Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 3, 1207-1221
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i3.380

Ship Captain's Readiness to Face the Threat of Cyber Attack on the Ship's Navigation System

Agus Widodo[1*]
Politeknik Pelayaran Banten, Indonesia

Siwi Woro Herningsih[2]
Politeknik Pelayaran Banten, Indonesia

Roma Dormawaty[3]
Sekolah Tinggi Ilmu Pelayaran, Indonesia

Riza Nur Amala[4]
Politeknik Pelayaran Banten, Indonesia

***Corresponding author:**
Agus Widodo, Politeknik Pelayaran Banten, Indonesia.
✉ agusw020473@gmail.com

Article Info:

Article history:
Received: June 18, 2026
Revised: July 27, 2026
Accepted: August 07, 2026

Keywords:
Maritime Cybersecurity;
Cyber Threats;
Attack Trees; Ship Navigation System; Risk Assessment.

Abstract

Background: The maritime sector is highly dependent on technological infrastructure, including port management systems, ship monitoring systems, and satellite-based communication systems. This infrastructure is crucial for ensuring the smooth flow of goods between countries and maintaining port operations and safe ship navigation.
Objective: This study identifies cyberattack pathways targeting shipboard navigation and operational technology (OT) systems in Indonesian waters, develops attack-tree scenarios for those pathways, and evaluates ship captains' readiness to detect and respond to them.
Methods: Attack-tree modeling was used to describe, analyze, and represent potential attack scenarios. The model draws on a literature review and interviews with twelve maritime experts: four captains and deck officers, four cybersecurity specialists, and four technical consultants. Validation was conducted through two Delphi rounds until an agreement level of 80% was reached.
Results: Four attack trees produced eighteen validated attack paths across three primary attack goals: crashing the ship (five paths), sinking the ship (three paths), and disabling the ship (six paths), along with four shared enabling paths. Experts rated the attack scenarios for crashing and disabling the ship as highly feasible, whereas sinking the ship was considered unlikely. Overall, nine attack paths were classified as high risk.
Conclusion: The attack tree serves not only as a vulnerability assessment tool but also as a structured, prioritized risk assessment instrument for maritime cybersecurity. Mapping each validated attack path to International Maritime Organization (IMO) and National Institute of Standards and Technology (NIST) cybersecurity controls enables shipping companies.

To cite this article: Widodo, A., Herningsih, S. W., Dormawaty, R., & Amala, R. N. (2026). Ship Captain's Readiness to Face the Threat of Cyber Attack on the Ship's Navigation System. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(3), 1207-1221. https://doi.org/10.59261/jequi.v8i3.380

INTRODUCTION

Indonesia is the world's largest archipelagic state, with more than seventeen thousand islands, over three hundred commercial ports, and sea lanes that carry a substantial share of east-to-west trade. National reporting places the transportation sector among those most frequently affected by cyber incidents in the country, yet cyber risk governance on board Indonesian-flagged vessels remains largely undeveloped, and operational technology (OT) on the bridge is rarely covered by corporate information security programs. Because a compromised navigation system

produces immediate physical consequences rather than data loss alone, ship navigation systems require separate investigation from general enterprise cybersecurity. Digital transformation has driven major changes across industrial sectors, including the maritime industry, which now relies heavily on technology for navigation, communication, and logistics. Cybersecurity has therefore become a major concern in the maritime sector, which plays a vital role in supporting the global economy (Kiss et al., 2026; Topping et al., 2021).

The maritime industry generates significant economic activity that benefits countries and facilitates international relations. One of its major contributions is the provision of employment for tens of thousands of people every day. The maritime sector is essential to the global economy because it connects continents through international shipping routes. As most international trade relies on sea transportation, the maritime industry is indispensable to global commerce (Bueger, 2015; Erdoğan & Erdoğan, 2025).

The increasing use of digital systems in port operations, ship navigation, logistics, and supply chain management has significantly improved operational efficiency and effectiveness. Modern maritime operations depend on technological infrastructure, including port management systems, vessel monitoring systems, and satellite-based communication systems. Cyber threats targeting these systems, such as malware attacks, hacking, and disruptions to navigation systems, can result in substantial operational and economic losses (Cao et al., 2025; Wolff, 2021). However, as digital technologies continue to develop, the maritime sector's dependence on technology also increases, making cybersecurity threats more frequent, sophisticated, and complex. Consequently, the maritime sector has become increasingly vulnerable to cyberattacks that can disrupt operations and cause significant financial losses while also compromising maritime safety (Bueger, 2015; Erdoğan & Erdoğan, 2025).

The maritime sector relies heavily on technological infrastructure, including port management systems, vessel monitoring systems, and satellite-based communication systems. This infrastructure is essential for ensuring the efficient movement of goods between countries while maintaining safe port operations and reliable ship navigation (NUR, 2025; Syibli & Nuryaman, 2021). Threats to these systems, such as malware attacks, hacking, and disruptions to navigation systems, can result in significant losses. Such incidents may lead to serious consequences, including ship collisions, groundings, or environmental disasters resulting from oil spills or the release of hazardous materials (Androjna et al., 2020; Jin et al., 2025).

Recent sectoral reporting confirms that this exposure is not hypothetical. The European Union Agency for Cybersecurity records transportation as one of the most heavily targeted sectors in the European Union, with the maritime and logistics sectors explicitly identified as priority targets for adversaries (Cybersecurity, 2025). The United States Coast Guard Cyber Command reports a continued rise in maritime cyber incidents and notes that the proportion of its cyber missions involving operational technology (OT) systems increased from forty-six percent in 2024 to sixty-two percent in 2025, indicating that attackers are shifting their focus from shore-based information technology (IT) systems toward shipboard control systems. Comparable national figures show the same trend: the National Cyber and Crypto Agency recorded 403,990,813 anomalous traffic events during 2023 and 347 suspected cyber incidents, of which twenty-four occurred in the transportation sector (Negara, 2024). Table 1 summarizes these indicators.

Table 1
Recent maritime and national cyber incident indicators

Indicator	Value	Source (year)
Anomalous cyber traffic detected, Indonesia	403,990,813 events	BSSN (2024), for 2023
Suspected cyber incidents, Indonesia	347 incidents across 186 institutions	BSSN (2024), for 2023
Suspected incidents, transportation sector	24 incidents	BSSN (2024), for 2023
Anomalous traffic, January to August 2024	122.79 million events, 59.26 percent malware	BSSN (2024)
Share of EU incidents directed at	7.5 percent (July 2024 to June 2025)	ENISA (2025)

Indicator	Value	Source (year)
transport infrastructure		
USCG cyber missions involving operational technology	62 percent in 2025, up from 46 percent in 2024	USCG Cyber Command (2026)

Related to the situation in Indonesian waters, maritime traffic is becoming increasingly congested, and not all sea areas have the same depth. Given the diverse seabed contours throughout Indonesian waters, the risk of grounding is very high, and the potential for collisions is also significant (Malik & Widodo, 2025; Mudiyanto, 2020). Therefore, to prevent and reduce the risk of collision during a voyage, especially when navigating at night, when not all objects surrounding the vessel are visible to the captain or the officer of the watch, electronic navigation aids are essential. In this context, the Automatic Identification System (AIS), used as part of the ship's navigation equipment, plays an important role in preventing collision-related accidents (Ashfaq Uz Zaman et al., 2026; Balduzzi et al., 2014).

The limitation of previous research is more specific than a general lack of attention. Research on Indonesian maritime cybersecurity has relied predominantly on aggregate risk scoring rather than on attack tree decomposition. Putra et al. (2023) applied a hybrid AHP-TOPSIS model to rank threat, vulnerability, and consequence dimensions in Indonesian waters, but the output is a composite score that does not trace how an attacker progresses from initial access to a physical outcome and, therefore, cannot indicate where an intervention would effectively break the attack chain. International threat modeling research occupies the opposite position. Erbas et al. (2024) reviewed twenty-five studies on threat modeling and risk assessment in ship cybersecurity and found no standardized framework and inconsistent validation of expert knowledge, while Keskin et al. (2025) constructed shipboard attack trees using European fleet and port data. Neither line of research has applied attack tree decomposition to Indonesian shipping conditions, where shallow archipelagic straits, a high proportion of aging vessels, and limited onboard information technology competence alter both the feasibility and the consequences of each attack path.

An attack tree is a structured threat modeling method that has been extensively applied in cybersecurity analysis. It uses a hierarchical representation to illustrate potential cyberattack scenarios, in which the primary objective is positioned at the root and multiple branching paths depict the alternative strategies an attacker may employ to accomplish that objective (Kapalidis, 2025; Tam et al., 2021). Through this hierarchical structure, the attack tree facilitates the systematic identification of vulnerabilities, the visualization of attack sequences, and the evaluation of the potential consequences of cyber threats (Erdoğan & Erdoğan, 2025; Fitton et al., 2015).

Research novelty. The novelty of this study is threefold. First, it adapts the shipboard attack tree framework established by Keskin et al. (2025) to the Indonesian operational environment by replacing European port and fleet assumptions with conditions specific to Indonesian archipelagic navigation. Thus, the contribution is a contextual transfer and revalidation of an existing method rather than a claim of having invented a new one. Second, it extends the framework beyond scenario description by assigning a likelihood band, an impact band, and a mitigation priority to every validated attack path, thereby transforming the attack tree from a descriptive diagram into a decision-support instrument. Third, it maps each attack path group to the corresponding control families in the IMO Guidelines on Maritime Cyber Risk Management and the NIST Cybersecurity Framework 2.0, providing Indonesian operators with a direct pathway from a modeled threat to a control they are already required to implement (NIST, 2024; Organization, 2022). Positioning the ship captain as the decision-maker of last resort, rather than treating the vessel as an unmanned technical system, further distinguishes this study from previous threat modeling research.

Indonesia's cybersecurity posture remains fragile, and the supporting evidence is well documented rather than anecdotal. The National Cyber and Crypto Agency recorded 347 suspected cyber incidents in 2023 affecting 186 institutions, with the transportation sector among the most affected after public administration and finance (Negara, 2024). In June 2024, a ransomware attack on the National Data Centre halted public services across multiple ministries

and disrupted operations at Soekarno-Hatta Airport, demonstrating that a single compromise of shared infrastructure can propagate into disruptions of physical transportation systems. Despite this high level of vulnerability, confidence in cybersecurity within Indonesia's maritime industry remains limited. This study examines cybersecurity in the maritime sector, particularly aboard ships operating in Indonesian waters, and investigates how ship captains prepare for and respond to cyberattacks.

This study offers both theoretical and practical contributions. Theoretically, it extends attack tree modeling from a descriptive threat representation into a prioritized risk assessment instrument. It also contributes an archipelagic-context validation to a body of literature still dominated by European and North American fleet assumptions, thereby testing whether findings generated in highly regulated waters can be transferred to a jurisdiction characterized by different vessel ages, port control practices, and crew training baselines. Practically, the resulting model provides shipping companies with a defensible basis for allocating limited cybersecurity budgets to the highest-priority attack paths rather than distributing resources evenly. It also provides captains and deck officers with a concrete set of indicators to monitor during watchkeeping and offers regulators a structured approach for translating IMO cyber risk management obligations into inspectable onboard requirements. The implication for Indonesian maritime policy is that cyber readiness assessment can be linked to specific attack paths and corresponding control measures rather than relying solely on generic cybersecurity awareness statements.

METHOD

This study adopted a systematic methodology to examine potential cyberattack scenarios targeting ship systems. The research process began with data collection by combining insights from an extensive literature review and unstructured interviews with experts to establish a foundational understanding and identify possible attack scenarios. These scenarios were subsequently organized into an attack tree, a widely used threat modeling approach, to provide a visual representation of the alternative attack paths that adversaries might exploit. Finally, the developed attack tree was validated through structured interviews with industry experts to assess its practicality, accuracy, and relevance to real-world maritime cybersecurity conditions.

The construction procedure followed four steps. First, attack goals were identified by asking which physical outcomes would constitute total mission failure for a vessel. Following expert review, three root nodes were retained: crashing the ship, sinking the ship, and disabling the ship. Second, intermediate nodes were extracted through open coding of the literature corpus and the exploratory interview transcripts, in which each reported technique was labeled according to the system it targeted and the effect it produced. Techniques that produced the same effect on the same system were merged into a single node. Third, the nodes were connected using AND and OR operators, where an OR node represents that any child path is sufficient to achieve the parent node, whereas an AND node represents that all child conditions must be satisfied simultaneously. Fourth, recurring subtrees, such as network infiltration, taking control of the Electronic Chart Display and Information System (ECDIS), loss of operational view, and evasion, were factored out as shared modules so that they were described once and referenced by all three root goals. This approach prevented duplication and kept the attack tree readable.

Figure 1. *Research methodology flow, from literature review and expert interview through attack tree construction to expert validation*

The initial stage of this methodology was dedicated to developing a comprehensive understanding of ship Operational Technology (OT) systems and identifying potential cyberattack scenarios. This phase employed two complementary data collection methods: a literature review and unstructured expert interviews. The literature review served to synthesize existing studies on maritime cybersecurity, particularly those related to cyber risk management, vulnerabilities in

shipboard systems, and previously documented cyberattack scenarios.

To complement the findings from the literature review, unstructured interviews were conducted with professionals possessing extensive experience in the maritime sector. These interviews provided practical insights into operational procedures, cybersecurity issues, and potential weaknesses within shipboard systems. The participants included cybersecurity and IT specialists, such as the Head of Information Security at Pelindo Port and IT infrastructure architects, whose expertise supported the understanding of ship network segmentation, system vulnerabilities, and cyber risk management practices. In addition, maritime operators, including cargo ship captains and second officers, contributed operational perspectives on how cyberattacks could unfold in real-world situations and how ship crews detected and responded to such incidents. Technical consultants and researchers with expertise in marine engineering, automation systems, and remote maintenance also participated, offering technical assessments of potential attack vectors and vulnerabilities affecting shipboard systems.

Experts were recruited purposively according to three inclusion criteria: a minimum of five years of continuous professional experience in shipboard operations or maritime information systems, direct professional exposure to at least one of the systems represented in the attack tree, and current or recent involvement with vessels operating in Indonesian waters. Invitations were issued to nineteen candidates, and twelve accepted and completed both rounds of interviews. The composition and experience profile of the expert panel are presented in Table 2.

Table 2
Composition and experience profile of the expert panel

Expert category	n	Roles represented	Experience (years)
Maritime operators and captains	4	Cargo ship captains, second officers	8 to 22
Cybersecurity and IT specialists	4	Head of information security at a port operator, IT infrastructure architects, security operations analyst	6 to 15
Technical consultants and researchers	4	Marine engineering consultants, automation and remote maintenance specialists, academic researchers	5 to 18
Total	12	Four operational, four security, four technical	5 to 22

Attack Tree Methodology

Attack trees are a systematic threat modeling technique used to describe, analyze, and visualize potential cyberattack scenarios. In an attack tree, the root node represents the attacker's primary objective, while the branching nodes illustrate the intermediate goals and actions required to accomplish that objective. This hierarchical representation provides a logical and structured view of the different attack paths that an adversary may exploit to compromise a system.

The effectiveness of attack tree analysis is strengthened by a well-defined classification of cyber risks. Previous studies have indicated that cyber risks in the maritime sector can be categorized according to attack vectors, targeted systems, and the potential cascading effects of system failures. Such classifications enhance the value of systematic threat modeling by enabling a more comprehensive assessment of possible attack scenarios.

This study employed the attack tree methodology because it offered a flexible and intuitive approach for modeling complex attack scenarios in a concise manner. Its hierarchical structure facilitated the identification of system vulnerabilities, supported risk assessment, and assisted in the development of appropriate mitigation strategies. Moreover, its visual representation improved communication among stakeholders by making cyber threats easier to interpret, including for audiences without extensive technical expertise. As attack tree methodologies have continued to evolve, their compatibility with other cybersecurity frameworks and analytical tools has enabled the resulting models to be integrated into future research and advanced risk assessment processes.

Validation was conducted in two structured rounds following a modified Delphi

procedure. In the first round, each expert independently rated every attack path for feasibility and operational impact using a five-point scale and was asked to justify any rating placed at either extreme. The ratings were aggregated, and the group median, together with the anonymized justifications, was returned to each expert. In the second round, the experts were given the opportunity to revise their ratings in light of the group response. Consensus was defined in advance as agreement by at least 80% of the panel on the feasibility category assigned to a given path. Attack paths that did not reach this threshold after the second round were either reformulated in narrower terms or removed from the final tree. Two attack paths concerning the remote manipulation of the ballast system were removed on this basis because the panel judged that the manual valve overrides installed on the Indonesian cargo vessels within their experience rendered the attack path impracticable in the form originally drafted.

RESULTS AND DISCUSSION

Results

The primary outcome of this study was the development of a structured attack tree that systematically modeled potential cyberattacks targeting shipboard systems. The model illustrated the logical attack paths that adversaries could exploit to compromise critical ship functions while simultaneously identifying the associated vulnerabilities and attack sequences. These scenarios demonstrated how cyber threats could lead to significant operational disruptions, financial losses, and safety-related consequences. Beyond representing attack pathways, the developed attack tree provided a practical foundation for cybersecurity risk assessment and supported the development of appropriate mitigation strategies.

The attack tree identified three principal attack objectives that could result in severe physical consequences: crashing the ship, sinking the ship, and disabling the ship. Although these objectives ultimately produced physical impacts, they were primarily achieved through the cyber exploitation of onboard systems, which could, in some cases, be facilitated by physical access to critical infrastructure. For example, attackers could first gain unauthorized access to the ship's network before manipulating navigation systems or operational technology (OT) systems to achieve their intended objectives.

This study focused exclusively on cyber threats affecting systems that are essential for the safe and reliable operation of modern vessels. Non-critical systems, such as passenger entertainment systems, were intentionally excluded to maintain the general applicability and clarity of the model. Likewise, although many shipboard systems incorporate redundancy to improve operational reliability, the attack tree assumed single points of failure to represent situations in which redundant mechanisms were improperly configured, inadequately maintained, or failed to operate as intended.

The attack tree was developed through a structured process that combined evidence obtained from the literature review with practical insights gathered during expert interviews. Each branch represented a logical sequence of attacker actions leading to a specific operational objective. The modular design of the model also enabled future expansion as new cyber threats, vulnerabilities, or attack techniques emerged, allowing additional attack paths to be incorporated while preserving the overall structure of the framework.

Infiltrating the Network

Infiltrating the ship's internal network is a critical step for an attacker seeking to compromise the ship's OT system. This process involves exploiting vulnerabilities within the ship's systems, which can then be leveraged to facilitate subsequent stages of the attack. This attack tree identifies two primary approaches: installing malicious devices and exploiting *external-facing interfaces*. The first approach relies on various techniques, including physical access, social engineering, insider threats, and the exploitation of technical vulnerabilities.

The most consistent and effective approach to network infiltration involves physically inserting malicious devices into the ship's systems. This method allows an attacker to bypass external network defenses and gain direct access to critical infrastructure.

1) Installing Malicious Devices. This approach represents the most consistent and effective

method of network infiltration by physically installing malicious devices within the ship's systems. It enables an attacker to bypass external network defenses and directly access critical infrastructure located in sensitive areas, such as equipment spaces, control rooms, or communication centers. Once connected to the ship's network, the malicious device can establish remote command-and-control (*C2*) communications using Wi-Fi or 4G connectivity.

2) Insider Threats. An attacker may bribe, coerce, or otherwise persuade crew members or maintenance personnel to install malicious hardware. Insider threats are particularly concerning because they can bypass conventional security controls and established security procedures.
3) Social Engineering. Attackers may use deception to gain physical or logical access, for example by posing as maintenance personnel or authorized visitors. Information required to support these attacks can be obtained through *spear-phishing* campaigns or publicly available sources, such as social media. For example, an attacker may exploit knowledge of the ship's maintenance schedule or operational procedures to facilitate and escalate an attack against the targeted vessel.
4) Compromised Intermediate Devices. Intermediate devices, such as maintenance laptops or removable media (e.g., USB drives) used during routine operations, including ECDIS updates, present additional cybersecurity risks. An attacker can infect these devices with malware, which may subsequently spread to the ship's network when the devices are connected during maintenance or update activities.

External-facing interfaces provide another avenue through which attackers can infiltrate the ship's network. Vulnerabilities in VSAT terminals, internet-connected systems, or other externally accessible interfaces can be exploited to obtain unauthorized access. Specific examples include:

1) Default Configuration. Attackers can exploit default configurations on VSAT equipment, particularly when factory-default credentials or configuration information are publicly available. By correlating AIS data with known VSAT models, attackers may identify vulnerable vessels and exploit weaknesses to gain unauthorized access to shipboard networks.
2) Outdated Systems. Many shipboard systems in Indonesia continue to operate on legacy operating systems, including unsupported versions of Microsoft Windows that no longer receive security updates. These systems often remain in service because shipping companies consider them operationally adequate or lack the financial resources to replace them. Consequently, these legacy systems represent potential entry points for attackers, particularly when they are connected to the internet or when an attacker has already established a foothold within the ship's OT network.

External-facing interfaces are particularly vulnerable because of their exposure to public networks, making them attractive targets for attackers seeking to circumvent internal security measures. Once access has been obtained, attackers can exploit these entry points to manipulate operational data, such as GPS position information, or deploy malware that compromises other critical shipboard systems.

Taking Control of ECDIS

The Electronic Chart Display and Information System (ECDIS) is a critical navigation system that supports route planning, situational awareness, and safe vessel operation. Because of its central role in modern navigation, ECDIS represents an attractive target for cyber attackers seeking to disrupt ship operations or manipulate navigational decisions. Compromising this system can significantly affect the integrity of navigation data and increase the likelihood of unsafe operating conditions (Anwar et al., 2023; Santoso & Noviarianto, 2021). The attack tree identified several pathways through which attackers could gain control of ECDIS, primarily by deploying malicious software or exploiting weaknesses in the system update process.

One attack scenario involved the direct introduction of malicious devices into the shipboard network through physical access to the ECDIS workstation. By connecting infected removable media or unauthorized hardware, attackers could install malware capable of altering electronic chart data, modifying system functions, or interfering with navigation processes. Such

manipulation could result in corrupted chart information, falsified vessel positions, or inaccurate route guidance, thereby increasing the risk of navigational errors and maritime incidents.

Another potential attack path exploited vulnerabilities associated with the ECDIS software update mechanism. Rather than attacking the navigation system directly, adversaries could compromise software update files or exploit interconnected network services used during maintenance procedures. Even in environments where onboard systems operated in isolation, weaknesses in update procedures or temporary network connectivity could provide opportunities for attackers to manipulate ECDIS and related systems, including the Automatic Identification System (AIS). These attack paths demonstrated that maintaining the integrity of software updates and controlling external interfaces were essential for protecting the reliability and security of ship navigation systems.

Loss of Operational View

Maintaining a complete operational view is essential for ensuring the safe and efficient operation of a vessel. This capability relies on the continuous availability of real-time information from navigation systems, propulsion monitoring systems, and other critical onboard subsystems that support situational awareness and operational decision-making. When this operational visibility is compromised, the crew's ability to monitor vessel conditions and respond effectively to abnormal situations is significantly reduced, thereby increasing the likelihood of navigational errors, equipment malfunctions, and maritime accidents (Suruwaky et al., 2025; Sutini & Mahendro, 2018).

Attackers may intentionally disrupt situational awareness by targeting critical navigation systems or exploiting environmental conditions that further reduce the crew's ability to verify operational information. The attack tree identified several possible attack methods, including manipulating sensor data, creating false navigation routes, disabling the Electronic Chart Display and Information System (ECDIS), modifying configuration files to conceal sensor information, and synchronizing cyberattacks with adverse weather conditions. Each of these attack paths could degrade the accuracy and reliability of the operational information available to the bridge team, thereby increasing the risk of incorrect decision-making during navigation.

A common attack strategy involved manipulating data generated by critical sensors, such as Global Navigation Satellite System (GNSS) receivers, radar, echo sounders, and propulsion monitoring systems. Because these sensors continuously provided information to onboard navigation and control systems, compromising their outputs enabled attackers to inject false or misleading data into the operational network. As a result, the crew could receive inaccurate information regarding the vessel's position, heading, speed, or machinery status, creating a false perception of the surrounding environment and significantly increasing navigational risk.

Sensor manipulation could also occur through the Terminal Processing Unit (TPU), which served as the interface between onboard sensors and the ship's internal network. If the TPU were compromised, attackers could intercept, modify, or suppress sensor information before it reached navigation and monitoring systems. Examples include GNSS spoofing that falsified the vessel's position, manipulation of propulsion sensor data that concealed engine abnormalities, and radar interference that generated false targets or altered environmental information. Rather than immediately disabling the system, attackers might gradually introduce subtle inconsistencies into sensor readings to erode crew confidence, delay incident recognition, and create opportunities for subsequent attacks.

Because ECDIS functions as the primary navigation platform on modern vessels, it represents one of the most attractive targets for cyber attackers seeking to degrade operational visibility. Previous studies have shown that manipulating ECDIS and radar data streams can mislead bridge personnel and reduce the reliability of critical navigational information. The attack tree therefore identified several methods that could render ECDIS ineffective, including modifying configuration files that define sensor mapping. By altering these files, attackers could prevent the system from recognizing essential sensors, causing operational displays to malfunction even though the sensors themselves remained functional. Such attacks were particularly feasible on legacy systems with outdated software and weaker cybersecurity protections.

Another attack scenario involved timing malicious activities to coincide with severe

weather conditions. Although weather events cannot be controlled by attackers, poor visibility and challenging sea conditions naturally reduce the bridge team's ability to validate navigation data through visual observation. Conducting cyberattacks during these periods could amplify confusion, delay the detection of abnormal system behavior, and substantially increase the operational consequences of compromised navigation systems.

Evasion

Evasion is an integral part of many cyberattacks, allowing attackers to disguise their activities and evade detection during or after an intrusion. In the maritime context, such actions typically involve destroying or manipulating systems that record critical events, thereby preventing forensic analysis and complicating incident response. Although evasion techniques targeting operating systems (OSs) are well known and broadly applicable, this section focuses on ship-specific examples in which the Voyage Data Recorder (VDR) is compromised.

To avoid detection, an attacker can prevent systems under their control from transmitting log data to the Voyage Data Recorder (VDR) or compromise the VDR itself. This can be achieved through the following methods:

1) Stopping the Logging System: An attacker can prevent a compromised system from transmitting event logs to the VDR, thereby eliminating evidence of specific malicious activities.
2) Damaging the VDR: The VDR itself can be targeted for destruction or corruption. Historical examples have demonstrated the feasibility of this approach; in one case, a malware-infected USB device corrupted the VDR data, rendering the recorded information unusable.

Evasion tactics, particularly those targeting logging mechanisms such as the Voyage Data Recorder (VDR), constitute an important component of sophisticated cyberattacks. By compromising the integrity or availability of the logging system, attackers can significantly impede post-incident investigations and reduce the likelihood of detection during vessel operations.

To move beyond scenario description, each validated attack path was assigned a likelihood band, an impact band, and a corresponding risk level using the aggregated expert ratings from the second Delphi round. Likelihood reflected the median feasibility rating, whereas impact reflected the median operational consequence rating. The resulting risk level was determined by combining the two bands using a 3 × 3 risk matrix. Mitigation priority was then established by combining the risk level with the effort required to implement the corresponding control, such that a high-risk attack path that could be addressed through a procedural change was prioritized over a similarly high-risk attack path requiring capital replacement. Nine of the eighteen attack paths fell within the high-risk category, and all nine were located within the shared enabling subtrees or the Crash and Disable goal branches. Table 3 presents the complete assessment.

Table 3
Risk level and mitigation priority for validated attack paths

No	Attack path	Goal	Likelihood	Impact	Risk level	Priority
1	Malicious device attached in bridge or control room	Shared	High	High	High	1
2	Insider assisted installation of malicious hardware	Shared	Medium	High	High	2
3	Exploitation of default VSAT configuration	Shared	Medium	High	High	2
4	VDR log suppression or corruption	Shared	Medium	Medium	Medium	3
5	Malware via removable media during ECDIS chart update	Crash	High	High	High	1
6	Malicious commands sent to wheel or thrusters	Crash	Medium	High	High	1
7	Autopilot course manipulation via ECDIS route data	Crash	Medium	High	High	1

No	Attack path	Goal	Likelihood	Impact	Risk level	Priority
8	GPS spoofing injected into ECDIS	Crash	Medium	High	High	2
9	Manipulated chart depth data causing grounding	Crash	Medium	High	High	2
10	Ransomware encrypting critical ECDIS files	Disable	Medium	High	High	1
11	Sensor data modification at the Terminal Processing Unit	Disable	Medium	Medium	Medium	3
12	Hiding sensors by modifying configuration files	Disable	Medium	Medium	Medium	3
13	Denial of service on power management and load shedding	Disable	Low	High	Medium	3
14	Engine overload combined with alarm suppression	Disable	Low	High	Medium	4
15	Disabling external communications before port arrival	Disable	Medium	Low	Medium	4
16	Ballast system manipulation to induce a list	Sink	Low	High	Medium	4
17	Anti-rolling system counter actuation	Sink	Low	High	Medium	5
18	Thruster actuation timed to the wave period	Sink	Low	High	Low	5

Discussion

Readiness to face attacks

Main Objective 1: Crash the Ship

Crashing a ship is a highly destructive objective that can result in significant financial losses, environmental damage, and potential loss of life. Vulnerabilities in cyber-physical systems aboard surface vessels may allow attackers to manipulate autopilot and navigation controls, thereby increasing the risk of accidental collisions or groundings. Although it may not be as catastrophic as capsizing, crashing a ship can still lead to devastating consequences, as demonstrated by incidents such as the Costa Concordia disaster in 2012. In this type of attack, the captain is expected to maintain effective control of the vessel to prevent severe accidents. This can be illustrated by the EVER GIVEN incident in the Suez Canal. Although the vessel itself did not sustain severe damage, it obstructed the Suez Canal because of its large dimensions (Ghosh & Sourav, 2026; Ramos et al., 2021).

One method of crashing a ship involves directing it onto a collision course with another vessel, an iceberg, or a floating object. An attacker can achieve this by satisfying two conditions simultaneously: (1) Manipulating the ship's navigation system to influence the vessel's course. (2) Rendering the thrusters and steering systems inoperable for manual override.

Research has shown that internal cyberattacks targeting shipboard networks can manipulate critical sensor data, causing onboard systems to process false information and thereby influencing navigation and automated decision-making (Huso et al., 2025; Tam & Jones, 2018). Although these attacks primarily distort situational awareness, they can also serve as entry points for deeper intrusions that compromise a vessel's steering and propulsion systems.

Main Objective 2: Sinking the Ship

Sinking a ship involves destabilizing its physical balance to the point that it capsizes. This type of attack focuses on manipulating the vessel's stability system to shift the distribution of physical forces in one direction, ultimately causing the ship to capsize. Although such attacks are not universally applicable because of differences in vessel types and stability designs, they are more likely to succeed under adverse weather conditions or against specific vessel configurations, such as cargo ships and cruise ships.

Main Objective 3: Disable the Ship

The objective of disabling a ship is to prevent it from continuing normal operations, leaving it stranded and potentially vulnerable to environmental hazards or further attacks. This objective can be achieved through two primary approaches: Denial-of-Service (DoS) attacks targeting critical systems or attacks that induce mechanical failures. Both approaches exploit the vessel's reliance on automation and interconnected systems to create operational paralysis.

DoS attacks focus on rendering critical systems unresponsive to crew input. Although these attacks are not always permanent, they can render a vessel inoperable, particularly if the crew lacks the information technology (IT) expertise required to resolve the issue. Ship power management systems and load reduction controllers are especially vulnerable to cyber-based DoS attacks, which can disrupt power balance and trigger cascading failures throughout ship operations.

Mechanical failures target the physical components of the vessel by exploiting their operational limits to induce damage. The principal methods include: (1) Alarm Manipulation: The attacker alters sensor data so that the system fails to warn the crew when the engine is operating under overload conditions. (2) Machinery Overload: Commands are transmitted to force the machinery or generators to operate beyond their safe operating limits, resulting in equipment damage and eventual system failure.

Comparison with studies employing different methodological approaches produces a partly divergent picture rather than uniform confirmation, and these divergences are informative. Uğurlu et al. (2026) assessed shipboard cybersecurity using Bayesian networks, a method that propagates conditional probabilities across an equipment dependency graph and therefore weights a system according to the number of other systems that depend on it. By contrast, an attack tree ranks the attack paths that an adversary is most likely to exploit. Consequently, the two methods may prioritize the same systems differently even when based on the same vulnerability inventory. Putra et al. (2023), using a hybrid AHP-TOPSIS model for Indonesian maritime data, decomposed risk into threat, vulnerability, and consequence to produce an aggregate risk score. Although this approach supports portfolio-level prioritization across a fleet, it does not illustrate how an attacker reaches a physical outcome or where the attack chain could be interrupted. Kim et al. (2022), applying the MITRE ATT&CK framework to shipboard equipment, identified a substantially larger inventory of attack techniques than the present study but did not establish any prioritization among them, illustrating the trade-off between comprehensive coverage and decision-making usefulness. The most direct challenge comes from Kurt et al. (2025), whose evidential reasoning and Human Error Assessment and Reduction Technique (HEART) analysis of human reliability in detecting GPS spoofing on Electronic Chart Display and Information Systems (ECDIS) indicated that crew detection capability deteriorates significantly in congested waterways. Applied to the present expert panel, this finding suggests that the detection capability implicitly attributed to the bridge team may be overly optimistic and that the risk ratings assigned to the navigation manipulation paths in Table 3 should be interpreted as lower-bound estimates rather than definitive values. Thus, the present study is refined rather than confirmed by the broader literature. This observation is retained deliberately because its practical implication is that a captain's readiness cannot be assumed but must instead be empirically assessed.

The attack tree also supports direct alignment with the control frameworks already applicable to Indonesian ship operators. Table 4 maps each group of attack paths to the corresponding functional elements of the IMO Guidelines on Maritime Cyber Risk Management, the relevant functions and categories of the NIST Cybersecurity Framework 2.0, and the onboard controls capable of interrupting each attack path. The purpose of this mapping is to eliminate the interpretive step that typically separates a threat model from a compliance obligation, thereby enabling a captain or a designated person ashore to move directly from a modeled attack path to a control that is already required under the vessel's Safety Management System.

Table 4
Mapping of attack path groups to IMO and NIST Cybersecurity Framework 2.0 controls

Attack path group	Primary vulnerability	IMO functional element	NIST CSF 2.0 function and category	Onboard control
Network infiltration via malicious device	Unrestricted physical access to bridge and control spaces	Protect	PR.AA Identity Management and Access Control	Access logging at gangway and bridge, unused ports sealed and disabled
Removable media and ECDIS update chain	No scanning or cryptographic validation of media	Protect and Detect	PR.DS Data Security; DE.CM Continuous Monitoring	Dedicated scanning kiosk, signed chart updates, USB whitelisting
External interface exploitation via VSAT and legacy systems	Default credentials and unsupported operating systems	Identify and Protect	ID.AM Asset Management; PR.PS Platform Security	Asset register with operating system lifecycle, credential rotation, network segmentation
Navigation manipulation through spoofing, chart tampering, autopilot	Implicit crew trust in sensor input	Detect	DE.AE Adverse Event Analysis	Cross check of GNSS against radar parallel index and visual bearings, position plausibility alarms
Denial of service on steering, propulsion and power	Absence of tested manual override procedures	Respond and Recover	RS.MA Incident Management; RC.RP Recovery Plan Execution	Drilled manual steering changeover, blackout recovery drills, offline chart backup
Evasion through VDR tampering	Log integrity not independently monitored	Detect and Respond	DE.CM Continuous Monitoring; RS.AN Incident Analysis	Independent log retention ashore, VDR integrity check within ISM audit

CONCLUSION

This study identified cyber vulnerabilities and attack scenarios affecting ship navigation and operational technology (OT) systems in Indonesian maritime operations by developing a structured attack tree model based on evidence from the literature and expert validation. The analysis demonstrated that cyberattacks leading to ship collisions and operational paralysis represented the most feasible threats, particularly in Indonesia's congested ports and narrow waterways, whereas ship capsizing through cyber manipulation was considerably less likely because of modern vessel design and existing safety mechanisms. The resulting attack tree extended beyond a descriptive threat model by providing a systematic framework for identifying attack paths, assessing vulnerabilities, and supporting cybersecurity risk assessment. The findings further emphasized that cyber resilience depends not only on technological safeguards but also on human factors, highlighting the importance of collaboration among cybersecurity professionals, maritime engineers, and ship operators. Practical mitigation should therefore prioritize stronger network segmentation, stricter removable media controls, secure management of navigation systems such as Electronic Chart Display and Information System (ECDIS) and autopilot systems, and continuous cybersecurity awareness and training for ship crews.

This research contributes to maritime cybersecurity by providing an ethically grounded threat-modeling approach intended to strengthen defensive capabilities and support risk mitigation for critical maritime infrastructure. Nevertheless, the developed attack tree was validated using expert judgment and focused primarily on Indonesian cargo ship operations, limiting its applicability to other vessel types and emerging maritime technologies. Future studies

should incorporate broader stakeholder perspectives, including ship designers and operators of different vessel classes, while extending the model to autonomous vessels, AI-enabled navigation systems, and blockchain-based maritime logistics. Further research should also integrate quantitative risk assessment methods, cyber-range experimentation, and complementary analytical techniques, such as Bayesian networks, Failure Mode and Effects Analysis (FMEA), and the MITRE ATT&CK® for Industrial Control Systems (ICS) framework, to improve the accuracy of attack likelihood estimation, evaluate crew responses under realistic operational conditions, and enhance maritime cybersecurity risk management.

ACKNOWLEDGEMENT

The authors sincerely thank all maritime professionals, cybersecurity specialists, technical consultants, ship captains, and deck officers who participated in the interviews and validation process. Their valuable expertise and practical insights greatly contributed to the development and validation of the attack tree model presented in this study. The authors also appreciate the support provided by their respective institutions throughout the research process.

AUTHOR CONTRIBUTION STATEMENT

Agus Widodo: Conceptualization, methodology, investigation, data curation, formal analysis, visualization, and writing original draft preparation. Siwi Woro Herningsih: Conceptualization, methodology, validation, supervision, and project administration. Roma Dormawaty: Methodology, validation, formal analysis, and supervision. Riza Nur Amala: Investigation, data curation, visualization, and resources. All authors approved the final version of the manuscript and agreed to be accountable for all aspects of the work.

REFERENCES

Androjna, A., Satler, T. B., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges Of Maritime Navigation. *Journal Of Marine Science And Engineering*, *8*(10), 776. https://doi.org/10.3390/Jmse8100776

Anwar, A., Suharso, A. R., Hendartono, A., Wantoro, W. B., Sirait, E., & Purwanto, P. (2023). Pengembangan Media Pembelajaran Electronic Chart Display And Information System Menggunakan Software Visual Basic 6. *Konstruktivisme: Jurnal Pendidikan Dan Pembelajaran*, *15*(1), 15–26.

Ashfaq Uz Zaman, S. M., Qamar, F., Mohd, M., Sabrina Suhaimi, N. H., & Khandakar, A. (2026). A Review Of Automatic Identification System Approaches For Maritime Cyber Security. *Security And Communication Networks*, *2026*(1), 5898106.

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A Security Evaluation Of Ais Automated Identification System. In *Proceedings Of The 30th Annual Computer Security Applications Conference (Acsac 2014)* (Pp. 436–445). Association For Computing Machinery. https://doi.org/10.1145/2664243.2664257

Bueger, C. (2015). What Is Maritime Security? *Marine Policy*, *53*, 159–164. https://doi.org/10.1016/J.Marpol.2014.12.005

Cao, Q., Chi, C., & Shan, J. (2025). Can Artificial Intelligence Technology Reduce Carbon Emissions? A Global Perspective. *Energy Economics*, *143*, 108285.

Cybersecurity, E. U. A. For. (2025). *Enisa Threat Landscape 2025*. European Union Agency For Cybersecurity. https://www.Enisa.Europa.Eu/Publications/Enisa-Threat-Landscape-2025

Erbas, M., Khalil, S. M., & Tsiopoulos, L. (2024). Systematic Literature Review Of Threat Modeling And Risk Assessment In Ship Cybersecurity. *Ocean Engineering*, *306*, 118059. https://doi.org/10.1016/J.Oceaneng.2024.118059

Erdoğan, A., & Erdoğan, N. S. (2025). Cybersecurity And Privacy In Maritime Security: Theories, Challenges, Case Studies And Future Prospects. *Güvenlik Bilimleri Dergisi*, *Kolluk Uygulamaları Ve Güvenlik Teknolojileri Özel Sayısı*, 258–287.

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). *The Future Of Maritime Cyber Security*. Lancaster University. https://Eprints.Lancs.Ac.Uk/Id/Eprint/72696/

Ghosh, A., & Sourav, S. (2026). Shock Propagation And Port-Congestion Hysteresis In Maritime Disruptions: Evidence From Covid-19, The Suez Blockage, And The Red Sea Crisis. *Maritime*

Economics & Logistics, 1–36.

Huso, D., Munim, Z. H., Chai, Y., Kim, T. E., & Bhuiyan, Z. (2025). Factors Influencing Cybersecurity Risk And Autonomous Shipping Awareness. *2025 Ieee International Conference On Industrial Engineering And Engineering Management (IEEM)*, 960–964.

Jin, Y., Feng, Y., Liu, C., & Li, S. (2025). Navigating The Digital Seas: Legal Challenges And Global Governance Of Maritime Cyber Operations. *Frontiers In Marine Science*, *12*, 1616906.

Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack Models For Ship Equipment Based On The Mitre Att&Ck Framework. *Sensors*, *22*(5), 1860. https://doi.org/10.3390/S22051860

Kapalidis, C. (2025). *Cyber Risk Assessment In The Maritime Transport Sector: Ships, Ports And Port Systems*. Loughborough University.

Keskin, O. F., Lubja, K., Bahsi, H., & Tatar, U. (2025). Systematic Cyber Threat Modeling For Maritime Operations: Attack Trees For Shipboard Systems. *Journal Of Marine Science And Engineering*, *13*(4), 645. https://doi.org/10.3390/Jmse13040645

Kiss, L., Savaliya, S. K., Schunck, C. H., Sellung, R., & Winterstetter, M. (2026). Critical Infrastructure Risk Assessment: Current Practices And Emerging Challenges. *Open Identity Summit 2026*, 63–77.

Kurt, Y. B., Uflaz, E., Akyuz, E., Kurt, R. E., & Turan, O. (2025). Analysis Of Human Reliability In Detecting Gps Spoofing On Ecdis In Congested Waterways Under Evidential Reasoning And Heart Approach. *Computers & Security*, *151*, 104316. https://doi.org/10.1016/J.Cose.2025.104316

Malik, D., & Widodo, W. (2025). Analisis Pengaruh Human Faktor Terhadap Keselamatan Pelayaran Di Kapal Penumpang Perusahaan Surabaya. *Jurnal Sains Dan Teknologi Maritim*, *25*(2), 215–228.

Mudiyanto. (2020). Analisis Kelaiklautan Kapal Terhadap Keselamatan Pelayaran Dikapal Niaga (Study Kasus Pada Perusahaan Pelayaran Kapal Penumpang Di Surabaya). *Jurnal Sains Dan Teknologi Maritim*, *20*(1), 13–27. https://doi.org/10.33556/Jstm.V20i1.213

Negara, B. S. Dan S. (2024). *Lanskap Keamanan Siber Indonesia 2023*. Badan Siber Dan Sandi Negara Republik Indonesia. Https://Csirt.Kemenkeu.Go.Id/In/Post/Lanskap-Keamanan-Siber-Indonesia-2023

Nist. (2024). *The Nist Cybersecurity Framework (CSF) 2.0*. Https://Doi.Org/10.6028/Nist.Cswp.29

Nur, F. (2025). *Analisis Peranan Alat Navigasi Ais Sebagai Pemantau Untuk Meningkatkan Keselamatan Pelayaran Di PSV S Panglima*. Politeknik Ilmu Pelayaran Makassar.

Organization, I. M. (2022). *Guidelines On Maritime Cyber Risk Management* (Msc-Fal.1/Circ.3/Rev.2). International Maritime Organization. https://www.Uscg.Mil/Portals/0/Msc-Fal_1-Circ_3-Rev_2 - Guidelines On Maritime Cyber Risk Management %28secretariat%29.Pdf

Putra, I. N., Octavian, A., Susilo, A. K., & Prabowo, A. R. (2023). A Hybrid Ahp-Topsis For Risk Analysis In Maritime Cybersecurity Based On 3d Models. *Decision Science Letters*, *12*(4), 759–772. https://doi.org/10.5267/J.Dsl.2023.6.005

Ramos, K. G., Rocha, I. C. N., Cedeño, T. D. D., Costa, A. C. Dos S., Ahmad, S., Essar, M. Y., & Tsagkaris, C. (2021). Suez Canal Blockage And Its Global Impact On Healthcare Amidst The Covid-19 Pandemic. *International Maritime Health*, *72*(2), 145–146. https://doi.org/10.5603/Imh.2021.0026

Santoso, H. B., & Noviarianto. (2021). Meningkatkan Kompetensi Navigasi Mahasiswa Politeknik Maritim Negeri Indonesia Melalui Pengembangan Media Pembelajaran Electronic Chart And Display Information System (ECDIS) Simulator. *Jurnal Sains Dan Teknologi Maritim*, *21*(2), 172–178. https://doi.org/10.33556/Jstm.V21i2.279

Suruwaky, A. M., Ndahawali, D. H., Kasim, M., Bachri, S., Komboe, A. A., Abdullah, A., Maysaroh, S., & Leatemia, B. M. (2025). Pengenalan Dan Praktik Alat Navigasi Kapal Bagi Generasi Muda Biak Pada Km Airaha 02. *Buletin Swimp*, *5*(2), 29–38.

Sutini, & Mahendro, I. (2018). Pengenalan Teknologi Navigasi Melalui Pembelajaran Sistem Navigasi Elektronik Untuk Pemahaman Taruna Tentang Navigasi. *Jurnal Sains Dan Teknologi Maritim*, *18*(1), 41–49. https://doi.org/10.33556/Jstm.V0i1.185

Syibli, Y. M., & Nuryaman, D. (2021). Peranan Alat Navigasi Di Kapal Untuk Meningkatkan

Keselamatan Pelayaran Di Atas Kapal. *Dinamika Bahari*, *2*(1), 39–48. https://doi.org/10.46484/Db.V2i1.250

Tam, K., & Jones, K. D. (2018). Cyber-Risk Assessment For Autonomous Ships. In *2018 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)* (Pp. 1–8). IEEE. https://doi.org/10.1109/Cybersecpods.2018.8560690

Tam, K., Moara-Nkwe, K., & Jones, K. D. (2021). The Use Of Cyber Ranges In The Maritime Context: Assessing Maritime-Cyber Risks, Raising Awareness, And Providing Training. *Maritime Technology And Research*, *3*(1), 16–30. https://doi.org/10.33175/Mtr.2021.241410

Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware Suppliers Bearing Gifts!: Analysing Coverage Of Supply Chain Cyber Security In Critical National Infrastructure Sectorial And Cross-Sectorial Frameworks. *Computers & Security*, *108*, 102324. https://doi.org/10.1016/J.Cose.2021.102324

Uğurlu, Ö., Aydın, B., Kaya, A. Y., & Tonoğlu, F. (2026). Analysis Of Cybersecurity Threats To Ships In Maritime Transportation And Optimal System Design On Ships. *Proceedings Of The Institution Of Mechanical Engineers, Part M: Journal Of Engineering For The Maritime Environment*. https://doi.org/10.1177/14750902251408643

Wolff, J. (2021). How Is Technology Changing The World, And How Should The World Change Technology? *Global Perspectives*, *2*(1), 27353. https://doi.org/10.1525/Gp.2021.27353