JWP (Jurnal Wacana Politik)
ISSN 2502 - 9185 : E-ISSN: 2549-2969
Vol. 10, No. 2, May 2025: 239 - 245

CYBERSECURITY CHALLENGES IN THE MALACCA STRAITS: INDONESIA'S STRATEGIC APPROACH THROUGH BSSN AND IMIC

Robby Rizaldy, Satriya Wibawa and Arfin Sudirman
Department Internationa Relation, Padjadjaran University, Bandung,
E-mail: robby22001@unpad.ac.id; arfin.sudirman@unpad.ac.id; satriya.wibawa@unpad.ac.id

ABSTRACT. The government's attention is anticipated to be directed towards the proper management of maritime cybersecurity in the Malacca Strait, given the intricate nature of the dangers involved. This will assist Indonesia's objectives as a Global Maritime Axis. Indonesia has created institutional synergies through BSSN and BAKAMLA to ensure that daily operations in this area are at the forefront of minimizing maritime cybersecurity threats. Using theories of cybersecurity, maritime security, and security cooperation, this article aims to understand the cooperation between these institutions, namely BSSN through BDS and BAKAMLA with IMIC, in the field of maritime security, including the mitigation of maritime cybersecurity threats that jeopardize national sovereignty. The essay uses a descriptive qualitative method to show how Indonesia is working hard to merge these two agencies so they can better address maritime cybersecurity in Indonesian waters and this paper was validated by interviewing several actors or strategic position holders in IMIC and BSSN who play a direct role in the technical field. This involves working together to address marine cybersecurity concerns in the "Nusantara Jaya," or Malacca Strait. Though decisions from the Indonesian House of Representatives (DPR RI) are still pending, in practice, collaboration between these government entities is dependent on the legal frameworks provided by Indonesian laws and regulations controlling marine security, safety, and law enforcement. After these frameworks are put into effect, it is envisaged that they will make maritime management and operations clearer and avoid redundancies between the pertinent agencies.

Keywords: Journal; Cybersecurity; Maritime Security; Cooperative Security; Indonesia Maritime Information Center.

INTRODUCTION

Indonesia is one of the world's most maritime nations, with a coastline that stretches 95,181 kilometers and a maritime area that covers 3.25 million square kilometers, or almost 63 percent of its entire land. Indonesia, which is made up of over 7,000 islands, is 5,120 kilometers long and lies between the Pacific and Indian oceans. Indonesia boasts the longest coastline in Southeast Asia and is the 15th largest country in the world by area thanks to its vast marine domain (PUSHIDROSAL, 2018). Based on the most recent data available, the Indonesian Internet Service Providers Association (APJII) projects that out of 278,696,200 people who will be alive in 2023, 221,563,479 will be internet users in Indonesia. According to the APJII 2024 Internet penetration report, Indonesia has a 79.5% internet penetration rate. Indonesia is ranked seventh in Southeast Asia for internet penetration, according to data from Internet World Stats. The percentage of the population using the internet in the nation as of July 2022 was 76.3%. In light of these circumstances, Indonesia has a noticeably high demand for information and awareness regarding technology, particularly internet usage. Due to the nation's geographical dispersion among islands, it is essential to have access to quick and reasonably priced internet and communication services.

The present global shift to the digital era has made information access easier than ever before, making quick fixes necessary because information technology is developing so quickly. Additionally, cultural lifestyles that require ease and speed in carrying out tasks have been met by technological advancements. The fact that information is now used for employment, education, pleasure, and other purposes makes sense since it has become an indispensable part of daily life. Multiple approaches are used to gather different sorts of data, which are then assembled to create information. Drawing on Ralston and Reilly, Safrudin Chamidi defines information as facts and data derived from natural phenomenon observations that are presented in written or graphical form and have a particular value (Chamidi, 2004).

The idea that combat will undergo significant and lasting changes has been reinforced by the development of information. "Cyber Warfare," "Information Warfare," "Network-Centric Warfare," "Information Operations," and "Command and Control Warfare" are some of the new terms used to describe conflicts (Borden, 1999). The use of information systems, such as computers, communication networks, and databases, typically for military objectives, is referred to as "information warfare"(Proborini, 2016). Information warfare is a type of warfare that emphasizes command and control over information while avoiding the use of force.

DOI: https://doi.org/10.24198/jwp.v10i2.57343
Submited: 16 September 2024, Accepted: 28 January 2025, Publish: 02 May 2025

The deployment of informational technology tools like viruses, worms, and electromagnetic waves—which harm opposing information infrastructure, disrupt adversary information systems, and transmit false information—is likewise fueled by the ongoing growth of technology (Lewis, 2021). As a result, information has emerged as a critical component that needs to be independently handled to promote national security and thwart these kinds of emerging warfare.

The Republic of Indonesia Number 53 of the 2017 Presidential Regulation demanded the National Cyber and Crypto Agency (BSSN) be established. Implementing national cybersecurity policies is a major responsibility of BSSN, which reports directly to the President. Along with safeguarding Indonesia's land, air, and space domains, one of its duties is to secure marine cybersecurity. The goal of BSSN is to monitor, oversee, and coordinate initiatives aimed at enhancing cybersecurity in Indonesian government organizations as well as the business sector (*TENTANG BSSN*, 2021). The organization seeks to locate and safeguard vital infrastructure that is susceptible to cyberattacks, such as marine infrastructure that is essential to the safety and efficient operation of Indonesian waterways.

Due to Indonesia's critical need for cybersecurity, several government agencies, including the National Police (POLRI), the Indonesian Armed Forces (TNI), and other ministries, have established dedicated teams to handle cyber threats. Admiral TNI Aan Kurnia, the Head of Bakamla, officially opened the Indonesia Maritime Information Centre (IMIC) on July 22, 2020, to enhance maritime sector security and mitigate threats. The IMIC was established by Indonesia through the Maritime Security Agency (Bakamla) (Lubabah, 2020). A joint decree from eight ministries and agencies concerning data and information exchange for maritime law enforcement follows the establishment of IMIC, which not only addresses information warfare but also embodies Article 63, Paragraph (1), Letter c of Law No. 32 of 2014 concerning Maritime Affairs, and Presidential Regulation No. 178 of 2014 on the Establishment of the Maritime Security Agency. To support the interests of the Indonesian government and the public, IMIC is tasked with creating periodic reports, such as weekly, monthly, and annual reports, as well as maritime publications that will probably be important in the future and will continue to be developed.

Since they are leading the Indonesian government's efforts to defend the country's sovereignty from cyber threats in the maritime domain, BSSN and BAKAMLA are expected to work closely together and coordinate at a high level. One of Indonesia's biggest maritime logistics operators, for example, claimed in March 2024 that a hacking group had gained access to its cargo database, possibly exposing private data about shipments and clients (Source: The Jakarta Post, "Major Maritime Logistics Operator Suffers Data Breach," March 22, 2024). In July 2023, a ransomware attack caused disruptions to the container management system at Tanjung Priok Port, resulting in several days of delays in cargo handling and logistics distribution (Affairs, 2013).

The economic security and sovereignty of Indonesia are at risk due to these occurrences. Concerns over the duties of BSSN and KOMINFO have been raised by recent occurrences, such as the cyberattack on the National Data Center (PDNS), which also influenced several government organizations and the state of the national economy. In the first quarter of 2024, there were 61 digital security incidents in Indonesia, according to data from the Southeast Asia Freedom of Expression Network (SAFEnet). The breakdown shows that there were nearly twice as many incidents in January 2024—13 in January, 20 in February, and 27 in March—than there were in the same time the year before. These incidents show how urgent it is to treat cybersecurity as a danger, and they also show how crucial it is for agencies to work together and coordinate—BAKAMLA through IMIC and BSSN, in particular—to protect Indonesia's maritime sovereignty.

This essay presents a fresh perspective on maritime cyber security issues by examining the roles and ideas of institutions such as BSSN and IMIC. It focuses on maritime cyber security in Indonesia, particularly in the Malacca Strait. This approach contrasts with previous works, such as those by Khanisa (Khanisa, 2022), which are limited to ASEAN and general maritime security topics, as well as writings from NEO (Neo, 2021) that discuss potential cyber security threats in the Malacca Strait.

This essay discusses the challenges of maritime cybersecurity in the Malacca Strait, focusing on Indonesia's strategic approach through the collaboration between BSSN (Badan Siber dan Sandi Negara) and IMIC (Indonesian Maritime Information Center). Unlike previous writings that only addressed cybersecurity in Indonesia, this essay explores the inter-agency strategies of BSSN and IMIC aimed at maintaining maritime cybersecurity, particularly in the Malacca Strait.

METHOD

This research employs a qualitative method. The data collection technique utilized is a Literature Review, which involves gathering relevant information from books, journals, and online articles, as well as information from mass media sources such as interviews conducted by newspapers or magazines with relevant stakeholders (BSSN, BAKAMLA, Indonesian Government).

Data collection related to maritime cyber security in the Malacca Strait that occurred in recent times, this condition is very important because it involves several important actors such as BSSN and IMIC which have a direct effect on Indonesia's national security so the author feels it is important to conduct a literature study accessed through the internet and previous literature research. This triangulation involves comparing observational results with interviews of relevant parties, contrasting public opinions with personal viewpoints, and examining the perspectives of various experts to achieve comprehensive and credible outcomes. including preventing threats to the marine industry and taking appropriate action in the event of an attack.

RESULT AND DISCUSSION

The Urgency of Maritime Security

Defense and military issues are directly related to national security. Non-military security risks, on the other hand, have become more prevalent in recent years. These threats can affect human security and include those about health, the economy, natural disasters, and international concerns.

Since maritime areas have weaker security standards than terrestrial and aerial domains, they are particularly vulnerable to transnational crimes. As a result, maritime security has gained prominence in many countries today. Maritime channels are used for the majority of international trade. International vessels navigate maritime areas daily. Because of this circumstance, countries are concentrating more of their national security efforts on maritime security. Maritime security includes border security, which is a critical point of entry for transnational crime into a nation, in addition to cargo and port security.

Threats from maritime regions can affect other nations as well, thus responding to them will require cooperation. To protect sea lanes, facilitate and secure the daily global trade that takes place in maritime areas, and ensure the security of maritime activities, such as passenger transport (both legal and illegal) and the fight against illegal, unreported, and unregulated (IUU) fishing, these collective efforts involve maritime security cooperation. One type of cooperative effort to address threats to marine security is the United Nations Convention on the Law of the Sea (UNCLOS).

The UN Convention on the Law of the Sea, or UNCLOS, provides the legal foundation for ocean governance and is regarded as the global maritime constitution. Exclusive economic zones (EEZs), the continental shelf, and the partition of territorial waters are all included. In addition, UNCLOS provides a resource for maritime conflicts, especially those involving territorial issues. The International Maritime Organization (IMO) Convention exists in addition to UNCLOS. The IMO promotes the creation of new initiatives to improve maritime security and safety, while UNCLOS provides the legal foundation for maritime law. These include the International Convention for the Safety of Life at Sea (SOLAS) 1974 and its 2002 and 2005 protocols, which deal with ship and port security, as well as the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) 1988. The International Maritime Organization (IMO) is an organization that focuses on maritime safety and mandates that ships operate by international norms. The security of maritime traffic, including commercial ships, shipbuilding, freight, radio communications, and navigation, is particularly covered by SOLAS 1974. To aid in the advancement of marine legal concerns, the UN established The United Nations Open-ended Informal Consultative Process on Oceans and the Law of the Sea in 1999. The UN started focusing on marine safety and security around 2008.

Maritime Security Indonesia

Indonesia is the largest archipelagic country in the world, with two-thirds of its territory consisting of vast oceans.

Consequently, the potential of its marine economy can be developed for the nation's advancement, encompassing sectors such as fish farming, fisheries processing industries, biotechnology and marine industries, energy, and mineral resources, marine tourism, maritime transportation, maritime industries and services, as well as other non-conventional marine resources.

However, Indonesian waters have been dubbed "the most dangerous waters" due to the prevalence of maritime security crimes such as sea robbery and piracy, illegal fishing, territorial violations, separatist movements, terrorism threats, and various other transnational crimes (Dewan Kelautan Indonesia,

2010). In March 2024, a hacker group claimed to have accessed the cargo database of one of Indonesia's largest maritime logistics operators. Sensitive information related to shipments and customers was potentially leaked, and in the same month, the container management system at Tanjung Priok Port was reported to have been disrupted by a ransomware attack. This attack caused delays in loading and unloading processes and logistics distribution for several days.

These are real incidents experienced by the Indonesian government concerning cybersecurity threats in the maritime sector. In his journal article "Concepts of Maritime Security Paper Centre for Strategic Studies: New Zealand. Centre for Strategic Studies New Zealand Discussion Paper: Victoria University of Wellington, June 2009," Rahman defined maritime cybersecurity (Rahman, 2009) the measures or actions taken to prevent, detect, respond to, and recover from cyber threats that could affect the safety, security, and operation of ships and maritime facilities. It also includes the protection of user and organizational assets against security risks in the cyber environment. The government is also working to raise public awareness to collectively recognize the potential in maritime areas and protect them through the development of communication networks with relevant agencies and social approaches to coastal communities. Internationally, Indonesia collaborates with countries and international organizations to safeguard international waterways that facilitate the daily mobility of goods and services. Indonesia's interests in the maritime domain are evident from the contribution of the marine sector to the national economy, which serves as a backbone for the nation's economy. One tangible manifestation of Indonesia's attention to its maritime domain is the establishment of the ASEAN Maritime Forum, which addresses issues of navigation safety, search and rescue (SAR), and marine pollution. Indonesia has also entered into bilateral MOUs with Singapore and Australia regarding maritime security. Maritime security in the Southeast Asian region is Indonesia's responsibility, given that two-thirds of its waters fall under Indonesian jurisdiction (Desiana & Prima, 2022).

National maritime security tends to be dynamic over time due to violations and/or criminal activities in and through the sea, such as illegal, unreported, and unregulated (IUU) fishing, fuel smuggling, piracy, hijacking, smuggling (of humans, weapons, and narcotics), cybercrime, illegal entry, destruction of marine cultural heritage, and other transnational crimes. These issues remain a priority for law enforcement and authorities in Indonesian waters, to achieve national maritime security stability, necessitating cooperative efforts and synergies in the field of maritime security (Susanto, & Munaf, 2015).

Indonesia's National Interests and Their Relation to Maritime Security

Given its strategic location as the world's largest archipelagic nation, Indonesia's national interests are intimately linked to maritime security. Protecting the country's sovereignty, territorial integrity, and economic success all depend heavily on maritime security. According to Marsetio (2018), who wrote the book "Managing Indonesia's Maritime Potential": "Maritime security is not only about protecting territorial waters but also about ensuring the sustainability of marine resources, safeguarding trade routes, and ensuring the well-being of coastal communities."

Territorial integrity and sovereignty are two of the most important elements of Indonesia's national interests in the maritime environment. "The development of the maritime economy is one of the national development priorities to realize Indonesia as the world's maritime axis" (Source: Bappenas, RPJMN 2020-2024) is what the Indonesian government has included to support this in the National Medium-Term Development Plan (RPJMN) 2020–2024. This demonstrates the government's determination to reinforce Indonesia's role as the world's maritime axis. Meanwhile, international maritime law expert Prof. Dr. Hasjim Djalal emphasizes the importance of regional stability in achieving Indonesia's national interests, saying that "Indonesia's maritime security has direct implications for the stability of Southeast Asia and Indo-Pacific regions" (Djalal, 2023). Stated differently, Indonesia is presently seen as one of the major players on the international scene, supporting the government's endeavor to establish Indonesia as the world's maritime axis.

Indonesia has taken strategic actions to achieve these national goals, such as bolstering its naval fleet, improving its ability for surveillance, and promoting international collaboration. In his book "Maritime Security: An Introduction" (2008), Michael McNicholas claims that maintaining maritime security entails dealing with matters like port security, ship security, technological breakthroughs, and information technology that are closely tied to a country's national interests. Modern threats to national interests frequently cross international borders and cannot be handled by one nation acting alone, which makes security cooperation such as that exemplified by the MOU with Singapore essential.

A New Memorandum of Understanding (MoU) on Maritime Security Cooperation between Indonesia and Singapore was signed in 2023. "This Memorandum of Understanding strengthens the commitment of both countries to maintain stability and maritime security in the region, including addressing transnational crimes and protecting the marine environment," said Retno Marsudi, Indonesia's foreign minister (Source: Indonesian Ministry of Foreign Affairs, Press Release, 2023). Singapore and Australia have signed bilateral cooperation agreements to adopt cooperative security methods, similar to Indonesia, realizing their limited ability to handle regional concerns.

The Roles of BSSN and BAKAMLA in Maritime Security Collaboration

The Indonesian Navy (TNI AL), the National Police (POLRI Air), Immigration (border areas), BASARNAS, LAPAN, and other military and non-military organizations work along with BAKAMLA, a non-ministerial government entity, which is in charge of maritime security and safety activities. The main tasks carried out by BAKAMLA and associated organizations include law enforcement, monitoring, controlling, and surveillance. In the book "Command and Control of Maritime Security and Safety: Based on an Early Warning System" (Susanto, & Munaf, 2015), BAKAMLA highlights maritime security as a major security concern associated with the maritime areas' growing strategic role as the primary conduit for international economic exchanges between nations.

The security of Indonesia's vital maritime infrastructure is aided by the work of the BSSN (National Cyber and Crypto Agency). As per the National Cyber and Crypto Agency Presidential Regulation No. 28 of 2021, "BSSN is tasked with implementing cybersecurity and cryptography at the national level" (Article 2). The National Cyber Security Operation Center (NCSOC), housed inside BSSN, keeps an eye out for cyber threats to important national infrastructure, including the maritime industry. As stated in the BSSN Annual Report 2023, "NCSOC has successfully detected and mitigated over 1000 cyberattacks targeting national maritime infrastructure, demonstrating the importance of cybersecurity in maintaining Indonesia's maritime sovereignty". To achieve national security and sovereignty, these two government institutions work in tandem with one another and have different roles to play. Indonesia's national interests at sea depend on stable maritime security, which affects both national security and prosperity. For the information systems and networks that support marine operations to remain secure, risks to maritime security, particularly maritime cybersecurity, must be addressed.

According to recent analyses, the Malacca Strait region faces the following maritime cyber threat characteristics: disruption of digital logistics supply chains, manipulation of Automatically Identification System (AIS) information, attacks on port infrastructure, and hacking of ship navigation systems (Neo, 2021). Presidential Regulation No. 53/2017 created BSSN as the government organization in charge of national cyber security. While IMIC is a strategic maritime information center created to: Monitor maritime activities, Integrate data across agencies, and Develop Cyber Security Capabilities, its responsibilities include Coordinating National Cyber Defense and Mitigating Strategic Cyberthreats (*TENTANG BSSN*, 2021).

The following measures support maritime regional security: 1. cross-agency collaboration, hybrid threat risk assessments, and real-time monitoring systems. 2. Automatic Identification System (AIS) Data Manipulation AIS is a crucial system for tracking movements, identifying ships, and preventing collisions. Disguising a vessel's identity, deleting a vessel from radar, or supplying inaccurate information that could interfere with marine logistics activities are all examples of AIS data manipulation. 3. Port Infrastructure Attacks Port infrastructure that is digitally integrated is susceptible to cyberattacks. Shipping delays, the loss of important data, or even the cessation of port operations are all possible outcomes of these attacks. 4. Disruption of the Digital Logistics Supply Chain Attacks on the supply chain can significantly affect the distribution of commodities, operational effectiveness, and the state of the global economy as the maritime logistics industry becomes increasingly digitalized.

Presidential Regulation No. 53/2017 created the National Cyber and Crypto Agency (BSSN), whose major duty is to oversee and preserve national cyber security. Among the strategic roles of BSSN are: 1. National Cyber Defense Coordination In order to address strategic and multifaceted threats, BSSN is entrusted with coordinating cyber security initiatives from multiple industries. 2. Mitigation of Strategic Cyberthreats As a recognized organization, BSSN detects, evaluates, and eliminates cyber threats that could jeopardize national security. 3. Development of Cybersecurity Capabilities In addition to developing national cyber talent through certification, training, and fortifying technical infrastructure, BSSN keeps advancing technological capabilities (*TENTANG BSSN*, 2021).

To aid in the strategic management of maritime security, the Indonesian Maritime Information Centre (IMIC) was established. Among the IMIC's significant responsibilities are: 1. Keeping an eye on maritime operations IMIC keeps an eye on maritime operations in real-time to identify possible dangers, such as cyberattacks. 2. Integrating Cross-Agency Data To increase productivity and danger response, IMIC acts as a hub for data integration from multiple relevant organizations, including shipping corporations, ports, and navies. 3. Support for Maritime Area Security · A real-time monitoring system is one way that IMIC contributes to marine area security. · Evaluation of the risks associated with hybrid threats, which combine cyber and physical threats. o Coordinating across agencies to address dangers. (IMIC, 2024).

Indonesia, the world's largest archipelagic nation, considers maritime security to be crucial. Interagency cooperation is essential to improving marine security and monitoring. The requirement to integrate signal detection capabilities with marine information systems leads to collaboration efforts between the Indonesia Marine Information Center (IMIC), overseen by BAKAMLA, and the Signal Detection Center (BDS) under BSSN. "The integration of BSSN's signal detection capabilities with BAKAMLA's maritime information system will enhance the effectiveness of Indonesia's maritime surveillance and security," states Vice Admiral TNI Aan Kurnia, Head of BAKAMLA.

The sharing of data and information is one of the primary components of this partnership. Data on signal detection that can be included in the IMIC system is provided by BSSN via BDS. "We are committed to sharing relevant signal detection data to strengthen IMIC's analytical capabilities in identifying maritime threats," said Dr. Hinsa Siburian, Head of BSSN in the Annual Report, 2024. The two organizations work together on technology development as well. One of the project's key initiatives is an artificial intelligence-based early detection system to spot illicit activity at sea. According to Dr. Dicky R. Munaf, Head of IMIC, "this project combines BSSN's expertise in signal analysis with BAKAMLA's experience in maritime operations" (Sugiharto & Shafwatullah, 2021). By cooperative operations, this collaboration is also made possible. An international smuggling network was successfully detected in 2024 through the "Nusantara Jaya" operation, which BDS-BSSN and IMIC-BAKAMLA carried out. The Joint Operation Report, 2024 quotes Rear Admiral TNI Tatang Sulaiman, Deputy for Operations and Training at BAKAMLA, as saying, "This operation demonstrates the effectiveness of our collaboration in securing Indonesia's maritime areas."

Managing Maritime Cyber Security Presents Difficulties; 1) Insufficient Resources Budgetary and human resource limitations affect both BSSN and IMIC's ability to handle increasingly sophisticated cyberthreats. There is always a need for improvement in worker competencies and technology infrastructure. 2) Maritime Sector Cyber Awareness Is Low A lot of marine businesses don't realize how important cyber security is. The absence of mitigating methods to address dangers has resulted from this lack of knowledge. 3) The intricacy of regional cooperation Effective cooperation is frequently hampered by national policy, capacity, and priority disparities, even in the face of programs like ReCAAP (Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia).

BSSN and IMIC can offer the following strategic solutions to address these issues: 1) Fortifying the Infrastructure of Technology It is essential to invest in cutting-edge technology like big data analytics and artificial intelligence (AI). Early cyber threat detection and response capabilities can be enhanced by these technologies. 2) Awareness and Education Regular training sessions and cybersecurity awareness efforts are necessary. To increase awareness of the dangers and necessary mitigation strategies, this training needs to be obligatory for all participants in the marine business. 3) Harmonization of Regional Policies To harmonize cybersecurity norms, it is crucial to create a shared framework with other nations. The maritime region's threat mitigation measures will be more effective and easier to coordinate thanks to this policy harmonization (Neo, 2021)

CONCLUSION

With Indonesia's character as an archipelago and the country's focus on becoming the world's maritime axis, it is time for Indonesia to start improving the maritime cyber security system to maintain the sovereignty of territorial boundaries, one of which is through the Signal Detection Center (BDS) under the BSSN state institution and also in sea activities can be carried out by BAKAMLA through the Indonesia Maritime Information Center (IMIC).

Special attention is needed to address the strategic challenge of maritime cyber security in the Malacca Strait. IMIC and BSSN play a critical role in handling ever-more-complex cyberthreats. Cyber dangers in

the marine region can be reduced by cross-sectoral cooperation, policy harmonization, education, and technological strengthening. Maintaining marine security in important locations like the Malacca Strait will require constant investment in both technology and human resources.

The pros and cons of the latest proposed law on BAKAMLA should reflect the government and alternatives can be found because Indonesia's needs related to sea surveillance are high and overlapping ministries make sectoral ego very pronounced in the process. The author argues that the above article can be a reference material in that it is very effective and can be done by 2 institutions that focus on and complement each other regarding maritime cyber security in the Malacca Strait. The "Nusantara Jaya" operation that collaborated with BSSN and BAKAMLA succeeded in uncovering an international smuggling network, this can be further improved and towards more advanced sea surveillance effectiveness using AI and renewable technology, as long as the sectoral ego and overlap can be resolved.

While the existing form of cooperation and regular meetings between Indonesia, Singapore, and Malaysia should be strengthened by creating or renewing a joint agreement to overcome maritime security cyber threats, security can be safer and prevention can be overcome as soon as possible with improved cooperation and inter-agency coordination between BSSN and IMIC.

REFERENCE

Affairs, I. M. of F. (2013). *Maritime Security Cooperation between Indonesia and Singapore*.

Borden, A. (1999). *What is Information Warfare? [Online]*. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf

Chamidi, S. (2004). Kaitan antara Data and Informasi Pendidikan. *Jurnal Pendidikan and Kebudayaan*, *48*, 311–328.

Desiana, R., & Prima, S. C. (2022). Cyber security policy in Indonesian shipping safety. *Journal of Maritime Studies and National Integration*, *5*(2), 109–117. DOI: https://doi.org/10.14710/jmsni.v5i2.13673

Dewan Kelautan Indonesia. (2010). Maritime Security Policy. In *Maritime Security Policy*.

Djalal, H. (2023). Indonesia's maritime security has direct implications for the stability of Southeast Asia and Indo-Pacific regions. *Indonesian Maritime Journal*, *12*. IMIC. (2024). *No Title*.

Khanisa. (2022). ASEAN Maritime Security: The Global Maritime Fulcrum in the Indo-Pacific. In *ASEAN Maritime Security: The Global Maritime Fulcrum in the Indo-Pacific*. DOI: https://doi.org/10.1007/978-981-19-2362-3

Lewis, B. C. (2021). *Information Warfare*.

Lubabah, R. G. (2020). *Kepala Bakamla Resmikan Pusat Informasi Maritim Indonesia*. https://www.merdeka.com/peristiwa/kepala-bakamla-resmikan%02pusat-informasi-maritim-indonesia.htm

Neo, M. (2021). *The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore*. *42*(42), 2021.

Proborini, D. (2016). Sisi Gelap Era Informasi: Information Warfare and Perang Virtual. *Jurnal Globalisasi and Masyarakat Informasi*, 1–6.

PUSHIDROSAL. (2018). *DATA KELAUTAN YANG MENJADI RUJUKAN NASIONAL DILUNCURKAN*. https://www.pushidrosal.id/berita/5256/DATA-KELAUTAN-YANG-MENJADI-RUJUKAN-NASIONAL--DILUNCURKAN/

Rahman, C. (2009). Concepts of Maritime Security Paper Centre for Strategic Studies : New Zealand. *Centre for Strategic Studies New Zealand Discussion Paper: Victoria University of Wellington*, *June 2009*.

Sugiharto, A., & Shafwatullah, P. (2021). Maritime Diplomacy in Building Maritime National Security in Indonesia. *Jurnal Maritim Indonesia*, *9*(2), 121–131.

Susanto, & Munaf, D. (2015). *Komando dan Pengendalian Keamanan dan Keselamatan Laut: Berbasis Sistem Peringatan Dini*. Jakarta: Gramedia Pustaka Utama.

TENTANG BSSN. (2021). https://www.bssn.go.id/tentang-bssn/