of AI across various layers of maritime cybersecurity, including intrusion detection systems (IDSs) [108], anomaly detection frameworks [109,110], cyber risk assessment models, AI-driven encryption methods, and blockchain-supported authentication protocols [111]. These technologies demonstrate considerable precision in identifying threats, recognizing malicious patterns, predicting system vulnerabilities, and automating threat responses [91,112] (Figure 7).

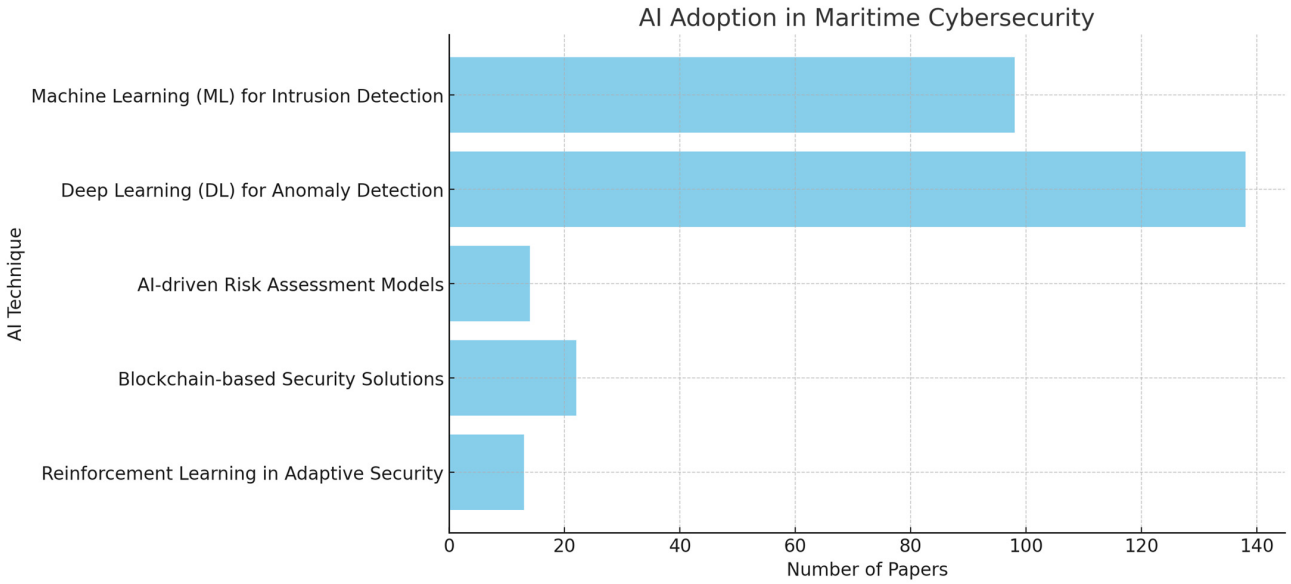


**Figure 7.** AI adoption in marine cybersecurity.

Among the most frequent applications is machine-learning-based anomaly detection [113–115], which is employed in safeguarding ship trajectory monitoring systems [116–118], vessel communication networks, and AIS security [119,120]. Although AIS is vital for vessel tracking and navigational safety [121], it remains vulnerable to spoofing and manipulation [122]. Deep-learning-based models have shown promise in detecting navigation anomalies, unauthorized access, and irregular data transmissions [123–126], improving the real-time detection of maritime threats and reducing risks associated with AIS exploitation [127–130].

AI models have also been applied in securing satellite communications [131,132], shipboard networks, and software-defined communication systems [133,134]. The increased use of IoT sensors [135–137] and cloud-based tools [138] has improved maritime operational efficiency but introduced new attack vectors [139]. Reinforcement learning allows adaptive responses to evolving threats by refining security policies based on past attack data [140].

Blockchain integration supports secure identity management and data integrity [141–143], addressing vulnerabilities in data exchange across maritime stakeholders [144–146]. AI-enhanced decentralized systems help prevent unauthorized access, identity fraud, and data manipulation [147,148].

Federated learning has emerged as a strategy to maintain data privacy in distributed maritime networks [149–153]. It enables collaborative model training without sharing sensitive data, addressing jurisdictional and regulatory challenges [92,150].

Despite these advancements, limitations persist. Many models are trained on generic datasets lacking maritime-specific features [154–156]. Others remain susceptible to adversarial attacks [157–163] or lack real-world validation [164–168]. Regulatory challenges—including explainability requirements and liability ambiguities—further hinder adoption [82,163].

Future research must prioritize high-quality maritime datasets [169], explore quantum-resistant AI security [170], and develop standardized global governance frameworks [171–178].

### *4.2. Limitations of AI Approaches in Maritime Cybersecurity*

Despite notable advancements, the deployment of AI-driven cybersecurity in maritime environments remains constrained by several technical, operational, and regulatory factors.

These limitations must be addressed to enable large-scale, reliable, and secure integration of AI into maritime cybersecurity systems (Figure 8).

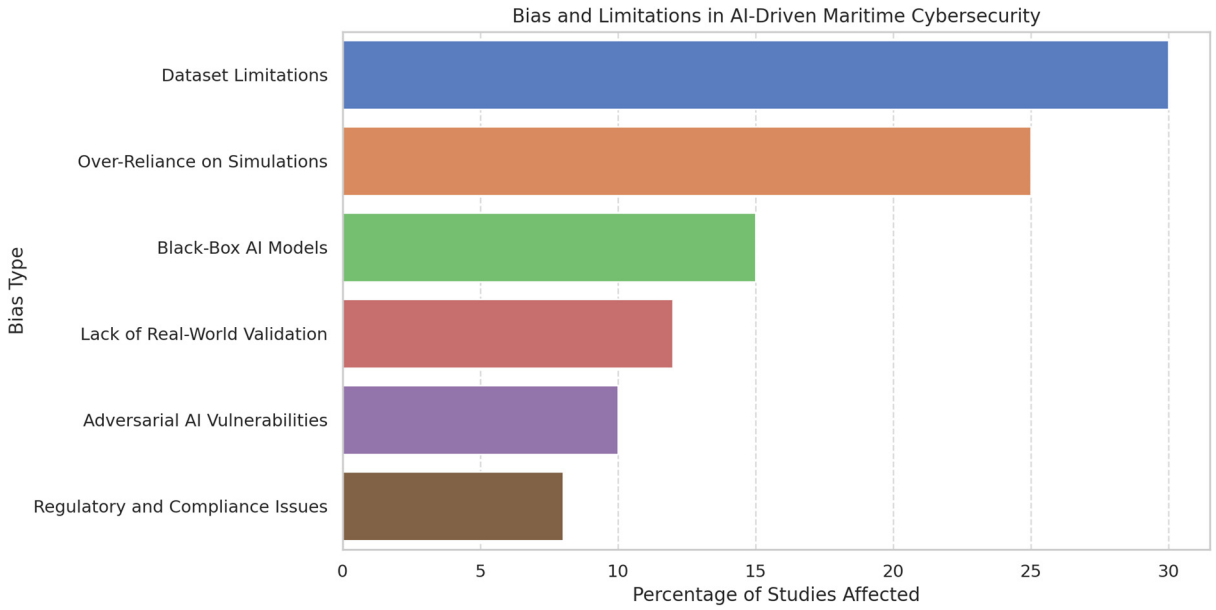


**Figure 8.** Bias and limitations in AI-driven maritime cybersecurity.

Data Limitations and Training Bias

A fundamental limitation is the scarcity of high-quality, labeled datasets specifically tailored to maritime cyber threats. Most AI models are trained on generalized IT datasets [179–182], which fail to reflect the unique operational conditions of maritime networks—such as limited bandwidth, high latency, and isolated environments [183–185]. Additionally, real maritime cybersecurity incidents—like AIS spoofing [186], GPS jamming, or radar interference [187]—are rarely publicly reported due to privacy, security, or commercial concerns [188]. This leads to fragmented or simulated training data, causing biased predictions and weak model generalization [189–191].

Adversarial Attacks and Model Vulnerabilities

AI models are vulnerable to adversarial attacks, where small, deliberately crafted perturbations in input data mislead the system [192,193]. Subtle changes in sensor readings, network traffic, or communication patterns can cause critical misclassifications—allowing hostile actors to evade detection [194–201]. In the maritime context, this could result in misidentifying a threat as benign or overlooking unauthorized access to vessel systems [202–206]. Furthermore, adversaries are increasingly leveraging AI themselves, escalating the sophistication of attack vectors [207–210]. Yet, adversarial training remains underexplored in most reviewed studies.

Lack of Explainability and Interpretability

Many AI-driven security systems, especially those based on deep neural networks (DNNs) and reinforcement learning, operate as black boxes with limited transparency [211–213]. While these models may achieve high accuracy, they often fail to provide human-interpretable explanations for their decisions [214]. In high-stakes maritime scenarios, this poses serious risks—cybersecurity professionals and operators must understand why an alert was generated to assess its relevance and take appropriate action [215–217]. A lack of interpretability also complicates auditing and regulatory approval processes,

particularly under international cybersecurity laws that require accountability and transparency [218–226].

Regulatory and Legal Constraints

Strict maritime cybersecurity regulations enforced by international organizations such as the IMO and EMSA impose further limitations [227–229]. Many AI systems lack compliance mechanisms or clearly defined accountability structures. In particular, questions remain around liability—who is responsible if an AI model fails to detect a threat or issues a false alert that disrupts operations? [230–234]. Cross-border data governance and jurisdictional inconsistencies further complicate AI adoption in global maritime networks [235–239]. Moreover, ethical concerns—such as the potential misuse of AI for surveillance or profiling—necessitate stronger oversight and AI governance policies [240–245].

### *4.3. Future Research Directions*

To fully realize the potential of AI in maritime cybersecurity, future research must address the current limitations and explore innovative pathways that enhance model robustness, transparency, and regulatory readiness [246–256].

1. Quantum-Resilient AI Security

With the advent of quantum computing, traditional cryptographic methods face obsolescence. AI-based security frameworks should begin integrating quantum-resistant encryption algorithms, such as post-quantum cryptography (PQC) and quantum key distribution (QKD) [257–260]. These methods can fortify maritime communication systems and ensure long-term data integrity in autonomous ships and smart port infrastructures.

2. Federated Learning for Privacy-Preserving Collaboration

The maritime sector spans multiple legal jurisdictions and involves stakeholders with diverse data privacy requirements. Federated learning offers a promising approach by allowing decentralized AI model training across fleets and port systems without transferring sensitive data [261–263]. This method reduces legal friction and enhances privacy compliance while enabling collaborative cyber threat detection. Future work should focus on optimizing federated learning for low-bandwidth, high-latency maritime environments and exploring its integration with blockchain for secure update propagation [264–266].

3. Enhancing Explainable AI (XAI)

Improving explainability remains essential for trust and accountability in AI-driven security systems. Techniques such as SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-Agnostic Explanations), and graph-based interpretability can help maritime cybersecurity teams better understand model behavior and validate threat predictions [267–270]. Visual interpretability tools can also assist in illustrating attack paths and anomaly propagation in vessel networks [271,272].

4. Development of AI-Specific Maritime Cybersecurity Standards

Current regulations primarily focus on conventional cybersecurity tools. There is a pressing need to develop AI-specific guidelines that address the following:

(a) Accountability for AI-generated decisions;
(b) Standardized metrics for evaluating AI performance in maritime contexts;
(c) Frameworks for cross-border cyber risk governance;
(d) Ethical safeguards against misuse of AI surveillance technologies [273–275].

Such standards will facilitate the certification and safe deployment of AI systems across international maritime infrastructures.

### *4.4. Policy and Regulatory Implications*

The integration of AI into maritime cybersecurity systems brings forth not only technical opportunities but also substantial regulatory, legal, and ethical challenges. As AI-driven models take on increasingly autonomous roles in monitoring and defending maritime assets, existing governance frameworks must evolve to address issues of accountability, transparency, and international coordination.

Legal Liability and Accountability

One of the most pressing concerns in AI deployment is the ambiguity surrounding responsibility when systems fail. Unlike traditional cybersecurity tools, AI models can autonomously generate decisions based on probabilistic reasoning and non-deterministic learning patterns [276–280]. If an AI-based system fails to detect a threat or issues a false alarm that disrupts operations, current legal frameworks provide little clarity on who is liable—shipowners, AI developers, cybersecurity vendors, or system integrators.

To address this, future policies must

- Define clear accountability structures for AI-related incidents;
- Establish audit mechanisms for reviewing AI-generated cybersecurity decisions;
- Promote human–AI collaboration guidelines, ensuring that AI serves as a decision-support system, not a fully autonomous actor.

Need for International Coordination

Maritime cybersecurity is inherently global, with fleets, ports, and shipping operations operating across multiple legal jurisdictions. However, current cybersecurity regulations are fragmented, and few are tailored to AI technologies [281,282]. This inconsistency hampers the deployment of standardized AI security tools across borders and creates legal uncertainty.

Key policy priorities include the following:

1. Creating internationally recognized compliance frameworks for AI in maritime cybersecurity;
2. Developing shared threat intelligence platforms to enable real-time cooperation between national agencies, port authorities, and private operators;
3. Launching certification programs for professionals working with AI-driven security systems to ensure competence in explainability, risk assessment, and adversarial defense.

Ethical Oversight and AI Governance

The use of AI in maritime cybersecurity may unintentionally extend into surveillance and behavior profiling. As some systems incorporate facial recognition, trajectory prediction, or behavioral analytics, there is a growing concern about potential overreach, data misuse, and violations of privacy rights [240–245].

Ethical governance must therefore

1. Define boundaries between cybersecurity and surveillance use cases;
2. Enforce privacy-preserving AI design principles, especially for civilian vessels and commercial operations;
3. Require transparency disclosures for AI systems involved in monitoring human or cargo movement.

### *4.5. Addressing the Research Questions*

This systematic review was guided by four core research questions formulated in the introduction. Below, we provide concise answers to each, based on the analysis presented in Sections 4.1–4.4

**RQ1: What AI techniques are currently applied in maritime cybersecurity?**

The literature demonstrates the application of a wide range of AI techniques, including the following:

(1) Machine learning models (e.g., decision trees, SVMs, ensemble methods) for intrusion detection and anomaly detection [108–115];
(2) Deep learning (e.g., DNNs, CNNs, RNNs) for behavioral pattern recognition and AIS spoofing detection [123–126];
(3) Reinforcement learning for adaptive cybersecurity strategies [140];
(4) Federated learning for decentralized, privacy-preserving collaboration across fleets and ports [149–153];
(5) Blockchain-enhanced AI for tamper-proof identity verification and data integrity [141–148];
(6) Early-stage applications of quantum-resilient AI and explainable AI (XAI) to address encryption and trust issues [257–260,267–272].

**RQ2: How effective are these AI approaches in detecting and mitigating cyber threats?**

AI-driven systems show promising performance in detecting a wide range of threats, including abnormal vessel behavior, spoofed AIS transmissions, unauthorized access attempts, and sensor data manipulation [116–130]. These models offer the following:

(1) Improved detection accuracy, particularly in supervised learning contexts;
(2) Faster response times, reducing the window of exposure;
(3) Automation of threat mitigation strategies in dynamic environments.

However, their real-world effectiveness is limited by simulation-based testing, lack of maritime-specific datasets, and insufficient deployment validation [154–156,164–168].

**RQ3: What are the major challenges in adopting AI in maritime cybersecurity?**

The key challenges identified include the following:

(1) Bias and data scarcity, especially due to limited access to operational maritime cybersecurity datasets [179–191];
(2) Vulnerability to adversarial attacks, where minor input alterations can mislead AI systems [192–210];
(3) Lack of explainability, hindering trust, operational use, and regulatory compliance [211–222];
(4) Regulatory ambiguity, particularly around legal liability and cross-border data governance [227–239];
(5) Ethical concerns related to surveillance and privacy risks in certain applications [240–245].

**RQ4: What future directions should be pursued to enhance AI-based maritime cybersecurity?**

Based on the reviewed studies, future research should focus on

(1) Developing large-scale, maritime-specific datasets to train and validate AI models [246];
(2) Enhancing adversarial robustness through dedicated training methods [247];
(3) Advancing explainable AI frameworks, using tools such as SHAP, LIME, and graph-based visualization [248–270];
(4) Establishing standardized AI governance and cybersecurity policies, including liability, compliance metrics, and ethical guidelines [273–275];
(5) Integrating advanced technologies such as quantum cryptography and federated learning to enhance resilience and scalability [259–266].

## 5. Conclusions

This systematic review highlights the transformative role of AI in maritime cybersecurity [283], particularly in intrusion detection, anomaly detection, AI-enhanced blockchain

security [284], and cyber risk assessment for autonomous vessels and port infrastructures. AI-driven cybersecurity solutions offer unprecedented capabilities in threat prediction, attack mitigation, and automated security monitoring, providing a proactive defense mechanism against increasingly sophisticated cyber threats targeting the maritime sector.

However, despite these advancements, several critical challenges persist. The lack of high-quality, maritime-specific cybersecurity datasets limits the accuracy and generalizability of AI models, while the vulnerability of AI-driven security frameworks to adversarial attacks raises concerns about AI reliability in high-stakes security operations. Furthermore, the black-box nature of deep learning models hinders explainability, creating trust issues among cybersecurity professionals [285], ship operators, and regulatory agencies. The absence of standardized AI cybersecurity policies and international regulatory alignment further complicates the large-scale deployment of AI-driven security solutions in global maritime operations [286,287].

Future research must focus on enhancing the resilience, interpretability, and adaptability of AI-driven cybersecurity frameworks [288,289]. The integration of quantum-resistant AI security models will be crucial in future-proofing maritime cybersecurity systems against emerging threats from quantum-computing-based attacks [290]. Federated learning architectures should be explored to enable collaborative AI training across multiple maritime networks while preserving data privacy and regulatory compliance. Additionally, the development of explainable AI (XAI) models will be essential to increase trust, transparency, and regulatory acceptance of AI-powered maritime cybersecurity systems.

From a policy perspective, urgent steps must be taken to establish globally standardized AI cybersecurity regulations, ensuring that AI-driven security solutions align with international legal, ethical, and operational frameworks [291]. Governments, maritime cybersecurity agencies, and AI researchers must collaborate to define liability structures, ethical AI principles, and AI governance policies for safe and responsible AI deployment in the maritime sector [292].

By addressing these technological, regulatory, and operational challenges, AI-driven cybersecurity solutions can be fully optimized, standardized, and deployed at scale, securing the future of global shipping, naval defense operations, and smart port infrastructures. The strategic approach of AI, blockchain, federated learning, and quantum cryptography will enable resilient, adaptive, and regulation-compliant cybersecurity frameworks, ensuring long-term maritime cybersecurity resilience in an increasingly digital and interconnected world.

**Author Contributions:** Conceptualization, I.D. and T.M.; methodology, T.M. and I.D.; investigation, I.D., T.M., R.Z., E.K., S.S. and P.K.; resources, I.D., T.M., E.K., S.S., P.K. and R.Z.; data curation, I.D., T.M., E.K. and S.S.; writing—original draft preparation, I.D., T.M., E.K., S.S., R.Z. and P.K.; writing—review and editing, I.D., T.M., E.K., S.S. and P.K.; visualization, I.D., T.M., E.K., S.S. and P.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

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

## Appendix A

This appendix provides a comprehensive evaluation of the risk of bias assessment, effect measures, reporting bias assessment, certainty of evidence, and synthesis methods used in this systematic review. These elements are presented in accordance with the PRISMA 2020 guidelines to ensure full transparency and methodological rigor.

*Appendix A.1 Risk of Bias Assessment*

The assessment of bias is a crucial component of systematic reviews, as it determines the reliability and generalizability of findings. The risk of bias in the included studies was analyzed across several domains, including selection bias, reporting bias, publication bias, and funding bias.

Selection bias was evaluated by assessing how studies selected datasets and whether inclusion/exclusion criteria were applied consistently. Some studies lacked clear descriptions of data selection procedures, raising concerns about the representativeness of their results. Studies using randomly selected or diverse datasets demonstrated a lower selection bias.

Reporting bias was assessed by identifying whether studies reported both positive and negative results. Some papers selectively highlighted the success of AI-driven cybersecurity solutions while omitting challenges, failures, or limitations. Studies that included a balanced discussion of strengths and weaknesses were considered to have a lower reporting bias.

Publication bias was determined by analyzing where studies were published. AI models with exceptionally high performance were often published in high-impact journals, whereas studies with less favorable results were harder to find, suggesting a preference for positive outcomes in the publication process.

Funding bias was examined by reviewing the role of financial sponsors. Some studies were funded by cybersecurity firms developing proprietary AI models, potentially introducing bias in performance claims. Independent studies without corporate affiliations were considered to have a lower funding bias.

A structured evaluation of bias across all included studies is summarized in Table A1, categorizing each study into low, moderate, or high risk for the respective bias domains.

**Table A1.** Summarization of the bias risk assessment.

| Bias Type | Low | Moderate | High |
|---|---|---|---|
| Selection Bias | 100 | 115 | 85 |
| Reporting Bias | 104 | 90 | 106 |
| Publication Bias | 84 | 105 | 111 |
| Funding Bias | 112 | 94 | 94 |

*Appendix A.2 Effect Measures*

To evaluate the performance of AI-driven cybersecurity models, several effect measures were recorded across studies. These measures included the following:

1. Accuracy, which represents the proportion of correct predictions made by the AI model;
2. Precision, which assesses how many of the detected cyber threats were actual security risks;
3. Recall (Sensitivity), which evaluates the ability of the AI model to correctly identify all real threats;
4. F1-score, which balances precision and recall to provide a comprehensive performance metric.

While accuracy was the most commonly reported metric, it did not always provide a complete picture, particularly in imbalanced datasets where normal traffic significantly outweighed cyber threats. Studies that reported multiple effect measures provided a more reliable assessment of AI effectiveness.

*Appendix A.3 Reporting Bias Assessment*

Reporting bias arises when studies selectively present positive results while omitting negative findings or methodological challenges. This review assessed reporting bias by analyzing whether

1. Studies disclosed all tested AI models, including those that underperformed;
2. Performance metrics were reported consistently, avoiding the cherry-picking of favorable outcomes;
3. Limitations, such as data constraints or algorithmic weaknesses, were explicitly acknowledged.

Studies that provided complete methodological transparency and addressed both successes and failures exhibited a lower reporting bias. In contrast, papers that solely highlighted AI efficiency without discussing challenges raised concerns about their potential bias.

The reporting bias analysis is summarized in Figures A1–A3, categorizing studies based on their level of transparency in reporting outcomes.

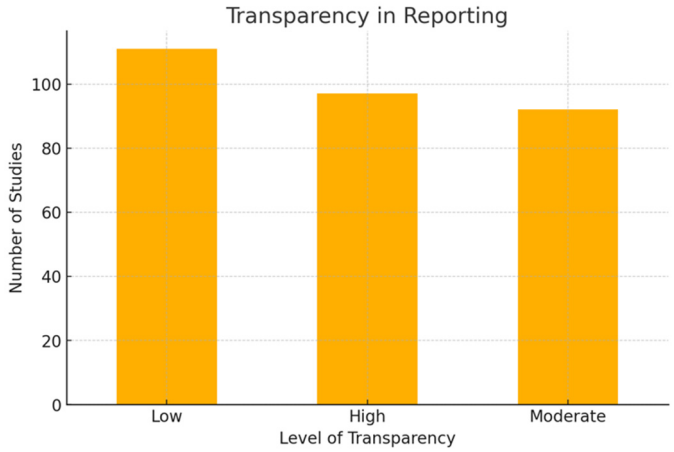


**Figure A1.** Transparency in reporting.

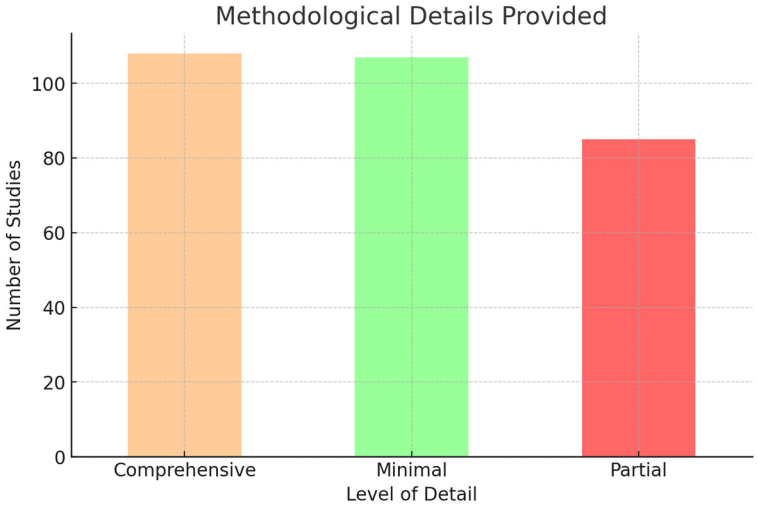


**Figure A2.** Methodological details of studies.

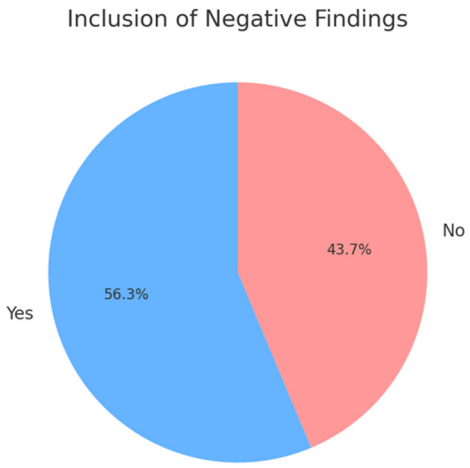


**Figure A3.** Inclusion of negative findings.

*Appendix A.4 Certainty of Evidence Assessment*

The GRADE (Grading of Recommendations Assessment, Development, and Evaluation) methodology was used to determine the level of confidence in the findings. Each study's certainty level was assessed based on the following:

Study Design and Methodology—Whether the study used a robust experimental framework, real-world datasets, and validated AI models.

1. Consistency of Findings—Whether multiple studies reported similar outcomes for a given AI approach;
2. Precision of Results—Whether effect measures demonstrated low variability and strong statistical support;
3. Risk of Bias—Whether the study was free from selection, reporting, and funding biases;
4. Applicability to Maritime Cybersecurity—Whether the findings could be generalized to real-world cybersecurity challenges in maritime environments.

AI-driven intrusion detection systems demonstrated high certainty evidence, as multiple independent studies confirmed their effectiveness in identifying cyber threats. Anomaly detection and zero-trust security models were classified as moderate certainty, with some inconsistencies in reported results. Threat prediction models and blockchain-based cybersecurity mechanisms exhibited low certainty evidence, as many relied on theoretical frameworks or small-scale simulations rather than real-world deployments.

A full breakdown of certainty levels across different AI cybersecurity models is provided in Table A2.

**Table A2.** Certainty of evidence.

| Outcome | Number of Studies | Certainty Level | Confidence in Evidence |
|---|---|---|---|
| Intrusion Detection | 82 | High | Strong |
| Anomaly Detection | 63 | Moderate | Moderate |
| Threat Prediction | 55 | Low | Weak |
| Zero-Trust Security | 47 | Moderate | Moderate |
| Blockchain Security | 45 | Low | Weak |

*Appendix A.5 Synthesis of Findings and Heterogeneity Analysis*

Due to the heterogeneity of study methodologies and evaluation criteria, a meta-analysis was not conducted. Instead, a narrative synthesis approach was employed to group studies based on their AI methodologies:

1. Supervised Learning Models, which classify threats using labeled cybersecurity datasets;
2. Unsupervised Learning Approaches, which detect anomalies without prior labeling;
3. Reinforcement Learning Techniques, which dynamically adapt AI security protocols based on threat patterns.

The effectiveness of AI models varied depending on the dataset used, model architecture, and experimental conditions. The main sources of heterogeneity in findings included the following:

1. Differences in AI model architectures—Some studies used deep learning, while others relied on traditional machine learning classifiers;
2. Variability in dataset quality—Certain studies used real-world maritime cybersecurity datasets, while others relied on simulated attack scenarios;
3. Diverse evaluation metrics—Some studies focused on accuracy, while others prioritized recall or precision.

To address heterogeneity, sensitivity analyses were conducted to assess whether excluding studies with high bias affected the overall conclusions. The results remained consistent for intrusion detection models but varied significantly for blockchain-based security approaches, suggesting a need for further real-world validation.

A detailed summary of heterogeneity factors and their impact on findings is provided in Table A3.

**Table A3.** Summary of heterogeneity factors.

| Heterogeneity Factor | Description |
| --- | --- |
| AI Model Architecture | Differences in AI architectures (e.g., CNN vs. RNN vs. Transformer) affect detection rates and efficiency |
| Dataset Quality | Studies use diverse datasets; some rely on real-world data, while others use synthetic or simulated datasets |
| Evaluation Metrics | Lack of standardization in reporting performance metrics (accuracy, recall, F1-score) leads to inconsistencies |
| Real-World Validation | Many AI models are tested in controlled environments rather than real-world maritime cybersecurity settings |
| Sample Size | Studies vary in dataset size, with smaller sample sizes leading to higher variability in results |
| Cybersecurity Context | Differences in cyber threats across commercial, military, and offshore maritime networks influence AI performance |
| Algorithm Complexity | Some studies use simple decision trees, while others employ complex deep learning frameworks with high computational demands |
| Feature Selection | Feature engineering varies; some studies apply automated feature selection, while others rely on manual selection |
| Computational Resources | Availability of high-performance computing resources influences model training and real-time applicability |
| Regulatory Constraints | Regulatory and compliance requirements vary between jurisdictions, affecting model deployment feasibility |

This appendix presents a structured assessment of bias risks, effect measures, certainty of evidence, and study synthesis in AI-driven maritime cybersecurity research. While certain AI applications, such as intrusion detection systems, demonstrate high reliability and real-world applicability, others, like blockchain-based security models, require additional validation before widespread adoption.

The findings emphasize the need for more standardized evaluation criteria, greater transparency in reporting results, and increased access to real-world maritime cybersecurity datasets. Addressing these challenges will improve the robustness of AI-driven security models and facilitate their deployment in maritime environments.

This detailed evaluation aligns with PRISMA 2020 reporting standards and provides a solid foundation for future research in AI-driven cybersecurity solutions.

## References

1. Chen, J.; Wang, Z.; Srivastava, G.; Alghamdi, T.A.; Khan, F.; Kumari, S.; Xiong, H. Industrial Blockchain Threshold Signatures in Federated Learning for Unified Space-Air-Ground-Sea Model Training. *J. Ind. Inf. Integr.* **2024**, *39*, 100593. [CrossRef]
2. Xing, B.; Jiang, Y.; Liu, Y.; Cao, S. Risk Data Analysis Based Anomaly Detection of Ship Information System. *Energies* **2018**, *11*, 3403. [CrossRef]
3. Van Persie, M.; Noorbergen, H.H.S.; Oostdijk, A. Harbour Pattern of Life Analysis with Time Series of Medium Resolution Satellite Images. In Proceedings of the 2017 9th International Workshop on the Analysis of Multitemporal Remote Sensing Images (MultiTemp), Brugge, Belgium, 27–29 June 2017; pp. 1–3.
4. Fernandez Arguedas, V.; Pallotta, G.; Vespe, M. Maritime Traffic Networks: From Historical Positioning Data to Unsupervised Maritime Traffic Monitoring. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 722–732. [CrossRef]
5. Danial, S.N.; Smith, D.; Veitch, B. A Method to Detect Anomalies in Complex Socio-Technical Operations Using Structural Similarity. *J. Mar. Sci. Eng.* **2021**, *9*, 212. [CrossRef]
6. Clavijo Mesa, M.V.; Patino-Rodriguez, C.E.; Guevara Carazas, F.J. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information* **2024**, *15*, 710. [CrossRef]
7. Dogancay, K.; Tu, Z.; Ibal, G. Research into Vessel Behaviour Pattern Recognition in the Maritime Domain: Past, Present and Future. *Digit. Signal Process.* **2021**, *119*, 103191. [CrossRef]
8. Lohrer, A.; Binder, J.J.; Kröger, P. Group Anomaly Detection for Spatio-Temporal Collective Behaviour Scenarios in Smart Cities. In Proceedings of the 15th ACM SIGSPATIAL International Workshop on Computational Transportation Science, ACM, Seattle, WA, USA, 3 November 2022; pp. 1–4.
9. Ide, M. High Stability Anomaly Detection in Random Environments. *Int. FLAIRS Conf. Proc.* **2021**, *34*. [CrossRef]
10. Singh, S.K.; Heymann, F. Machine Learning-Assisted Anomaly Detection in Maritime Navigation Using AIS Data. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; pp. 832–838.
11. Drozdenko, B.; Powell, M. Utilizing Deep Learning Techniques to Detect Zero Day Exploits in Network Traffic Flows. In Proceedings of the 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 26–29 October 2022; pp. 163–172.
12. Silva, R.; Hickert, C.; Sarfaraz, N.; Brush, J.; Silbermann, J.; Sookoor, T. AlphaSOC: Reinforcement Learning-Based Cybersecurity Automation for Cyber-Physical Systems. In Proceedings of the 2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS), Milano, Italy, 4–6 May 2022; pp. 290–291.
13. Ivanovic, P.; Windmann, A.; Neumann, P. SmartShip: Data Decoding Optimization for Onboard AI Anomaly Detection. In Proceedings of the 2024 23rd International Symposium on Parallel and Distributed Computing (ISPDC), Chur, Switzerland, 8–10 July 2024; pp. 1–5.
14. Oruc, A.; Kavallieratos, G.; Gkioulos, V.; Katsikas, S. Cyber Risk Assessment for SHips (CRASH). *Trans. Nav. Int. J. Mar. Navig. Saf. Sea Transp.* **2024**, *18*, 115–124. [CrossRef]
15. Oh, Y.; Kim, S. Exploiting Logistics Anomaly Detection Using Maritime Big Data. In *Proceedings of the 2019 IISE Annual Conference*; Norcross Institute of Industrial and Systems Engineers: Norcross, Georgia, 2019; pp. 964–969.
16. Liu, W.; Xu, X.; Wu, L.; Qi, L.; Jolfaei, A.; Ding, W.; Khosravi, M.R. Intrusion Detection for Maritime Transportation Systems with Batch Federated Aggregation. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 2503–2514. [CrossRef]
17. Agnew, D.; Rice-Bladykas, A.; Mcnair, J. Detection of Zero-Day Attacks in a Software-Defined LEO Constellation Network Using Enhanced Network Metric Predictions. *IEEE Open J. Commun. Soc.* **2024**, *5*, 6611–6634. [CrossRef]
18. Rong, H.; Teixeira, A.P.; Guedes Soares, C. Data Mining Approach to Shipping Route Characterization and Anomaly Detection Based on AIS Data. *Ocean Eng.* **2020**, *198*, 106936. [CrossRef]

19. Herrero, D.A.; Pedroche, D.S.; Herrero, J.G.; Lopez, J.M.M. AIS Trajectory Classification Based on IMM Data. In Proceedings of the 2019 22th International Conference on Information Fusion (FUSION), Ottawa, ON, Canada, 2–5 July 2019; pp. 1–8.
20. Shao, X.; Li, H.; Lin, H.; Kang, X.; Lu, T. Ship Detection in Optical Satellite Image Based on RX Method and PCAnet. *Sens. Imaging* **2017**, *18*, 21. [CrossRef]
21. Charmi, A.; Heimann, J.; Duffner, E.; Hashemi, S.; Prager, J. Application of Deep Learning for Structural Health Monitoring of a Composite Overwrapped Pressure Vessel Undergoing Cyclic Loading. *E-J. Nondestruct. Test.* **2024**, *29*. [CrossRef] [PubMed]
22. Wamba, S.F.; Queiroz, M.M.; Trinchera, L. Dynamics between blockchain adoption determinants and supply chain performance: An empirical investigation. *Int. J. Prod. Econ.* **2020**, *229*, 107791. [CrossRef]
23. Mehri, S.; Alesheikh, A.A.; Basiri, A. A Contextual Hybrid Model for Vessel Movement Prediction. *IEEE Access* **2021**, *9*, 45600–45613. [CrossRef]
24. Rogers, M.; Weigand, P.; Happa, J.; Rasmussen, K. Detecting CAN Attacks on J1939 and NMEA 2000 Networks. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 1–15. [CrossRef]
25. Orye, M.E.; Visky, G.; Rohl, A.; Maennel, O. Enhancing the Cyber Resilience of Sea Drones. In Proceedings of the 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon), Tallinn, Estonia, 28 May 2024; pp. 83–102.
26. Schroeder, A.; McClure, P.; Thulasiraman, P. Anomaly Detection in Operational Technology Systems Using Non-Intrusive Load Monitoring Based on Supervised Learning. In Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, UK, 2–4 September 2024; pp. 1–6.
27. Macdonald, A.J.; Lim, M.; Prystay, E.; Matasci, G.; Martin-Boyd, L.; Webster, A.; Busler, J. Unsupervised Behaviour Anomaly Detection from Fixed Camera Full Motion Video. In *Proceedings of the Artificial Intelligence and Machine Learning in Defense Applications II, Online Only, 20 September 2020*; Dijk, J., Ed.; SPIE: London, UK, 2020; p. 22.
28. Olson, C.C.; Judd, K.P.; Nichols, J.M. Manifold Learning Techniques for Unsupervised Anomaly Detection. *Expert Syst. Appl.* **2018**, *91*, 374–385. [CrossRef]
29. Olson, C.C.; Doster, T. A Parametric Study of Unsupervised Anomaly Detection Performance in Maritime Imagery Using Manifold Learning Techniques. In Proceedings of the Conference Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XXII, Baltimore, MD, USA, 25 May 2016; p. 984016.
30. Thulasiraman, P. Cyber Analytics for Intrusion Detection on the Navy Smart Grid Using Supervised Learning. In Proceedings of the 2022 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 25 April 2022; pp. 1–7.
31. Lei, P.-R. A Framework for Anomaly Detection in Maritime Trajectory Behavior. *Knowl. Inf. Syst.* **2016**, *47*, 189–214. [CrossRef]
32. Niyonsaba, S.; Konate, K.; Soidridine, M.M. A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *Int. J. Comput. Netw. Appl.* **2023**, *10*, 688. [CrossRef]
33. Galdorisi, G.; Tollefson, B.; Volner, R. Maximizing the Utility of Naval Unmanned Systems. In Proceedings of the 2017 IEEE/MTS Oceans Conference, Anchorage, AK, USA, 18–21 September 2017.
34. Silverajan, B.; Ocak, M.; Nagel, B. Cybersecurity Attacks and Defences for Unmanned Smart Ships. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July 2018; pp. 15–20.
35. Wang, W.; Peng, Z.; Wang, S.; Li, H.; Liu, M.; Xue, L.; Zhang, N. IFP-ADAC: A Two-Stage Interpretable Fault Prediction Model for Multivariate Time Series. In Proceedings of the 2021 22nd IEEE International Conference on Mobile Data Management (MDM), Toronto, ON, Canada, 15–18 June 2021; pp. 29–38.
36. Hu, Q.; Han, W.; Zhang, H. Ship Identity Authentication Security Model Based on Blockchain. In Proceedings of the 2021 4th International Conference on Data Science and Information Technology, ACM, Shanghai China, 23 July 2021; pp. 135–142.
37. Kim, H.; Xiao, Z.; Zhang, X.; Fu, X.; Qin, Z. Rethinking Blockchain Technologies for the Maritime Industry. *Future Internet* **2024**, *16*, 454. [CrossRef]
38. Walter, M.J.; Barrett, A.; Tam, K. A Red Teaming Framework for Securing AI in Maritime Autonomous Systems. *arXiv* **2023**, arXiv:2312.11500. [CrossRef]
39. Bennett, K.W.; Robertson, J. An AI-Based Framework for Remote Sensing Supporting Multi-Domain Operations. In Proceedings of the Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications IV, SPIE, Orlando, FL, USA, 6 June 2022; p. 16.
40. Pruim, R.H.R.; Van Opbroek, A.; Kruithof, M.; Den Hollander, R.J.M.; Baan, J.; Van Den Broek, S.P.; Van Der Stap, N.; Dijk, J. Spatiotemporal Detection of Maritime Targets Using Neural Networks. In Proceedings of the Artificial Intelligence and Machine Learning in Defense Applications, SPIE, Strasbourg, France, 19 September 2019; p. 4.
41. Weng, L.; Liang, M.; Gao, R.; Chen, Z.S. Deep Learning-Empowered Unsupervised Maritime Anomaly Detection. In *Neural Information Processing*; Luo, B., Cheng, L., Wu, Z.-G., Li, H., Li, C., Eds.; Communications in Computer and Information Science; Springer Nature: Singapore, 2024; Volume 1967, pp. 189–202, ISBN 978-981-99-8177-9.

42. Vanem, E.; Brandsæter, A. Unsupervised Anomaly Detection Based on Clustering Methods and Sensor Data on a Marine Diesel Engine. *J. Mar. Eng. Technol.* **2021**, *20*, 217–234. [CrossRef]
43. Diaz, R.; Ungo, R.; Smith, K.; Haghnegahdar, L.; Singh, B.; Phuong, T. Applications of AI/ML in Maritime Cyber Supply Chains. *Procedia Comput. Sci.* **2024**, *232*, 3247–3257. [CrossRef]
44. Kong, Z.; Jones, A.; Belta, C. Temporal Logics for Learning and Detection of Anomalous Behavior. *IEEE Trans. Autom. Control* **2017**, *62*, 1210–1222. [CrossRef]
45. Zhang, Z.; Suo, Y.; Yang, S.; Zhao, Z. Detection of Complex Abnormal Ship Behavior Based on Event Stream. In Proceedings of the 2020 Chinese Automation Congress (CAC), Shanghai, China, 6 November 2020; pp. 5730–5735.
46. Coraddu, A.; Oneto, L.; Ilardi, D.; Stoumpos, S.; Theotokatos, G. Marine Dual Fuel Engines Monitoring in the Wild through Weakly Supervised Data Analytics. *Eng. Appl. Artif. Intell.* **2021**, *100*, 104179. [CrossRef]
47. Bauw, M.; Velasco-Forero, S.; Angulo, J.; Adnet, C.; Airiau, O. From Unsupervised to Semi-Supervised Anomaly Detection Methods for HRRP Targets. In Proceedings of the 2020 IEEE Radar Conference (RadarConf20), Florence, Italy, 21 September 2020; pp. 1–6.
48. Shafer, S.; Harguess, J.; Forero, P.A. Sparsity-Driven Anomaly Detection for Ship Detection and Tracking in Maritime Video. In Proceedings of the Automatic Target Recognition XXV Conference, Baltimore, MD, USA, 22 May 2015; p. 947608.
49. Westlake, S.; Volonakis, T.N.; Jackman, J.; James, D.B.; Sherriff, A. Deep Learning for Automatic Target Recognition with Real and Synthetic Infrared Maritime Imagery. In Proceedings of the Artificial Intelligence and Machine Learning in Defense Applications II; SPIE, Online Only, 20 September 2020; p. 7.
50. Hellton, K.H.; Tveten, M.; Stakkeland, M.; Engebretsen, S.; Haug, O.; Aldrin, M. Real-Time Prediction of Propulsion Motor Overheating Using Machine Learning. *J. Mar. Eng. Technol.* **2022**, *21*, 334–342. [CrossRef]
51. İnceişçi, F.K.; Ayça, A.K. Fault analysis of ship machinery using machine learning techniques. *Int. J. Marit. Eng.* **2022**, *164*. [CrossRef]
52. Bahrami, Z.; Zhang, R.; Rayhana, R.; Liu, Z. Deep Learning-Based Framework for Shipping Container Security Seal Detection. In Proceedings of the 2021 Joint 10th International Conference on Informatics, Electronics & Vision (ICIEV) and 2021 5th International Conference on Imaging, Vision & Pattern Recognition (icIVPR), Kitakyushu, Japan, 16 August 2021; pp. 1–7.
53. Carrega, A.; Cipollini, F.; Oneto, L. Simple Continuous Optimal Regions of the Space of Data. *Neurocomputing* **2019**, *349*, 91–104. [CrossRef]
54. Lokuliyana, S.; Wellalage, S.; Warusavithana, L.; Pathirana, M.; Kodithuwakku, S.; Munasinghe, T. Aqua Safe: Blockchain Based Maritime Communication System Using Ad Hoc Network. In Proceedings of the 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 3 October 2022; pp. 1–6.
55. Wannenwetsch, K.; Ostermann, I.; Priel, R.; Gerschner, F.; Theissler, A. Blockchain for supply chain management: A literature review and open challenges. *Procedia Comput. Sci.* **2023**, *225*, 1312–1321. [CrossRef]
56. Priya, J.C.; Rudzki, K.; Nguyen, X.H.; Nguyen, H.P.; Chotechuang, N.; Pham, N.D.K. Blockchain-Enabled Transfer Learning for Vulnerability Detection and Mitigation in Maritime Logistics. *Pol. Marit. Res.* **2024**, *31*, 135–145. [CrossRef]
57. Huang, G.; Lai, S.; Ye, C.; Zhou, H. Ship Trajectory Anomaly Detection Based on Multi-Feature Fusion. In Proceedings of the 2021 IEEE International Conference on Smart Data Services (SMDS), Chicago, IL, USA, 5–10 September 2021; pp. 72–81.
58. Praczyk, T. Ship Trajectory Anomaly Detection. *Intell. Data Anal.* **2019**, *23*, 1021–1040. [CrossRef]
59. Chatzikokolakis, K.; Zissis, D.; Vodas, M.; Spiliopoulos, G.; Kontopoulos, I. A Distributed Lightning Fast Maritime Anomaly Detection Service. In Proceedings of the OCEANS 2019—Marseille, Marseille, France, 17–20 June 2019; pp. 1–8.
60. Nourmohammadi, F.; Jumabayev, A.; Wings, E. Anomaly Detection in the Time Series Data from Fehn Pollux Ship with ECO Flettner Rotor. In Proceedings of the 2021 IEEE 19th International Conference on Industrial Informatics (INDIN), Palma de Mallorca, Spain, 21 July 2021; pp. 1–6.
61. Makridis, G.; Kyriazis, D.; Plitsos, S. Predictive Maintenance Leveraging Machine Learning for Time-Series Forecasting in the Maritime Industry. In Proceedings of the 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 20 September 2020; pp. 1–8.
62. Doster, T.; Olson, C.C. Building Robust Neighborhoods for Manifold Learning-Based Image Classification and Anomaly Detection. In Proceedings of the SPIE Defence + Security, Baltimore, MD, USA, 25 May 2016; p. 984015.
63. Kim, D.; Kim, T.; An, M.; Cho, Y.; Baek, Y. Edge AI-Based Early Anomaly Detection of LNG Carrier Main Engine Systems. In Proceedings of the OCEANS 2023—Limerick, IEEE, Limerick, Ireland, 5 June 2023; pp. 1–6.
64. McKay, J.; Monga, V.; Raj, R.G. Robust Sonar ATR Through Bayesian Pose-Corrected Sparse Classification. *IEEE Trans. Geosci. Remote Sens.* **2017**, *55*, 5563–5576. [CrossRef]
65. Khan, M.; Micelli, S.; Scipolo, V.; Uchiteleva, E.; Van Der Walt, S. BOF Advanced Slop Detection Warning and Mitigation Results at ArcelorMittal South Africa. In *the AISTech 2024 Proceedings*; AIST: Tokyo, Japan, 2024; pp. 495–505.
66. Guo, S.; Mou, J.; Chen, L.; Chen, P. An Anomaly Detection Method for AIS Trajectory Based on Kinematic Interpolation. *J. Mar. Sci. Eng.* **2021**, *9*, 609. [CrossRef]

67. d'Afflisio, E.; Braca, P.; Millefiori, L.M.; Willett, P. Maritime Anomaly Detection Based on Mean-Reverting Stochastic Processes Applied to a Real-World Scenario. In Proceedings of the 2018 21st International Conference on Information Fusion (FUSION), Cambridge, UK, 10–13 July 2018; pp. 1171–1177.
68. Haruna, M.; Gebremeskel, K.G.; Troscia, M.; Tardo, A.; Pagano, P. Mechanisms for Securing Autonomous Shipping Services and Machine Learning Algorithms for Misbehaviour Detection. *Telecom* **2024**, *5*, 1031–1050. [CrossRef]
69. Tirkolaee, E.B.; Sadeghi, S.; Mooseloo, F.M.; Vandchali, H.R.; Aeini, S. Application of machine learning in supply chain management: A comprehensive overview of the main areas. *Math. Probl. Eng.* **2021**, *1*, 1476043. [CrossRef]
70. Yang, Z.; Li, S.; Da, X.; Wang, J.; Yang, K.; Ma, Y. Robust Online Compensation and Magnetic Anomaly Detection on a Rotating Platform with Three-Axis Magnetometers. *IEEE Trans. Geosci. Remote Sens.* **2025**, *63*, 1–11. [CrossRef]
71. Shahir, H.Y.; Glasser, U.; Shahir, A.Y.; Wehn, H. Maritime Situation Analysis Framework: Vessel Interaction Classification and Anomaly Detection. In Proceedings of the 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, USA, 29 October–1 November 2015; pp. 1279–1289.
72. Choo, K.-K.R.; Dehghantanha, A.; Dietrich, G. Machine Learning and Cyber Threat Intelligence and Analytics: An Overview and Introduction to the Mini-Track. In Proceedings of the 54th Hawaii International Conference on System Sciences, Koloa, Kauai, HI, USA, 5–8 January 2021.
73. Zainudin, A.; Alief, R.N.; Putra, M.A.P.; Akter, R.; Kim, D.-S.; Lee, J.-M. Blockchain-Based Decentralized Trust Aggregation for Federated Cyber-Attacks Classification in SDN-Enabled Maritime Transportation Systems. In Proceedings of the 2023 IEEE International Conference on Communications Workshops (ICC Workshops), Rome, Italy, 28 May 2023; pp. 182–187.
74. Abielmona, R.; Falcon, R.; Vachon, P.W.; Groza, V.Z. Vessel Tracking and Anomaly Detection Using Level 0/1 and High-Level Information Fusion Techniques. In *Soft Computing Applications*; Balas, V.E., Jain, L.C., Kovačević, B., Eds.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2016; Volume 357, pp. 769–780, ISBN 978-3-319-18415-9.
75. Huang, J.; Zhu, F.; Huang, Z.; Wan, J.; Ren, Y. Research on Real-Time Anomaly Detection of Fishing Vessels in a Marine Edge Computing Environment. *Mob. Inf. Syst.* **2021**, *2021*, 1–15. [CrossRef]
76. Syed, M.A.B.; Ahmed, I. A CNN-LSTM Architecture for Marine Vessel Track Association Using Automatic Identification System (AIS) Data. *Sensors* **2023**, *23*, 6400. [CrossRef]
77. Glashier, T.; Kromanis, R.; Buchanan, C. Temperature-Based Damage Detection for the Commissioning Dataset of the MX3D Bridge. *E-J. Nondestruct. Test.* **2024**, *29*, 1–8. [CrossRef]
78. Czaplewski, B.; Dzwonkowski, M. A Novel Approach Exploiting Properties of Convolutional Neural Networks for Vessel Movement Anomaly Detection and Classification. *ISA Trans.* **2022**, *119*, 1–16. [CrossRef]
79. He, J.; Liu, Z.; Zhang, Y.; Jin, Z.; Zhang, Q. Power Allocation Based on Federated Multi-Agent Deep Reinforcement Learning for NOMA Maritime Networks. *IEEE Internet Things J.* **2025**. [CrossRef]
80. Cheng, R.; Liang, M.; Li, H.; Yuen, K.F. Benchmarking Feed-Forward Randomized Neural Networks for Vessel Trajectory Prediction. *Comput. Electr. Eng.* **2024**, *119*, 109499. [CrossRef]
81. Murray, B.; Perera, L.P. Unsupervised Trajectory Anomaly Detection for Situation Awareness in Maritime Navigation. In Proceedings of the Volume 6A: Ocean Engineering; American Society of Mechanical Engineers, Virtual, 3 August 2020; p. V06AT06A024.
82. Aurdal, L.; Løkken, K.H.; Klausen, R.A.; Brattli, A.; Palm, H.C. Adversarial Camouflage (AC) for Naval Vessels. In Proceedings of the Artificial Intelligence and Machine Learning in Defense Applications, SPIE, Strasbourg, France, 19 September 2019; p. 17.
83. Zheng, H.; Zhu, W.; Wu, Y.; Chen, P. Detection of Abnormal Ship Trajectory Points Based on Statistical Learning. In Proceedings of the 2022 International Conference on Computer Technologies (ICCTech), Melaka, Malaysia, 24–26 February 2022; pp. 110–115.
84. Olesen, K.V.; Boubekki, A.; Kampffmeyer, M.C.; Jenssen, R.; Christensen, A.N.; Hørlück, S.; Clemmensen, L.H. A Contextually Supported Abnormality Detector for Maritime Trajectories. *J. Mar. Sci. Eng.* **2023**, *11*, 2085. [CrossRef]
85. Yousaf, A.; Amro, A.; Kwa, P.T.H.; Li, M.; Zhou, J. Cyber Risk Assessment of Cyber-Enabled Autonomous Cargo Vessel. *Int. J. Crit. Infrastruct. Prot.* **2024**, *46*, 100695. [CrossRef]
86. Thomopoulos, S.C.A.; Rizogannis, C.; Thanos, K.G.; Dimitros, K.; Panou, K.; Zacharakis, D. OCULUS Sea$^{TM}$ Forensics: An Anomaly Detection Toolbox for Maritime Surveillance. In *Business Information Systems Workshops*; Abramowicz, W., Corchuelo, R., Eds.; Lecture Notes in Business Information Processing; Springer International Publishing: Cham, Switzerland, 2019; Volume 373, pp. 485–495, ISBN 978-3-030-36690-2.
87. Svenson, P.; Holst, A.; Wallberg, A.; Nevalainen, P.; Farahnakian, F.; Álamo, A.; Germinara, V.; Schweizer, D.; Leicht, M.; Anneken, M.; et al. AI-ARC Baltic Demo: Detecting Illegal Activities at Sea. In Proceedings of the 2024 27th International Conference on Information Fusion (FUSION), Venice, Italy, 8 July 2024; pp. 1–8.
88. Pitropakis, N.; Logothetis, M.; Andrienko, G.; Stefanatos, J.; Karapistoli, E.; Lambrinoudakis, C. Towards the Creation of a Threat Intelligence Framework for Maritime Infrastructures. In *Computer Security*; Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., et al., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 11980, pp. 53–68, ISBN 978-3-030-42047-5.

89. Nita, C.; Vandewal, M. CNN-Based Object Detection and Segmentation for Maritime Domain Awareness. In Proceedings of the Artificial Intelligence and Machine Learning in Defense Applications II, SPIE, Online Only, 20 September 2020; p. 4.
90. Emerson, T.H.; Doster, T.; Olson, C.C. Path-Based Background Model Augmentation for Hyperspectral Anomaly Detection. In Proceedings of the 2018 9th Workshop on Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS), Amsterdam, The Netherlands, 23–26 September 2018; pp. 1–5.
91. Bombara, G.; Vasile, C.-I.; Penedo, F.; Yasuoka, H.; Belta, C. A Decision Tree Approach to Data Classification Using Signal Temporal Logic. In Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, ACM, Vienna, Austria, 11 April 2016; pp. 1–10.
92. Tian, B.; Wu, Y.; Hong, H. A Review of Research on Magnetic Detection Methods for Underwater Target. In Proceedings of the 2024 3rd International Conference on Artificial Intelligence and Computer Information Technology (AICIT), Yichang, China, 20 September 2024; pp. 1–6.
93. Burton, J.; Soare, S.R. Understanding the Strategic Implications of the Weaponization of Artificial Intelligence. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019; pp. 1–17.
94. Gkerekos, C.; Lazakis, I.; Theotokatos, G. *Exploiting Machine Learning for Ship Systems Anomaly Detection and Healthiness Forecasting*; Royal Institution of Naval Architects: London, UK, 2018.
95. Christos, S.C.; Panayiotis, T.; Panagiotis, P.; Nikos, D.; Tzioridis, Z.; Christos, G. Development of a Novel Decision-Making Tool for Vessel Efficiency Optimization Using IoT and DL. In Proceedings of the 2021 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, 7 December 2021; pp. 479–483.
96. Freitas, S.; Silva, H.; Almeida, J.M.; Silva, E. Convolutional Neural Network Target Detection in Hyperspectral Imaging for Maritime Surveillance. *Int. J. Adv. Robot. Syst.* **2019**, *16*, 1729881419842991. [CrossRef]
97. Nguyen, D.; Vadaine, R.; Hajduch, G.; Garello, R.; Fablet, R. A Multi-Task Deep Learning Architecture for Maritime Surveillance Using AIS Data Streams. In Proceedings of the 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA), Turin, Italy, 1–3 October 2018; pp. 331–340.
98. Gunes, B.; Kayisoglu, G.; Bolat, P. Cyber Security Risk Assessment for Seaports: A Case Study of a Container Port. *Comput. Secur.* **2021**, *103*, 102196. [CrossRef]
99. Kontopoulos, I.; Varlamis, I.; Tserpes, K. A Distributed Framework for Extracting Maritime Traffic Patterns. *Int. J. Geogr. Inf. Sci.* **2021**, *35*, 767–792. [CrossRef]
100. Yoo, J.; Jo, Y. Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology. *Sensors* **2023**, *23*, 5033. [CrossRef]
101. Gribbestad, M.; Hassan, M.U.; Hameed, I.A. Transfer Learning for Prognostics and Health Management (PHM) of Marine Air Compressors. *J. Mar. Sci. Eng.* **2021**, *9*, 47. [CrossRef]
102. Dhoot, A.; Nazarov, A.N.; Koupaei, A.N.A. A Security Risk Model for Online Banking System. In Proceedings of the 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, IEEE, Moscow, Russia, 19–20 March 2020; pp. 1–4.
103. Huang, H.; Xu, B.; Luo, H.; Zhuang, H.; Liu, X.; Ma, L. Anomaly Detection-Oriented High-Frequency Signal Storage for Diesel Engines. In Proceedings of the 2021 IEEE 4th International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 13 August 2021; pp. 360–363.
104. Schaum, A.; Allman, E.; Stites, M. Clairvoyant Fusion Detection of Ocean Anomalies in WorldView-2 Spectral Imagery. In Proceedings of the SPIE Optical Engineering + Applications, San Diego, CA, USA, 19 September 2016; p. 99760G.
105. Hoque, X.; Sharma, S.K. Ensembled Deep Learning Approach for Maritime Anomaly Detection System. In *Proceedings of ICETIT 2019*; Singh, P.K., Panigrahi, B.K., Suryadevara, N.K., Sharma, S.K., Singh, A.P., Eds.; Lecture Notes in Electrical Engineering; Springer International Publishing: Cham, Switzerland, 2020; Volume 605, pp. 862–869, ISBN 978-3-030-30576-5.
106. Kharchenko, V.; Illiashenko, O.; Fesenko, H.; Babeshko, I. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis. In *Multimedia Communications, Services and Security*; Dziech, A., Mees, W., Niemiec, M., Eds.; Communications in Computer and Information Science; Springer International Publishing: Cham, Switzerland, 2022; Volume 1689, pp. 66–79, ISBN 978-3-031-20214-8.
107. Botts, C.H. A Novel Metric for Detecting Anomalous Ship Behavior Using a Variation of the DBSCAN Clustering Algorithm. *SN Comput. Sci.* **2021**, *2*, 412. [CrossRef]
108. Zhou, A.; Zhu, Q.; Zhang, J.; Meng, K. Ship Intrusion Detection Technology Based on Bayesian Optimization Algorithm and XGBoost. In Proceedings of the 2023 3rd International Conference on Electrical Engineering and Control Science (IC2ECS), Hangzhou, China, 29 December 2023; pp. 1647–1652.
109. Zor, C.; Kittler, J. Maritime Anomaly Detection in Ferry Tracks. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 2647–2651.
110. Keane, K.R. Detecting Motion Anomalies. In Proceedings of the 8th ACM SIGSPATIAL Workshop on GeoStreaming, ACM, Redondo Beach, CA, USA, 7 November 2017; pp. 21–28.

111. Hasan, H.R.; Salah, K. Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters. *IEEE Access* **2018**, *6*, 46781–46793. [CrossRef]
112. Lee, J.; Nam, D.-W.; Lee, J.; Moon, S.; Oh, A.; Yoo, W. A Study on the Composition of Image-Based Ship-Type/Class Identification System. In Proceedings of the 2020 22nd International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 16–19 February 2020; pp. 203–206.
113. Srivastava, A.; Gupta, V.; Malik, P. AI-Driven Maritime Anomaly Detection Using Enhanced Feature Encoding and Transfer Learning. *arXiv* **2024**, arXiv:2401.00112. [CrossRef]
114. Li, M.; Zhou, J.; Chattopadhyay, S.; Goh, M. Maritime Cybersecurity: A Comprehensive Review. *arXiv* **2024**, arXiv:2409.11417. [CrossRef]
115. Li, X.; Du, Y.; Chen, Y.; Nguyen, S.; Zhang, W.; Schönborn, A.; Sun, Z. Data Fusion and Machine Learning for Ship Fuel Efficiency Modeling: Part I—Voyage Report Data and Meteorological Data. *Commun. Transp. Res.* **2022**, *2*, 100074. [CrossRef]
116. Nikula, R.-P.; Ruusunen, M.; Böhme, S.A. On Training Data Selection in Condition Monitoring Applications—Case Azimuth Thrusters. *Appl. Sci.* **2022**, *12*, 4024. [CrossRef]
117. Wang, T.; Ye, C.; Zhou, H.; Ou, M.; Cheng, B. AIS Ship Trajectory Clustering Based on Convolutional Auto-Encoder. In *Intelligent Systems and Applications*; Arai, K., Kapoor, S., Bhatia, R., Eds.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2021; Volume 1251, pp. 529–546, ISBN 978-3-030-55186-5.
118. Soleimani, B.H.; Souza, E.N.D.; Hilliard, C.; Matwin, S. Anomaly Detection in Maritime Data Based on Geometrical Analysis of Trajectories. In Proceedings of the 18th International Conference on Information Fusion, Washington, DC, USA, 6–9 July 2015.
119. Pappagallo, A.; Ortame, F.; Massacci, G.; Sisti, F.; Pugliese, F. Deep Learning for the Classification of Ports in Maritime Transport Statistics via AIS Data. In *Learning and Intelligent Optimization*; Festa, P., Ferone, D., Pastore, T., Pisacane, O., Eds.; Lecture Notes in Computer Science; Springer Nature Switzerland: Cham, Switzerland, 2025; Volume 14990, pp. 318–332, ISBN 978-3-031-75622-1.
120. Mazzarella, F.; Vespe, M.; Alessandrini, A.; Tarchi, D.; Aulicino, G.; Vollero, A. A Novel Anomaly Detection Approach to Identify Intentional AIS On-off Switching. *Expert Syst. Appl.* **2017**, *78*, 110–123. [CrossRef]
121. Nguyen, D.; Simonin, M.; Hajduch, G.; Vadaine, R.; Tedeschi, C.; Fablet, R. Detection of Abnormal Vessel Behaviours from AIS Data Using GeoTrackNet: From the Laboratory to the Ocean. In Proceedings of the 2020 21st IEEE International Conference on Mobile Data Management (MDM), Versailles, France, 30 June–3 July 2020; pp. 264–268.
122. Androjna, A.; Perkovič, M.; Pavic, I.; Mišković, J. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Appl. Sci.* **2021**, *11*, 5015. [CrossRef]
123. Sadeghi, Z.; Matwin, S. Anomaly Detection for Maritime Navigation Based on Probability Density Function of Error of Reconstruction. *J. Intell. Syst.* **2023**, *32*, 20220270. [CrossRef]
124. Boudehenn, C.; Jacq, O.; Lannuzel, M.; Cexus, J.-C.; Boudraa, A. Navigation Anomaly Detection: An Added Value for Maritime Cyber Situational Awareness. In Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14 June 2021; pp. 1–4.
125. Zhu, F. Abnormal Vessel Trajectories Detection in a Port Area Based on AIS Data. In Proceedings of the ICTE 2015, American Society of Civil Engineers, Dailan, China, 25 September 2015; pp. 2043–2049.
126. Zang, Y.; Mukherjee, A.; Fei, C.; Liu, T.; Lampropoulos, G. Deep Learning for Anomaly Detection in Maritime Vessels Using AIS-Cued Camera Imagery. In Proceedings of the SPIE Defence + Security, Anaheim, CA, USA, 4 May 2017; p. 101900G.
127. Velasco-Gallego, C.; Lazakis, I. RADIS: A Real-Time Anomaly Detection Intelligent System for Fault Diagnosis of Marine Machinery. *Expert Syst. Appl.* **2022**, *204*, 117634. [CrossRef]
128. Bouritsas, G.; Daveas, S.; Danelakis, A.; Thomopoulos, S.C.A. Automated Real-Time Anomaly Detection in Human Trajectories Using Sequence to Sequence Networks. In Proceedings of the 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Taipei, Taiwan, 18–21 September 2019; pp. 1–8.
129. Liu, D.; Shi, G. Ship Collision Risk Assessment Based on Collision Detection Algorithm. *IEEE Access* **2020**, *8*, 161969–161980. [CrossRef]
130. Yang, Y.; Liu, Y.; Li, G.; Zhang, Z.; Liu, Y. Harnessing the Power of Machine Learning for AIS Data-Driven Maritime Research: A Comprehensive Review. *Transp. Res. Part E Logist. Transp. Rev.* **2024**, *183*, 103426. [CrossRef]
131. Zhang, C.; Liu, J.; Zhi, J.; Zhang, X.; Wang, J.; Wu, Z. OceanCL-IDS: A Continual Learning-Based Intrusion Detection System for Ocean-Going Ship-Satellite Communication Network. In Proceedings of the 2023 7th International Conference on Transportation Information and Safety (ICTIS), Xi'an, China, 4 August 2023; pp. 1150–1155.
132. Zhang, Y.; Jin, Q.; Liang, M.; Ma, R.; Liu, R.W. Vessel Behavior Anomaly Detection Using Graph Attention Network. In *Neural Information Processing*; Luo, B., Cheng, L., Wu, Z.-G., Li, H., Li, C., Eds.; Lecture Notes in Computer Science; Springer Nature Singapore: Singapore, 2024; Volume 14451, pp. 291–304, ISBN 978-981-99-8072-7.
133. Ha, X.S.; Le, H.T.; Metoui, N.; Duong-Trung, N. DeM-CoD: Novel Access-Control-Based Cash on Delivery Mechanism for Decentralized Marketplace. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2020; pp. 71–78.

134. Sicard, F.; Hotellier, E.; Francq, J. An Industrial Control System Physical Testbed for Naval Defense Cybersecurity Research. In Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 6–10 June 2022; pp. 413–422.
135. Elsisi, M.; Yu, J.-T.; Lai, C.-C.; Su, C.-L. A Drone-Assisted Deep Learning-Based IoT System for Monitoring Ship Emissions in Ports Considering Adversarial Attacks. *IEEE Trans. Instrum. Meas.* **2024**, *73*, 1–11. [CrossRef]
136. Janani, K.; Ramamoorthy, S. IoT Security and Privacy Using Deep Learning Model: A Review. In Proceedings of the 2021 International Conference on Intelligent Technologies (CONIT), Hubli, India, 25 June 2021; pp. 1–6.
137. Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y.B. A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 2677–2690. [CrossRef]
138. Asalomia, L.B.; Nita, S.L.; Mihailescu, M.I.; Marascu, V.; Samoilescu, G.; Racuciu, C. AI-Enabled Analysis of Electric Signals from Gyrocompass for Enhanced Navigation Management with Cybersecurity Considerations. In Proceedings of the 2023 8th International Conference on Mathematics and Computers in Sciences and Industry (MCSI), Athens, Greece, 14 October 2023; pp. 107–115.
139. Queiroz, M.M.; Telles, R.; Bonilla, S.H. Blockchain and Supply Chain Management Integration: A Systematic Review of the Literature. *Supply Chain Manag.* **2020**, *25*, 241–254. [CrossRef]
140. Michałowska, K.; Riemer-Sørensen, S.; Sterud, C.; Hjellset, O.M. Anomaly Detection with Unknown Anomalies: Application to Maritime Machinery. *IFAC-Pap.* **2021**, *54*, 105–111. [CrossRef]
141. Wang, Y.; Chen, P.; Wu, B.; Wan, C.; Yang, Z. A Trustable Architecture over Blockchain to Facilitate Maritime Administration for MASS Systems. *Reliab. Eng. Syst. Saf.* **2022**, *219*, 108246. [CrossRef]
142. Yang, T.; Cui, Z.; Alshehri, A.H.; Wang, M.; Gao, K.; Yu, K. Distributed Maritime Transport Communication System With Reliability and Safety Based on Blockchain and Edge Computing. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 1–11. [CrossRef]
143. Antunes, N.; Ferreira, J.C.; Pereira, J.; Rosa, J. Grid-Based Vessel Deviation from Route Identification with Unsupervised Learning. *Appl. Sci.* **2022**, *12*, 11112. [CrossRef]
144. Han, P.; Ellefsen, A.L.; Li, G.; Holmeset, F.T.; Zhang, H. Fault Detection With LSTM-Based Variational Autoencoder for Maritime Components. *IEEE Sens. J.* **2021**, *21*, 21903–21912. [CrossRef]
145. Bobrovnikova, K.; Lysenko, S.; Hurman, I.; Kwiecień, A. Machine Learning Based Techniques for Cyberattacks Detection in the Internet of Things Infrastructure. In Proceedings of the IntelITSIS'2022: 3rd International Workshop on Intelligent Information Technologies and Systems of Information Security, Khmelnytskyi, Ukraine, 23–25 March 2022.
146. Terzi, S.; Zacharaki, A.; Nizamis, A.; Votis, K.; Ioannidis, D.; Tzovaras, D.; Stamelos, I. Transforming the Supply-Chain Management and Industry Logistics with Blockchain Smart Contracts. In Proceedings of the 23rd Pan-Hellenic Conference on Informatics, ACM, Nicosia, Cyprus, 28 November 2019; pp. 9–14.
147. Boudehenn, C.; Cexus, J.-C.; Boudraa, A.A. A Data Extraction Method for Anomaly Detection in Naval Systems. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–4.
148. Cocker, E.; Bert, J.A.; Torres, F.; Shreve, M.; Kalb, J.; Lee, J.; Poimboeuf, M.; Fautley, P.; Adams, S.; Lee, J.; et al. Low-Cost, Intelligent Drifter Fleet for Large-Scale, Distributed Ocean Observation. In Proceedings of the OCEANS 2022, Hampton Roads, IEEE, Hampton Roads, VA, USA, 17 October 2022; pp. 1–8.
149. Singh Popli, M.; Singh, R.P.; Kaur Popli, N.; Mamun, M. A Federated Learning Framework for Enhanced Data Security and Cyber Intrusion Detection in Distributed Network of Underwater Drones. *IEEE Access* **2025**, *13*, 12634–12646. [CrossRef]
150. Xu, X.A.; Lin, Y.; Ye, C. Fault diagnosis of marine machinery via an intelligent data-driven framework. *Ocean Eng.* **2023**, *289*, 116302. [CrossRef]
151. Graser, A.; Weissenfeld, A.; Heistracher, C.; Dragaschnig, M.; Widhalm, P. Federated Learning for Anomaly Detection in Maritime Movement Data. In Proceedings of the 2024 25th IEEE International Conference on Mobile Data Management (MDM), Brussels, Belgium, 24 June 2024; pp. 77–82.
152. Szarmach, M.; Czarnowski, I. Multi-Label Classification for AIS Data Anomaly Detection Using Wavelet Transform. *IEEE Access* **2022**, *10*, 109119–109131. [CrossRef]
153. Koola, P.M. Cybersecurity: A Deep Dive Into the Abyss. *Mar. Technol. Soc. J.* **2018**, *52*, 31–43. [CrossRef]
154. Shi, Y.; Long, C.; Yang, X.; Deng, M. Abnormal Ship Behavior Detection Based on AIS Data. *Appl. Sci.* **2022**, *12*, 4635. [CrossRef]
155. Badrudin, A.; Sumantri, S.H.; Gultom, R.A.G.; Apriyanto, N.P.; Wijaya, H.R.; Sutedja, I. Ship Trajectory Prediction for Anomaly Detection Using Ais Data and Artificial Intelligence: A Systematic Literature Review. *J. Theor. Appl. Inf. Technol.* **2023**, *101*, 50929–50937.
156. Pool, J.; Beyrami, E.; Gopal, V.; Aazami, A.; Gupchup, J.; Rowland, J.; Li, B.; Kanani, P.; Cutler, R.; Gehrke, J. Lumos: A Library for Diagnosing Metric Regressions in Web-Scale Applications. In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, ACM, Virtual Event, 23 August 2020; pp. 2562–2570.

157. Forti, N.; d'Afflisio, E.; Braca, P.; Millefiori, L.M.; Willett, P.; Carniel, S. Maritime Anomaly Detection in a Real-World Scenario: *Ever Given* Grounding in the Suez Canal. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 13904–13910. [CrossRef]
158. Jaszewski, M.; Parameswaran, S.; Hallenborg, E.; Bagnall, B. Evaluation of Maritime Object Detection Methods for Full Motion Video Applications Using the PASCAL VOC Challenge Framework. In Proceedings of the SPIE IS&T Electronic Imaging, San Francisco, CA, USA, 4 March 2015; p. 94070Y.
159. Bedja-Johnson, Z.; Wu, P.; Grande, D.; Anderlini, E. Smart Anomaly Detection for Slocum Underwater Gliders with a Variational Autoencoder with Long Short-Term Memory Networks. *Appl. Ocean Res.* **2022**, *120*, 103030. [CrossRef]
160. Handayani, M.P.; Antariksa, G.; Lee, J. Anomaly Detection in Vessel Sensors Data with Unsupervised Learning Technique. In Proceedings of the 2021 International Conference on Electronics, Information, and Communication (ICEIC), Jeju, Repubic of Korea, 31 January 2021; pp. 1–6.
161. Brandsæter, A.; Vanem, E.; Glad, I.K. Efficient On-Line Anomaly Detection for Ship Systems in Operation. *Expert Syst. Appl.* **2019**, *121*, 418–437. [CrossRef]
162. McKinnon, C.; Carroll, J.; McDonald, A.; Koukoura, S.; Plumley, C. Investigation of Anomaly Detection Technique for Wind Turbine Pitch Systems. *IET Conf. Proc.* **2021**, *2021*, 277–282. [CrossRef]
163. Jousselme, A.-L.; Pallotta, G. Dissecting Uncertainty-Based Fusion Techniques for Maritime Anomaly Detection. In Proceedings of the 2015 18th International Conference on Information Fusion (Fusion), Washington, DC, USA, 6–9 July 2015; p. 34.
164. Morariu, A.-R.; Lund, W.; Björkqvist, J. Engine Vibration Anomaly Detection in Vessel Engine Room. *IFAC-PapersOnLine* **2022**, *55*, 465–469. [CrossRef]
165. Sidibé, A.; Shu, G.; Ma, Y.; Wanqi, W. Big Data Framework for Abnormal Vessel Trajectories Detection Using Adaptive Kernel Density Estimation. In Proceedings of the 2nd International Conference on Big Data Research, ACM, Weihai, China, 27 October 2018; pp. 43–46.
166. Karataş, G.B.; Karagoz, P.; Ayran, O. Trajectory Pattern Extraction and Anomaly Detection for Maritime Vessels. *Internet Things* **2021**, *16*, 100436. [CrossRef]
167. Anneken, M.; Fischer, Y.; Beyerer, J. Evaluation and Comparison of Anomaly Detection Algorithms in Annotated Datasets from the Maritime Domain. In Proceedings of the 2015 SAI Intelligent Systems Conference (IntelliSys), London, UK, 10–11 November 2015; pp. 169–178.
168. Karatuğ, Ç.; Arslanoğlu, Y.; Guedes Soares, C. Design of a Decision Support System to Achieve Condition-Based Maintenance in Ship Machinery Systems. *Ocean Eng.* **2023**, *281*, 114611. [CrossRef]
169. Zhou, K.; Li, J.; Xiao, Y.; Yang, J.; Cheng, J.; Liu, W.; Luo, W.; Liu, J.; Gao, S. Memorizing Structure-Texture Correspondence for Image Anomaly Detection. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 2335–2349. [CrossRef]
170. Vadisetty, R.; Polamarasetti, A. Quantum Computing For Cryptographic Security With Artificial Intelligence. In Proceedings of the ICCMA, London, UK, 11–13 November 2024. [CrossRef]
171. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. In *Intelligent Information and Database Systems*; Nguyen, N.T., Jearanaitanakij, K., Selamat, A., Trawiński, B., Chittayasothorn, S., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12034, pp. 202–217, ISBN 978-3-030-42057-4.
172. Maganaris, C.; Protopapadakis, E.; Doulamis, N. Outlier Detection in Maritime Environments Using AIS Data and Deep Recurrent Architectures. *arXiv* **2024**, arXiv:2406.09966.
173. Han, X.; Armenakis, C.; Jadidi, M. DBSCAN Optimization for Improving Marine Trajectory Clustering and Anomaly Detection. *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2020**, *XLIII-B4-2020*, 455–461. [CrossRef]
174. Chang, S.-J.; Yeh, K.-H.; Peng, G.-D.; Chang, S.-M.; Huang, C.-H. From Safety to Security—Pattern and Anomaly Detections in Maritime Trajectories. In Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, 21–24 September 2015; pp. 415–419.
175. Jiao, J.-B.; Li, W.-F. Ship Abnormal Behavior Detection Based on KD-Tree and Clustering Algorithm. In Proceedings of the 2023 8th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 21 April 2023; pp. 1315–1318.
176. Fernández-Barrero, D.; Fontenla-Romero, O.; Lamas-López, F.; Novoa-Paradela, D.; R-Moreno, M.D.; Sanz, D. SOPRENE: Assessment of the Spanish Armada's Predictive Maintenance Tool for Naval Assets. *Appl. Sci.* **2021**, *11*, 7322. [CrossRef]
177. Brandsater, A.; Vanem, E.; Glad, I.K. Cluster Based Anomaly Detection with Applications in the Maritime Industry. In Proceedings of the 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), Shanghai, China, 16–18 August 2017; pp. 328–333.
178. Martínez, F.; Sànchez, L.E.; Santos-Olmo, A.; Rosado, D.G.; Fernàndez-Medina, E. Maritime cybersecurity: Protecting digital seas. *Int. J. Inf. Secur.* **2024**, *23*, 1429–1457. [CrossRef]

179. Zhou, K.; Xiao, Y.; Yang, J.; Cheng, J.; Liu, W.; Luo, W.; Gu, Z.; Liu, J.; Gao, S. Encoding Structure-Texture Relation with P-Net for Anomaly Detection in Retinal Images. In *Computer Vision—ECCV 2020*; Vedaldi, A., Bischof, H., Brox, T., Frahm, J.-M., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12365, pp. 360–377, ISBN 978-3-030-58564-8.
180. Vorkapić, A.; Radonja, R.; Babić, K.; Martinčić-Ipšić, S. Machine Learning Methods in Monitoring Operating Behaviour of Marine Two-Stroke Diesel Engine. *Transport* **2020**, *35*, 462–473. [CrossRef]
181. Kim, J.-S.; Lee, J.-S.; Kim, K.-I. Anomalous Vessel Behavior Detection Based on SVR Seaway Model. *Int. J. FUZZY Log. Intell. Syst.* **2019**, *19*, 18–27. [CrossRef]
182. Zhou, Y.; Wright, J.; Maskell, S. A Generic Anomaly Detection Approach Applied to Mixture-of-Unigrams and Maritime Surveillance Data. In Proceedings of the 2019 Sensor Data Fusion: Trends, Solutions, Applications (SDF), Bonn, Germany, 15–17 October 2019; pp. 1–6.
183. Monemi, M.; Fallah, M.A. A Novel Scheme for Determination of Vessel Heading Using Airborne Magnetic Wake Scanning. *Int. J. Appl. Electromagn. Mech.* **2023**, *71*, 261–271. [CrossRef]
184. Alvarez, M.; Arguedas, V.F.; Gammieri, V.; Mazzarella, F.; Vespe, M.; Aulicino, G. AIS Event-Based Knowledge Discovery for Maritime Situational Awareness. In Proceedings of the 19th International Conference on Information Fusion, Heidelberg, Germany, 5–8 July 2016; pp. 1874–1880.
185. Nikula, R.-P.; Ruusunen, M.; Keski-Rahkonen, J.; Saarinen, L.; Fagerholm, F. Probabilistic Condition Monitoring of Azimuth Thrusters Based on Acceleration Measurements. *Machines* **2021**, *9*, 39. [CrossRef]
186. Visky, G.; Rohl, A.; Katsikas, S.; Maennel, O. AIS Data Analysis: Reality in the Sea of Echos. In Proceedings of the 2024 IEEE 49th Conference on Local Computer Networks (LCN), Normandy, France, 8 October 2024; pp. 1–7.
187. Kumar, D.; Harris, S.; Daniel, L.; Hoare, E.; Pirkani, A.; Gashinova, M.; Cherniakov, M. Repeatable Wave Data for Sub-THz Radar Marine Target Detection Experiments. In Proceedings of the 2023 20th European Radar Conference (EuRAD), Berlin, Germany, 20 September 2023; pp. 148–151.
188. Li, H.; Li, W.; Wang, S.; Yang, H.; Guan, J.; Zhang, Y. STAD: Ship Trajectory Anomaly Detection in Ocean with Dynamic Pattern Clustering. *Ocean Eng.* **2024**, *313*, 119530. [CrossRef]
189. Magnussen, B.B.; Bläser, N.; Jensen, R.M.; Ylänen, K. Destination Prediction of Oil Tankers Using Graph Abstractions and Recurrent Neural Networks. In *Computational Logistics*; Mes, M., Lalla-Ruiz, E., Voß, S., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2021; Volume 13004, pp. 51–65, ISBN 978-3-030-87671-5.
190. Radon, A.N.; Wang, K.; Glasser, U.; Wehn, H.; Westwell-Roper, A. Contextual Verification for False Alarm Reduction in Maritime Anomaly Detection. In Proceedings of the 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, USA, 29 October–1 November 2015; pp. 1123–1133.
191. Anneken, M.; Jousselme, A.-L.; Robert, S.; Beyerer, J. Synthetic Trajectory Extraction for Maritime Anomaly Detection. In Proceedings of the 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 12–14 December 2018; pp. 1048–1053.
192. Öster, A. A Human Perception View on Holistic Anomaly Detection Systems for Maritime Engine Rooms. In Proceedings of the International Offshore and Polar Engineering Conference, Rhodes, Greece, 16–21 June 2024; Volume 1, p. 4310.
193. Maia, R.F.P.; Antunes, C.M. Anomaly Detection in Multivariate Temporal Data for Vessels Abnormal Behaviour Detection. In *CAPSI 2019 Proceedings*; AISEL: Lisbon, Portugal, 2019.
194. Rong, H.; Teixeira, A.P.; Soares, C.G. Maritime Traffic Network Extraction and Application Based on AIS Data. In Proceedings of the 2021 6th International Conference on Transportation Information and Safety (ICTIS), Wuhan, China, 22 October 2021; pp. 1244–1252.
195. Zheng, W.; Zhou, H.; Qiu, Z.; Ke, Z.; Tao, M.; Chen, Z. Sensor Correlation Network Based Anomaly Detection for Thermal Systems on Ships. In Proceedings of the 2020 IEEE 9th Data Driven Control and Learning Systems Conference (DDCLS), Liuzhou, China, 20 November 2020; pp. 302–307.
196. Kim, D.; Antariksa, G.; Handayani, M.P.; Lee, S.; Lee, J. Explainable Anomaly Detection Framework for Maritime Main Engine Sensor Data. *Sensors* **2021**, *21*, 5200. [CrossRef]
197. Felski, A.; Zwolak, K. The Ocean-Going Autonomous Ship—Challenges and Threats. *J. Mar. Sci. Eng.* **2020**, *8*, 41. [CrossRef]
198. Mbulwa, A.I.; Chekima, A.; Dargham, J.A.; Tung, Y.H.; Kitt, W.W. Anomaly Detection Using a Self-Sufficient Ad Hoc Electrical Impedance Tomography Sensor Deployed Within Imaged Space. *Int. J. Emerg. Technol. Adv. Eng.* **2019**, *9*, 101–105.
199. Gao, M.; Shi, G.; Li, S. Online Prediction of Ship Behavior with Automatic Identification System Sensor Data Using Bidirectional Long Short-Term Memory Recurrent Neural Network. *Sensors* **2018**, *18*, 4211. [CrossRef]
200. Cankar, M.; Petrovic, N.; Pita Costa, J.; Cernivec, A.; Antic, J.; Martincic, T.; Stepec, D. Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps. In Proceedings of the Companion of the 2023 ACM/SPEC International Conference on Performance Engineering, ACM, Coimbra, Portugal, 15 April 2023; pp. 201–205.

201. Zhang, B.; Hirayama, K.; Ren, H.; Wang, D.; Li, H. Ship Anomalous Behavior Detection Using Clustering and Deep Recurrent Neural Network. *J. Mar. Sci. Eng.* **2023**, *11*, 763. [CrossRef]
202. Guo, Z.-X.; Shui, P.-L. Anomaly Based Sea-Surface Small Target Detection Using K-Nearest Neighbor Classification. *IEEE Trans. Aerosp. Electron. Syst.* **2020**, *56*, 4947–4964. [CrossRef]
203. Progoulakis, I.; Nikitakos, N.; Dalaklis, D.; Yaacob, R. Cyber-Physical Security for Ports Infrastructure. *Int. Marit. Transp. Logist. J.* **2022**, *11*, 105. [CrossRef]
204. Eljabu, L.; Etemad, M.; Matwin, S. Anomaly Detection in Maritime Domain Based on Spatio-Temporal Analysis of AIS Data Using Graph Neural Networks. In Proceedings of the 2021 5th International Conference on Vision, Image and Signal Processing (ICVISP), Kuala Lumpur, Malaysia, 18–20 December 2021; pp. 142–147.
205. Amro, A.; Oruc, A.; Gkioulos, V.; Katsikas, S. Navigation Data Anomaly Analysis and Detection. *Information* **2022**, *13*, 104. [CrossRef]
206. Tu, E.; Zhang, G.; Rachmawati, L.; Rajabally, E.; Huang, G.-B. Exploiting AIS Data for Intelligent Maritime Navigation: A Comprehensive Survey From Data to Methodology. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 1559–1582. [CrossRef]
207. Venskus, J.; Treigys, P.; Bernatavičienė, J.; Tamulevičius, G.; Medvedev, V. Real-Time Maritime Traffic Anomaly Detection Based on Sensors and History Data Embedding. *Sensors* **2019**, *19*, 3782. [CrossRef] [PubMed]
208. Samonte, M.J.C.; Laurenio, E.N.B.; Lazaro, J.R.M. Enhancing Port and Maritime Cybersecurity Through AI-Enabled Threat Detection and Response. In Proceedings of the 2024 8th International Conference on Smart Grid and Smart Cities (ICSGSC), Shanghai, China, 25–27 October 2024; pp. 412–420. [CrossRef]
209. Pelissero, N.; Laso, P.M.; Puentes, J. Impact Assessment of Anomaly Propagation in a Naval Water Distribution Cyber-Physical System. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26 July 2021; pp. 518–523.
210. Ribeiro, C.V.; Paes, A.; Oliveira, D.D. AIS-Based Maritime Anomaly Traffic Detection: A Review. *Expert Syst. Appl.* **2023**, *231*, 120561. [CrossRef]
211. Gąsienica-Józkowy, J.; Knapik, M.; Cyganek, B. An Ensemble Deep Learning Method with Optimized Weights for Drone-Based Water Rescue and Surveillance. *Integr. Comput.-Aided Eng.* **2021**, *28*, 221–235. [CrossRef]
212. Potamos, G.; Stavrou, E.; Stavrou, S. Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis. *Sensors* **2024**, *24*, 3458. [CrossRef]
213. Xia, Z.; Gao, S. Analysis of Vessel Anomalous Behavior Based on Bayesian Recurrent Neural Network. In Proceedings of the 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), Chengdu, China, 1 April 2020; pp. 393–397.
214. Moharir, M.; Adyathimar, K.B.; Shobha, G.; Soni, V. Scapy Scripting to Automate Testing of Networking Middleboxes. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 293–298. [CrossRef]
215. Hu, Y.; Li, Y.; Pan, Z. A Dual-Polarimetric SAR Ship Detection Dataset and a Memory-Augmented Autoencoder-Based Detection Method. *Sensors* **2021**, *21*, 8478. [CrossRef]
216. Smith, J.; Nouretdinov, I.; Craddock, R.; Offer, C.; Gammerman, A. Conformal Anomaly Detection of Trajectories with a Multi-Class Hierarchy. In *Statistical Learning and Data Sciences*; Gammerman, A., Vovk, V., Papadopoulos, H., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2015; Volume 9047, pp. 281–290, ISBN 978-3-319-17090-9.
217. Smith, P.F.; Thulasiraman, P.; Oriti, G.; Vygoder, M.; Gudex, J. Anomaly Detection in Shipboard Operational Technology Systems Using Cyber Analytics. In Proceedings of the 2024 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), Taichung, Taiwan, 6 November 2024; pp. 1–7.
218. Toloue, K.F.; Jahan, M.V. Anomalous Behavior Detection of Marine Vessels Based on Hidden Markov Model. In Proceedings of the 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), Kerman, Iran, 28 February–2 March 2018; pp. 10–12.
219. Coleman, J.; Kandah, F.; Huber, B. Behavioral Model Anomaly Detection in Automatic Identification Systems (AIS). In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0481–0487.
220. Neves, J.; Maia, R.; Conceicao, V.; Marques, M.M. Behaviour Analysis and Anomaly Detection Algorithms for the Maritime Integrated Surveillance Awareness. In Proceedings of the 2019 IEEE Underwater Technology (UT), Kaohsiung, Taiwan, 16–19 April 2019; pp. 1–5.
221. Kullberg, A.; Skog, I.; Hendeby, G. Learning Motion Patterns in AIS Data and Detecting Anomalous Vessel Behavior. In Proceedings of the 2021 IEEE 24th International Conference on Information Fusion (FUSION), Sun City, South Africa, 1 November 2021; pp. 1–8.
222. Liu, B.; de Souza, E.N.; Hilliard, C.; Matwin, S. Ship Movement Anomaly Detection Using Specialized Distance Measures. In Proceedings of the 18th International Conference on Information Fusion, Washington, DC, USA, 6–9 July 2015; pp. 1113–1120.
223. Kumar, P.; Maharajan, A. Maritime Cybersecurity Leveraging Artificial Intelligence Mechanisms Unveiling Recent Innovations and Projecting Future Trends. *KSII Trans. Internet Inf. Syst.* **2024**, *18*, 3010–3039. [CrossRef]

224. Lalasa, K.L.; Srija, R.J.V.; Kumar, K.P. Maritime Security—Illegal Fishing Detection Using Deep Learning. In Proceedings of the 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chikkaballapur, India, 18 April 2024; pp. 1–5.
225. Musgrave, P.; Thulasiraman, P. FDIA Detection Methods on a Navy Smart Grid AMI Data Set Using Autoenocoder Neural Networks: A Case Study. In Proceedings of the 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2022; pp. 876–882.
226. Klemm, J.; Niemi, A.; Sill Torres, F. Predicting Ship Tracks in Waterways Using Long Short-Term Memory. In Proceedings of the OCEANS 2024—Halifax, IEEE, Halifax, NS, Canada, 23 September 2024; pp. 1–7.
227. Herrera, M.; Sasidharan, M.; Merino, J.; Parlikad, A.K. Handling Irregularly Sampled IoT Time Series to Inform Infrastructure Asset Management. *IFAC-PapersOnLine* **2022**, *55*, 241–245. [CrossRef]
228. Yang, Y.; He, D.; Vijayakumar, P.; Gupta, B.B.; Xie, Q. An Efficient Identity-Based Aggregate Signcryption Scheme With Blockchain for IoT-Enabled Maritime Transportation System. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 1520–1531. [CrossRef]
229. Bao, J.; Zheng, X.; Zhang, J.; Ji, X.; Zhang, J. Data-Driven Process Planning for Shipbuilding. *Artif. Intell. Eng. Des. Anal. Manuf.* **2018**, *32*, 122–130. [CrossRef]
230. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cyber-Attacks Against the Autonomous Ship. In *Computer Security*; Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2019; Volume 11387, pp. 20–36, ISBN 978-3-030-12785-5.
231. Sedik, A.; Emara, H.M.; Hamad, A.; Shahin, E.M.; A. El-Hag, N.; Khalil, A.; Ibrahim, F.; Elsherbeny, Z.M.; Elreefy, M.; Zahran, O.; et al. Efficient Anomaly Detection from Medical Signals and Images. *Int. J. Speech Technol.* **2019**, *22*, 739–767. [CrossRef]
232. Liang, M.; Weng, L.; Gao, R.; Li, Y.; Du, L. Unsupervised Maritime Anomaly Detection for Intelligent Situational Awareness Using AIS Data. *Knowl.-Based Syst.* **2024**, *284*, 111313. [CrossRef]
233. Durlik, I.; Miller, T.; Kostecka, E.; Tuński, T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. *Appl. Sci.* **2024**, *14*, 8420. [CrossRef]
234. Laxhammar, R.; Falkman, G. Inductive Conformal Anomaly Detection for Sequential Detection of Anomalous Sub-Trajectories. *Ann. Math. Artif. Intell.* **2015**, *74*, 67–94. [CrossRef]
235. Zhao, L.; Shi, G. Maritime Anomaly Detection Using Density-Based Clustering and Recurrent Neural Network. *J. Navig.* **2019**, *72*, 894–916. [CrossRef]
236. Liu, Y.; Duan, Y.; Gong, S.; Wang, M. Performance Optimization of Maritime IoT Communication under MIMO–Massive 5G with Uncertain Turbulence. *Phys. Commun.* **2022**, *53*, 101713. [CrossRef]
237. Khalil, A.A.; Rahman, M.A. SHIP: Securing Hashed Timelock Contracts in Payment Channel Networks. In Proceedings of the 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, 2 October 2023; pp. 1–2.
238. Chen, S.; Huang, Y.; Lu, W. Anomaly Detection and Restoration for AIS Raw Data. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–11. [CrossRef]
239. Forti, N.; Millefiori, L.M.; Braca, P.; Willett, P. Anomaly Detection and Tracking Based on Mean–Reverting Processes with Unknown Parameters. In Proceedings of the ICASSP 2019—2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 12–17 May 2019; pp. 8449–8453.
240. Pu, S.; Lam, J.S.L. Blockchain adoptions in the maritime industry: A conceptual framework. *Marit. Policy Manag.* **2021**, *48*, 777–794. [CrossRef]
241. Wang, Y.; Liu, J.; Liu, R.W.; Liu, Y.; Yuan, Z. Data-driven methods for detection of abnormal ship behavior: Progress and trends. *Ocean Eng.* **2023**, *271*, 113673. [CrossRef]
242. Anneken, M.; Fischer, Y.; Beyerer, J. A Multi-Agent Approach to Model and Analyze the Behavior of Vessels in the Maritime Domain. In Proceedings of the 9th International Conference on Agents and Artificial Intelligence, Porto, Portugal, 24–26 February 2017; pp. 200–207.
243. May Petry, L.; Soares, A.; Bogorny, V.; Brandoli, B.; Matwin, S. Challenges in Vessel Behavior and Anomaly Detection: From Classical Machine Learning to Deep Learning. In *Advances in Artificial Intelligence*; Goutte, C., Zhu, X., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12109, pp. 401–407, ISBN 978-3-030-47357-0.
244. Susanto, H.; Wibisono, G. Marine Vessel Telemetry Data Processing Using Machine Learning. In Proceedings of the 2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Bandung, Indonesia, 18–20 September 2019; pp. 128–135.
245. Pelissero, N.; Laso, P.M.; Jacq, O.; Puentes, J. Towards Modeling of Naval Systems Interdependencies for Cybersecurity. In Proceedings of the OCEANS 2021, IEEE, San Diego, CA, USA, 20 September 2021; pp. 1–7.
246. Zissis, D.; Chatzikokolakis, K.; Spiliopoulos, G.; Vodas, M. A Distributed Spatial Method for Modeling Maritime Routes. *IEEE Access* **2020**, *8*, 47556–47568. [CrossRef]

247. Alipek, S.; Mälzer, M.; Beck, S.; Kexel, C.; Moll, J.; Krozer, V.; Kassner, J.; Heinecke, T.; Rose, J.; Berger, M. Potential and Limitations of Anomaly Detection via Tower-Radar Monitoring of Wind Turbine Blades in Regular Operation with Convolutional Networks. *E-J. Nondestruct. Test.* **2024**, *29*, 1–11. [CrossRef]
248. Hoeber, O.; Ul Hasan, M. Supporting Event-Based Geospatial Anomaly Detection with Geovisual Analytics. In Proceedings of the 6th International Conference on Information Visualization Theory and Applications, Berlin, Germany, 11–14 March 2015; pp. 17–28.
249. Huang, Z.; Wan, J.; Huang, J.; Jia, G.; Zhang, W. A Collaborative Anomaly Detection Approach of Marine Vessel Trajectory (Short Paper). In *Collaborative Computing: Networking, Applications and Worksharing*; Wang, X., Gao, H., Iqbal, M., Min, G., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer International Publishing: Cham, Switzerland, 2019; Volume 292, pp. 279–294, ISBN 978-3-030-30145-3.
250. Feng, M.; Xu, H. MSNET-Blockchain: A New Framework for Securing Mobile Satellite Communication Network. In Proceedings of the 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–9.
251. d'Afflisio, E.; Braca, P.; Chisci, L.; Battistelli, G.; Willett, P. Maritime Anomaly Detection of Malicious Data Spoofing and Stealth Deviations from Nominal Route Exploiting Heterogeneous Sources of Information. In Proceedings of the 2021 IEEE 24th International Conference on Information Fusion (FUSION), Sun City, South Africa, 1 November 2021; pp. 1–7.
252. Zhang, B.; Ren, H.; Wang, P.; Wang, D. Research Progress on Ship Anomaly Detection Based on Big Data. In Proceedings of the 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 16 October 2020; pp. 316–320.
253. Ferlansyah, N.M.; Suharjito, S. A Systematic Literature Review of Vessel Anomaly Behavior Detection Methods Based on Automatic Identification System (AIS) and Another Sensor Fusion. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 287–292. [CrossRef]
254. Tyasayumranani, W.; Hwang, T.; Hwang, T.; Youn, I.-H. Anomaly Detection Model of Small-Scaled Ship for Maritime Autonomous Surface Ships' Operation. *J. Int. Marit. Saf. Environ. Aff. Shipp.* **2022**, *6*, 224–235. [CrossRef]
255. Kalogeraki, E.-M.; Papastergiou, S.; Mouratidis, H.; Polemi, N. A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments. *Appl. Sci.* **2018**, *8*, 1477. [CrossRef]
256. Pelissero, N.; Laso, P.M.; Puentes, J. Model Graph Generation for Naval Cyber-Physical Systems. In Proceedings of the OCEANS 2021, IEEE, San Diego, CA, USA, 20 September 2021; pp. 1–5.
257. Thakur, A.S.; Alex, T.L.; Nighojkar, A. Artificial Intelligence in Maritime Anomaly Detection: A Decadal Bibliometric Analysis (2014–2024). *J. Inst. Eng. India Ser. C* **2025**, *106*, 665–689. [CrossRef]
258. Sahoo, S.; Mohanta, R.K.; Pani, P.P.; Mohapatra, S.K.; Chakravarty, S. A Multi-Faceted Approach for Underwater Sonar Rock vs Mine Classification Using Machine Techniques. In Proceedings of the 2024 1st International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU), Bhubaneswar, India, 1 March 2024; pp. 1–5.
259. Seong, N.; Kim, J.; Lim, S. Graph-Based Anomaly Detection of Ship Movements Using CCTV Videos. *J. Mar. Sci. Eng.* **2023**, *11*, 1956. [CrossRef]
260. Kim, S.-Y.; Mukhiddinov, M. Data Anomaly Detection for Structural Health Monitoring Based on a Convolutional Neural Network. *Sensors* **2023**, *23*, 8525. [CrossRef]
261. Tienin, B.W.; Cui, G.; Nana, Y.A.T.; Ukwuoma, C.C.; Esidang, R.M.; Senouci, M.R. FedRS-Net: A Federated Learning Approach for Collaborative Multi-Modal Maritime Analytics. In Proceedings of the 2024 27th International Conference on Information Fusion (FUSION), Venice, Italy, 8 July 2024; pp. 1–8.
262. Liu, R.W.; Liang, M.; Nie, J.; Deng, X.; Xiong, Z.; Kang, J.; Yang, H.; Zhang, Y. Intelligent Data-Driven Vessel Trajectory Prediction in Marine Transportation Cyber-Physical System. In Proceedings of the 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Melbourne, Australia, 6–8 December 2021; pp. 314–321.
263. Mehri, S.; Alesheikh, A.A.; Basiri, A. A Context-Aware Approach for Vessels' Trajectory Prediction. *Ocean Eng.* **2023**, *282*, 114916. [CrossRef]
264. Schneider, J.; Klüner, A.; Zielinski, O. Towards Digital Twins of the Oceans: The Potential of Machine Learning for Monitoring the Impacts of Offshore Wind Farms on Marine Environments. *Sensors* **2023**, *23*, 4581. [CrossRef]
265. Xiong, W.; Guo, Y.; Yang, Q.; Yang, K.; Gao, Y.; Tian, Y. Risk Assessment for Search and Rescue Ships Based on Back Propagation Neural Network. In Proceedings of the 2020 6th International Conference on Big Data and Information Analytics (BigDIA), Shenzhen, China, 4–6 December 2020; pp. 289–294.
266. Guan, Y.; Xu, H.; Li, C. A Method of Ship Wake Detection in SAR Images Based on Reconstruction Features and Anomaly Detector. In Proceedings of the IGARSS 2023—2023 IEEE International Geoscience and Remote Sensing Symposium, IEEE, Pasadena, CA, USA, 16 July 2023; pp. 6398–6401.

267. Shin, H.; Lin, Q.; Son, J. Detecting Anomalies in AOA Data Measured for Indoor Positioning to Improve Accuracy. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 5895–5905.
268. Abreu, F.H.O.; Soares, A.; Paulovich, F.V.; Matwin, S. Local Anomaly Detection In Maritime Traffic Using Visual Analytics. In Proceedings of the Workshop Proceedings of the EDBT/ICDT 2021 Joint Conference on CEUR-WS.org, Nicosia, Cyprus, 23–26 March 2021.
269. Singh, S.K.; Fowdur, J.S.; Gawlikowski, J.; Medina, D. Leveraging Graph and Deep Learning Uncertainties to Detect Anomalous Maritime Trajectories. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 23488–23502. [CrossRef]
270. Palm, H.C.; Aurdal, L.; Brattli, A.; Glimsdal, E.; Klausen, R.A.; Løkken, K.H. Supporting Artificial Intelligence with Artificial Images. In Proceedings of the Target and Background Signatures IV, SPIE, Berlin, Germany, 9 October 2018; p. 21.
271. Wei, Z.; Xie, X.; Zhang, X. Maritime Anomaly Detection Based on a Support Vector Machine. *Soft Comput.* **2022**, *26*, 11553–11566. [CrossRef]
272. Ji, I.H.; Lee, J.H.; Kang, M.J.; Park, W.J.; Jeon, S.H.; Seo, J.T. Artificial Intelligence-Based Anomaly Detection Technology over Encrypted Traffic: A Systematic Literature Review. *Sensors* **2024**, *24*, 898. [CrossRef]
273. Kontopoulos, I.; Spiliopoulos, G.; Zissis, D.; Chatzikokolakis, K.; Artikis, A. Countering Real-Time Stream Poisoning: An Architecture for Detecting Vessel Spoofing in Streams of AIS Data. In Proceedings of the 2018 IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, 12–15 August 2018; pp. 981–986.
274. Fera, F.; Spandonidis, C. A Fault Diagnosis Approach Utilizing Artificial Intelligence for Maritime Power Systems within an Integrated Digital Twin Framework. *Appl. Sci.* **2024**, *14*, 8107. [CrossRef]
275. Sugathan, D.; Revanth, M.; Kumar, V.P.; Desai, S.; Keshava, L. eSPY Carting Systems: The Real-Time Tracking Mechanism Architecture. In Proceedings of the 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), Bangalore, India, 10–11 June 2021; pp. 184–190.
276. Li, K.; Guo, J.; Li, R.; Wang, Y.; Li, Z.; Miu, K.; Chen, H. The Abnormal Detection Method of Ship Trajectory with Adaptive Transformer Model Based on Migration Learning. In *Spatial Data and Intelligence*; Meng, X., Li, X., Xu, J., Zhang, X., Fang, Y., Zheng, B., Li, Y., Eds.; Lecture Notes in Computer Science; Springer Nature: Cham, Switzerland, 2023; Volume 13887, pp. 204–220, ISBN 978-3-031-32909-8.
277. Nguyen, D.; Vadaine, R.; Hajduch, G.; Garello, R.; Fablet, R. *GeoTrackNet* —A Maritime Anomaly Detector Using Probabilistic Neural Network Representation of AIS Tracks and *A Contrario* Detection. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 5655–5667. [CrossRef]
278. Osekowska, E.; Carlsson, B. Learning Maritime Traffic Rules Using Potential Fields. In *Computational Logistics*; Corman, F., Voß, S., Negenborn, R.R., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2015; Volume 9335, pp. 298–312, ISBN 978-3-319-24263-7.
279. Anneken, M.; Fischer, Y.; Beyerer, J. Anomaly Detection Using B-Spline Control Points as Feature Space in Annotated Trajectory Data from the Maritime Domain. In Proceedings of the 8th International Conference on Agents and Artificial Intelligence; SCITEPRESS—Science and and Technology Publications: Rome, Italy, 2016; pp. 250–257.
280. Longo, G.; Orlich, A.; Musante, S.; Merlo, A.; Russo, E. MaCySTe: A Virtual Testbed for Maritime Cybersecurity. *SoftwareX* **2023**, *23*, 101426. [CrossRef]
281. d'Afflisio, E.; Braca, P.; Millefiori, L.M.; Willett, P. Detecting Anomalous Deviations From Standard Maritime Routes Using the Ornstein–Uhlenbeck Process. *IEEE Trans. Signal Process.* **2018**, *66*, 6474–6487. [CrossRef]
282. Yan, Z.; Song, X.; Zhong, H.; Yang, L.; Wang, Y. Ship Classification and Anomaly Detection Based on Spaceborne AIS Data Considering Behavior Characteristics. *Sensors* **2022**, *22*, 7713. [CrossRef]
283. Diaz, R.; Smith, K.; Bertagna, S.; Bucci, V. Digital Transformation, Applications, and Vulnerabilities in Maritime and Shipbuilding Ecosystems. *Procedia Comput. Sci.* **2023**, *217*, 1396–1405. [CrossRef]
284. Ntshangase, L.H.; Bauk, S. Blockchain Applications and Cybersecurity Threats: A Review. In Proceedings of the 2024 28th International Conference on Information Technology (IT), Zabljak, Montenegro, 21 February 2024; pp. 1–4.
285. Bernabé, P.; Gotlieb, A.; Legeard, B.; Marijan, D.; Sem-Jacobsen, F.O.; Spieker, H. Detecting Intentional AIS Shutdown in Open Sea Maritime Surveillance Using Self-Supervised Deep Learning. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 1166–1177. [CrossRef]
286. Kontopoulos, I.; Varlamis, I.; Tserpes, K. Uncovering Hidden Concepts from AIS Data: A Network Abstraction of Maritime Traffic for Anomaly Detection. In *Multiple-Aspect Analysis of Semantic Trajectories*; Tserpes, K., Renso, C., Matwin, S., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 11889, pp. 6–20, ISBN 978-3-030-38080-9.
287. Wei, T.; Wang, T.; Dong, T.; Jing, M.; Chen, S.; Xu, C.; Liu, Y.; Wu, J.; Gao, L. Comparative Analysis of SAR Ship Detection Methods Based on Deep Learning. *IET Conf. Proc.* **2024**, *2023*, 3918–3925. [CrossRef]

288. Ali, Z.; Hussain, T.; Su, C.-L.; Sadiq, M.; Jurcut, A.D.; Tsao, S.-H.; Lin, P.-C.; Terriche, Y.; Elsisi, M. A New Paradigm for Adaptive Cyber-Resilience of DC Shipboard Microgrids Using Hybrid Signal Processing With Deep Learning Method. *IEEE Trans. Transp. Electrif.* **2025**, *11*, 4280–4295. [CrossRef]
289. Venskus, J.; Kurmis, M.; Andziulis, A.; Lukosius, Z.; Voznak, M.; Bykovas, D. Self-Learning Adaptive Algorithm for Maritime Traffic Abnormal Movement Detection Based on Virtual Pheromone Method. In Proceedings of the 2015 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Chicago, IL, USA, 26–29 July 2015; pp. 1–6.
290. Vanem, E.; Storvik, G.O. Dynamical Linear Models for Condition Monitoring with Multivariate Sensor Data. *Int. J. COMADEM* **2018**, *21*, 7–18.
291. Shahir, A.Y.; Tayebi, M.A.; Glasser, U.; Charalampous, T.; Zohrevand, Z.; Wehn, H. Mining Vessel Trajectories for Illegal Fishing Detection. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 1917–1927.
292. Kumar, P.; Gupta, G.P.; Tripathi, R.; Garg, S.; Hassan, M.M. DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2472–2481. [CrossRef]