QISTINA: Jurnal Multidisiplin Indonesia
P-ISSN: 2964-6278 E-ISSN: 2964-1268
Vol. 4 No. 2 Desember 2025

Cyber Threats to Maritime Navigation: Case Studies of Boats and Ports in Ambon, Maluku

Raesha Syahnaz[1] Surachman Surjaatmadja[2] Arifuddin Uksan[3]
Graduate Students, Faculty of National Security, Maritime Security, Defense University, Bogor, West Java, Indonesia[1]
Faculty of National Security, Maritime Security, Defense University, Bogor, West Java, Indonesia[2,3]
Email: raeshanazz@gmail.com[1] isur.atmadja@gmail.com[2] arifuddinuksan123@gmail.com[3]

Abstrak

Penelitian ini menganalisis ancaman siber pada sistem navigasi maritim di Ambon, Maluku, dengan fokus pada kapal nelayan, kapal patroli, dan pelabuhan kecil. Analisis dilakukan melalui integrasi observasi lapangan dan regulasi nasional, seperti Perpres No. 95/2018 tentang SPBE, Permenhub No. 134/2016 tentang Rencana Keamanan Fasilitas Pelabuhan, dan Permen KP No. 42/2016 tentang VMS. Hasil menunjukkan kapal nelayan masih memakai GPS sederhana tanpa perlindungan siber, kapal patroli memiliki sistem lebih maju namun minim firewall, sedangkan pelabuhan kecil masih mengandalkan sistem manual yang rawan manipulasi data. Berdasarkan temuan ini, disusun Cyber Security Plan (CSP) terintegrasi dengan Port Security Plan (PSP) dan Port Facility Security Plan (PFSP), mencakup perlindungan data pelabuhan, peningkatan literasi digital nelayan, penyediaan firewall untuk armada patroli, serta integrasi Aids to Navigation (AtoN) virtual. Penelitian menegaskan pentingnya keterpaduan kebijakan pusat dan daerah guna memperkuat keamanan siber maritim Ambon sebagai model kawasan timur Indonesia.
Kata Kunci: Keamanan Siber; Navigasi Maritim; Kapal Nelayan; Pelabuhan Kecil

Abstract

This study analyzes cyber threats to maritime navigation systems in Ambon, Maluku, focusing on fishing boats, patrol boats, and small ports. The analysis was conducted through the integration of field observations and national regulations, such as Presidential Regulation No. 95/2018 on SPBE, Minister of Transportation Regulation No. 134/2016 on Port Facility Security Plans, and Minister of Maritime Affairs and Fisheries Regulation No. 42/2016 on VMS. The results show that fishing vessels still use simple GPS without cyber protection, patrol boats have more advanced systems but minimal firewalls, while small ports still rely on manual systems that are prone to data manipulation. Based on these findings, an integrated Cyber Security Plan (CSP) was developed with the Port Security Plan (PSP) and Port Facility Security Plan (PFSP), covering port data protection, improving fishermen's digital literacy, providing firewalls for the patrol fleet, and integrating virtual Aids to Navigation (AtoN). The study emphasizes the importance of integrated central and regional policies to strengthen maritime cyber security in Ambon as a model for eastern Indonesia.
Keywords: *Cybersecurity; Maritime Navigation; Fishing Vessels; Small Ports*

INTRODUCTION

In recent decades, information technology has developed rapidly and influenced almost all aspects of human life. Artificial intelligence (AI) is even considered one of the fastest-growing technologies in the world (A. Oppermann (2022)), including in the maritime sector. Digitalization in this field not only presents opportunities, but also gives rise to exaggerated expectations, as if AI will soon completely replace the role of humans in shipping and decision-making. This optimism is reflected in the belief that AI can significantly improve maritime safety, promote more environmentally friendly sea transportation through innovations in fuel,

navigation, and ship design, while also providing economic benefits for ship owners who adopt it. In line with this, the size of the AI industry market continues to show rapid growth from year to year, and various projections estimate that this exponential trend will continue in the future (Figure 1).

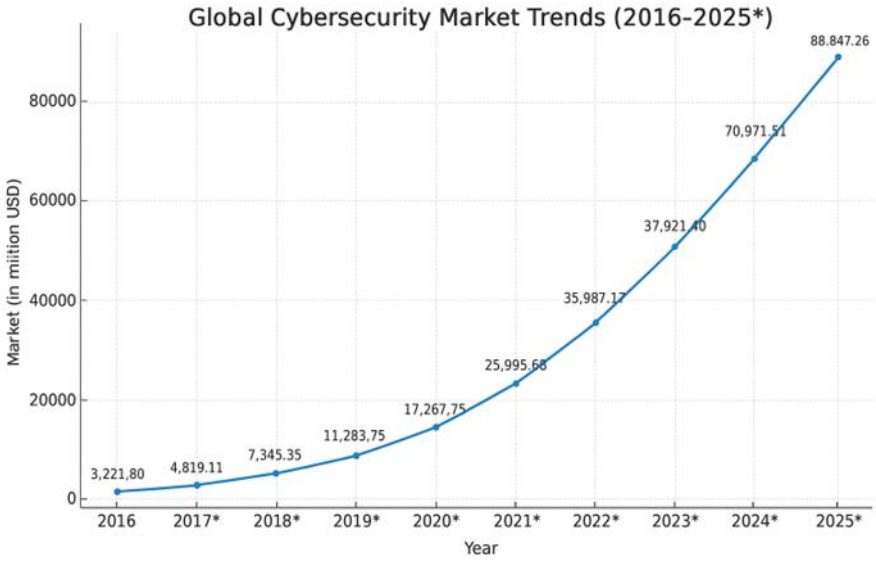

Figure 1. Growth Of The Artificial Intelligence Industry Market Size (2016–2025) In Millions Of US Dollars (A. Oppermann, 2022)

On the other hand, reality shows that cyber threats are growing at an alarming rate. It is projected that global losses due to cybercrime will reach US$10.5 trillion per year by the end of 2025, making it the third largest "economy" in the world after the United States and China. The complexity of cyber attacks is increasing along with the use of AI for both defense and crime. A 2024 survey of large companies in the United States shows that 56% of corporations have identified AI as a risk factor, a dramatic increase from the previous year (Fortune, 2024). The Cybercrime Trends 2025 report also notes that 87% of global organizations have been the target of AI-based attacks (The CFO, 2025). In addition to technical threats, the human resource gap exacerbates the situation. The number of job vacancies in cybersecurity has risen sharply from 1 million in 2013 to 3.5 million in 2021, and is expected to remain the same in 2025 (Cybersecurity Ventures, 2025). Although Generative AI technology is projected to reduce the need for specialized education for entry-level positions by 2028 (Mediabrief, 2023), the current shortage of experts remains a major obstacle. On the other hand, global spending on cybersecurity is estimated to reach US$1.75 trillion in the 2021–2025 period (Cybersecurity Ventures, 2021), with the corporate sector allocating more than US$213 billion in 2024 for security software alone (Motley Fool, 2024). However, risks stemming from human error, such as phishing, weak passwords, and threats from insiders, remain a dominant vulnerability.

In the Indonesian context, this study focuses on Ambon, Maluku, which is one of the main centers of maritime activity in the eastern region. Ambon has a fishing port that serves hundreds of traditional and modern fishing boats, as well as a number of small ports that serve as inter-island logistics distribution hubs. This dense shipping activity presents potential vulnerability to cyber threats, especially to navigation systems, most of which still use simple devices without adequate protection. In addition, the presence of a Navy patrol base makes Ambon a strategic point for maritime security surveillance. From an academic perspective, Ambon represents the typical conditions of eastern Indonesia's maritime regions, which remain relatively underdeveloped compared to the maritime industrial centers in the west. This

provides an opportunity for research to assess the gap between national cybersecurity regulations and real conditions in the field. Thus, this study not only evaluates cyber threats to maritime navigation systems on fishing boats, patrol vessels, and small ports in Ambon but also offers a comprehensive overview of Indonesia's readiness to face maritime security challenges in the digital era.

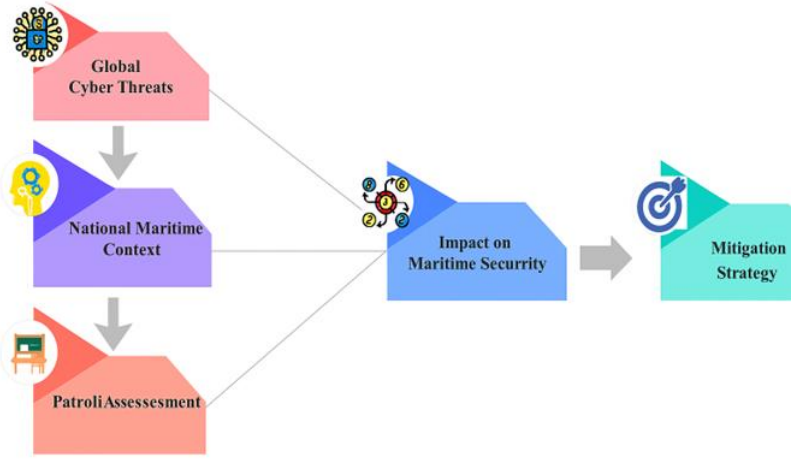

Figure 2. Research Conceptual Framework

RESEARCH METHODS

This study employs a descriptive qualitative approach to systematically, factually, and accurately describe the potential and forms of cyber threats to maritime navigation systems, particularly on fishing vessels, patrol boats, and small ports in Indonesia. This approach is chosen because the issue of maritime cybersecurity encompasses not only technical dimensions but also institutional, regulatory, and human resource preparedness aspects. According to Creswell and Creswell (2017), the qualitative method is relevant for exploring complex socio-technological phenomena through contextual and interpretative analysis. Therefore, this research focuses on the interpretation of data and the construction of comprehensive understanding rather than on quantitative hypothesis testing. The primary data source in this study is secondary data, collected from various official documents, research reports, academic publications, as well as governmental and international regulations. The data include national policy documents related to maritime and cybersecurity, such as the *Shipping Law*, regulations from the Ministry of Transportation, and the *National Cybersecurity Strategy*. Additionally, this research utilizes reports from international institutions such as the *International Maritime Organization (IMO)*, *INTERPOL*, and global cybersecurity companies that highlight threat trends in the maritime industry. Academic journal articles, conference proceedings, and case studies of cyber incidents involving small ports and vessels also serve as essential comparative references. Data collection is conducted through systematic literature review, policy document mapping, and the selection of relevant sources aligned with the research focus. Data analysis employs content analysis to critically examine narrative patterns concerning navigation vulnerabilities, modes of cyberattacks, and existing mitigation policies, as well as thematic analysis to categorize data into key themes, including types of cyber threats, technical and institutional vulnerabilities, and national readiness in responding to maritime cyberattacks. The results of these analyses are synthesized to formulate strategies for strengthening national maritime cybersecurity, with a case study in Ambon representing vulnerable regions in eastern Indonesia. This approach is expected to provide a comprehensive understanding that enhancing cybersecurity is an integral component of reinforcing Indonesia's maritime resilience.

RESEARCH RESULTS AND DISCUSSION

Technical Vulnerabilitie

Ports and Vessel Activities

Field observations indicate that most fishing vessels in Ambon still rely on simple navigation devices such as handheld GPS units and commercial fish finders, which lack any form of cybersecurity protection. This condition significantly increases their vulnerability to *jamming* and *spoofing* attacks. Small-scale patrol boats possess relatively more advanced navigation systems, yet these are not supported by adequate firewalls or security software. Similarly, small ports in the Ambon region face comparable challenges, as communication and logistics management systems are still largely manual, with only a few having adopted digital integration. These technical gaps can be exploited by malicious actors to disrupt maritime safety and the effectiveness of surveillance activities. This context is particularly critical considering the strategic role of Ambon Port as a major maritime transport hub in the Maluku region. Yos Sudarso Port, along with local piers such as Batu Merah and Gudang Arang, serves a wide range of vessels, including passenger ships, cargo carriers, and inter-island pioneer vessels (Simpel, 2025). Maritime activity at these ports continues to increase, as reflected in 1,345 vessel visits recorded between January and June 2025, compared to 1,264 visits during the same period in the previous year (Antara News Ambon, 2025a).

Patrol Vessels and Maritime Security

The Indonesian government's efforts to strengthen maritime infrastructure in Maluku and North Maluku are reflected in the inauguration of 21 new seaports, including the Batu Merah People's Wharf in Ambon, designed to accommodate vessels of up to 500 DWT. The presence of these ports is expected to facilitate logistical distribution, support coastal economic activities, and enhance inter-island connectivity (Antara News Ambon, 2025b). The modernization of port infrastructure, accompanied by increasing vessel traffic, has further solidified Ambon's position as a maritime hub in eastern Indonesia. In addition, maritime security initiatives in the Ambon region have demonstrated significant progress through fleet modernization and inter-agency coordination. A key strategic measure is the deployment of KRI Dorang-874, a 60-meter fast patrol vessel commissioned to strengthen the Naval Patrol Unit (Satrol) of Lantamal IX Ambon. The vessel is equipped with a surveillance radar with a range of approximately 100 nautical miles, a maximum speed of 24 knots, and a crew capacity of 55 personnel. This capability is expected to enhance detection, surveillance, and rapid response capacity against illegal activities and border violations within Maluku's waters (Antara News Ambon, 2025a).

Furthermore, maritime security strategies have been reinforced through joint inter-agency patrols, involving state vessels (*Kapal Negara*), aerial surveillance, and coordination between Bakamla, the Indonesian Navy, National Police (Polri), and the Ministry of Marine Affairs and Fisheries (KKP). The use of intelligence data and satellite technology has strengthened early detection capabilities against non-traditional maritime threats such as illegal fishing, smuggling, and transnational crimes (Antara News Ambon, 2025b). However, field observations reveal considerable limitations in small patrol vessels operated by the Water Police Unit (Polair) of Maluku Regional Police. Most of the fleet consists of small-type speedboats (C-1 to C-3) powered by low-capacity outboard engines. Their navigation systems generally rely on handheld GPS units and commercial fish finders, without cybersecurity features such as firewalls or protective software. This condition exposes the vessels to potential GPS jamming and spoofing attacks, undermining maritime surveillance effectiveness, particularly in border zones and strategic shipping routes. Compared to KRI Dorang-874, which

possesses more advanced detection systems, the technological disparity among smaller patrol vessels represents a serious security gap (Field Observation Ambon, 2025; Antara News Ambon, 2025c).

Fishermen and Fishing Vessels

Fishing activities and fishing vessels in Maluku play a strategic role in supporting national food security as well as Indonesia's maritime economy. The Nusantara Fishing Port (PPN) Ambon regularly conducts technical and nautical inspections of fishing vessels prior to departure. These inspections cover navigational readiness, safety standards, and the technical conditions of vessels and crew. The procedure aims not only to ensure the safety of fishing operations but also to serve as an early prevention mechanism against maritime accidents and non-compliant fishing practices (Ministry of Marine Affairs and Fisheries, 2025). On a broader scale, the Fisheries Management Area (WPP) 718 in Maluku possesses substantial annual fishery production potential, estimated at approximately 1,118,510 tons per year. This capacity positions Maluku as one of Indonesia's major fishery centers, supported by key port networks such as PPN Ambon, PPN Tual, PPN Dobo, Benjina, and Saumlaki. These ports serve as hubs for fish landing, logistical distribution, and catch monitoring, collectively strengthening the implementation of sustainable fishing practices (Provincial Government of Maluku, 2024).

In addition to reinforcing existing port functions, the government is currently developing the Integrated Fishing Port (New Port Ambon) as a national strategic project. This initiative is expected to enhance the fisheries supply chain, improve distribution capacity, and facilitate seafood exports from Maluku to domestic and international markets. Through this infrastructure development, Ambon is projected to become a key logistics hub for the blue economy, further consolidating Indonesia's position in the global seafood trade. However, alongside this substantial potential lies a new layer of vulnerability related to the digitalization of fisheries. Many fishing vessels particularly those operating from small ports have begun using modern navigational tools such as handheld GPS, fish finders, and digital radio communications. Yet, these devices are generally not equipped with firewalls, data encryption, or adequate cybersecurity systems. This condition creates exposure to threats such as GPS spoofing, vessel position data manipulation, and disruptions to navigational communication, which can mislead vessel routes or affect catch efficiency.

Navigation and Supporting Systems

The navigation systems and supporting maritime infrastructures in Ambon play a vital role in ensuring safety and efficiency in maritime activities. The Ambon Navigation District emphasizes the use of the Automatic Identification System (AIS) as one of the key instruments in modern navigation. Through AIS, vessels can automatically transmit critical information such as position, destination, speed, and navigational status, which serves not only to enhance maritime safety but also to support more efficient sea traffic monitoring and management (Kapal Pedia, 2024). In line with this, the Harbormaster and Port Authority Office (KSOP) Class I Ambon has developed a port data system that includes detailed profiles of registered ports, docks, locations, and operational areas. This data serves as the foundation for integrated port planning and operational control. However, challenges persist as not all docks or smaller ports around Ambon are equipped with modern facilities or possess sufficient channel depth to accommodate large-capacity vessels (Simpel, 2025). This infrastructural gap has significant implications for logistics distribution, inter-island connectivity, and the effectiveness of navigational systems that rely on adequate supporting facilities across various port nodes.

Regulatory Aspect

Ship navigation systems both on fishing vessels and patrol boats have been found to be highly vulnerable to cyberattacks (Silgado, 2018; Bartlett et al., 2015; Johnson et al., 2007). International reports highlight that modern maritime technologies have increasingly integrated Information Technology (IT) and Operational Technology (OT) without adequate segmentation, allowing vulnerabilities in OT systems to be exploited as entry points into IT networks. The primary vulnerabilities involve GPS, AIS, radar, and ECDIS**,** all of which have, in several documented cases, been manipulated to display false vessel positions or even disrupt navigational control (Glomsvoll & Bonenberg, 2017). These global findings align with field observations in Ambon**,** where fishing vessels largely rely on simple navigation tools such as handheld GPS and commercial fish finders, while small patrol boats lack adequate firewalls or digital protection systems. Such conditions signify a serious risk of both external intrusion and internal negligence. From a regulatory perspective, policy analysis indicates that the maritime cybersecurity framework in Indonesia already possesses a normative foundation. For instance, Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (SPBE) underscores the importance of securing digital infrastructure and information systems across strategic sectors, including maritime transport. Additionally, Regulation of the Head of Bakamla No. 1 of 2017 on the Organizational Structure of Bakamla outlines the agency's role in ensuring maritime safety and security, including supervision of navigational systems. Meanwhile, Law No. 32 of 2014 on Maritime Affairs mandates the comprehensive protection of marine resources and infrastructure, which should logically extend to cybersecurity. However, field findings in Ambon reveal that the implementation of these regulations remains uneven, particularly across small ports and local fishing communities. Interviews with maritime patrol officers indicate that regulatory dissemination remains limited, and technical standards for navigational system protection have not been consistently applied.

Human Resource Readiness and Cybersecurity Implementation

Field observations in Ambon reveal that human resource capacity remains a major constraint in strengthening maritime cybersecurity. Most local fishers exhibit limited digital literacy and lack awareness of potential cyber threats affecting basic navigation devices such as handheld GPS units and commercial fish finders. As a result, they are highly vulnerable to signal jamming and spoofing incidents. At the operational level, maritime patrol personnel demonstrate relatively better technical proficiency; however, the number of officers specifically trained in maritime cybersecurity remains insufficient to ensure continuous and effective surveillance. Similarly, administrators of small ports acknowledge the absence of formal cybersecurity training, particularly in communication systems and data management practices. The analysis also indicates that while regulatory frameworks exist including Presidential Regulation No. 95 of 2018 (SPBE), Minister of Transportation Regulation No. 134 of 2016, and Minister of Marine Affairs and Fisheries Regulation No. 42 of 2016 (VMS) their implementation in Ambon remains uneven. Most small ports still rely on manual systems for communication and logistics management, with limited digital infrastructure. Furthermore, small-scale fishing vessels under 30 GT are exempt from the VMS requirement, reducing the effectiveness of digital monitoring and protection mechanisms. Physical and digital infrastructure disparities are also apparent. While Ambon's main port maintains official profiles and operational data through the Port Authority (KSOP), smaller ports and local jetties lack standardized data protection protocols or cybersecurity devices. The absence of a regional Cyber Security Plan (CSP) further amplifies these vulnerabilities, leaving navigation and logistics systems susceptible to data manipulation, spoofing, and communication disruptions.

Discussion

The increasing maritime traffic underscores Ambon's role as a regional connectivity hub while simultaneously heightening the urgency of securing its digital infrastructure. Without clear policy standards for protecting critical maritime systems, ports remain highly vulnerable to cyberattacks particularly given the persistence of legacy technologies and the rapid proliferation of the Internet of Things (IoT) (Filitz, 2019). Such vulnerabilities have been vividly illustrated through several global cases. At Antwerp Port, hackers collaborating with a drug-smuggling network successfully infiltrated the terminal operating system, tracked containers carrying narcotics, and removed them while concealing their digital traces. This operation persisted from 2011 to 2013 before being discovered (Jones et al., 2016). Similarly, a cyber incident at San Francisco Port resulted in a virtual displacement of the port's location by approximately twenty miles north, creating navigational disruptions under foggy conditions. These cases demonstrate that cyber intrusions targeting port infrastructure not only enable illicit cargo manipulation but also expose how deeply digital systems can be exploited by increasingly sophisticated cybercriminal networks. Beyond these global examples, Aids to Navigation (AtoN) including both traditional markers such as lighthouses and buoys, and newer virtual AtoN systems integrated through AIS-INS displays represent another area of vulnerability. While virtual AtoN significantly enhances navigational efficiency, the inherent weaknesses of AIS systems render them susceptible to spoofing and other cyber interferences. Consequently, fishing vessels, patrol boats, ports, and navigational support systems face interconnected cyber risks that demand systematic mitigation through regulatory instruments, technical safeguards, and inter-agency collaboration.

The findings indicate that despite the modernization of major fleets and the expansion of port infrastructure, the technological and cybersecurity dimensions of Ambon's maritime sector remain critically underdeveloped. The reliance on basic, unprotected navigation devices exposes small patrol vessels and fishing boats to cyber intrusions that can compromise both navigational safety and operational communication. Moreover, increasing vessel density and expanded port connectivity have intensified the urgency of implementing a comprehensive maritime cybersecurity framework. Without explicit policies to safeguard digital infrastructures, port information systems remain susceptible to manipulation and disruption, as evidenced by international precedents such as the Antwerp and San Francisco incidents (Jones et al., 2016). Maritime security within the fisheries sector is determined not solely by physical and technical vessel conditions but also by the cyber resilience of the digital systems employed onboard. Dependence on unprotected digital navigation systems increases exposure to cyberattacks capable of disrupting economic activities and endangering crew safety. Accordingly, strengthening the fisheries sector in Maluku requires a dual approach: first, improving the technical and operational safety of fishing vessels through consistent regulatory enforcement, routine inspections, and seaworthiness certification; and second, enhancing digital security through crew cybersecurity training, the adoption of protective software, and technological support from governmental and research institutions. Integrating these two dimensions would produce a fisheries management system that is adaptive, sustainable, and resilient to emerging cyber threats, positioning Maluku as both a national fisheries hub and a model for digitally secure maritime resilience within Indonesia's blue economy framework.

Beyond the physical constraints of port infrastructure, digital resilience emerges as another pressing challenge. Although Automatic Identification Systems (AIS) have significantly improved maritime transparency and navigational safety, they are not immune to cyber threats. Global incidents of AIS/GPS spoofing and jamming demonstrate how easily navigational data can be manipulated, creating substantial operational and safety risks for both vessels and port

authorities. This issue is particularly relevant in Ambon, where many smaller ports still lack standardized cybersecurity protocols or advanced digital support infrastructure. Thus, while the implementation of AIS and the digitalization of port data represent meaningful progress, the coexistence of limited physical infrastructure and pervasive cyber risks underscores the need for an integrated strategy encompassing physical modernization, digital infrastructure enhancement, and cybersecurity reinforcement across navigation and port management systems. Furthermore, the findings suggest that the ongoing efforts to strengthen physical maritime infrastructure and modernize fleets have not been paralleled by equivalent advancements in digital security. The unsegmented integration of Information Technology (IT) and Operational Technology (OT) in maritime systems exposes both civilian and state vessels to systemic cyber risks that can compromise navigation, logistics, and national security (Glomsvoll & Bonenberg, 2017). In Ambon's context, where digital literacy and cybersecurity awareness among fishers and local port operators remain low, this vulnerability is particularly acute. The disparity between national legal norms and local-level implementation further emphasizes the need for more operational legal instruments and stronger regional oversight mechanisms.

Institutionally, the gap between policy formulation and field execution highlights the necessity of both vertical integration between national frameworks such as Law No. 32/2014, Presidential Regulation No. 95/2018, and Bakamla/Ministry of Marine Affairs and Fisheries regulations and horizontal coordination among fishers, port managers, patrol officers, and regulators. Effective implementation requires these layers of governance to function cohesively to ensure maritime cybersecurity readiness. (Figure 3) These insights also reinforce the importance of developing an integrated Cyber Security Plan (CSP) aligned with the Port Security Plan (PSP) and Port Facility Security Plan (PFSP). A CSP should encompass both technical measures such as firewalls, intrusion detection systems, and secure communication networks and procedural safeguards, including data protection standards and incident response mechanisms (Androjna et al., 2020). Ultimately, the study concludes that Ambon's success in achieving resilient maritime cybersecurity depends on the synergy between regulatory frameworks, institutional capacity, and human resource development. Only through this integrated approach can Ambon serve as a model for cybersecurity governance in Eastern Indonesia, reinforcing the nation's broader Global Maritime Fulcrum (Poros Maritim Dunia) vision.

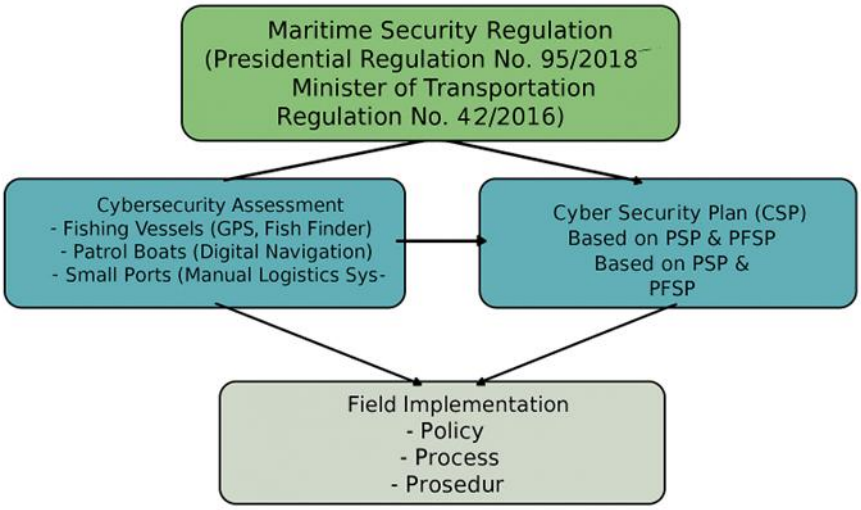

Figure 3. Framework of Cyber Threat Evaluation Results on Maritime Navigation Systems in Ambon

CONCLUSION

This study confirms that cyber threats to maritime navigation systems in Ambon—particularly those used by fishing vessels, patrol boats, and small ports represent a tangible issue requiring urgent mitigation. The analysis identifies three primary factors undermining maritime resilience: technical vulnerabilities in navigation devices, gaps in regulatory implementation, and limited human resource capacity. These conditions not only pose potential risks to navigational safety but may also weaken maritime surveillance functions vital to national defense. Based on these findings, the study proposes several key recommendations. First, there is a need to strengthen technical regulations that are more operational and feasible to implement at the level of fishing vessels and small ports. Second, the government should promote investment in navigation technologies that meet minimum cybersecurity standards, including protection mechanisms against jamming and spoofing. Third, enhancing human resource capacity should be prioritized through digital literacy training for fishermen, port operators, and maritime patrol personnel. Furthermore, cross-sector collaborationmboth among national agencies and with international partners must be reinforced to ensure the establishment of shared standards in safeguarding maritime cybersecurity.

BIBLIOGRAPHY

A. Oppermann (2022). Artificial Intelligence Market Size. DataSeries. https://medium.com/dataseries/artificial-intelligence-market-size-a99e194c184a. Diakses, 18 Sept 2025

Androjna, A., Brcko Satler, T., 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

Bartlett, S., Offermans, G., Shue, C. Enhanced Loran. (2015). A Wide-Area Multi-Application PNT Resiliency Solution. *GPS World* , *26*, 58–64.

Cappelletti, M., & Garth, B. (1978). *Access to justice: A world survey*. Sijthoff and Noordhoff.

Cybersecurity Ventures (2021). Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/. Diakses, 10 Sept 2025.

Cybersecurity Ventures (2025). Cybersecurity Jobs Report: 3.5 Million Unfilled Positions in 2025. https://cybersecurityventures.com/jobs/. Diakses, 15 Sept 2025.

Filitz, J. (2019). Maritime port systems cyber security vulnerability. *NMIO Tech. Bull*, *13*, 22–27.

Fortune, (2024). AI Risks in Fortune 500 Companies Soar 473.5%. https://fortune.com/2024/08/18/ai-risks-fortune-500-companies-generative-artificial-intelligence-annual-reports/. Diakses, 17 Sept 2025.

Glomsvoll, O and Bonenberg, L. (2017). GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea. *J. Navig*, *70*, 33–48.

International Maritime Organization. (2021). *Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.2)*. IMO Publishing.

International Telecommunication Union. (2020). *Global cybersecurity index 2020*. ITU Publications.

Johnson, G., Swaszek, P., Hartnett, R., Shalaev, R., and Wiggins, M. (2007). An Evaluation of eLoran as a Backup to GPS. In Proceedings of the 2007 IEEE Conference on Technologies for Homeland Security, Woburn, MA, USA, 16–17 May 2007; pp. 95–100.

Jones, K., Tam, K., and Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. *Eng. Technol. Ref, 1*

Kapal Pedia (2024). Automatic Identification System (AIS) Dalam Navigasi Kapal. https://kapalpedia.com/automatic-identification-system-ais-dalam-navigasi-kapal/. Diakses, 12 Sept 2025

Keputusan Menteri Kelautan dan Perikanan Republik Indonesia Nomor 91 Tahun 2024 tentang Rencana Kerja Kementerian Kelautan dan Perikanan Tahun 2025.

Mediabrief (2023). Gartner Unveiled Its Cybersecurity Predictions for 2024. https://mediabrief.com/gartner-unveiled-its-cybersecurity-predictions-for-2024/. Diakses, 15 Sept 2025.

Motley Fool (2024). 2 Cybersecurity Stocks (Other Than CrowdStrike) to Buy Hand Over Fist Today.https://www.fool.com/investing/2024/06/12/2-cybersecurity-stocks-crowdstrike-buy-fist-today/. Diakses, 10 Sept 2025.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

Pemerintah Provinsi Maluku. (2024). *Sistem Akuntabilitas Kinerja Instansi Pemerintah (SAKIP): Rencana Strategis (RENSTRA) Provinsi Maluku 2025-2026*. https://malukuprov.go.id/renstra-2025-2026/

Peraturan Kepala Badan Keamanan Laut Republik Indonesia Nomor 1 Tahun 2017 tentang Organisasi dan Tata Kerja Bakamla.

Peraturan Menteri Kelautan dan Perikanan Republik Indonesia Nomor 42 Tahun 2016 tentang Sistem Pemantauan Kapal Perikanan (Vessel Monitoring System/VMS).

Peraturan Menteri Perhubungan Nomor PM 39 Tahun 2020 tentang Penyelenggaraan Telekomunikasi Pelayaran. Jakarta: Kemenhub.

Peraturan Menteri Perhubungan Republik Indonesia Nomor 134 Tahun 2016 tentang Tata Cara Penyusunan dan Pengesahan Rencana Keamanan Pelabuhan dan Fasilitas Pelabuhan.

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 95.

Ridwan, M., & Sudirman, A. (2022). Cybersecurity awareness in Indonesian maritime transportation: Challenges and opportunities. *Journal of Maritime Studies and National Integration, 6*(2), 101–115. https://doi.org/10.14710/jmsni.v6i2.12345

Silgado, D.M. (2018). Cyber-Attacks: A Digital Threat Reality Affecting the Maritime Industry. *World Marit. Univ. Diss*, 9–26.

Soekanto, S. (2008). *Faktor-faktor yang mempengaruhi penegakan hukum*. Rajawali Pers.

The CFO (2025). The AI Cybercrime Wave Has Now Reached 87% of Global Businesses," March 10. https://the-cfo.io/2025/03/10/the-ai-cybercrime-wave-has-now-reached-87-of-global-businesses/. Diakses, 17 Sept 2025.

Undang-Undang Republik Indonesia Nomor 32 Tahun 2014 tentang Kelautan. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 294.