Build a Human-Centric maritime transportation cybersecurity protection system based on *MARITIME*

Shihao Zhou*, YiMing Wang

Three Gorges Navigation Authority, YiChang, China

Abstract. As a critical infrastructure, maritime transportation is facing increasing cyber security threats. The existing protection methods have obvious deficiencies in dealing with the specific human factors in this field, the wide distribution of ships and regional differences. To this end, we propose *MARITIME*, a new human-centric and system resilience-oriented cybersecurity framework to enhance the defense and resilience of maritime transportation systems under complex cyber-attacks. The framework systematically divides the process of cybersecurity preparedness and response into two phases, covering four core capabilities of prevention, awareness raising, threat detection, and system recovery. It also supports flexible and customizable deployment strategies to adapt to diverse operational environments. Through the verification of several typical use cases, *MARITIME* shows good effectiveness and adaptability in the real maritime situation, and provides a feasible path for improving the security of the shipping system.

Keywords: Maritime Transportation; Cybersecurity; Human-centric Framework; System Resilience

1. Introduction

Maritime transport systems (MTS) have undergone rapid digital transformation in recent decades, driven by the integration of advanced technologies such as smart ports, smart containers, and land-based shipping infrastructure [1][2]. These innovations have greatly enhanced operational efficiency, cargo visibility and maritime safety [3]. However, the increasing digitalization has also exposed MTS to more and more cyber threats, making cyber security a key issue in the modern shipping industry [4].

The maritime domain has historically been less affected by cybersecurity concerns compared to other domains such as electrical grids and water treatment facilities [5]. However, the rapid digitalization of maritime transportation has made it a target for cyber-attacks, underscoring the

* Corresponding Author: Shihao Zhou (2772613724@qq.com)

importance of MTS cybersecurity [6]. Cyber-attacks on MTS can cause harm beyond economic losses and disruptions; they can impact crew and passenger safety, critical infrastructure, and the environment [6]. Therefore, ensuring the cybersecurity of MTS is not just important but also imperative, highlighting the urgent need for robust and effective security measures.

While cybersecurity research and practices have been relatively effective in other sectors, such as power grids and water treatment systems , their direct application to the maritime domain presents unique challenges [7].The Maritime Transport System (MTS) has several unique characteristics, such as reliance on human operators and their reliability, complex ship operation mechanisms , and the wide distribution of ships at the national and regional levels, making existing methods difficult to be directly applied [8].While cybersecurity frameworks such as NIST have achieved some degree of standardization in other industries, their effectiveness in the maritime domain is unclear as a unified consensus on cybersecurity practices has not yet developed [9].Although existing security frameworks recognize the importance of human factors, they often lack a truly human-centric design that systematically integrates human behavior into cybersecurity mechanisms [9][10][11][12][13]. The ideal framework of this kind should have a deep understanding of user needs and conduct extensive user research to ensure its usability and practicality. Meanwhile, many existing frameworks lack the adaptability to regional differences, forcing users to adopt fixed models, which may not be suitable for their localized scenarios [7]. Furthermore, the integration of cyber security and maritime security is also of vital importance. Many ship shore-based support system for ships to provide security services, once the attack, can affect not only directly affected vessels, could also spread to the whole supply chain and global navigation system [14].Due to the high interconnection of these systems, any shore-based infrastructure that controls the scheduling of multiple vessels may be affected by cyber threats, thereby causing a broader impact on the overall shipping efficiency and reliability [15]. Therefore, the safety responsibility for shore-based facilities should not be borne by a single vessel alone, but rather a core issue of common concern for the entire supply chain and the shipping industry [16].

To address these pressing challenges, we propose *MARITIME*, a novel human-centric and resilience-oriented cybersecurity framework specifically tailored for Maritime Transportation Systems (MTS) [9][17]. *MARITIME* pays particular attention to the unique challenges faced in the maritime transportation system, especially human factors and regional differences [17][18].The framework divides the cybersecurity of MTS into two core phases: a pre-incident phase that emphasizes preparedness, prevention, and awareness of cyber threats [19], and a

post-incident phase that concentrates on detecting, responding to, and recovering from incidents [17][18][19][20].To the best of our knowledge, *MARITIME* is the first cybersecurity framework that systematically integrates "human factors" elements and is oriented towards the maritime field, reflecting the innovative contribution of this study [9].Through the design of these two stages, *MARITIME* has achieved security coverage of the entire process and all elements of MTS, and established a comprehensive and systematic security guarantee mechanism [19]. Furthermore, this framework has good adaptability, can dynamically respond to the constantly evolving threat environment, and effectively bridge the gap between cyber security and maritime security, thereby providing more robust and efficient protection capabilities in the maritime field.

MARITIME is committed to addressing the limitations of existing cybersecurity approaches in the maritime domain by focusing on human factors and regional differences [21].To address the challenges brought by human factors, we have introduced a risk assessment tool integrating human factors analysis in the pre-event stage, aiming to deepen the understanding of the role of humans in risk assessment and enhance the reliability of operators and the quality of decision-making [22].To address the issue of regional differences, we have constructed a regional threat intelligence framework in the post-event stage. By establishing regional threat information sources, we provide threat intelligence with more targeted and localized characteristics, thereby enhancing the accuracy and timeliness of threat detection and response [23].Furthermore, in both stages, we have introduced the human-AI teaming mechanism to enhance the collaboration ability between humans and artificial intelligence (AI) [24]. This mechanism aims to combine the empirical judgment of human experts with the data analysis and automation capabilities of AI, thereby enhancing the efficiency and accuracy of threat identification and handling, and ensuring that potential threats are detected and properly handled before they cause harm [25][26].

Our framework has an exploratory nature in terms of how humans are incorporated and how AI is utilized for human-AI teaming. To gain a deeper understanding of the role of humans in the process of cyber security, we model humans as two types of roles: "attackers" and "defenders". As attackers, they may cause damage to maritime transportation systems (MTS) by implanting malicious payloads, triggering ship collisions or leading to stranding accidents, etc. As defenders, humans play a crucial role both before and after the event. In the pre-event stage, operators are the core force for implementing preventive measures and enhancing the ability of situation awareness. Their vigilance and participation directly affect the continuous and safe

operation of the system. In the post-event stage, humans, as the first responders, assume significant responsibilities in event detection, emergency response, and system recovery, and work in collaboration with AI systems to enhance response efficiency. To further explore the application potential of AI in human-machine collaboration, we list several technical examples that can assist humans at different stages: In the pre-event stage, AI-driven threat intelligence models can be used to predict potential cyber-attack trends; In the post-event stage, an AI-based event detection system can achieve faster and more accurate anomaly identification, serving as an early warning mechanism to alert operators before the actual threat occurs. Furthermore, the framework emphasizes the establishment of a cybersecurity trust mechanism between humans and machines, aiming to enhance human confidence in the capabilities and reliability of AI, thereby achieving an efficient and trustworthy collaboration model. By integrating these components, *MARITIME* enhances the overall cybersecurity posture of MTS and improves adaptability to human and regional variations, offering a novel and practical approach for building resilient maritime security infrastructures.

2. Related Work

This section reviews recent advancements in three key areas relevant to our research: maritime cybersecurity, human-centric cybersecurity, and cybersecurity intelligence. By synthesizing insights from these domains, we aim to develop a more robust and adaptive cybersecurity framework for Maritime Transportation Systems (MTS).

Maritime Cybersecurity: With the increasing frequency of maritime cyber-attacks, the shipping industry is facing more and more cybersecurity challenges [9][27]. Core navigation and communication systems, such as Automatic Identification System (AIS), Global Navigation Satellite System (GNSS) and Electronic Chart Display and Information System (ECDIS), have been shown to have significant vulnerabilities, Can be use the operation of the serious consequences [9][27][28].Although existing research has explored system-level defense and reinforcement mechanisms [29][30], attention to the interaction between cybersecurity and human factors, as well as the systematic application of artificial intelligence (AI) in maritime environments, remains limited [9][31]. To address this gap, we have proposed a *MARITIME* framework that integrates human factors and the collaboration of artificial intelligence. This study proposes the *MARITIME* framework from the perspective of the collaborative integration of human factors and artificial intelligence technologies. Based on drawing on and expanding the existing cybersecurity framework [32], and in combination with the actual operating

environment of the maritime transportation system, the human-machine collaboration mechanism is adaptively reconstructed and functionally enhanced. It aims to comprehensively enhance the security, adaptability and practical value of the system.

Human-Centric Cybersecurity: In cybersecurity, human beings are not only a source of potential threats, but also a key defense force, playing a dual role of attacker and defender [33]. As an attacker, it can cause damage to the system by stealing access credentials, deploying malware, or physically destroying critical facilities ; As defenders, humans play an irreplaceable role in various aspects such as security preparedness, risk prevention, threat detection, incident response, and system recovery [21][34].Existing studies have pointed out the core position of "human reliability" in cybersecurity and emphasized that through cybersecurity training and awareness enhancement programs, it is possible to effectively improve the behavioral stability and decision-making quality of operating personnel [35]. On this basis, we further explore how to make the existing people-oriented safety framework adapt to the unique operational characteristics and safety requirements of the maritime transportation system, and promote the construction of a more targeted and practical guarantee mechanism.

Cybersecurity Intelligence: Cybersecurity intelligence models play a crucial role in threat prediction and risk mitigation [26][37]. Such models integrate statistical analyses such as logistic regression and deep learning with artificial intelligence (AI) technologies to model and evaluate the possibility of cyber-attacks [35][38]. By identifying potential security threats in advance, these models support the formulation of active defense strategies, thereby significantly enhancing the cybersecurity resilience of the system. This study draws on the existing mature intelligence modeling methods and introduces them into the *MARITIME* framework to enhance its capabilities in threat prediction and intelligence analysis, and ensure that the framework design is consistent with the best practices in the current field of cyber security [9].

Through a comprehensive review of maritime cybersecurity, human-centered security approaches, and cybersecurity intelligence models, it is clear that current solutions often lack effective integration across these areas. In response to this issue, this paper proposes the *MARITIME* framework and elaborates on its design principles and architecture in detail in the following text, aiming to achieve the deep integration and collaborative operation of the above key elements in the maritime cyber security scenario and promote the construction of a more adaptable and practical security protection system.

3. The *MARITIME* Framework

As shown in Figure1, *MARITIME* includes five key components: (a) a human-centric risk assessment tool in the pre-incident phase, (b) a human-AI teaming approach for threat intelligence in the pre-incident phase, (c) a cybersecurity training and awareness program in the pre-incident phase, (d) a regional threat intelligence framework in the post-incident phase, and (d) a human-AI teaming approach for incident detection and response in the post-incident phase. Collectively, these components form a comprehensive and adaptive cybersecurity solution for MTS.

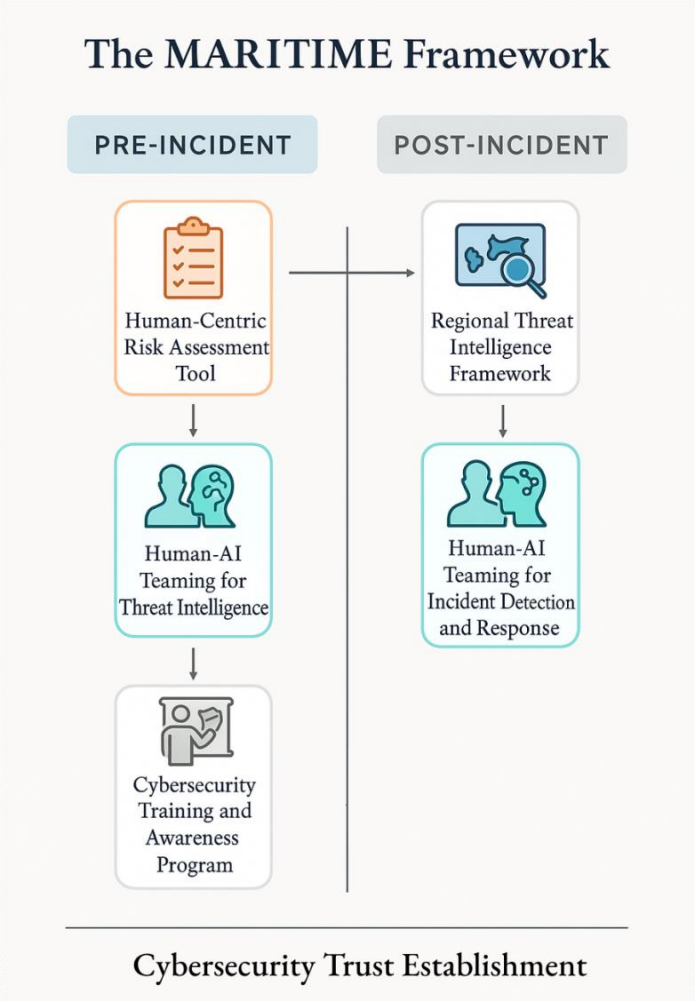

Figure 1. The *MARITIME* framework.

3.1. Overview of *MARITIME*

MARITIME divides the preparation and response of cybersecurity into two phases: the pre-incident phase and the post-incident phase. This two-stage design ensures that the cybersecurity protection is comprehensive, which can not only carry out active defense before the threat occurs, but also make efficient response after the security incident. By structuring the

cybersecurity process into the two phases described above, *MARITIME* covers the security needs of all aspects of the Maritime Transport System (MTS) and effectively responds to evolving cyber-attack threats, thereby significantly improving the overall resilience and robustness of the system. The following will provide a detailed introduction to each component in the framework.

3.2. Human-Centric Risk Assessment Tool

In the pre-incident stage, incorporating human factors into cybersecurity risk assessment is the key to achieving effective risk identification. Maritime Transportation Systems (MTS), unlike many other cyber-physical domains, are uniquely dependent on human operators, who not only manage system functions but also play a pivotal role in ensuring the safety and operational efficiency of vessels. For human error to bring security risk, we put forward a risk assessment tool for people-centric, man-made factors clearly integrated into the traditional cybersecurity risk model.

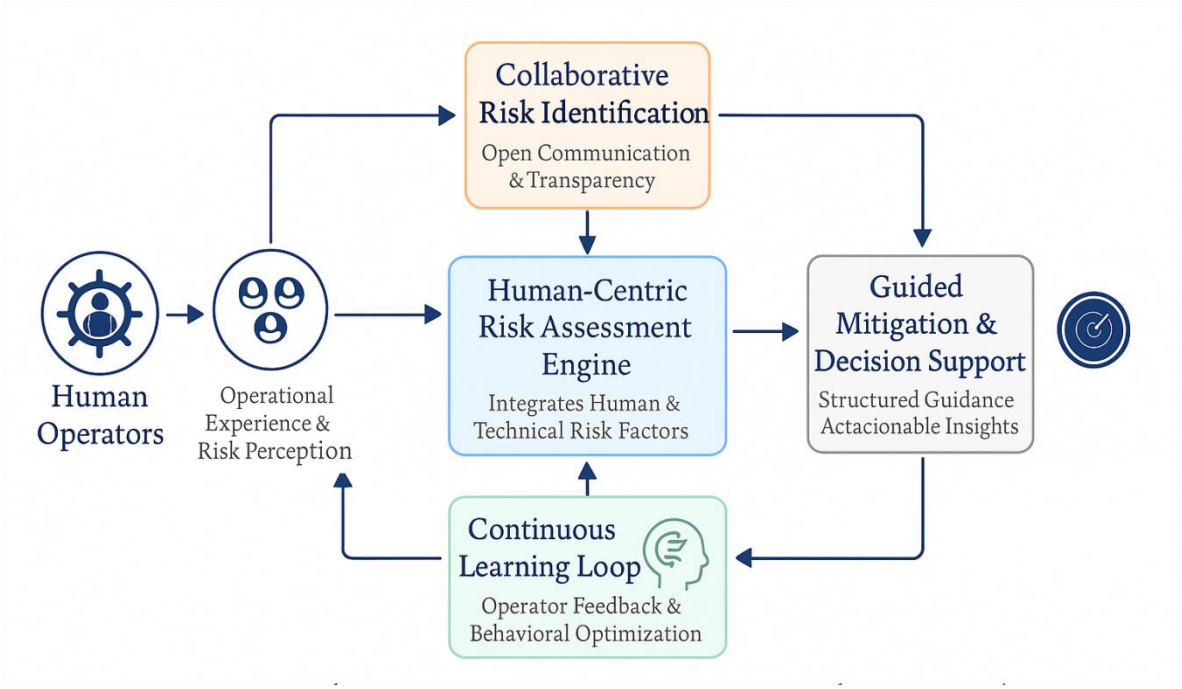

Figure 2. Human-Centric Risk Assessment Process in Maritime Cybersecurity (Pre-Incident Phase).

The tool aims to improve personnel reliability, promote trust, and facilitate ongoing operator involvement by embedding human factors at the core of the evaluation process. It achieves its objective by focusing on a number of key dimensions at the risk assessment stage. It emphasizes open communication and transparency, ensuring that human operators are actively involved in identifying and assessing risks associated with human error. This collaborative evaluation mechanism not only helps to gain valuable experience and professional insight of front-line

operators, but also enhances their sense of responsibility and participation in cybersecurity. At the same time, the tool provides systematic guidance and actionable processes to support risk assessment and mitigation, thus improving the safety, reliability and decision-making quality of operators in practical tasks. On this basis, a set of continuous learning and improvement mechanism is also built to encourage operators to constantly optimize their own cybersecurity behavior and operational norms in practice. In addition, the design of the tool gives full consideration to the actual demand of operating personnel and performance goals, make the safety risk is no longer seen as pure administrative burden, but the core component part of the overall cybersecurity strategy. Overall, it effectively Bridges the gap between cybersecurity and maritime security, focusing not only on technical vulnerabilities, but also incorporating human factors into the assessment system, so as to predict and intervene before potential problems turn into actual cyber incidents(See Figure2).In the field of with the core appeal of maritime safety, the integration of the prospective ability has important practical significance and strategic value.

3.3. Human-AI Teaming for Threat Intelligence

In the pre-incident stage, particular emphasis was placed on threat intelligence prediction and analysis. To enhance engagement in this process, we propose a human-machine collaboration method (See Figure3). Our approach utilizes an AI-driven threat intelligence model to enhance operator engagement and reliability. These AI models, which serve as threat intelligence predictors, are designed to identify and analyze potential cyber threats in order to act on them before they become an immediate threat. Their role is to act as early warning systems, alerting operators to potential risks and thus enabling proactive response. However, they are not intended to replace human decision-makers, but to serve as auxiliary tools. Essentially, these models are like complex filters that identify relevant threats from a large amount of raw threat data, providing human operators with a more manageable and context-specific perspective. This not only simplifies the threat intelligence process, but also improves overall situational awareness by ensuring that operators are always up-to-date and engaged. Through this collaborative model, human-machine teams can effectively assess the severity of threats, analyze trends, and evaluate countermeasures, helping to make more informed and effective cybersecurity decisions. What’s more, this man-machine synergy promotes a culture of continuous learning and improvement. In continuous interactions, AI models can point out potential overviews and provide additional insights, which will help operators keep up with the evolving threat landscape and improve their skills and knowledge over time, leading to a greater focus on cybersecurity across the shipping industry.

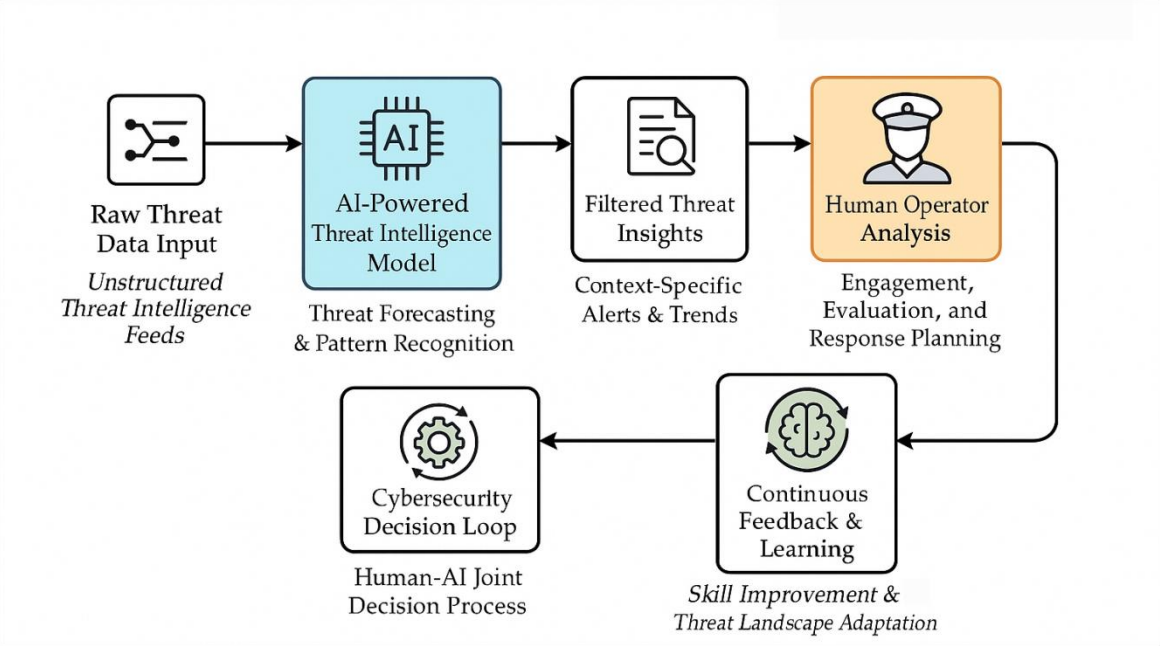

Figure 3. Human-AI Teaming Process for Threat Intelligence Forecasting in Maritime Cybersecurity (Pre-Incident Phase).

3.4. Cybersecurity Training and Awareness Program

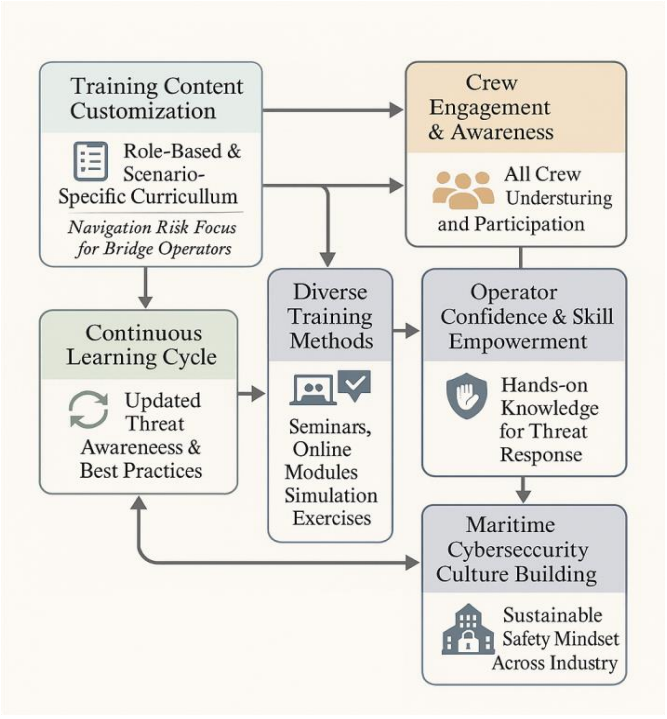

Figure 4. Structure of the Cybersecurity Training and Awareness Program in the Pre-Incident Phase of Maritime Cybersecurity Preparedness.

The last preparatory measure in the pre-incident phase is the cybersecurity training and awareness enhancement program. The program aims to enhance the reliability of operators in the Maritime Transport System (MTS) by increasing their cybersecurity awareness and

providing skills support to respond to the critical role humans play in daily ship operations and their critical role in cybersecurity preparedness, and ultimately promoting the continuous development of the shipping industry towards a direction of cybersecurity awareness. To accomplish this, the program focuses on teaching operators the knowledge and capabilities needed to identify and respond to cyber threats, including threat identification, safe ship management, and incident response planning (See Figure4). This systematic training helps to shape a safety culture involving all staff, enabling each crew member not only to understand potential cyber risks but also to have the confidence and ability to actively participate in risk mitigation.

The several key strategies adopted in this project are as follows:

- Customized training content: The training content is tailored to the specific responsibilities of the operators to ensure its practicality and relevance. For example, for bridge operators, the focus is on navigation-related threats and precautions.
- Diversified training methods: Utilize multiple training modalities, such as seminars, online courses, and simulation training, to accommodate different learning styles.
- Ongoing learning and adaptation: Cybersecurity is not a one-time achievement but a continuous process, and this program is designed to keep human operators updated with the latest threats and best practices.

The success of the project will not only be reflected in the cultivation of an operation team with solid knowledge and skills in cyber security, but also in the stimulation of the enthusiasm and initiative of practitioners to ensure the cyber security of the shipping industry. By endowing operators with correct knowledge and skills, the reliability of personnel has been enhanced, and the construction and deepening of the cybersecurity culture throughout the shipping industry have been promoted.

3.5. Regional Threat Intelligence Framework

In the post-incident phase, we introduce a regional threat intelligence framework. This framework aims to address the differences in cybersecurity prevention levels among different regions and solve problems such as the wide distribution of ships and inconsistent cybersecurity standards in different shipping areas.

The framework is built on two core pillars: one is the collection and integration of regional threat intelligence sources, and the other is the artificial intelligence-based threat intelligence analysis model customized for different shipping regions (See Figure5).

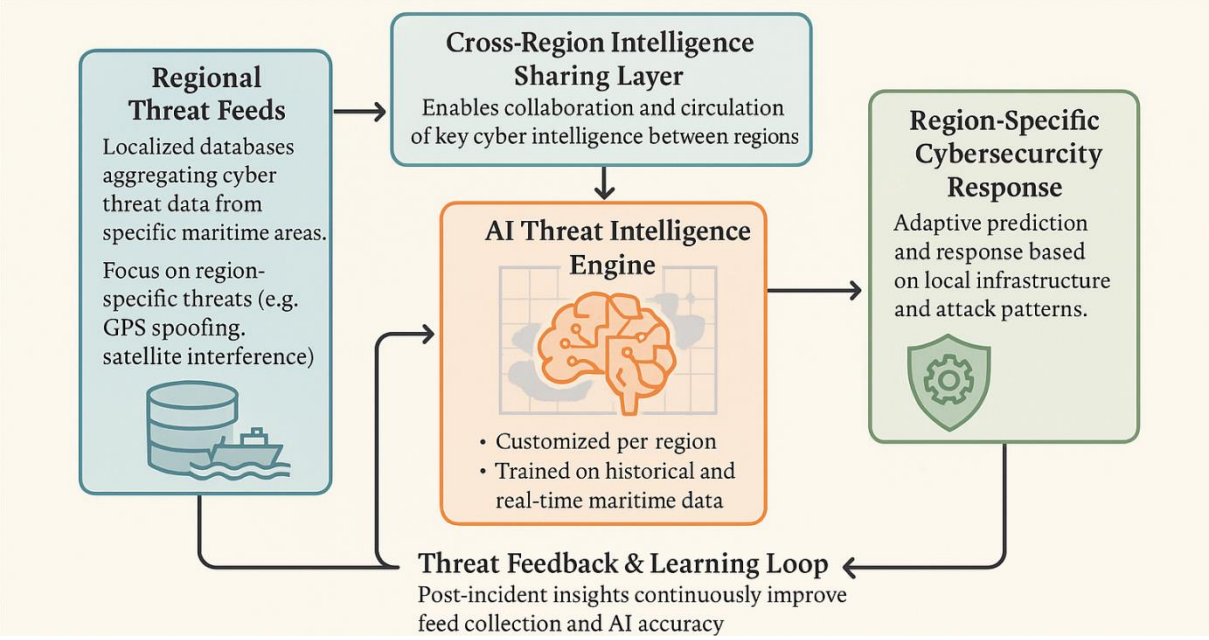

Figure 5. Regional Threat Intelligence Framework for Maritime Cybersecurity.

Collection of Regional Threat Feeds: A regional threat intelligence source is essentially a database used to summarize and store local cyber threat information and intelligence in a specific shipping area. For example, in shipping areas that are frequently subject to GPS spoofing attacks, intelligence sources will give priority to collecting and analyzing relevant data on GPS spoofing technologies and their development trends in this area. This mechanism not only helps to establish a network threat perception system based on regional characteristics, but also provides key support for formulating accurate and efficient defense strategies. Its goal is not to comprehensively monitor all potential threats, but to actively identify and respond to the unique security challenges faced by each region. In addition, these threat intelligence sources not only provide real-time information on attack types, frequency, and exploited vulnerabilities, but also serve as a cross-regional intelligence sharing platform, facilitating collaboration between different shipping regions and promoting the circulation and sharing of valuable intelligence. To be clear, however, this regional-centric perspective is not intended to fragment the industry as a whole, but rather to recognize and respect regional differences in the cybersecurity environment, infrastructure maturity, and threat landscape. The fundamental purpose is to ensure that each shipping area has access to targeted and adaptive defense means, so as to ensure its own security while promoting the coordinated and sustainable development of the entire industry.

AI-Powered Threat Intelligence Models: By regionalizing and deploying the AI-based threat intelligence model to each shipping region, it can integrate historical data and real-time

intelligence to effectively analyze and predict network threats. Optimizing the model based on the security characteristics, vulnerability distribution and attack patterns of different regions can ensure that its prediction results not only have high accuracy, but also highly conform to the local actual security requirements. For example, a threat model applicable to one coast may fail in other regions due to differences in infrastructure, levels of cybersecurity practice, or temporal and spatial distribution of threat events. Therefore, the core goal of this pillar is to provide both time-sensitive and targeted threat intelligence, promote the defense mechanism from passive response to active defense, so as to more effectively respond to the differentiated security challenges faced by each shipping region.

3.6. Human-AI Teaming for Incident Detection and Response

In the post-incident phase, the *MARITIME* framework also emphasizes the application of human-machine collaboration in incident detection and response. This collaborative approach ensures that human operators always maintain decision-making dominance, while artificial intelligence technology is used to enhance their judgment and response capabilities. In this mode, a human operator acts as the first responder, relying on their own expertise and experience to handle the incident. Their roles are not limited to passively responding to emergencies, but should also actively participate in strategic decision-making and emergency preparedness. The event detection system driven by artificial intelligence plays a key role in this process. These systems are designed to provide real-time intelligence and actionable insights to assist decision-makers in responding to threats quickly and efficiently. They act as a highly intelligent early warning mechanism, continuously monitoring network activities and automatically identifying and marking suspicious behaviors. Its functions are not limited to basic alert prompts, but also cover in-depth analysis and strategic suggestions. For instance, AI can predict potential future attacks based on historical data and current threat patterns, and issue early warnings to operators before potential risks emerge, thereby enabling the early deployment of defense measures and preventing incidents from causing actual damage (See Figure6).

It is important to note that the AI model used in this framework fully considers ethical and legal considerations and that AI can only be used as an auxiliary tool to provide operators with the necessary information and insights to support informed decision making, while the final decision remains in human control.

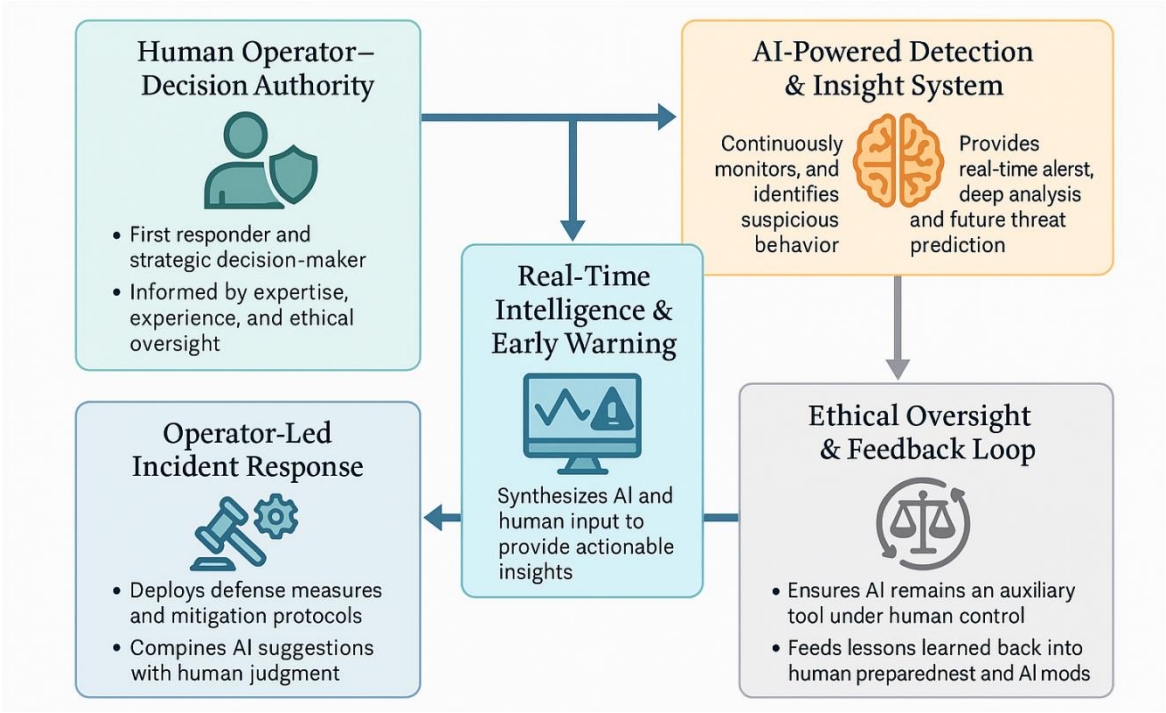

Figure 6. Human-Machine Collaboration for Incident Detection and Response.

4. Core Methods

The system architecture of the framework includes the above five modules, and these modules communicate with each other through standardized interfaces. The following is mainly to introduce the core key technologies of each module.

4.1. Human-Centric Risk Assessment Engine

Human-Centric Risk Assessment Tool mainly rely on human-centric risk assessment engine. The core of this engine is a weighted risk aggregation model, which integrates the two dimensions of human factors risk and technical risk. Specifically, we define a set of normalized human-centric metrics $H = \{h_1, h_2, \ldots, h_m\}$, each with a value $v_{h_i} \in [0,1]$

representing the observed risk level (e.g., fatigue, training adequacy, response latency), and corresponding weight $w_{h_i} \in [0,1]$. In parallel, a set of technical cybersecurity indicators $T = \{t1, t2, \ldots, tn\}$ is defined with similar structure. The overall human risk component is computed as

$$R_H = \sum_{i=1}^{m} w_{h_i} \cdot v_{h_i}$$

and the technical component as

$$R_T = \sum_{j=1}^{\mathrm{n}} w_{t_\mathrm{j}} \cdot v_{t_\mathrm{j}}$$

with w_{t_j} representing the contextual importance of technical factors. These are synthesized into a final hybrid risk score using a linear fusion model:

$$R_{\text{total}} = \alpha \cdot R_H + \beta \cdot R_T \ , \ \ where\ \alpha + \beta = 1$$

allowing the framework to prioritize human or technical risk based on operational context. To ensure adaptability, weights w_{h_i} and w_{t_j} are dynamically calculated using contextual relevance functions $C_{h_i}(t)$ and $C_{\mathrm{t_j}}(t)$, such that

$$w_{h_i}(t) = \frac{C_{h_i}(t)}{\sum_{k=1}^{m} C_{h_k}(t)} \ \ , \ \ w_{t_\mathrm{j}}(t) = \frac{C_{\mathrm{t_j}}(t)}{\sum_{k=1}^{m} C_{\mathrm{t}_k}(t)}$$

enabling the engine to adjust its focus in response to changing conditions (e.g., navigation complexity, environmental stress, or personnel workload). The resulting risk score is then passed downstream to the mitigation and decision support module, while also feeding into a continuous learning loop that updates the model based on operator behavior and feedback. This tightly integrated approach ensures that the system is not only sensitive to human-driven risks but also capable of proactively identifying and addressing them before they escalate into full-scale incidents.

4.2. AI-Powered Threat Intelligence Model

The threat intelligence model driven by artificial intelligence aims to realize the proactive cybersecurity protection with human-machine collaboration as the core by transforming massive maritime intelligence data into actionable and context-aware intelligence information. This model first acquires the original threat signals $X = \{\mathrm{x_1}, \mathrm{x_2}, \ldots, \mathrm{x_n}\}$ from ship logs, port networks and external network threat intelligence (CTI) sources. Each threat data point $\mathrm{x_i}$ is processed by a threat prediction function based on neural network:

$$f_\theta(x_i) = (y_i, s_i)$$

where y_i represents the predicted threat category (e.g., malware, phishing, denial-of-service), and $s_i \in [0,1]$ denotes the model's computed severity score. To ensure that the model output is consistent with the actual situation of maritime operations, the system further introduces a context calibration function to generate the adjusted severity score:

$$\tilde{s}_i = \gamma \cdot s_i + (1-\gamma) \cdot g(\phi, x_i)$$

where ϕ encodes environmental and operational factors (e.g., navigation phase, port type) , $g(\phi, x_i)$ is a heuristic or rule-based relevance function, and $\gamma \in [0,1]$ balances model confidence against contextual modifiers.The calibrated score $\tilde{s}_i$ will be presented to the human operator through a visual interface, and combined with the detailed AI reasoning process, it will provide transparent and understandable explanation basis for each alarm.

Rather than operating entirely autonomously, the model serves as an auxiliary filtering tool to help the operator focus on the most relevant and time-sensitive threats. Feedback from the human operator (including disposal decisions, false alarm markers, and response actions) will be continuously transmitted back to the system, and the classifier f_θ and context function g will be continuously optimized through the online learning mechanism, thus forming a closed-loop feedback system.

4.3. Cybersecurity Training and Awareness Platform

In order to further train operator cybersecurity consciousness, we specially constructed cybersecurity training and awareness platform (See Figure7). The platform is a dynamic learning System for multi-user roles, which can effectively improve the reliability of personnel in the Maritime Transportation System (MTS) by integrating cybersecurity awareness into daily operation processes. Platform based on role generation corresponding training module T_i , each associated with a set of learning objectives $L_i = \{l_1, l_2, \ldots, l_n\}$, such as threat identification, safe navigation, and response protocols.Each crew member u will be assigned a personalized training path based on their operational responsibilities and learning preferences, and will participate in various teaching methods $M_j \in \{seminars, online\ modules, simulation\ exercises, \ldots\}$.

The individual training performance score S_u is calculated by the weighted sum of all learning objective assessment scores:

$$.S_u = \sum_{i=1}^{n} w_i \cdot a_{u,i}$$

where $a_{u,i}$ is the normalized score of users u on learning objective l_i , and w_i represents the contextual importance of that objective.

To keep the system adaptive and threat relevant, the platform introduces a continuous learning mechanism that uses real-time threat intelligence updates $\Delta T(t)$ to drive content evolution, where emerging threats are mapped to their respective learning objectives through a threat-skill correlation matrix R_{ts}.When a new threat τ_k emerges, the relevant training module T_i is updated as

$$T_i^{new} = T_i^{old} + \eta \cdot R_{ts}(k,:)$$

ensuring training content remains current. Operator readiness is then quantified through a cybersecurity readiness index:

$$CRI_u = \lambda_1 \cdot S_u + \lambda_2 \cdot C_u + \lambda_3 \cdot A_u$$

which combines training performance S_u , engagement metrics C_u and real-world awareness activation A_u , with the weights $\lambda_1 + \lambda_2 + \lambda_3$=1. Ultimately, the readiness of all crew members will be aggregated and evaluated, and this Index is defined as the Maritime Cybersecurity Culture Index (MCCI):

$$MCCI = \frac{\sum_{u \in U} \rho_u \cdot CRI_u}{\sum_{u \in U} \rho_u}$$

Where ρ_u represents the criticality of the crew member's role.

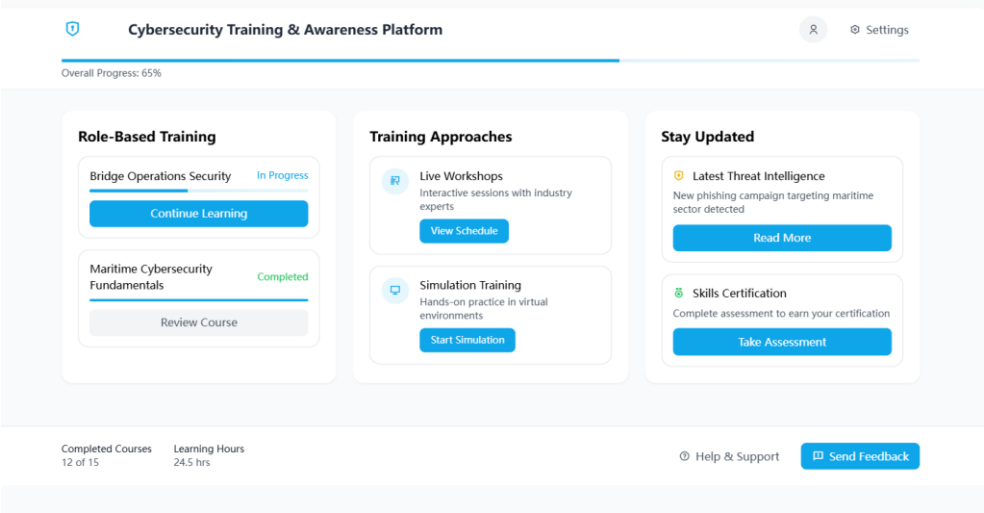

Figure 7. Cybersecurity Training and Awareness Platform Interface.

This end-to-end implementation mechanism not only ensures the precise transmission and high participation of cybersecurity knowledge, but also supports the continuous monitoring of personnel performance and the continuous optimization of organizational culture, thereby establishing a sustainable security awareness system throughout the maritime industry.

4.4. Regional Threat Intelligence Framework

Unlike the Threat Intelligence Modell introduced in Section 4.2, which supports pre-incident operator-level decisions, the regional threat intelligence framework is designed to provide support for post-hoc response and strategic security reinforcement at the regional level. On the basis of the original artificial intelligence driven model, the framework introduces localized

threat data collection, cross-regional intelligence sharing, and regional customized model optimization mechanisms, and constructs a scalable architecture that can effectively deal with the heterogeneity problem in the maritime network environment. The implementation of this framework defines an aggregated region-specific threat source F_r ,where each region r compiles real-time and historical cyber incident data—such as GPS spoofing, AIS manipulation, or port-side malware propagation—into structured input vectors $X_{r,i}$.

These are fed into a regional AI threat engine:

$$f_\theta(x_{r,i}) = (y_{r,i}, s_{r,i})$$

which outputs predicted threat types $y_{r,i}$ and severity levels $s_{r,i}$, trained on the threat patterns and infrastructure context of region r .To further improve the regional adaptability of the analysis, a context calibration layer is introduced to adjust the severity score:

$$\tilde{s}_{r,i} = \alpha_r \cdot s_{r,i} + (1 - \alpha_r) \cdot h(\phi(x_{r,i}))$$

where α_r reflects confidence in AI predictions, and $h(\phi(x_{r,i})$ adjusts severity based on region-specific factors ϕ_r , such as port density, network maturity, or vessel profile.The calibrated output $\tilde{s}_{r,i}$ is used to drive targeted regional cybersecurity response measures, assisting maritime regulatory authorities in implementing timely and practical security protection actions.To facilitate collaborative situational awareness, a Cross-Region Intelligence Sharing Layer synchronizes key intelligence summaries $\sum_{r \to r'}$ across different maritime zones, allowing each regional model f_θ to evolve not only from local data but also from peer regions via gradient-informed updates

$$\theta_r^{(t+1)} = \theta_r^{(t)} + \Delta feedback(F_r, \Sigma_{r' \to r})$$

This entire loop is reinforced through a post-incident feedback mechanism, where real-world outcomes feed back into F_r and model optimization, forming a continuous learning cycle.

4.5. Human-AI Teaming for Incident Detection and Response

The implementation of the Human-AI Teaming mechanism in the MARITIME framework is centered on a dual-layered architecture that integrates real-time AI-driven detection with human-in-the-loop decision-making to ensure ethical, effective, and timely incident response. The system receives the telemetry data stream D(t) from sources such as communication logs, system alarms and sensor outputs, and processes it as a feature vector representation:

$$X(t) = \{x_1, x_2, \ldots, x_n\}$$

These feature vectors are input into a trained anomaly detection model f_θ to generate the corresponding anomaly scores:

$$A_i = f_\theta(x_i) \in [0,1]$$

Subsequently, these scores will be compared with an adaptive threshold to determine whether an alarm is triggered:

$$\tau(t) = \mu_T + \lambda\sigma_T$$

where μ_T and σ_T are the mean and standard deviation of A over a sliding window T, and λ is a risk sensitivity coefficient. If $A_i > \tau(t)$, an alert is generated and displayed to the operator via an explainable interface (See Figure8).

Figure 8. Human-AI Teaming Incident Detection and Response Platform Interface.

To support operator understanding and intervention, the system provides each alert with contextual metadata (e.g., alert source, affected subsystem, past incident similarity), ensuring that the AI' s outputs are transparent and explainable. The human operator, informed by operational knowledge K_{human}, makes the final response decision D_{final}, guided by both system recommendations and situational judgment.

$$D_{\text{final}} = \arg\max_{r_i \in R} [\beta_1 \cdot \text{Conf}(r_i) + \beta_2 \cdot \text{Relevance}(r_i, K_{\text{human}})]$$

All incidents and response outcomes are logged in a feedback repository, which is used to periodically update model parameters and thresholding functions, enabling continuous learning and improved detection precision over time. Through this architecture, the system enhances maritime cybersecurity by ensuring that artificial intelligence strengthens (rather than replaces)

human responsibility in incident detection and response.

5. Evaluation

The focus of this assessment is to verify the effectiveness and feasibility of the core components in this framework by selecting several key tasks. Specifically, we conducted exploratory analysis and effect verification on multiple key components through the method of simulated safety tests. Throughout the entire assessment process, we did not disclose any genuine security vulnerabilities, nor did we carry out any actual attack activities. We only verified the system design logic and response mechanism in a controlled environment to ensure the security and compliance of the assessment process.

5.1. Case Based Risk Assessment

Overview The first core component we evaluated is the "human-centered risk assessment tool", whose goal is to systematically integrate human factors into the cybersecurity risk assessment to enhance the reliability of operators. The evaluation process adopts a case-based simulation method, utilizes the recorded maritime cybersecurity incidents, and on this basis, expands the human error scenarios that may exacerbate the impact of the incidents or weaken cybersecurity. To this end, we have constructed a structured analytical framework, relying on a network event database specifically for collecting human factor elements. This framework can rigorously assess the role of human behavior in cyber risks and provide operational decision support for formulating targeted mitigation strategies, thereby enhancing the overall cyber security resilience of the maritime transportation system.

Preparation The first step of this assessment is to build a database covering historical and potential cybersecurity incidents, all of which involve the role of human factors. This dataset is sourced from multiple channels, including recorded cybersecurity incidents and data from expert interviews, the latter of which is used to enrich and validate the database content. The collected events are not limited to historical real events, but also include hypothetical and potential scenarios, so as to provide a solid basis for the analysis and ensure that the risk assessment is both based on reality and covers possible future threat scenarios. After completing the data construction, we classified the events based on the role background in which human errors occurred, and they were divided into four distinct risk types: risks related to planning and general preparation, risks during operations, risks during crisis management, and risks related to post-incident activities. This detailed classification is conducive to a deeper understanding

of the specific manifestations and impact paths of human errors in different situations, thus improving the comprehensiveness and pertinence of risk assessment.

Analysis In the next step of work, we will adopt the hierarchical analysis method to assess the severity and occurrence frequency of various risks. Starting from the entire database, we progressively focused on smaller but more relevant subsets of data corresponding to specific risk subcategories. For each relevant data subset, we apply the logistic regression model to estimate the occurrence probabilities of various risks based on the identified key variables.

Table 1. Risk Assessment Results.

Risk Sub-Category	Severity (1–5)	Frequency (1–5)	Control Strategies
Infrastructure-based Risks	4.5	4.0	Implement standard security controls, user and device authentication, security monitoring and logging, security information and event management, and security awareness training.
Application-based Risks	4.0	3.5	Apply standard controls, conduct vulnerability scanning and management, adopt secure software development practices, and provide training for software users.
Human-based Risks	5.0	3.0	Conduct human factors analysis, deliver targeted training, promote trustworthy AI systems, and engage shipowners and crew consistently to enhance participation and effectiveness.
Ship-on-Land Infrastructure Risks	4.5	4.0	Ensure secure infrastructure placement, establish physical security layers, implement monitoring and training, and enforce layered defence.
Cyber-Physical Systems Risks	4.0	3.5	Utilize DNP3.0-secure devices, enforce standard controls, and provide awareness training for users of integrated cyber-physical components.
Information-based Risks	3.5	3.0	Apply encryption, enforce access control, implement standard data security protocols, and offer awareness training for data stakeholders.

Results The outcome of this hierarchical risk assessment is a detailed categorization of cyber risks within MTS based on human factors, as shown in Table 1. Each sub-category of risk is assigned a severity and frequency score, providing a structured way to prioritize and address cyber threats in light of potential human errors. As an example, Risk 3 (Human-based risks)

received the highest severity score, indicating a critical vulnerability in current human-centric cybersecurity approaches (See Figure9).

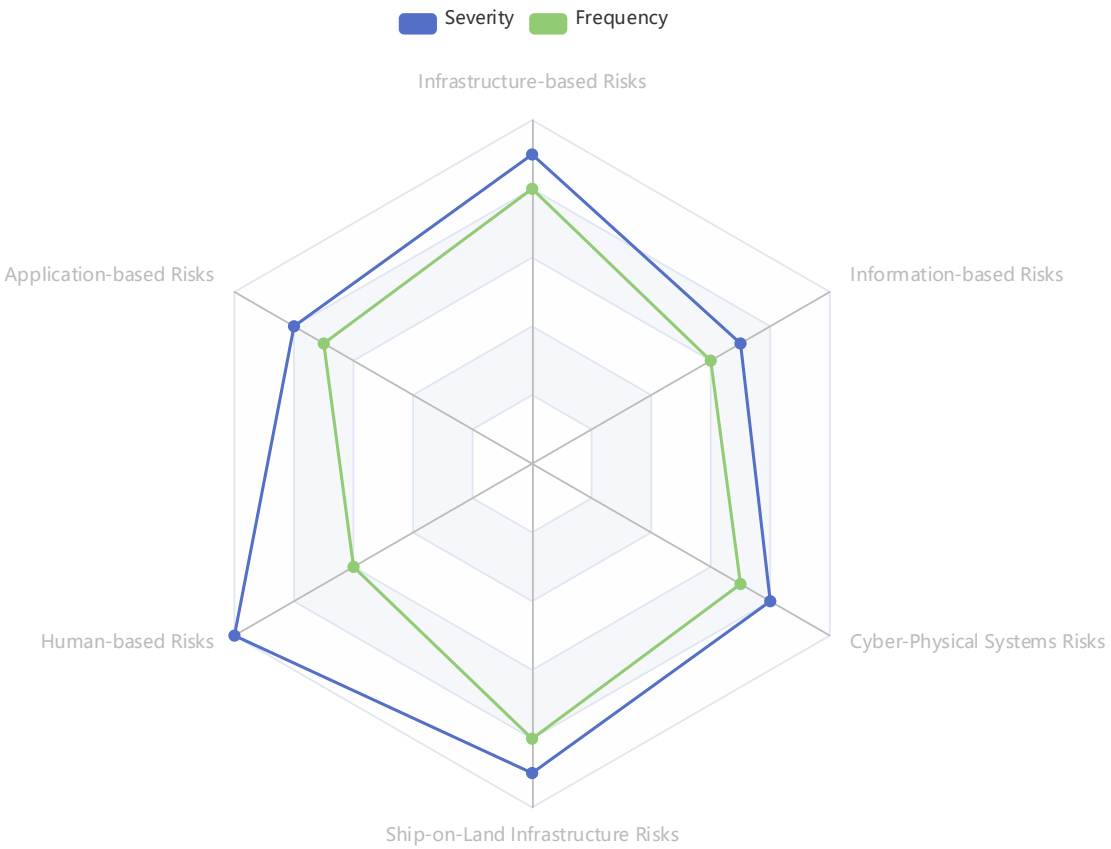

Figure 9. Radar chart of cyber risk sub-categories based on severity and frequency.

The evaluation also specified control strategies for each sub-category, enhancing human reliability. These strategies, which include awareness training, human-AI teaming, and robust device management, are crucial for mitigating risks and ensuring the safety and efficiency of MTS. More importantly, Table 1 shows how the risk assessment framework can be adapted to different MTS, demonstrating its customizability and adaptability. For example, risks related to ship-on-land infrastructure, such as Risk 4, are particularly prominent, highlighting the need for tailored security solutions for these systems. This table serves as a blueprint for future evaluations, guiding researchers and practitioners in focusing their efforts on the most critical areas of risk. Overall, the risk assessment framework proved effective in identifying risks related to human factors and providing tailored security solutions, demonstrating its potential to enhance the resilience of MTS.

5.2. Simulation of Human-AI Teaming for Threat Intelligence

Overview The second component that we evaluate is the human-AI teaming approach for threat intelligence in the pre-incident phase. With the help of the threat intelligence model driven by artificial intelligence, this method aims to improve the situation awareness ability and response initiative of operators, so as to enhance their decision-making reliability. This assessment covers the development and deployment process of these models, with a focus on their effectiveness in providing accurate and timely intelligence information.

Preparation In this assessment, the first step is to build an AI-driven threat intelligence model. These models are designed to analyze and predict cyber threats based on historical data and real-time intelligence. The model development process begins with data collection, systematically organizing various threat scenarios that have occurred and are potentially possible in the maritime Traffic System (MTS), and constructing a comprehensive dataset. This dataset provides a solid foundation for the training and testing of artificial intelligence models, ensuring that the models can identify a wide variety of threat patterns and have good generalization capabilities. This is followed by model selection and training. Based on the characteristics of the constructed dataset, we select appropriate AI technical solutions, such as logistic regression or deep learning models, etc. Subsequently, the selected model is trained, and its performance is optimized by parameter tuning to evaluate its prediction accuracy for future threats. In addition, the evaluation includes the deployment of these models in a controlled experimental environment to simulate various threat scenarios to test their performance and responsiveness under real-time operational conditions.

Analysis This assessment is not limited to analyzing the technical performance of artificial intelligence models, but further focuses on the key role played by human participation in it. Specifically, we assess the effectiveness of this mechanism in enhancing the reliability of operators and their participation in threat intelligence activities. The evaluation focused on how the safety awareness training program enhanced the operator's sense of responsibility and contributed to continuous learning and competence development. In addition, the practical impact of the human-machine collaborative method in threat intelligence prediction and analysis was also evaluated. This collaborative approach ensures that the generated intelligence is not only timely but also closely aligned with the specific business requirements and scenario characteristics of the vessel's operation.

Results The results of this evaluation are reflected in Figure 10, which demonstrates the effectiveness of the human-AI teaming approach in threat intelligence forecasting and analysis.

The figure shows a significant improvement in the accuracy of threat intelligence, with a marked decrease in false positives and an increase in true positives. This indicates that with the support of the human-machine collaboration mechanism, the system can identify the actual existing network threats more effectively and significantly reduce the interference caused by irrelevant information at the same time.

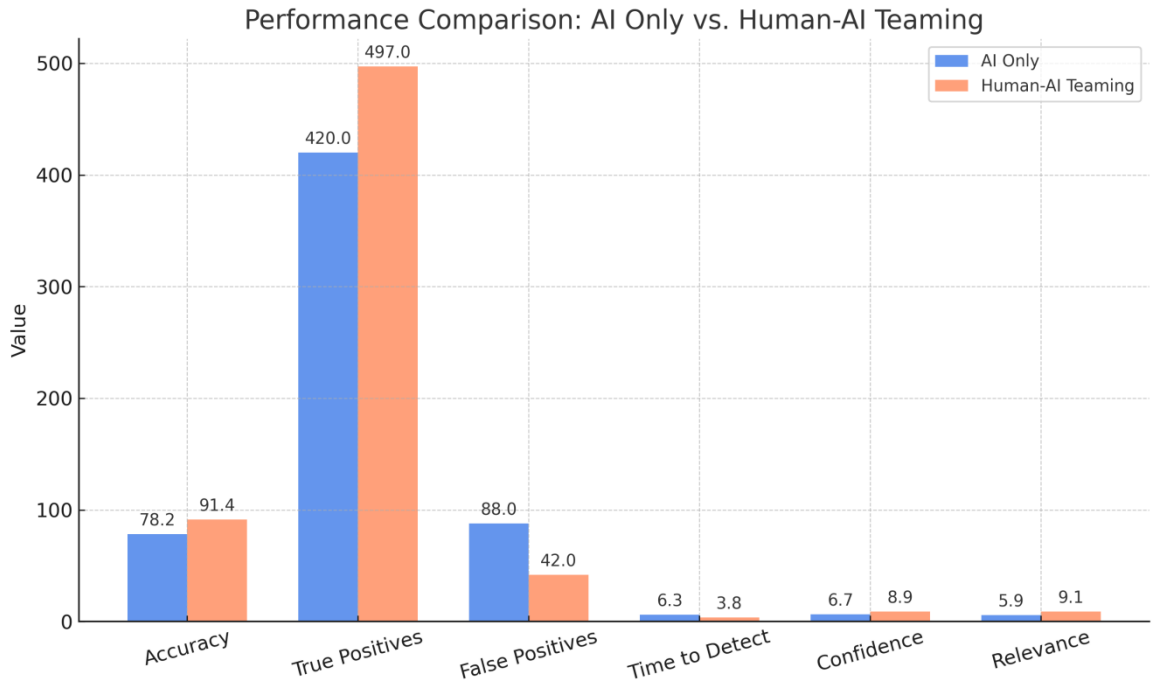

Figure 10. Performance comparison between AI-only and Human-AI teaming in threat intelligence tasks. The Human-AI approach shows increased accuracy, higher true positive rates, and improved operational relevance.

More importantly, the chart also shows the trend of continuous learning and capability improvement brought about by human-machine collaboration. Emphasizing the value of human participation makes the generated threat intelligence not only technically accurate but also more in line with the actual needs of the daily operation of ships, possessing a high degree of practicality and operability.

5.3. Simulation of Human-AI Teaming for Incident Detection and Response

Overview The third key component that we evaluate is the human-AI teaming approach for incident detection and response in the post-incident phase. Under the premise of ensuring that the human operator retains the final control, the method uses artificial intelligence technology to enhance its situation awareness and response ability. The system adopts a two-layer architecture design, which combines automatic anomaly detection with the decision-making

mechanism of people in the loop, which improves the efficiency of incident response and ensures the ethical compliance and decision-making reliability in the operation process. The assessment focuses on the development and deployment of an AI-driven event detection system, verifying its ability to provide real-time intelligence and actionable insights.

Preparation To simulate the application of human-machine collaboration in incident detection and response, we constructed a controlled maritime network security experimental environment. The evaluated system integrates a pre-trained AI anomaly detection model with an interpretable operator interface and simulates post-event response conditions in real scenarios through real-time telemetry data such as communication logs and sensor outputs. The operators involved in the assessment first received a brief training on the system interface and decision-making process. During the simulation process, they receive alarm information generated by artificial intelligence - this information is accompanied by rich context metadata, and they make response decisions in combination with system suggestions and their own judgments. The test scenarios cover both normal operating conditions and embedded threat events, thereby comprehensively evaluating the detection accuracy, alarm relevance, and the effectiveness of human responses of the system under conditions close to actual combat.

Analysis This evaluation not only examined the performance of the AI system in event detection, but also analyzed the actual effect of human-machine collaboration in event response. The AI model showed a stable and real-time anomaly detection ability, and the false alarm rate was within an acceptable range. At the same time, the interpretable operation interface helps the operator to quickly understand the alarm content and make scenario-based judgments and decisions. This human-machine cooperation mechanism not only improves the situation awareness ability, shorts the response time, but also significantly enhances the operator's decision-making confidence and response accuracy. More importantly, the ability to receive feedback from our operations and continue to improve it ensures that the way we handle incidents is always aligned with the actual business needs, as well as ethical and compliance standards.

Results As shown in Figure 11, by combining the AI-driven anomaly detection mechanism with the human decision-making process, the system can identify real events and non-threatening anomalies more effectively, thus improving the overall reliability of alerts. Furthermore, operators benefit significantly from the contextual information provided by the interpretable interface, which not only enhances their understanding of the current situation but also significantly accelerates the response speed. The system has also established a continuous

feedback mechanism, using the judgment input of the operators for the iterative update of the model to promote the gradual improvement of detection accuracy and adaptability. These results verify that retaining human control in the loop during the incident response process not only ensures that decisions comply with ethical and compliance requirements, but also significantly enhances the practical adaptability and system resilience of the maritime cybersecurity incident response system.

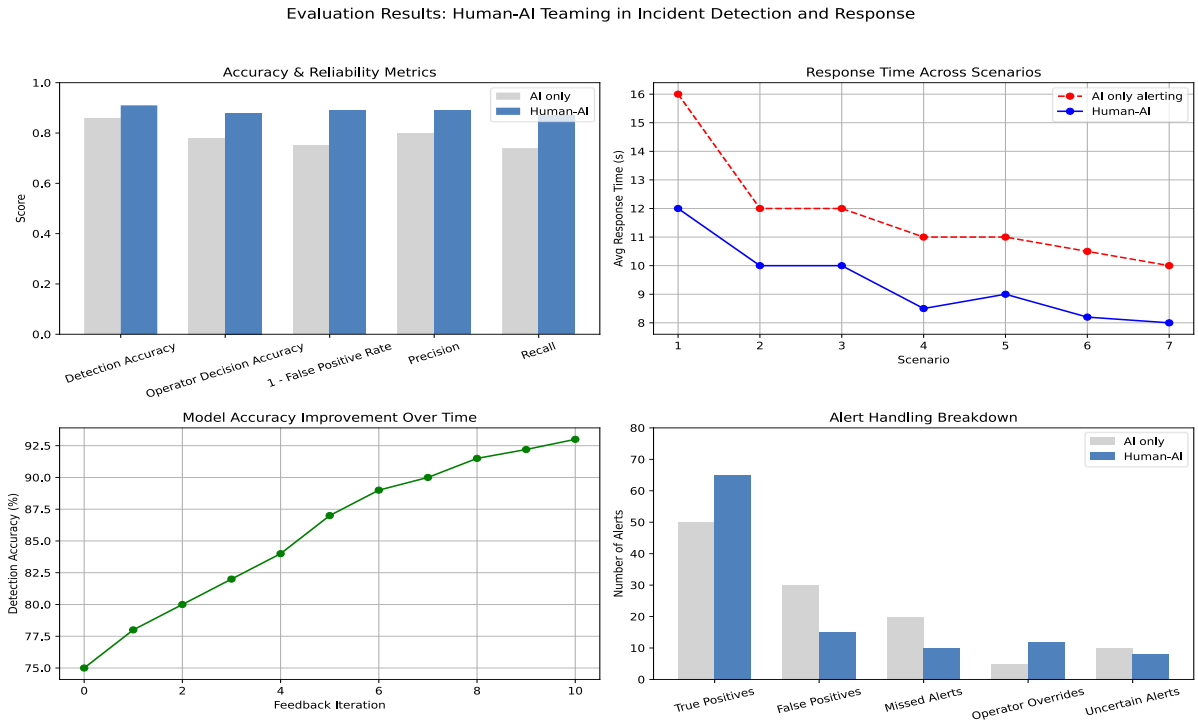

*Figure 11.*Human-AI Teaming Performance in Incident Detection and Response.

6. Conclusion and Future Work

We introduced *MARITIME*, a novel and adaptive cybersecurity framework designed specifically for the maritime domain. In contrast to other cybersecurity frameworks, such as NIST, *MARITIME* is tailored to the unique characteristics of MTS, particularly addressing human factors and the widespread regional distribution of vessels. *MARITIME* marks a significant advancement in addressing the emerging challenges in the cybersecurity of MTS, particularly in regions where cybersecurity preparedness is limited and where existing approaches are not adaptive enough. It calls for a shift in traditional cybersecurity practices, incorporating adaptive and customizable solutions, enhancing human engagement, and redefining relationships between human operators and AI technologies. Moving forward, we plan to refine these components within *MARITIME* through further research and development,

paving the way for a cybersecurity-aware and secure future for the maritime transportation system.

References

[1] Lokendra Sharma and. Maritime cybersecurity in the indo-pacific: envisioning a role for the quad . *Journal of the Indian Ocean Region*, 20(1):14–36, 2024. https://www.tandfonline.com/doi/abs/10.1080/19480881.2024.2341467.

[2] Ignacio de la Pe˜na Zarzuelo, Mar´ıa Jes´us Freire Soeane, and Beatriz L´opez Berm´udez. Industry 4.0 in the port and maritime industry: A literature review. *Journal of Industrial Information Integration*, 20:100173, 2020. https://www.sciencedirect.com /science/article/abs/pii/S2452414X20300480.

[3] Zeng, F.; Chen, A.; Xu, S.; Chan, H.K.; Li, Y. Digitalization in the Maritime Logistics Industry: A Systematic Literature Review of Enablers and Barriers. J. Mar. Sci. Eng. 2025, 13, 797. https://www.mdpi.com/2077-1312/13/4/797.

[4] Yu H, Meng Q, Fang Z, Liu J. Literature review on maritime cybersecurity: state-of-the-art. Journal of Navigation. 2023;76(4-5):453-466. doi:10.1017/S0373463323000164 .https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/literature-review-on-maritime-cybersecurity-stateoftheart/90F7A14DEA9148C793819170B2474A89.

[5] Panagiotis Radoglou-Grammatikis, Athanasios Liatifis, Christos Dalamagkas, Alexios Lekidis,Konstantinos Voulgaridis, Thomas Lagkas, Nikolaos Fotos, Sofia-Anna Menesidou, Thomas Krousarlis, Pedro Ruzafa Alcazar, et al. Electron: An architectural framework for securing the smart electrical grid with federated detection, dynamic risk assessment and self-healing. In *Pro-ceedings of the 18th International Conference on Availability, Reliability and Security*, pages 1–8,2023.https://dl.acm.org/doi/abs/10.1145 /3600160.3605161.

[6] Ammar M, Khan IA. Cyber Attacks on Maritime Assets and their Impacts on Health and Safety Aboard: A Holistic View. arXiv. 2024. https://arxiv.org/abs/2407.08406.

[7] Karamperidis, S.; Kapalidis, C.; Watson, T. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. J. Mar. Sci. Eng. 2021, 9, 1323. https://www.mdpi.com/2077-1312/9/12/1323.

[8] Simola J, Paavola J, Satopää P, et al. The Impact of Operational Technology Requirements in Maritime Industries[C]//Proceedings of the European Conference on Cyber Warfare and Security. Academic Conferences International Ltd, 2024 (1).https://jyx.jyu.fi/jyx/Record/jyx_123456789_96197.

[9] Li M, Zhou J, Chattopadhyay S, et al. Maritime Cybersecurity: A Comprehensive Review[J]. arXiv preprint arXiv:2409.11417, 2024.https://arxiv.org/abs/2409.11417.

[10] Raymaker A, Kumar A, Wong M Y, et al. A Sea of Cyber Threats: Maritime Cybersecurity from the Perspective of Mariners[J]. arXiv preprint arXiv:2506.15842, 2025.https://arxiv.org/abs/2506.15842.

[11] Afenyo M, Caesar L D. Maritime cybersecurity threats: Gaps and directions for future research[J]. Ocean & Coastal Management, 2023, 236: 106493.https://www.sciencedirect.com/science/article/abs/pii/S0964569123000182.

[12] Bolbot V, Kulkarni K, Brunou P, et al. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis[J]. International Journal of Critical Infrastructure Protection, 2022, 39: 100571.https://www.sciencedirect.com/science/article/pii/S1874548222000555.

[13] Dimakopoulou A, Rantos K. Comprehensive Analysis of Maritime Cybersecurity

Landscape Based on the NIST CSF v2. 0[J]. Journal of Marine Science and Engineering, 2024, 12(6): 919.https://www.mdpi.com/2077-1312/12/6/919.

[14] Ben Farah M A, Ukwandu E, Hindy H, et al. Cyber security in the maritime industry: A systematic survey of recent advances and future trends[J]. Information, 2022, 13(1): 22.https://www.mdpi.com/2078-2489/13/1/22.

[15] Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. Network 2022, 2, 123-138.https://www.mdpi.com/2673-8732/2/1/9.

[16] Alcaide J I, Llave R G. Critical infrastructures cybersecurity and the maritime sector[J]. Transportation Research Procedia, 2020, 45: 547-554.https://www.sciencedirect.com/science/article/pii/S2352146520302209.

[17] Nganga A, Scanlan J, Lützhöft M, et al. Enabling cyber resilient shipping through maritime security operation center adoption: A human factors perspective[J]. Applied Ergonomics, 2024, 119: 104312.https://www.sciencedirect.com/science/article/pii/S0003687024000899.

[18] Erstad E, Hopcraft R, Vineetha Harish A, et al. A human-centred design approach for the development and conducting of maritime cyber resilience training[J]. WMU Journal of Maritime affairs, 2023, 22(2): 241-266.https://link.springer.com/article/10.1007/s13437-023-00304-7.

[19] Ćelić J, Vukšić M, Baždarić R, et al. The challenges of cyber resilience in the maritime sector: Addressing the weak awareness of the dangers caused by cyber threats[J]. Journal of marine science and engineering, 2025, 13(4): 762.https://www.mdpi.com/2077-1312/13/4/762.

[20] Harish A V, Tam K, Jones K. Literature review of maritime cyber security: The first decade[J]. Maritime Technology and Research, 2025, 7(2): Manuscript-Manuscript.https://so04.tci-thaijo.org/index.php/MTR/article/view/273805.

[21] Turner A, McCombie S J, Uhlmann A J. The impacts of cyber threat in the maritime ecosystem[J]. Frontiers in Computer Science, 2024, 6: 1378160.https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1378160/full.

[22] Chae C J, Kim I C, Baumler R, et al. Ship Cybersecurity Risk Assessment for Safe Operation with Human Involvement: An Experimental Case Study[J]. WMU Journal of Maritime Affairs, 2024: 1-29.https://link.springer.com/article/10.1007/s13437-024-00353-6.

[23] Godfrey S, Cooper J R, Plater A J. Roving multiple camera array with Structure-from-Motion for coastal monitoring[J]. Journal of Marine Science and Engineering, 2023, 11(3): 591.https://www.mdpi.com/2077-1312/11/3/591.

[24] Bach T A, Babic A, Park N, et al. Using LLM-Generated Draft Replies to Support Human Experts in Responding to Stakeholder Inquiries in Maritime Industry: A Real-World Case Study of Industrial AI[J]. arXiv preprint arXiv:2412.12732, 2024.https://arxiv.org/abs/2412.12732.

[25] Khadka K, Ullah A B. Human factors in cybersecurity: an interdisciplinary review and framework proposal[J]. International Journal of Information Security, 2025, 24(3): 1-13.https://link.springer.com/article/10.1007/s10207-025-01032-0.

[26] Zhang Q, Cho J H, Moore T J, et al. DREVAN: deep reinforcement learning-based vulnerability-aware network adaptations for resilient networks[C]//2021 IEEE Conference on Communications and Network Security (CNS). IEEE, 2021: 137-145.https://ieeexplore.ieee.org/abstract/document/9705041.

[27] Karaś A. Maritime industry cybersecurity: a review of contemporary threats[J]. 2023.https://www.um.edu.mt/library/oar/handle/123456789/117971.

[28] Oruc A, Kavallieratos G, Gkioulos V, et al. Perspectives on the Cybersecurity of the

Integrated Navigation System[J]. Journal of Marine Science and Engineering, 2025, 13(6): 1087.https://www.mdpi.com/2077-1312/13/6/1087

[29] Wimpenny G, Šafář J, Grant A, et al. Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility[J]. The Journal of Navigation, 2022, 75(2): 333-345.https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/securing-the-automatic-identification-system-ais-using-public-key-cryptography-to-prevent-spoofing-whilst-retaining-backwards-compatibility/98E18D3253AD985BA7B75185EFB3538A.

[30] Khandker S, Turtiainen H, Costin A, et al. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience[J]. IEEE Access, 2022, 10: 29493-29505.https://ieeexplore.ieee.org/abstract/document/9667309.

[31] Pseftelis T, Chondrokoukis G. A study about the role of the human factor in maritime cybersecurity[J]. SPOUDAI-Journal of Economics and Business, 2021, 71(1/2): 55-72.https://www.econstor.eu/handle/10419/283673.

[32] Mouratidis H, Diamantopoulou V. A security analysis method for industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(9): 4093-4100.https://ieeexplore.ieee.org/abstract/document/8353731.

[33] Rajaram P, Goh M, Zhou J. Guidelines for cyber risk management in shipboard operational technology systems[C]//Journal of Physics: Conference Series. IOP Publishing, 2022, 2311(1): 012002.https://iopscience.iop.org/article/10.1088/1742-6596/2311/1/012002/meta.

[34] Weinstock, J.B.; Vargas, L.; Collin, R. Zooplankton Abundance Reflects Oxygen Concentration and Dissolved Organic Matter in a Seasonally Hypoxic Estuary. J. Mar. Sci. Eng. 2022, 10, 427.https://www.mdpi.com/2077-1312/10/3/427.

[35] Dash B, Ansari M F. An effective cybersecurity awareness training model: First defense of an organizational security strategy[EB/OL].(2022-4-30).https://d1wqtxts1xzle7.cloudfront.net/89862930/IRJET_V9I401-libre.pdf

[36] Wong K I. Rapid prototyping of a low-power, wireless, reflectance photoplethysmography system[C]//2010 International Conference on Body Sensor Networks. IEEE, 2010: 47-51.https://ieeexplore.ieee.org/abstract/document/5504809.

[37] Kumar P, Gupta G P, Tripathi R, et al. DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 24(2): 2472-2481.https://ieeexplore.ieee.org/abstract/document/9617134.

[38] Al-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of things: A survey on enabling technologies, protocols, and applications[J]. IEEE communications surveys & tutorials, 2015, 17(4): 2347-2376.https://ieeexplore.ieee.org/abstract/document/7123563.