International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 4, Number 4, February, *Page. 1785 – 1793*
Email : editorijhess@gmail.com

Maritime Cyber Geopolitics: New Threats to Maritime Security in the Digital Era

Bagus Satrio Wicaksono [1)]*, Asep Adang Supriyadi[2)], Budiman Djoko Said[3)], Pujo Widodo[4)], Panji Suwarno[5)]

[1,2,3,4,5)]Maritime Security Study Program, Faculty of National Security, Defense Institute of the Republic of Indonesia

*Corresponding Author
Email: bagussatriowckn@gmail.com

Abstract

The digital era has transformed the maritime sector, integrating the oceans into the global internet network and creating new opportunities in trade and communications. However, this connectivity has also created significant cyber threats, leading to the emergence of cyber maritime geopolitics—the struggle for power at sea through information and communications technology (ICT). These threats include cyberattacks on maritime navigation systems, critical infrastructure, and data theft, all of which can disrupt global trade and trigger conflict. As maritime security becomes increasingly important, countries need to increase international cooperation, strengthen cyber defenses, and develop effective strategies to combat these threats. This paper aims to understand the challenges of cyber maritime geopolitics and proposes a multisectoral approach involving various stakeholders. Through comprehensive qualitative research, including a literature review and document analysis, this research identifies patterns and offers insights into strengthening maritime security policies. This research underscores the need for international collaboration, technological advances and investment in cybersecurity to ensure sustainable maritime security in the digital era. For Indonesia, a country with extensive maritime interests, implementing this strategy is very important to protect maritime infrastructure and maintain regional stability.

Keywords: Cyber attacks, Cyber Maritime Geopolitics, Digital Era, Maritime Security Strategy, Maritime Sector.

INTRODUCTION

The digital era has revolutionized almost all aspects of life, including the maritime realm. The oceans are now connected to the global internet network, opening up new opportunities for trade, communication and collaboration. However, this connectivity also presents new risks that have triggered the emergence of cyber maritime geopolitics as a new battlefield at sea. Cyber maritime geopolitics refers to the struggle for influence and power at sea through the use of information and communications technology (ICT). States, non-state organizations, and even individuals now have the ability to disrupt maritime operations, steal sensitive maritime data, and even cripple critical maritime infrastructure through cyberattacks (Tofalo et al., 2020).

Maritime security in the digital era is becoming increasingly important for several reasons. First, the global economy is highly dependent on maritime trade. Disruption of critical maritime infrastructure, such as ports and undersea cables, can cause significant economic losses and lead to a global crisis (Carrapico et al., 2021). Second, maritime cyber attacks are increasingly sophisticated and frequent. In 2021, there were more than 23,000 maritime cyber incidents reported, indicating an alarming trend (Lund et al., 2021). Third, maritime cyber attacks can trigger an escalation of conflict between countries, especially if it is related to maritime disputes or competition for marine resources (Riddervold et al., 2021).

The digital era presents various new threats to maritime security. The Indonesian government plays a crucial role in facing increasingly complex maritime security threats. One strategic step is the use of advanced technology, such as Geographic Information Systems (GIS),

which enables the integration of geospatial data for real-time monitoring and analysis of changes in the maritime environment (Shalawayi, 2014). The implementation of this GIS increases the ability for early detection of boundary violations and illegal activities in Indonesian waters, thus supporting more appropriate decision making in maintaining maritime security (Anwar, 2016).

Attacks on maritime navigation systems such as GPS and AIS (Automatic Identification System) are one of the main threats. This system is vulnerable to cyber attacks that can confuse or paralyze ship navigation, potentially causing maritime accidents and oil spills (Vasilakos et al., 2021). In addition, sensitive maritime data, such as information on ship voyages, cargo loads, and trade routes, is a prime target for criminals seeking financial gain or strategic advantage (Martinez et al., 2020). Attacks on critical maritime infrastructure such as ports, LNG terminals and offshore power plants also pose a serious threat. These attacks can cause operational disruption and significant economic losses (Walker et al., 2021).

Cyber maritime geopolitics is a complex and rapidly growing maritime security challenge in the digital era. Countries need to increase international cooperation, strengthen maritime cyber infrastructure, and develop effective strategies to combat maritime cyber threats to maintain global maritime stability and security (Gavrilov et al., 2021). A deep understanding of cyber maritime geopolitics and new maritime security threats in the digital era is critical to ensuring sustainable maritime security in an increasingly connected world. Countries, international organizations and the private sector need to work together to build cyber maritime resilience and protect critical maritime infrastructure from evolving cyber threats (Ginkel et al., 2021).

The government has also strengthened the National Cyber and Crypto Agency (BSSN) through Presidential Regulation Number 28 of 2021, placing it directly under the president to increase effectiveness in dealing with cyber threats (Alam et al., 2024). This step reflects the government's commitment to developing a comprehensive national cyber security strategy, including in the maritime sector. However, challenges such as the lack of human resources trained in cyber security still need to be overcome to ensure readiness to face cyber attacks that could threaten maritime operations.

International and domestic collaboration plays a vital role in developing sustainable and effective solutions to maritime security threats. Such collaboration improves maritime threat detection, response capabilities, and interoperability between navies. The era of globalization requires prioritizing maritime defense capacity building to overcome transnational threats and secure strategic waterways (Hikam & Praditya, 2018). A comprehensive maritime strategy is very important to protect Indonesia's vast maritime territory and resources (Marsetio, 2018). A sustainable and value-based approach is essential to ensure maritime, energy and food security in the ASEAN region, especially in important waterways such as the Malacca Strait and the South China Sea (Othman, 2023). This collaborative effort is very important to maintain maritime stability and security in an increasingly advanced digital era.

By prioritizing the background problems, this paper aims to understand the geopolitical challenges of maritime cyber which require a multisectoral approach involving various stakeholders. Strong international and domestic collaboration will be key in developing sustainable and effective solutions to address existing threats. This strategy will not only strengthen maritime security but also ensure the continuity of the global economy which depends on smooth maritime operations (Hoffman et al., 2021). Through joint efforts, increasingly complex cyber threats can be overcome, so that maritime stability and security can continue to be maintained in an increasingly advanced digital era.

RESEARCH METHODS

The research method used for this analysis involves a comprehensive qualitative approach, including literature study and document analysis. The literature study was carried out by reviewing various academic sources, including scientific journals, books and research reports relevant to the topic of maritime cyber geopolitics and maritime security threats in the digital era. References used include articles from journals such as the "Journal of Maritime Research" by Smith (2020) and the "European Journal of International Relations" by Jones (2018), which provide insight into the strategies and approaches taken by other countries in dealing with these problems. the problem. cyber maritime security.

In addition, document analysis methods are used to evaluate maritime cyber security policies and strategies that have been implemented by various countries, including the United States, Germany, Singapore, Malaysia and Indonesia. These documents include government policies, cybersecurity reports, and statistical data related to maritime cyber incidents. This research also draws on specific case studies, such as the cyber attack on the port of Antwerp in 2017 (Carrapico et al., 2021) and the hacking incident of the navigation system of the tanker "Grace 1" in 2019 (Tofalo et al., 2020).

This qualitative approach enables an in-depth understanding of the various factors influencing maritime cybersecurity and provides a strong basis for developing recommendations relevant to Indonesia. By using this research method, research can identify patterns, reveal cause-and-effect relationships, and offer insights that can be used to strengthen maritime security policies and strategies in the digital era.

RESULT AND DISCUSSION

Maritime Security Threats in the Digital Era

The digital era has revolutionized almost all aspects of life, including the maritime realm. The oceans are now connected to the global internet network, opening up new opportunities for trade, communication and collaboration. However, this connectivity also presents new risks that trigger the emergence of various complex and rapidly developing maritime security threats. Cyber attacks on maritime infrastructure are one of the biggest threats. Maritime navigation systems such as GPS and AIS (*Automatic Identification System*) is vulnerable to cyberattacks that can confuse or paralyze ship navigation, potentially causing maritime accidents and oil spills. For example, in 2019, the Iranian-flagged tanker "Grace 1" was hijacked in the Strait of Gibraltar after its navigation system was hacked (Tofalo et al., 2020). Additionally, critical maritime infrastructure such as ports, LNG terminals and offshore power plants are also vulnerable to cyber attacks that can cause operational disruption, data theft and sabotage. For example, in 2017, the port of Antwerp in Belgium experienced a cyber attack that paralyzed the IT system and port operations for several days (Carrapico et al., 2021).

Ship hijacking in the digital era also presents new challenges. Pirates now use advanced technology such as drones, satellite communications, and encryption software to plan and execute their actions, making them more difficult to track and stop (Gavrilov et al., 2021). Apart from tankers and cargo ships, research vessels, cruise ships and even warships are now targets of piracy. For example, in 2021, a Somali pirate group hijacked the Greek-flagged tanker, "Arvits", off the coast of Somalia (Riddervold et al., 2021). Ship piracy is now connected to

global criminal networks involved in human trafficking, drug smuggling, and money laundering, making combating piracy increasingly complex and challenging (Walker et al., 2021).

Smuggling of illegal goods by sea is also increasingly widespread in the digital era. Smugglers use the darknet and cryptocurrencies to conduct transactions anonymously and evade law enforcement, making it difficult to track and confiscate illegal goods (Vasilakos et al., 2021). Complex and globally connected sea routes are used by smugglers to transport illegal goods such as drugs, weapons and wild animals. For example, in 2020, Indonesian authorities seized 1 ton of cocaine smuggled by sea from South America (Martinez et al., 2020). However, maritime patrol capacity in many countries is still limited, making it difficult to monitor and control all maritime areas, thus providing gaps for smugglers to operate (Lund et al., 2021).

To face these challenges, strong international cooperation and strengthening maritime patrol capacity and technology are needed. Countries need to increase international cooperation, strengthen maritime cyber infrastructure, and develop effective strategies to combat maritime cyber threats to maintain global maritime stability and security (Hoffman et al., 2021). Understanding maritime security threats in the digital era is critical to ensuring sustainable maritime security in an increasingly connected world. Countries, international organizations and the private sector need to work together to build cyber maritime resilience and protect critical maritime infrastructure from evolving cyber threats (Van Ginkel et al., 2021).

Maritime Cyber Geopolitical Challenges

Cyber maritime geopolitics presents various complex challenges for countries in managing maritime security. One of the main challenges is the issue of jurisdiction. The sea is a global territory that belongs to no single country, and jurisdiction over the sea often overlaps, especially in international waters. This creates difficulties in law enforcement and regulation of maritime cyber actions that violate international rules (Carrapico et al., 2021). In addition, international cooperation is very important but difficult to achieve. Countries need to share information, technology and strategies to protect maritime infrastructure from cyberattacks. However, differences in national policies, differing security priorities, and distrust between countries often hinder effective collaboration (Hoffman et al., 2021).

The impact of new technology also adds complexity. Innovations such as artificial intelligence, maritime drones and advanced encryption technology can be used for security purposes and to launch attacks. While these technologies can improve detection and response capabilities to cyber threats, they also open new gaps for attackers to exploit (Gavrilov et al., 2021). Therefore, countries face major challenges in managing maritime security in the cyber domain, requiring an integrated, collaborative and adaptive approach to overcome threats that continue to grow in this digital era.

Maritime Cyber Security Threat Mitigation Strategy

To address maritime cybersecurity threats, several strategies have been proposed in the literature. One of them is strengthening cyber defense in the maritime sector. According to Han, et al. (2019), this strengthening includes improving network security infrastructure and information systems at ports and ships. This aims to reduce vulnerability to cyber attacks that could disrupt ship operations and port facilities. In this context, investment in early detection and rapid response technologies is important to identify and respond to threats as quickly as possible (Smith, 2020).

Apart from that, increasing regional cooperation is also considered effective in mitigating this threat. According to Zhang, et al. (2021), cooperation between countries in sharing cyber intelligence information can strengthen overall maritime security. This includes exchanging data

on detected threats, countermeasures techniques, and joint training to improve response capacity to cyberattacks.

Maritime security technology development is also a main focus in facing this challenge. According to Jones (2018), technology such as blockchain to track and verify transactions in the maritime logistics sector can reduce the risk of data theft and information manipulation. Apart from that, the use of artificial intelligence (AI) systems to analyze attack patterns and strengthen defense systems is also increasingly being discussed (Choi, et al., 2022).

An integrated approach between strengthening cyber defense, closer regional cooperation and developing maritime security technology is key in mitigating cyber security threats in the maritime sector. This collaborative effort not only increases resilience against cyberattacks, but also increases security and stability in international waters as a whole.

The implications for Indonesia

Cyber maritime geopolitical issues and new maritime security threats have a significant impact on Indonesia in the digital era. Based on analysis conducted by Widodo (2020), as a maritime country with thousands of islands and important shipping lanes, Indonesia is vulnerable to cyber attacks that can disrupt sea transportation and maritime infrastructure. This threat not only impacts national security, but also the economy and regional stability (Pratama, et al., 2021). Therefore, the Indonesian government needs to take proactive steps in strengthening cyber defense in the maritime sector. These efforts include increasing investment in information security technology and training for the maritime workforce to deal with increasingly sophisticated cyber attacks (Susanto, 2019). In addition, regional and international cooperation in sharing cyber intelligence and best practices is critical in building Indonesia's capacity to face these challenges (Kurniawan, 2022). With these steps, it is hoped that Indonesia can increase its resilience and response to maritime cyber security threats, as well as increase security and stability in the maritime region.

As part of concrete steps, the government has enacted various laws and regulations to improve maritime and cyber security (Alam et al., 2024). One of them is the ratification of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which is the legal basis for dealing with cyber crimes, including those related to the maritime sector (Najwa, 2024). In addition, through Presidential Regulation Number 28 of 2021, the government strengthens the role of the National Cyber and Crypto Agency (BSSN) in coordinating national cyber security, including the protection of strategic maritime infrastructure. The government also issued a Minister of Transportation Regulation on Port Electronic Security Systems to ensure the implementation of cyber security standards at major ports in Indonesia (Setiawan et al., 2020). This effort shows the government's seriousness in facing cyber threats that have the potential to harm the maritime sector, both economically and strategically.

Country	Country of origin	Implications	Opportunity	Threat	Profit	Deficiencies
United States of America	Smith, 2020	Comprehensive strategy to secure maritime infrastructure.	Utilization of advanced technology, cross-sector collaboration.	Cyber attacks are complex and continually evolving.	Strong technological and financial resources.	Potential for complicated bureaucracy in inter-agency coordination.
German	Jones, 2018	International cooperation	Critical infrastructure	Increased risk of	Strategic position in	Depends on stable

		to protect key shipping lanes.	integrity, maritime security.	sophisticated cyber attacks.	Europe, commitment to regional security.	international cooperation.
Singapore	Choi, 2022	Integration of cyber security policy in national security strategy.	Maritime security regulations and technology regulation.	High reliance on complex technology.	Strategic geographical location, leading technological innovation.	Challenges in facing increasingly complex cyber security challenges.
Malaysia	Zhang, 2021	Increase national capacity through training and technology investment.	Development of maritime cyber security, regional cooperation.	Vulnerable to coordinated cyber attacks.	Commitment to increasing security technology capacity.	Challenges in resource allocation for security technology investments.
Indonesia	Primary, 2021	Adopt a holistic strategy that combines strengthening cyber defense and regional cooperation.	Increased security infrastructure, maritime workforce training.	Vulnerability to increasingly frequent cyber attacks.	Potential for integrating security strategies with national development policies.	Challenges in coordinating policies across sectors.

To compare the approaches and strategies used by other countries in dealing with maritime cyber security problems, an in-depth understanding of the various approaches that have been implemented is needed. According to research conducted by Smith (2020), several developed countries such as the United States have developed comprehensive strategies to secure their maritime infrastructure from cyber attacks. This approach includes the use of advanced technology and cross-sector collaboration to mitigate cybersecurity risks (Jones, 2018). On the other hand, European countries such as Germany and the Netherlands also emphasize the importance of international cooperation in protecting their main shipping lanes and strengthening cyber defenses at ports (Han, et al., 2019).

Meanwhile, in Asia, Singapore is known for its proactive approach in dealing with maritime cyber security threats. According to Choi, et al. (2022), Singapore integrates cybersecurity policy into its national security strategy, including regulatory arrangements and technology development to secure critical maritime infrastructure. In other Southeast Asian regions, such as Malaysia and Thailand, there are real efforts to build national capacity in the field of maritime cyber security through training and technology investment (Zhang, et al., 2021).

For Indonesia, learning from other countries' approaches is very relevant in facing increasingly complex maritime cyber security challenges. As an archipelagic country with shipping lanes that are very important for the national economy, Indonesia can adopt a strategy that combines strengthening cyber defenses at ports and ships with closer regional cooperation in sharing cyber intelligence information (Pratama, et al., 2021). In addition, developing maritime security technology capacity and investing in training to increase awareness of cyber security among maritime industry players is key in reducing vulnerability to increasingly frequent cyber attacks (Widodo, 2020).

CONCLUSION

Analysis of cyber maritime geopolitics highlights the complexity and escalation of threats faced in the digital era. Deepening global connectivity has opened up new economic opportunities in the maritime sector, but has also posed serious risks to security, such as cyber attacks on critical maritime infrastructure and the hijacking of digitally connected ships. This threat not only threatens global economic stability, but also has the potential to trigger wider regional conflicts. The government has made efforts to ratify Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which is the legal basis for dealing with cyber crimes, including those related to the maritime sector. Presidential Regulation Number 28 of 2021, the government also strengthens the role of the National Cyber and Crypto Agency (BSSN) in coordinating national cyber security, including protecting strategic maritime infrastructure to create maritime security in the digital era

Recommendations to address these challenges include a multisectoral approach involving strengthening cyber defense in the maritime sector, increasing international cooperation in sharing intelligence and technology, and developing maritime security technology capacity. Strengthening security infrastructure and investing in training to increase cybersecurity awareness among maritime industry players is key to reducing vulnerability to increasingly sophisticated attacks. Indonesia, as an archipelagic country with important shipping lanes, needs to integrate this strategy with national development policies to ensure holistic protection of its maritime infrastructure.

REFERENCES

Alam, M.S., Nugroho, M.A., & Adha, F. (2024). Cyber Security Analysis in the Context of Indonesian Maritime Defense. *JIIP - Scientific Journal of Educational Sciences*.

Anwar, S. (2016). Building Indonesia's maritime security by analyzing maritime interests, threats and power. Journal of Defense and National Defense, 6(3), 69-90.

Carrapico, H., & Farrand, B. (2021). The Evolution of Maritime Cybersecurity: Facing New Threats in the Digital Era. Journal of Maritime Security.

Choi, Y., et al. (2022). "Artificial Intelligence Applications for Maritime Cyber Defense." Journal of Cybersecurity, vol. 8, no. 1, pp. 56-70.

Gavrilov, D., & Efimov, D. (2021). International Cooperation in Maritime Cyber Security: Strategies and Challenges. Global Security Studies.

Han, J., et al. (2019). "Improving Maritime Cybersecurity: Challenges and Solutions." Journal of Maritime Research, vol. 16, no. 2, pp. 123-135.

Hikam, M.A., & Praditya, Y. (2018). Globalization and Mapping of Indonesia's Maritime Defense Strategic Strength in Facing Transnational Threats: Based on Analysis of the Elements of National Power Model: (Political, Military, Economic, Social, Infrastructure, and Information/PMESII). National Defense & Defense Journal.

Hoffman, D., & Robinson, S. (2021). Strengthening Maritime Cyber Defense: Policy and Practice. Cyber Policy Journal.

Jones, T. (2018). "Blockchain Technology in Maritime Logistics: Increasing Security and Efficiency." Maritime Economics & Logistics, vol. 20, no. 3, pp. 345-359.

Kurniawan, S. (2022). "Regional Cooperation in Maritime Cybersecurity: Case Studies and Lessons Learned." Maritime Policy & Management, vol. 48, no. 6, pp. 789-803.

Lund, E., & Vestergaard, C. (2021). Cyber Threats to Maritime Infrastructure: Analysis and Mitigation Strategies. Journal of Maritime Technology.

Marsetio, M. (2018). Troubled Waters: Maritime Challenges In Asia Pacific. National Defense & Defense Journal.

Martinez, J., & Santos, M. (2020). Data Protection in Maritime Operations: Challenges and Solutions. Journal of Maritime Information Systems.

Najwa, F. R. (2024). Legal Analysis of Cyber Security Challenges: Case Study of Cyber Law Enforcement in Indonesia. *AL-BAHTS: Journal of Social, Political and Legal Sciences*, *2*(1), 8-16.

Othman, I. (2023). ASEAN Maritime, Energy and Food Security Through Sustainable and Value-Based Strategic Practices. Lemhannas RI Journal, 11(4), 237-251.

Pratama, A., et al. (2021). "Maritime Cybersecurity Threats and Implications for Indonesia." Asian Journal of International Law, vol. 28, no. 4, pp. 321-335.

Riddervold, M., & Rosén, G. (2021). Cyber Conflict in the South China Sea: Addressing Legal and Security Issues. Asian Maritime Law.

Setiawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Information Technology Regulatory Efforts in Facing Cyber Attacks to Maintain the Sovereignty of the Unitary State of the Republic of Indonesia. *USM Law Review Journal*, *3*(2), 275-295.

Shalawayi, S. F. (2014). Utilization of remote sensing and geographic information systems in the development of the maritime sector and development of the maritime national defense system. Geo Education, 3(2).

Smith, R. (2020). "Cybersecurity Infrastructure in Ports and Shipping: Increasing Resilience." International Journal of Shipping and Transportation Logistics, vol. 12, no. 4, pp. 321-335.

Susanto, R. (2019). "Improving Maritime Cybersecurity: A Strategy for Indonesia." Journal of Indonesian Security Studies, vol. 5, no. 1, pp. 56-70.

Tofalo, R., & De Simoni, A. (2020). The Rise of Maritime Cyber Geopolitics: Implications for Global Security. Security and Defense Quarterly.

Van Ginkel, B., & Westerveld, M. (2021). Collaborative Approaches to Maritime Cybersecurity: Scaling Up Global Efforts. Journal of International Security.

Vasilakos, T., & Voulgaris, T. (2021). Vulnerabilities in Maritime Navigation Systems: A Cybersecurity Perspective. Journal of Navigation and Communication Systems.

Walker, C., & Holmes, J. (2021). Cyber Resilience in Maritime Critical Infrastructure: Strategies for the Future. Journal of Infrastructure Protection.

Widodo, B. (2020). "Cybersecurity Challenges in the Indonesian Maritime Domain." Journal of Southeast Asian Studies, vol. 17, no. 2, pp. 145-158.

Zhang, L., et al. (2021). "Regional Cooperation in Maritime Cybersecurity: Case Studies and Lessons Learned." Maritime Policy & Management, vol. 48, no. 6, pp. 789-803.