Cyber Security Policy in Indonesian Shipping Safety

Rizki Desiana* **and Sri Cempaka Prima**
Department of Maritime Security, Faculty of National Security, Indonesia Defense University

DOI: https://doi.org/10.14710/jmsni.v5i2.13673

Abstract

Technological sophistication does not escape cyber threats. The higher the complexity of technology, the more vulnerability to cyber attacks continues to increase. In Indonesia, there are only a few Maritime Cyber Security policies and social security socialisation within government institutions. It needs to become a priority for the government, given the increasing sophistication of technology every year and the growing vulnerability of cyber threats. This study used a qualitative method with a Grounded Theory design, and data collection techniques were literature study and interviews. Cyber regulations in Indonesia are still regulated in the Information Technology and Electronic Law (abbreviated as the ITE Law) or Law number 11 of 2008 and handled by the National Cyber and Crypto Agency. Meanwhile, the regulations related to Maritime Cyber have not given special rules in Indonesia. Several international countries implemented these government policies because they believe in the importance of maritime security. Several international countries have implemented these policies because they believe in the importance of maritime security in cyberspace. This is due to increasingly sophisticated technological developments and the changing times that are increasingly digitising. The Indonesian government must immediately prioritise maritime security issues related to cyber threats in the Indonesian shipping area and establish an institution responsible for cyber problems in Indonesia's maritime space. The existence of rules or policies related to cyber security in the marine space will improve shipping safety and security in Indonesia. In this paper, the author formulates the research problem of how the Indonesian government's policy deals with the threat of Maritime Cyber in the shipping sector in Indonesia.

Received:
June 8, 2022

Revised:
July 5, 2022

Accepted:
July 6, 2022

***Corresponding author:**
rizkidesiana122@gmail.com

Keywords: Threats; Maritime Cyber; Maritime Security; Policy; Shipping Safety.

Introduction

Indonesia is a maritime country known since the Majapahit Kingdom and the Sriwijaya Kingdom. In addition to these two great empires, Indonesia has a maritime history in its heyday, having the largest cabotage fleet in the world. This Jakarta Lloyd ocean fleet is in various world ports (Mangindaan 2011). The sea for Indonesia is a geostrategic centre that has the potential to unite and become a source of conflict between regions or countries. In addition, Indonesia has a strategic location between the intersection of two oceans and two continents, so the Indonesian sea area has become a highly significant sea lane for world trade routes and national and international shipping traffic. It means that Indonesia functions as the global supply chain system with this geographical position (Dahuri 2004).

Shipping safety is a condition manifested from an operation in shipping smoothly, by operating procedures and technical feasibility requirements for facilities and infrastructure and their supports. Meanwhile, shipping security is a condition that exists in the operation of shipping that is free from interference and actions that are against the law (Kadarisman 2017). In-Law No. 17 of 2008 explains that shipping is part of a very strategic sea transportation facility for national insight. It is a vital means

that support the goals of national unity and integrity because it can support and facilitate access to transportation and outreach to one another through waters. International institution regulates the safety policy in shipping or sea transportation, namely the International Maritime Organization (IMO). The global institution is in charge of managing matters concerning the safety of the lives of ship passengers and crew, marine treasures, and environmental sustainability at sea (Kusumaatmadja 2002).

Maritime cyber risk refers to the extent to which a potential circumstance threatens a technological asset. It could result in operational, safety or security-related failures in shipping as a result of information or systems being damaged, lost or compromised (IMO 2017). The increased risk of cyberspace is a consequence of the increased connectivity and dependence on global navigation systems. Cybersecurity refers to the protection of system information (hardware, software and related infrastructure), the data in them, and the services they provide from unauthorised access, damage or misuse (Mraković & Vojinovi 2019).

In shipping, technological systems are used for navigation at sea, such as the Global Positioning System (GPS), AIS (Automatic Identification System), and the Electronic Chart Display and Information System (ECDIS). Electronic Graphics displays and Information systems have significant weaknesses related to cyber security. Each has been identified as potentially vulnerable to attack. Because GPS and electronic graphic display and information systems are often integrated with AIS, and there are currently not enough developments or mechanisms to decrypt or authenticate signals, AIS is considered an easy target for cyberattacks. AIS and GPS have also proven vulnerable to hacking and gaining access to these systems by allowing criminals to disable one or more transit ships with a significant impact on world trade. Because successful cyber attacks on a ship can have many devastating effects; for example, if sophisticated cybercriminals manipulate a ship's online navigation system, the consequences would be disastrous for the crew and the ship's environment. Like AIS and GPS, ECDIS is also known to be vulnerable to exploiting web applications, so a skilled attack can take advantage of the ship's electronic infrastructure.

Some countries issued rules or guidelines regarding maritime cyber security. These countries view that not only maritime ports are suffering from cyber security worldwide, but all existing ships are at risk because of the advanced technology used by critical operating systems without risk management analysis. BIMCO is an international shipping association. To promote its agenda and objectives, the association maintains a close dialogue with governments and diplomatic representatives worldwide, including maritime administrations, regulatory agencies and other stakeholders in the European Union, United States and Asia fields.

In the maritime area, there has been a gradual adoption of technology that supports cyberspace over time, so the industry has been relatively slow in implementing effective risk mitigation and appreciating the extent to which ships and ports need to be guarded so far in dealing with cyberspace. Malicious attacks from maritime systems have come with many vulnerabilities due to not taking the necessary steps for cybersecurity mitigation and preparedness, including poor access control to system communications and employee manipulation (social engineering). The consequences of this type of problem are varied, including extortion, loss or compromise of sensitive business information and opportunistic criminal intrusion of operating system navigation charts.?

Implementing a broad-based security strategy is a formidable task in a fast-paced, multicultural and multilingual environment. Several core issues make security issues for the maritime industry very complicated. The first is the relationship between onboard and terrestrial systems. IMO, an international organisation under the United Nations Convention on the Law of the Sea (UNCLOS), adopts international shipping rules and standards in maritime safety and infence (IMO 2017). UNCLOS is registered on the world's oceans, placing gateways and assigning responsibilities to littoral and non-coastal states. Yet much of the infrastructure that supports land-based communications, this interdependence of land and sea infrastructure will only strengthen over the next decade, either through remotely monitored construction or fully automated unmanned vessels that are extraordinary without human intervention on board.

Second, there are many different classes of ships that all operate in different environments. These ships tend to have other computer systems built into them. This system will vary greatly depending on the class, usage, and working environment. Each ship category, defined by the Calcification Society, has specific requirements for onboard systems. In particular, ships are designed with an operational life of more than 25 years (IMO 2017), and a vessel can be reused several times during its lifetime. So it is not uncommon for these ships to load computer network ships and systems that are outdated and tend to experience cyber attacks. Third, many vessels that usually carry special equipment are not designed with cybersecurity. Some ageing operational technologies on board have proven inherently unreliable and unsafe, such as maritime navigation aids GPS and ECDIS, despite being mandated by IMO and designed according to international standards.

The maritime sector is also essential to global trade and transportation infrastructure. In addition, the sheer number of shipping-based trips that cross national lines creates an attractive geopolitical dimension for maritime cybersecurity due to separate countries and their policies. A policy can affect the country's goals from the economy, the environment, and other considerations. Therefore, maritime transportation as a sector poses a unique cybersecurity problem.

The threat of shipping in Indonesia still does not often happen because most ships In Indonesia still use a manual system. At the same time, some developed countries already have a computerised system on these ships. But this does not rule out the possibility that in the next 5 or 10 years, Indonesia will upgrade its boats to be more digital, as in developed countries in general. Due to the lack of cyber threat cases in the maritime area, the government is still not prioritising cyber threat issues in Indonesian shipping areas. There are no related regulations regarding maritime cyber security. If we look to the future, it is undeniable that Indonesian marines and companies can be exposed to cyber-attacks due to the lack of attention from the government and companies in the shipping sector.

Currently, the rules governing cyber are only in Law Number 11 of 2008 concerning ITE, where the law only discusses cyber issues broadly. The regulations regarding cyber are not explained in maritime areas where vast seas dominate Indonesia compared to land. Cyber attacks can come from the marine industry. Furthermore, Law Number 17 of 2008 Shipping is not explained what if there is a cyber threat in the Indonesian shipping area.

The projected future of shipping, driven by potential cost savings and a better working environment for seafarers, adds further complexity as small crews and autonomous vessels will further complicate the maritime threat landscape and introduce a broader range of possible outcomes and impacts. By examining future and current technologies, the scenarios in the following sections analyse what policy changes could improve cybersecurity against various possible attacks and consequences facing the evolving shipping industry. It focuses primarily on ships because port security is a significant concern but is better understood because of its similarity to existing onshore infrastructure (IMO 2017). In comparison, securing ocean vessels is poorly understood and must be addressed as a potential weak link to ensure global transport infrastructure and those who depend on it.

In Indonesia, the cyber policy was initiated by Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). However, many problems still arise in its implementation, mixing private and public affairs into one regulation. Law Number 17 of 2008 concerning Shipping does not mention cyber security in it, not to mention the overlap with various other regulatory regimes. With this, the Indonesian government does not yet have a policy in cyber security that includes policy principles and legal instruments for institutions that manage and are responsible for and deal with maritime cyber security. There is still a lack of regulations in Indonesia regarding Maritime Cyber Security. IMO Guidelines on Maritime Cyber Risk Management can reduce cyber crime in shipping, improve shipping security standards, and provide input for the Indonesian government in responding to cyber security problems in ministerial regulations and other government regulations. Better cyber security and safety, as well as the existence of a significant policy that is directed, both in the long, medium and short term, to improving shipping security in Indonesia. In maritime cyber security, it is still not handled differently from other crimes; cyber security requires comprehensive thinking to take it. Based on the above issue, the research question of the present article

is on how the Indonesian government policy deals with the threat of Maritime Cyber in the shipping sector in Indonesia.

Method

This study uses research methods with qualitative methods to analyse existing social conditions by explaining fully from the point of view of individual interpretation (Martono 2011). The use of qualitative methods is to seek a deep understanding of a phenomenon, fact or reality. The awareness characterises the qualitative approach that the world with various social problems is real. This research uses Grounded Theory, a method and system, as well as a strategy in research. Grounded theory is said to be the author's strategy in conducting based on the characteristics of the grounded theory, which aims to generate an approach from the data obtained by the author (Creswell 2009).

Maritime Security Theory

The definition and understanding of maritime security have changed quite drastically and have no accurate description; it is highly dependent on the context of the point of view and its use (Bueger 2014). From a military perspective, maritime security has traditionally focused on national security issues to protect the sovereignty of the state's territory from armed attack or other use of force and project the interests of the state elsewhere.

The defence perspective on maritime security was expanded to cover a broader range of threats. The United States is increasingly using the term "maritime security operations" to describe maritime enforcement operations against terrorism and the proliferation of weapons of mass destruction. The American government views naval security with the US National Strategy for Maritime Security.

The creation and maintenance of security at sea are essential in mitigating threats short of war, including piracy, terrorism, weapons proliferation, drug trafficking, and other illicit activities. Countering these irregular and transnational threats protects our homeland, enhances global stability, and secures freedom of navigation for the benefit of all nations. In the context of the American government creating and maintaining a safe sea, conditions are critical to reducing the threat of war, including piracy, terrorism, weapons proliferation, drug trafficking, and other illicit activities. Meanwhile, the International Maritime Organization (IMO), through the Maritime Safety Committee (MSC), states that there is a difference between maritime safety and maritime security. Maritime safety refers to efforts to prevent or minimise accidents at sea that might be caused by ships that are not standardised, ship crews who do not meet the requirements or operator error. In contrast, maritime security protects against actions that violate the rules.

In identifying the concept of maritime security, according to Christian Bueger, three things must be considered, namely (1) 'semiotics', which intends to map different meanings by exploring the relationship between maritime security and other concepts, (2) 'securitisation' framework which provides suggestions for understanding how different threats includes in maritime security, and (3) theory of security practice which aims to understand what actions are taken in the name of maritime security (Bueger 2015).

Barry Buzan explains that security issues result from construction, in line with the constructivist perspective. A topic becomes a security problem because there are actors who state that the issue is an existential threat to an entity. The theory explained by Buzan has three models in examining the cyber sector specifically: Hyper securitisation. This theory describes the threat and danger of securitising a country's network beyond the average level. Because a damaged network will collapse, diverse systems and sectors, such as the financial and military sectors, will be attacked.

Furthermore, Everyday Security Practice safeguards actors. It includes private organisations and businesses, mobilising normal individuals in two ways: securing individual partnerships and compliance in maintaining network security and making hyper security scenarios more plausible by combining familiar threat scenarios and experiences in daily life. Technification uses experts in the cyber technology field who will play a significant role in hyper security.

The development of information and communication technology currently being utilised in various sectors of the strategic environment has led to new products in the dynamics of the strategic environment. All dimensions of the strategic environment have been converted into cyberspace due to the influence of information and communication technology. The existence of cyberspace that is easier to reach and access must be balanced with the ability of the state to control and supervise its movement in the cyber world. Information and communication technology development can become a new means to penetrate, influence and infiltrate various strategic environments in Indonesia. The result of the strategic environment is also influenced by the condition of Indonesia, which is dominated by the sea (Buzan 2007).

Lack of Socialization of Maritime Cyber Security Government Policy on Maritime Cyber Security

Maritime cyber security in Indonesia is still entirely foreign to the public and the government. Even though Indonesia is a country with a reasonably vast sea, cyber threats in the maritime area are still safe, only a few threats occur, and these are not the main focus of handling them. Although cyber threats in Indonesia's naval regions are still relatively safe, the government, private sector and public cannot turn a blind eye to cyber threats in maritime provinces. Several threat events in the international marine area can provide new views or policies in the Indonesian maritime sector. In this study, the researcher interviewed several government agencies and shipping companies to observe the cyber threats in Indonesia, especially in the Indonesian Maritime region.

According to Taufik Wahyu Protomo, the Marine and Coastal Guard Unit (KPLP) of the Ministry of Sea Transportation, The government has not yet engaged in maritime cyber security. In Indonesia's naval area, without realising it, there can be cyber threats that seriously disrupt maritime security in Indonesian territory. Indonesia is a country that has vast seas by becoming an international crossing, but regulations regarding cyber security in Indonesian shipping do not yet exist. According to a source from KPLP, there are cyber attacks in Indonesian shipping areas. However, the government decided not to report the attacks because it is still manageable (Interview with Taufik Wahyu Protomo, February 1, 2021).

The Indonesian Coast Guard (Badan Keamanan Laut Republik Indonesia / Bakamla) as written in Article 3b of Presidential Regulation 178 of 2014 concerning Bakamla. The Directorate of Data and Information (Dit Datin) and the Marine Hazard Information Center (KPIML) have strengthened the information system's security so that the coordination line between Bakamla and the related Ministries/Agencies remains safe. Routinely, Dit Datin and KPIML experiment security of communication and information lines to ensure the proper implementation of the SPD and command-control functions. Dit Datin and KPIML apply Secure Socket Layer (SSL) to ensure system security, install firewalls from the network and application side, use private networks on all servers, and physically secure servers at Bakamla's head office.

In 2020, Bakamla launched the Indonesian Maritime Information Center (IMIC), a mandate of the Law as stipulated in article 63 paragraph 1c of Law Number 32 of 2014 concerning the Ocean, article 4 paragraph 1c of Presidential Regulation 178 of 2014 concerning the Maritime Security Agency. It has also followed up with SKB 8 ministries and institutions on the exchange of data and information in law enforcement at sea.

In essence, this IMIC aims to increase the capacity and capability of law enforcement by supporting valid and credible maritime information, increasing naval awareness and building maritime deterrence in Indonesian waters. IMIC output will include periodic reports in the form of weekly, monthly, and annual reports, as well as naval publications that may be needed in the future and will continue to develop. Furthermore, this product is open to the public, so it can also be used for the benefit of domestic and foreign research institutions and mass media. In 2019, there had a cyber security threat in the Indonesian shipping sector from the side of Seafarers' document compliance, where there had been cases of forgery of seafarers' certificates due to lack of implementation. Legally valid document. In the same year, the Directorate General of Sea

Transportation collaborated with the BSSN to effectively and efficiently strengthen cyber security and protect critical data in all online services and applications used within the Directorate General of Sea Transportation.

Lack of Socialization of Maritime Cyber Security

Both stakeholders and the community frequently discuss maritime threats. But, cyber threats remain a neglected issue. Whereas. It is highly urgent to be addressed by the government because it targets personal, business and state interests. From the results of interviews conducted by researchers regarding maritime cyber threats, they still lack these threats because, in Indonesia's naval area, there are very few cyber threats in the marine area. Unlike the United States, which already has a National Maritime Cyber Security Plan for a National Maritime Security Strategy that integrates cyber security into the principles of freedom of sea strategy, trade facilitation and defence ensure the conductive flow of shipments and facilitate the movement of goods and desired persons crossing borders. Those efforts were undertaken to minimise the threat.

The strategy used by the United States to pool maritime cybersecurity resources, stakeholders, and initiatives to aggressively mitigate current and non-longstanding maritime cyberspace threats and vulnerabilities and complement plans supporting a national maritime security strategy, government actions to close security gaps and vulnerabilities in maritime cyberspace for the next five years. The program will evolve as the public sector, private sector, and international partners develop cooperation and initiatives on marine cybersecurity. According to Ibnu Dwi Chayo, a Cyber Security Researcher, Indonesia is still lagging compared to Malaysia and Singapore; both countries have lacked attention to cybersecurity since 1997 and the 2000s. According to the Global Cyber Security Index, Malaysia and Singapore include the ten countries with the best cyber security in the world. In 2018, Malaysia and Singapore were in the top 10 (Interview with Ibnu Dwi Chayo, December 23, 2020).

In Indonesia at this time, cyber is still a new business; it is still a new thing, so it is not clear who is responsible. So if we can talk about cyber, it is the legal regime. There are three laws apart from the Criminal Code, so that the Criminal Code can be interpreted offline and online. If in those two cyber regimes, 3 ITE Laws were made in 2008 and then revised in 2016. There is Law on protecting personal data, which has not been completed.

Moreover, the Law on Cyber Security Resilience or called the PSC Act; this PSC is crucial because later, it will be clear who is responsible for cyber in Indonesia right now. The responsibility is unclear depending on what happens if the cybercrime belongs to the National Police Headquarters. For example, there will be a hack into the system. Ports of all kinds are the business of the Police. Still, when it reaches the defence of the country, After all, defence is the business of the TNI; At the same time, there is a BSSN; it should be able to act as a security guard and gather information as intelligence in cyberspace.

The government's lack of socialisation of cyber threats, especially in the maritime area with reasonably high users of marine services. President Joko Widodo, at the High-Level Conference (KTT) 9th East Asia Summit (EAS) on November 13, 2014, in Nay Pyi taw, Myanmar, emphasised the concept of Indonesia as the World Maritime Axis to make Indonesia a large, strong, and prosperous maritime country through the restoration of identity Indonesia as a maritime nation, safeguarding maritime naval interests and security, and empowering marine potential to realise Indonesia's economic equality (Masitoh 2018; Sambhi 2015). Consequently, the government must further enhance maritime security in the cyber field with technological sophistication in the future; Indonesia can prevent or anticipate cyber threats in the marine area.

Shipping Companies' Responses to Cyber Threats

No company or ship operating wholly or partially online is immune to cyber threats. Many factors hamper business digitisation. Many factors impede business digitisation. The most significant danger is security vulnerabilities, particularly cybersecurity. In the end, cyber incidents are the second most

important risk in running a company. Maritime cyber risk refers to the extent to which a technological asset is threatened by a potential circumstance or event, resulting in a shipping-related operational, safety or security failure due to information or systems being damaged, lost or compromised.

Cybersecurity is not only about preventing hackers from accessing systems and information but also about protecting digital assets and data, ensuring business continuity, and securing the maritime industry from external and internal threats. It is essential to keep ship systems safe from physical attack and ensure the integrity of support systems. The complexity associated with ships and tankers makes them vulnerable to high-impact attacks. Cyber incidents can last for hours, days, or weeks. When one vessel is affected by malware, it can spread malware to similar ships through the company network.

According to the Indonesian Classification Bureau, a national agency assigned by the Indonesian government to classify Indonesian-flagged commercial vessels, they have issued circulars in the form of derivatives of the IMO Guidelines. Speaking of Indonesian flagships, they will see that SE 35 of 2020 is in a place where in principle, its implementation is to follow the IMO guidelines that BKI submitted on July 30, 2019. The Circular Letter Number 35 of 2020, issued by the Director-General of Sea Transportation, previously Biro Klasifikasi Indonesia (BKI), has given the provisions of MSC-FAL.1/Circ.3 listed in TI Number 185 of 2019, which is to remind ship owners to ensure compliance with Maritime Cyber Risk Management available in the manual SMS before the first annual Document of (DOC) audit after January 1, 2021.

In principle, BKI conducts a risk assessment to "identify" needs and changes the Ship ISM Manual procedures. BKI will audit BKI vessels that have implemented the ISM Code because these rules are in the corridor of complying with the ISM Code. BKI performs classification according to the construction of the ship's hull and the ship's machinery and electrical system. The navigation tools and others are a statutory authority that will follow national and international regulations depending on the ship's designation plan (Interview with Dr Ir. Rudiyanto, December 08, 2020).

In contrast to the shipping company in Indonesia, in this case, the PT Pelni shipping system has not used digitalisation but a manual or analogue system. Also, they have not yet explored the rules issued by IMO regarding the Maritime Cyber Risk Management Guidelines. It is worrying, considering that PT Pelni is a large shipping company in Indonesia and carries out international shipping. With the development of the technology system, PT Pelni should be able to use the digitisation system in its shipping system, of course, with a security system that must also be strengthened (Interview with Mr Amin, January 07, 2021).

Indonesia Government Policies in Facing Cyber Maritime Threats in the Shipping Indonesia Sector

By facing future changes, shipping or transportation has strong potential to be developed, given the characteristics of being able to carry out mass assembly in Indonesia. Thus, the safety and security system is a critical factor that must be considered as a basis and benchmark for decision-making to determine the feasibility and safety of shipping. From these two aspects, it can be seen that in terms of facilities in the form of ships and infrastructure such as navigation systems and Human Resources (HR) involved in it. So with the security policy in shipping or sea transportation, he is also toured by international institutions.

With the increasing sophistication of global cyber attacks and the digitisation of shipping, maritime cybersecurity regulatory issues require immediate attention. One part of this process involves establishing appropriate conventions and applicable principles. Therefore, establishing solid and resilient maritime cybersecurity regulations must be carried out through international collaboration and in a manner that respects regional needs and shared economic interdependencies.

The impact of threats to security as a catalyst for creating and implementing a security regulatory architecture is not a new concept in the maritime space. Points out that threats such as piracy have acted as vehicles to accelerate global collective production, enhance naval security relations, and subsequently create security communities (Bueger 2015).

Shipping Company Responses to Cyber Threats

The Indonesian shipping company, in this case, PT Pelni, is a shipping company in Indonesia that does not have rules related to cyber security in their shipping system because they still use manual methods in the shipping system they use. in terms of regulations, they submit everything to the existing regulators, and they only carry out the rules that the regulator issues. According to them, every incident that occurred on the voyage was the negligence of the crew, not a cyber attack that hacked into their shipping system because they were still using the manual method.

Information technology systems, also known as enterprise systems, support organisations with data processing, communication and storage services. Enterprise systems are designed to achieve efficient digitisation of information services. Attacks against such systems aim to disrupt the company's activities. Still, they can potentially result in the theft of information which is far more damaging in terms of services and organisational goals. Therefore, the risk posed by such an attack is low to medium. Company data, operations, and procedural aspects can be potentially breached with little or no physical harm or loss of life.

Connectivity and reliance on the internet are now the norms. With many technologies critical to the operation and management of ships, these systems' security, safety and reliability are paramount. Therefore, the Indonesian maritime industry needs cyber security monitoring to ensure effective management and mitigation of emerging cyber threats.

Conclusion

Maritime cyber security in the Indonesian region is still not a priority among the government and companies that use shipping services. This is very different from other countries that are very concerned about their maritime cyber security. These countries believe in the importance of maritime security in the cyber field due to increasingly sophisticated technological developments and an increasingly digitalised era; increasingly sophisticated actions cannot ignore this in contrast to Indonesia, which still has not prioritised maritime security in the cyber sector. in the absence of rules related to maritime security in the cyber industry and security that is socialised to sea users to avoid cyber threats. The Indonesian shipping company has not passed the system issued by IMO, and there are still many shipping companies in Indonesia that have not been digitised, so they feel they have not it's time to follow the rules issued by IMO. They still feel safe from cyber threats. The shipping company is further upgrading the shipping system and standardisation while still strengthening its security system so that it is far from cyber-attacks; Indonesian companies can follow the rules issued by IMO in cyber security so that the shipping and shipping system can run smoothly and without interference from cybersecurity breaches.

References

Bueger, C. 2015. "What is Maritime Security?" *Marine Policy* 53: 159-164.

Buzan, Barry. 2007. "What is National Security in the Age of Globalization?" Refleks, Department of Foreign Affairs, Oslo, http://www.regjeringen.no/nb/dep/ud/ kampanjer/refleks/innspill/ sikkerhet/buzan.html?id=493187. Accessed August 21, 2021.

Creswell, John W. 2009. *Research Design: Qualitative*, *Quantitative, and Mixed Methods Approach 3rd Edition*. USA: Sage Publications Inc.

Dahuri, R., Rais, J., Ginting, S. P., & Sitepu, M. J. 2004. "Integrated management of coastal and marine resources. Fourth Printing." https://www.crc.uri.edu/download/2000_Dahuri_CP_ Integrated_Coastal_Marine.pdf. Accessed September 20, 2021.

International Maritime Organization (IMO). 2017. "Guidelines on Cyber Risk Management." MSC-FAL.1/Circ.3 5 July.

Kadarisman, M. 2017. "Kebijakan Keselamatan dan Keamanan Maritim dalam Menunjang Sistem Transportasi Laut." *Jurnal Manajemen & Transportasi Logistik* 4, no. 2: 177-192.

Kusumaatmadja, Mochtar. 2002. *Protection and Preservation of the Marine Environment, Seen from the Point of International and National Law*. Jakarta: the Archipelago Insight Study Center in collaboration with Sinar Graphic Publishers.

Mangindaan, Robert. "Indonesia and Maritime Security: What Is Its Importance?" http://www.fkpmaritim.org/indonesia-dan-keamanan-maritim-apa-arti-pentingnya/. Accessed May 8, 2020.

Martono, H.K. 2011. *Transportasi di Perairan Berdasarkan Undang-Undang Nomor 17 Tahun 2008.* Jakarta: Rajawali Press.

Mraković, I. and Vojinović, R. 2019. "Maritime Cyber Security Analysis-How to Reduce Threats?" *Transactions on Maritime Science* 8, no. 1: 132-139. DOI: 10.7225/toms.v08.n01.013.

Sambhi, Natalie. 2015. "Jokowi's 'Global Maritime Axis': Smooth Sailing or Rocky Seas Ahead?" *Security Challenges* 11, no. 2: 39–56. http://www.jstor.org/stable/26465437