Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 10 No. 1 (2024) pp.169-187
https://jurnal.idu.ac.id/index.php/defensejournal

Indonesia's Role as A Cyber Protector in the Southeast Asia Region

Dudy Heryadi[1], Robby Rizaldi[2], Tia Panca Rahmadhani[3], Feby Diah Miranti[4], Febyanti Juliastica[5*]
[1,2,3,4,5]Padjajaran University, Indonesia

dudy.heryadi@mail.unpad.ac.id[1], robby22001@mail.unpad.ac.id[2],
tiapa22001@mail.unpad.ac.id[3], feby22001@mail.unpad.ac.id[4]
febyanti22001@mail.unpad.ac.id[5*]
*Corresponding Author

Article Info

Article History:
Received: May 26, 2023
Revised: January 24, 2024
Accepted: April 30, 2024

Keywords:
Cyber Protector,
Cybersecurity,
Role Theory,
Securitization,
Southeast Asia

DOI:
http://dx.doi.org/10.33172/jp.v10i1.13097

Abstract

The rapid development of technology has finally opened up a new space that is connected through the internet. Southeast Asia is one of the regions with the highest percentage of internet users in the world. However, with this rapid digital growth, a new problem emerged. Cyberattacks that occurred in the Southeast Asia region caused a lot of data theft and failures in cyberspace systems in this region. Indonesia as chairman of ASEAN able to take advantage of the opportunity to handle the problem of cyberattacks in Southeast Asia. Therefore, this article discusses Indonesia's role in dealing with cyber security problems in Southeast Asia through Indonesia's role approach to Ego's Role Conception and Alter's Prescription. The research method used in this article is qualitative to explain Indonesia's role in mitigating cyber security problems in Southeast Asia. By using Systematic Review with Preferred Reporting Items for Systematic Reviews and Meta-analyses as a reference in conducting literature studies. The research results show that Indonesia can be a cyber protector in Southeast Asia in line with strengthened organizational structures, diplomacy with partner countries, and cooperation between agencies with an interest in cyber protection.

INTRODUCTION

Developments in digital technology innovation and expansion should be able to contribute to increasing cyber protection capabilities to achieve global security conditions in cyberspace through efforts to mobilize state resources (Bueger, Edmunds, & Mccabe, 2021). However, the World Economic Forum 2022 report points out that ransomware attacks on various sectors increased by 151% compared to 2021, causing

tens of millions of dollars in losses to businesses and governments. These attacks have global network circulation, with distribution patterns that are difficult to detect (World Economic Forum, 2022). Often these cyber-attacks become a national security problem in several countries and even escalate to regional threats (Abdullin, Davletgildeev, & Kostin, 2020). Because it is transnational, cooperation is needed both regionally and internationally to encourage the achievement of cyber security (Kostyuk & Gartzke, 2023).

In handling cyber security issues, there are differences in handling between developed countries and developing countries. In the context of developed countries, at the regional level, North America is the region with the highest level of cyber threats, in 2022, the United States had cyberattacks reaching 36,000 attacks per year, followed by Europe and Asia Pacific (Kateryna, 2022). As a country with strong technological and economic capabilities, the approach used by the U.S. in responding to cybersecurity issues is an offensive/defensive narrative using technical capabilities and economic power independently (Oosthoek & Doerr, 2020). The European region has the second highest threat level after North America, with a figure of 11 percent. Based on the National Cyber Security Index (NCSI), Europe is recorded to have 71.88% points. This can also be influenced by the role of the European Union, which has a cyber security market of more than €130 billion, more than 60,000 companies dealing with cybersecurity, and more than 660 cyber security expertise centers (Juncker, 2017). In addition, developed countries tend to have private actors who try to prevent cyberattacks, for example, what is done by Microsoft, Mandiant, and Sentinel One (Homburger, 2019).

In Southeast Asia, the country with the most cyberattacks is Singapore, with 3,122 attacks per year, followed by Malaysia, Indonesia, and Vietnam (World Economic Forum, 2022). This data also shows that Southeast Asia is a region that is still vulnerable to cyber-attacks. However, there are differences in the approach used by countries with weak technological capabilities. In this context, developing countries that have challenges in technical and economic capabilities and landscapes for handling cyberattacks that have not been established have random patterns and are temporary problem-solving, so the approach to this issue is limited to resolving attacks that have occurred but not yet at the stage to counteract attacks that might arise in the future (Egloff & Shires, 2022).

Within the Southeast Asian region, ASEAN has made efforts to raise and improve cybersecurity issues through joint forums and dialogue. Since 2001 at the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the issue of cybersecurity has become one of the meeting agendas, which resulted in the agreement of ASEAN ministers responsible for transnational crimes. ASEAN's response to the ASEAN Regional Forum (ARF) Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace, which emphasizes the creation of a legal (regulatory) framework against cybercrime, encourages cooperation and collaboration in dealing with crime, including cyber terrorism, abuse of cyberspace and promote increased public awareness in using cyber The creation of a National Computer Emergency Response Team (CERT) was mutually agreed upon to refine the ASEAN ICT Masterplan 2015. The plan emphasizes building trust related to cybersecurity through community empowerment and engagement as well as infrastructure development efforts with initiatives to promote network integrity and information security, data protection, and CERT cooperation (Novitasari, 2017).

From the efforts made, they are based on a perception of cyberspace divided into two groups (Betz & Stevens, 2011). The first group, called inclusive, is a country that considers technology as the primary key to entering cyberspace. This means that if there

is a problem in the world, then the thing that must be addressed is the technology. Hare also stated that liberal countries prioritize solving technology problems, such as malware and viruses, because they can disrupt the flow of information and business activities through cyberspace (Hare, 2015). Rivera argues that with the flow of information and social interaction in cyberspace, the liberal state tends to protect these individuals (Rivera, 2015). This is also a place to spread liberal-democratic values. This group includes the United States, Europe, and Singapore, which have fast-developing technology and developed binding cybersecurity-related rules and norms.

Table 1. Cyber Attacks in Several Countries in Southeast Asia (2016-2020) (National Cyber Security Index, 2023)

State	Hacker	Damage
Malaysia (2016)	Unknown	• Breaking into Customer Accounts • An undetectable $81 million transaction • Decreased customer confidence in Bank Negara Malaysia
Indonesia, Malaysia, Philippines (2017)	Unknown	• Ransomware attack on WannaCry • Thousands of computer systems in three countries experienced personal data compromise and hacking
Singapore (2018)	Unknown	• Ransomware attack on SingHealth • Theft of more than 1.5 million patient data, personal data protection
Vietnam (2019)	Unknown	• Phishing attacks on Vietnamese financial institutions • Theft of over $1 million from several banks
Malaysia (2020)	Unknown	• Hacking at the Malaysian Maritime Security Agency • Leakage of secret defense documents to the public

The second group, which is called exclusive, is the view that cyberspace is a place where computer hardware meets and then carries out social interactions (Betz & Stevens, 2011). This happens because when entering cyberspace, at the same time, it is also accompanied by the thoughts of the user. Hare stated that the second group is a country that tends to have an authoritarian regime and is influenced by its military level (Hare, 2015). The government considers that the existence of cyberspace is to threaten the sovereignty of its country. So, Rivera said that with this threat, the state will tend to control content from its formation to distribution made by cyberspace users (Rivera, 2015). An example is Malaysia, which refused the U.S. assistance because it would interfere with its sovereignty (Lynch et al., 2005), while China was able to cooperate with Malaysia and Thailand because of its approach that focuses on national sovereignty in handling cybersecurity cases (Kim, Go, Kim, Lee, & Lee, 2023)

When viewed from a comparison of cybersecurity in North America, Europe, and Southeast Asia, the distance between the two is still relatively large. Even so, ASEAN has made efforts to increase the importance of cybersecurity but is still less developed than other developed regions. Uniquely, ASEAN has a membership of countries with various types of government, which also influence the country's perception of cyberspace. Seeing how vulnerable the Southeast Asian region is to cyber-attacks compared to developed

countries such as North America and Europe, this article will try to explain Indonesia's role in mitigating cybersecurity issues in Southeast Asia. Indonesia as a sovereign country should have awareness of broader national interests so that it can collaborate and even make cross-border policies regarding cyber security mitigation in Southeast Asia, this is in line with Indonesia's bargaining position as the largest internet user in Southeast Asia. This study will also provide alternative views to governments and organizations related to cyber security in determining and creating cybersecurity policies aimed at maintaining and protecting sensitive data and computer infrastructure more strictly and firmly to implement cybersecurity resilience and the Economic Digitalization program in ASEAN

Research regarding the relationship between cybersecurity and Indonesia has been carried out by several researchers, including Amin & Huda (2021), Aulianisa & Indirwan (2020), Fransiska & Tobing (2023), Gati et al. (2020), Intan & Intan (2023), Iswardhana (2021), Kaburuan & Damayanti (2022), Kurta (2023), Marwan et al. (2022), Nugraha & Putri (2016), Paterson (2019), Rahardjo (2018), Rai et al., (2022), Saputri et al. (2020). From this research, several of them discuss the situation, conditions, urgency, and cybersecurity policies in Indonesia (Aulianisa & Indirwan, 2020; Intan & Intan, 2023; Marwan, Jiow, & Monteiro, 2022; Nugraha & Putri, 2016; Paterson, 2019; Rahardjo, 2018). Kurta (2023) is also discussing the stagnation of Indonesia's cybersecurity but with a comparative case study with the Philippines regarding their strategies in cyber security. Amin & Huda (2021) have researched efforts to harmonize international law regarding cybersecurity into domestic law. Fransiska & Tobing, (2023) researched the evaluation of Indonesia's readiness to strengthen cyber security through bilateral and multilateral cooperation. Kaburuan & Damayanti, (2022) researched the Indonesian National Police (Polri) strategy in fighting cybercrimes by utilizing Indonesia-ASEAN cooperation in AMMTC to increase networking and capacity building with countries in Southeast Asia. Rai et al. (2022) have studied Indonesia's role in securing cyberspace at the domestic, bilateral, and multilateral levels. Gati et al., (2020) have examined the relationship between AI and Indonesia's cybersecurity strategy. Finally, Iswardhana (2021) research efforts to improve Indonesia's cybersecurity using cyber diplomacy. For example Saputri et al., (2020) that researched Indonesian cyber diplomacy through ASEAN with Japan to conduct cyber exercises.

Through previous studies, there has been research that discusses Indonesia's role in cybercrime. This study also uses Holsti's role theory and examines various cyberspace scales. However, the study presented adds the concept of securitization by Barry Buzan to convince the public that cyber threats are something that must be handled so that they do not quickly spread and threaten human security. Therefore, this study will analyze Indonesia's potential to encourage increased cyber security in Southeast Asia. The study will be conducted with descriptive qualitative, purposive sampling on the relevant previous literature.

METHODS

This study uses a qualitative method to explain Indonesia's role in mitigating cyber security issues in Southeast Asia. A qualitative approach in international relations aims to study phenomena and actors and emphasizes explanations of the processes and phenomena that occur (Creswell, 2014). Therefore, through Indonesia's role in mitigating cyber security issues in Southeast Asia through a securitization approach. This study began by looking for previous research papers such as articles, books, and proceedings that were related to this research. The previous study is filtered based on title, keywords, and abstract which will ultimately produce several studies that are relevant to this study.

Then the relevant results of the previous study are elaborated on in this study so that the facts presented are more comprehensive and balanced. This method is called Systematic Review with Preferred Reporting Items for Systematic Reviews and Meta-analyses.

The analysis of the study uses the concept of role theory put forward by Holsti and the securitization approach by Buzzan. These two approaches will be used to see Indonesia's role in driving awareness among Southeast Asian countries on cybersecurity issues. This approach will look at the specific role played by Indonesia, departing from the particular role of the state in the problems being faced. Holsti (1970) revealed that the role of an actor is strongly influenced by two things, namely the ego's role conception and altered perceptions. According to Holsti, the emergence of an international system and the concept of superior and inferior states will encourage the division of states' roles in the global system. This concept will influence Indonesia's role by prevailing interests, goals, attitudes, values, culture, international laws, and social institutions.

RESULT AND DISCUSSION

Role Theory

In international relations, the state has a specific role (Holsti, 1970). The role and nature of a state will be dynamic (depending on specific issues), while the behavior of the state will be absolute according to the role being played. There are four major concepts in viewing the role concept, namely role performance or the role of performance, including decisions and actions. Second, ego's role conception or policymakers from the role conception or, in other words, are executives. The ego's role conception is influenced by interests, goals, attitudes and values, and personality needs. These things are concepts that arise from the perceptions of individual policy-making actors. Third, alter perceptions or the role of community interference or, in other words, legislature and social and cultural groups. Finally, position or place to process or process everything between ego's role conceptions and alter's perceptions is measured to produce output as a decision and action (Holsti, 1970). In this role performance, the role of the actor (in this case, the state, of Indonesia) will be the determinant of foreign policy. The issued foreign policy becomes the final part of a process that produces a decision and action in both static and dynamic roles.

Securitization Concept

Buzan first proposed the concept of securitization in international relations in the book "Security: A New Framework of Analysis". Buzan, Wæver, & Wilde (1998) argued that to create security conditions. Actors must take steps to go beyond the general rules in framing an issue. Actors must make political efforts or go beyond it. Meanwhile, securitization is an extreme political effort. Furthermore, they stated that in conducting security analysis and security articulation through the speech-act approach, three forms of units related to efforts to analyze the securitization process are needed, consisting of:

1. Referent objects. Something is seen as visibly threatened and formally demanded survival. Based on the traditional view, the referent object is usually the state or nation. For the state, the referent object is sovereignty. For the nation it is identity. However, the referent object at this time is limited to the state or nation and various spectrums that make it possible to become a referent object. Essentially, the actor raising the security issue could construct everything as a referent object. The factor that will later influence the success or failure of a point to become a security issue is the difference in the ability of actors to schedule the issue in question.

2. Securitizing actors. A person or group carrying out speech acts and turning an issue into a security issue. Securitization actors may come from bureaucrats, government, political leaders, lobbyists, interest groups, and pressure groups.
3. Functional actors. These are actors who affect the dynamics of a sector and play an important role but do not try to make the issue a security issue.

Meanwhile, the securitization process has two stages. The first stage of securitization describes issues considered existential threats to target objects or communities by state or non-state actors. The second, more critical, set concerns the success of securitization, which depends on whether or not the audience is convinced to accept that a particular object of reference is indeed existentially threatened. With the following explanation, it can be said that this research tries to analyze the issue of cyberattacks in Southeast Asia using the securitization theory. Indonesia, as an actor involved in this issue, is also collaborating with other actors to provide solutions in dealing with cyberattacks in Southeast Asia. There have been many cases of cyber threats that have occurred in Southeast Asia which have threatened national security, especially human security. Therefore, looking at this case, securitization needs to be carried out to reduce and mitigate other cyber threats.

Indonesia's Ego Role Conception

Using the role approach, in this section, the author will look at several factors that can influence policymakers in determining cyber security policies in Indonesia. The first discussion is to look at Indonesia's interest in this issue. In recent years cyberattacks that have occurred on the government and national industry, such as data hacking at the Ministry of Health or ransomware attacks on Indonesian Railways Company or PT KAI, can increase the government's interest and interest in securing information systems and influence cyber security policy-making. Indonesia has broader national interests to be able to establish cooperation and even cross-border policies related to cyber security mitigation in Southeast Asia. This aligns with Indonesia's bargaining position as Southeast Asia's most prominent internet user.

The next conception is about goals (objectives) owned by Indonesia. In cyber security, governments and organizations determine cyber security policies to maintain and protect sensitive data and computer infrastructure, which can encourage governments to make stricter and firmer policies. Guidelines and regulations issued by the government, such as Law Number 11 of 2008 concerning Information and Electronic Transactions (2008), Law Number 27 of 2022 concerning the Protection of Personal Data, Regulation of the Minister of Communication and Informatics Number 20 of 2016, and Presidential Regulation Number 53 of 2017 concerning the Establishment of the National Cyber and Crypto Agency (BSSN or *Badan Siber dan Sandi Negara*). Indonesia has also improved cybersecurity at the regional and national level, such as cross-country meetings such as the ASEAN Ministerial Conference on Cybersecurity (AMCC), Global Conference on Cyberspace (GCCS), and others to discuss handling cross-border cybersecurity aimed at transforming knowledge and establishing more specific cooperation to achieve national interests.

Conceptions about attitudes and values can be seen from people's attitudes and values towards cyber security, which influence national policy-making. People who are increasingly aware of the importance of cyber security encourage the government to make stricter policies and increase awareness of the importance of cyber security among the public. There needs to be collective awareness that makes cyber security a critical issue to be tightened to achieve this interest. Indonesia has a history of strong leadership

in ASEAN and is still considered influential in the ASEAN region. The conception of personality needs (personal needs) shows how policymakers' personal needs and personalities can influence policies. Policymakers who think critically and rationally can make more detailed and effective policies addressing cybersecurity issues. Indonesia, with a population of 270 million people and 215.63 million people in 2022-2023, has used the internet, and even increased every year. There is great potential that the Indonesian government must do in making decisions or national policies. So, Indonesia's need for cyber security shows the need to establish Indonesia's role in this issue.

The development of technology and human resources in the field of cyber security also plays a role in the field of cyber security, such as improving the quality of cyber security education and training or developing innovative cyber security systems, so that this can influence personal goals and needs to strengthen cyber security. Indonesia has made various efforts to deal with cyber security threats by carrying out technological developments such as the establishment of BSSN, the development of a National Cyber Security Strategy (SKSN or *Strategi Keamanan Siber Nasional*), cyber security applications, cyber security training, certification, and international cooperation. In addition, the development of global issues related to cybersecurity, such as spy software, cybercrimes committed by the state, or cyberattacks targeting critical sectors, are feared to have the potential to threaten the national stability and security Indonesian government and society. ASEAN itself launched a regional cyber security framework in 2018 that aims to strengthen cooperation between ASEAN countries in cyber security.

Indonesia’s Alter Prescription

Indonesia's role in mitigating cyber security issues in Southeast Asia is influenced by the influence of surrounding social and cultural groups. In the regional realm, Indonesia is a member of the international organization the Association of Southeast Asian Nations or ASEAN. So indirectly, Indonesia will play its role with the provisions that have been jointly determined under the auspices of ASEAN. ASEAN has organizational mechanisms and structures carried out by each of its members. The mechanism is carried out, such as the ASEAN Summit, held twice a year, discussing the issues faced and making several decisions together. Apart from the country level, ASEAN is also a meeting place for ministers and other high-ranking officials to discuss and handle the scope of cooperation such as politics-security, economics, socio-culture, environment, energy, tourism, and so on. So, ASEAN has a role as a country dialogue partner and a forum for cooperation with other countries worldwide. Unlike other intergovernmental organizations, ASEAN is unique in its role as a center for these Southeast Asian countries. The ASEAN Charter states "not to interfere in the internal affairs of ASEAN Member States" and "not to participate in any policy or activity ... that threatens the sovereignty, territorial integrity or political and economic stability of ASEAN Member States" (ASEAN, 2008). From this principle, there is the concept of non-interference, where if the consensus says they agree about cyber security, it is still not appropriately implemented at the national level (Dai & Gomez, 2018). Then the other member countries cannot interfere in these domestic affairs. This can be proven through data from the Global Cybersecurity Index (GCI) 2020 launched by the United Nations (International Telecommunication Union, 2020).

Table 2. Global Security Index of Southeast Asia (International Telecommunication Union, 2020)

Rank	State	Legal	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures	Total
1	Singapore	20.00	19.54	18.98	20.00	20.00	98.54
2	Malaysia	20.00	19.08	18.98	20.20	20.00	98.06
3	Indonesia	18.48	19.08	17.84	19.48	20.00	94.88
4	Vietnam	20.00	16.31	18.98	19.26	20.00	94.55
5	Thailand	19.11	15.57	17.64	16.84	17.34	86.50
6	Philippines	20.00	13.00	11.85	12.74	19.41	77.00
7	Brunei Darussalam	14.06	14.19	10.84	12.85	4.12	56.07
8	Myanmar	9.39	3.64	4.71	8.92	9.75	36.41
9	Lao PDR	11.7	3.27	0.00	1.23	4.07	20.34
10	Cambodia	7.38	2.50	1.69	3.29	4.26	19.12
11	Timor Leste	0.0	0.0	0.0	0.0	4.26	4.26

Based on the table, it proves that even though there is a consensus regarding the importance of enforcement and the creation of national institutions to deal with cyber security, the primary control is still the state itself. This phenomenon can occur due to the diversity of the country's economic development, which tends to be high, it turn has an impact on the country's maturity in sectoral development information and communication technologies (ICT), as well as the adoption of digital products and services such as the use of the digital economy (Dai & Gomez, 2018). The regime influences the country's maturity toward cyber force in that country (Rivera, 2015). Based on the table, Singapore has the highest score compared to other countries because it is a liberal country where the flow of information and technology is developed so that people get the right to benefit and protection from cyberspace. Meanwhile, Timor Leste, which is still relatively new to ASEAN, cannot compete with other countries due to limited infrastructure and the unstable regime in that country. If you look at Cambodia, it has been carried out from the level of law enforcement, but the organizational structure is still dangerous. However, this figure is still too small compared to other countries. Even though some sectors are still in development, at least with the existence of ASEAN, these countries can enhance cooperation efforts with each other not only with Southeast Asian countries but also with other countries such as the ASEAN plus three cooperation which includes Japan, South Korea, and China. In addition, ASEAN cooperates with other countries such as Australia, the U.S., Russia, etc.

The influence of big powers such as the U.S. and China also influences the actions of ASEAN countries. One example of the behavior of ASEAN countries towards this principle was when the U.S. wanted to assist ASEAN countries in handling cyberterrorism cases, and the Philippines accepted this assistance with open arms. Meanwhile, Malaysia refused the assistance provided by the U.S. because it felt that this assistance could

threaten its country's sovereignty (Lynch, et al., 2005). Ironically, Indonesia, which adheres to its non-aligned side, must gracefully refuse this assistance due to pressure from other ASEAN countries (Kim, Go, Kim, Lee, & Lee, 2023). Differences in perceptions about cyberspace itself cause the emergence of these state actions.

In the alter prescription, Indonesia is in the ASEAN regional area, which prioritizes working together to overcome a problem, on the other hand, it has a non-interference value where everything will return to the state's decision. In addition, there are differences in domestic economic and government factors that cause differences in handling cyberspace cases. Finally, all policies pursued by ASEAN countries are heavily influenced by the existence of big powers such as the U.S. and China, especially in the development of cyber security.

Indonesia's Role in Encouraging Cybersecurity Securitization in Southeast Asia

Before knowing the alternative roles that Indonesia can play in the context of securitizing moves, Indonesia has made efforts to raise awareness at the regional level on cyber security issues through the ASEAN regional organization (see Table 3). In the field of cybersecurity, the role of functional actors cannot be separated, and this is because cybersecurity is a broad issue and continues to innovate rapidly so that other actors besides the state are needed to support securitization actions. The vulnerability of cyberattacks makes Indonesia more aware of cybersecurity issues because they relate to national security. The following events led Indonesia to form the National Cyber and Crypto Agency as one of the institutions dealing with cybersecurity issues in Indonesia.

Table 3. Indonesia's Securitizing Role in Regional Forum (Processed by researchers, 2023)

No	Cooperation Framework/Forum	Policy Focus	Indonesia's Securitizing Role
1.	ASEAN Regional Forum Statement on Cooperation in the Field of Security of and the Use of Information and Communication Technologies (2010)	This agreement underscores the importance of international cooperation in addressing cybersecurity challenges.	Initiator
2.	ARF Work Plan on Enhancing Cooperation in the Area of Security of and in the Use of Information and Communication Technologies (2013)	A work plan that provides a framework for enhancing cooperation among member countries in the field of cyber security.	Initiator
3.	ARF Statement on Cooperation in the Field of Information Security (2016)	An agreement that emphasizes the importance of cooperation in addressing cybersecurity threats and promotes principles that promote security and stability in cyberspace	Initiator

4.	ARF Seminar on Cyber Incident Response and Recovery (2019)	Seminars aimed at raising awareness and building capacity in dealing with cybersecurity incidents and recovery.	Host
5.	ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) (2020)	The center was established as part of the ASEAN-Japan initiative to enhance the capacity of ASEAN members to deal with cyber security threats.	Initiator
6.	ASEAN Regional Forum Statement on the Prevention of and Response to Infectious Diseases Including the COVID-19 Pandemic (2020)	This agreement covers cybersecurity issues related to the COVID-19 pandemic, including the increased risk of cyberattacks during the pandemic	Initiator

Looking back at the derivative regulations governing the National Cyber and Crypto Agency, including Presidential Decree Number 28 of 2021 concerning the National Cyber and Crypto Agency and Regulation of the National Cyber and Crypto Agency (BSSN) Number 6 of 2021 concerning the Organization and Working Procedures of the National Cyber and Crypto Agency. These rules are very important to develop and navigate the governance and administration of BSSN. The National Cyber and Crypto Agency Regulation Number 6 of 2021 shows that the BSSN is under the president, and has the task of implementing governance in the field of cyber and password security. This regulation then becomes a guide for the management and implementation of BSSN. The organizational structure of BSSN governance is as follows:

1. To encourage the implementation of BSSN, derivative regulations include Presidential Regulation Number 47 of 2023 concerning National Cyber Security Strategy and Cyber Crisis Management. Then the National Cyber and Crypto Agency Regulation Number 8 of 2023 was stipulated with the consideration that to implement the provisions of Article 7 paragraph (4) of Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure, it is necessary to establish a National Cyber and Crypto Agency Regulation concerning the Information Infrastructure Protection Framework Vital.
2. National Cyber and Crypto Agency Regulation Number 2 of 2024 concerning Cyber Crisis Management is stipulated with the consideration that to implement the provisions of Article 33. As well as other regulations as a derivative of the BSSN regulations, namely Presidential Regulation Number 47 of 2023 concerning National Cyber Security Strategy and Cyber Crisis Management, it is necessary to establish Agency Regulations Cyber and National Code on Cyber Crisis Management.

BSSN itself does not have the authority or regulations contained in the law to follow up on cyber problems that occur in Indonesia. This is different from Singapore, which has a cyber security agency that has good cyber security readiness with its agency called the Cyber Singapore Agency (CSA). The Cybersecurity Bill was passed on February 5, 2018, and received the President's assent on March 2, 2018, to become the Cybersecurity Act.

The Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to:

1. Strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks. CII are computer systems directly involved in the provision of essential services. Cyberattacks on CII can have a debilitating impact on the economy and society. The Act provides a framework for the designation of CII and provides CII owners with clarity on their obligations to proactively protect the CII from cyberattacks. This builds resilience into the CII, protecting Singapore's economy and our way of life. The CII sectors are energy, water, banking and finance, healthcare, transport (which includes land, maritime, and aviation), Infocomm, media, security and emergency services, and government.
2. Authorize CSA to prevent and respond to cybersecurity threats and incidents. The Act empowers the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents to determine their impact and prevent further harm or cybersecurity incidents from arising. The powers that may be exercised are calibrated according to the severity of the cybersecurity threat or incident and the measures required for response. This assures Singaporeans that the Government can respond effectively to cybersecurity threats and keep Singapore and Singaporeans safe
3. Establish a framework for sharing cybersecurity information. The Act also facilitates information sharing, which is critical as timely information helps the government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The Act provides a framework for CSA to request information, and for the protection and sharing of such information.
4. Establish a light-touch licensing framework for cybersecurity service providers. CSA adopts a light-touch approach to license only two types of service providers currently, namely penetration testing and managed security operations center (SOC) monitoring. These two services are prioritized because providers of such services have access to sensitive information from their clients. They are also relatively mainstream in our market and hence have a significant impact on the overall security landscape. The licensing framework seeks to strike a balance between security needs and the development of a vibrant cybersecurity ecosystem.

Apart from that, another country example is Belgium, which is the country with the best cyber security according to National Cyber Security Index (2023) data. The cyber institution owned by Belgium is the Center for Cyber Security Belgium (CCB). CCB also collaborates with the national crisis center to ensure crisis management in cyber incidents and disseminate safety standards, guidelines, and norms. The CCB is also tasked with increasing awareness of cyber threats and efforts to be protected from these threats. To achieve this, CCB creates programs to increase awareness in the public and private spheres. Finally, the CCB can also propose Belgium's position regarding cyber security to European institutions, such as in certifying and labeling products and services. The following are the duties of the CCB:

1. Monitor, coordinate, and supervise the implementation of Belgian policy regarding cybersecurity.
2. Manage various projects related to cyber security using an integrated and centralized approach.
3. Ensure coordination between relevant government departments of public authorities and the private or scientific sector.
4. Proposing adaptations to the regulatory framework in the field of cybersecurity.

5. Handling crisis management in the event of a cyber incident in collaboration with the government's crisis and coordination center.
6. Establish and monitor security standards, guidelines, and measures for information systems across government and public institutions.
7. Coordinate Belgian representation at international cybersecurity forums and monitor international commitments.
8. Evaluate and certify the security of information and communication systems.
9. Increase awareness among users about information and communication systems.

Belgium has a cybersecurity strategy that has been designed by CCB 2.0 for 2021-2025. The strategy is as follows (1) strengthen the digital environment and increase trust in the digital environment, (2) arming computer and network users and administrators, (3) protect organizations and vital interests from all cyber threats, (4) respond to cyber threats, and (5) increasing public, private, and academic collaboration. The bodies responsible for cybersecurity in Belgium are:

1. The center for cybersecurity Belgium (CCB).
2. CERT. BE (detect, alert, and analyze cyber security problems; become a center for exchanging cyber security information).
3. The federal police (fighting ICT crime, the main actors that the public contacts have agencies such as the federal judicial police, the regional computer crime units (RCCUs), and the federal computer crime unit (FCCU). So, they will carry out evidence collection, track down perpetrators, and bring them to court RCCU).
4. The public prosecutor's office (the prosecutor's office has a cyber unit that focuses on investigating cybercrimes and encouraging international operational cooperation with European countries).
5. Defense (developing cyber strategies, policy plans, and capabilities needed to support military and intelligence operations, as well as those carried out in the cyber domain. Deals with technology in military operations).
6. The national crisis center (crisis management in collaboration with the CCB) ensures the organization and coordination of cyber emergency plans at the national level. Analyze risks, and provide legal and organizational support.
7. State security (VVSE) collects, analyzes and processes intelligence on activities that threaten or could threaten the country's internal security, the country's external security, or the country's scientific and economic potential. Maintaining appropriate contacts gathering intelligence from foreign agencies and sharing information.
8. The NSA (the National Security Administration) deals with confidential data, data encryption, and security verification.
9. The coordination unit for threat analysis (CUTA) of terrorist and extremist threats.
10. Sectoral authorities.
11. Federal public service economy.

Even though BSSN has been built with the hope of improving cyber security in Indonesia, this government agency of course faces a series of challenges in implementing its tasks. Based on the National Cyber and Crypto Agency Regulation Number 5 of 2020 concerning the Strategic Plan of the National Cyber and Crypto Agency for 2020-2024, several challenges faced by BSSN have been mentioned. The first challenge is related to the lack of cyber security awareness among individuals and government agencies. On the other hand, the development of technology 4.0 is increasingly developing and internet users are increasing every year. If it is not resolved immediately, it will become even more massive and could end up threatening the country's sovereignty. The second challenge is related to the management of national cyber security which includes managing cyber and

password human resources, cyber and password security policies or regulations (national cyber security strategy), cooperation, and the independence of cyber and password technology. BSSN as a cyber security institution has submitted a series of drafts for developing policies or regulations regarding cyber security. However, the process of uniting interests with other institutions seems to take a long time. One of them is regulations regarding national cybersecurity which should have been formulated since the BSSN was built because it can be the initial foundation for improving cybersecurity. However, this regulation was only passed in 2023, while cybercrime problems such as Bjorka's occurred in the previous year (Llewellyn, 2022). Thus, there are internal problems in Indonesia in establishing policies and regulations for cyber security in Indonesia.

In comparison, cybersecurity in Singapore has shown great improvement compared to Indonesia. Singapore's cyber security agency is called the Cyber Security Agency or CSA which has been established since 2017. They passed the Cyber Security Bill in 2018 which has now become the Cyber Security Law which contains the following (1) strengthen the protection of Critical Information Infrastructure (CII) against cyberattacks; (2) authorize the CSA to prevent and respond to cybersecurity threats and incidents, (3) establish a framework for sharing cybersecurity information, (4) establish a lightweight licensing framework for cybersecurity service providers (CSA Singapore, 2024). Based on this law, Singapore gives CSA a mandate to be able to directly handle cyber incidents that occur in Singapore.

Meanwhile, in Indonesia, no law regulates cybersecurity (National Cyber Security Index, 2023; Sudarmadi & Runturambi, 2019). Even though there are already regulations governing personal data, such as the Cyber Security Law in Indonesia, Law Number 11 of 2008 concerning Information and Electronic Transactions. However, cybersecurity does not only focus on personal data but is also related to information and network infrastructure, and resources with expertise in the field of cybersecurity. If BSSN only deals with personal data without being accompanied by improvements in infrastructure and human resources, the actions taken will only be preventive measures.

Apart from that, there is a need for good inter-institutional relations to achieve cybersecurity for a country. Based on CSI 2023, Belgium was in first place as the country with the best cybersecurity index that year. Apart from the adequate regulations, the Center of Cybersecurity Belgium or CCB stated in its cyber security strategy for 2020–2025 that cooperation and collaboration between actors is very necessary for achieving cyber security in Belgium (CCB, 2021). Each body in Belgium has its role in dealing with cybercrime. Just as the police mobilize to combat cybercrime, the prosecutor's cyber unit conducts cybercrime investigations, and the military on cyber strategies, policy plans, and capabilities needed to support military and intelligence operations, as well as those conducted in the cyber domain. Apart from that, CCB collaborates with the national crisis center for crisis management. Then in terms of international cooperation ratifying the EU NIS regime into national law, establishing bilateral cooperation, and collaborating with non-state actors such as private actors and academics.

The point this study highlight is that both CSA and CCB can run as they should because their internal obstacles have been overcome first. If Indonesia has harmonized a broad view of cyber security, it will accelerate the existence of a cyber security strategy in Indonesia. BSSN as Indonesia's cyber security agency has certainly shown better results than before, but it cannot be denied that it still needs to be improved in terms of internal matters between institutions. Indonesia has the opportunity to become a cyber protector if it has faced a series of obstacles internally and then externally.

Seeing these challenges, the author through this study remains optimistic that Indonesia can become a protector of cyber security in the ASEAN region because it can be seen from the seriousness of the Indonesian government through the development of the BSSN which becomes an independent institution and directly under coordination with the president, which makes it possible to obtain a direct mandate in taking action against cyber threats and can improve coordination between relevant institutions and ministries for cyber prevention itself so that the challenges described above can be immediately overcome. These institutions include the Indonesian National Police (Polri or *Kepolisian Republik Indonesia*) in cybercrime, the Indonesian National Armed Force (TNI or *Tentara Nasional Indonesia*), the Ministry of Defense of Indonesia in cyber defense, the Ministry of Foreign Affairs in cyber diplomacy, and other cyber institutions (Rosy, 2020).

Securitization actions carried out by functional actors, namely the BSSN to address strategic issues in maintaining national security stability in cyberspace, are realized by the following strategy, (1) strengthening cyber infrastructure security, (2) development and strengthening of the Computer Emergency Response Team (CERT), (3) prevention of cybercrimes and increasing international cooperation in the field of cyber, (4) strengthening the capacity of cybersecurity human resources, (5) completion of cybercrime clearance rate (Ginanjar, 2022).

A referent object can be interpreted as an object facing a severe threat and is related to individual and national security. When an attack paralyzes one member country, the impact will affect other member countries. This encourages the importance of sharing information among ASEAN member countries to work together multilaterally to counteract cyber threats. In the context of cybersecurity in Southeast Asia, cyber threats need to be mitigated through the active role of cooperation between ASEAN member countries through various dialogues formed together, indirectly, the actions taken by Indonesia have provided framing that the real referent objects in this issue are countries. Southeast Asia, which in terms of capabilities, still has a capability gap to deal with cyberattacks.

Indonesia as Cyber Protector of Southeast Asia

Previously, it was known how Indonesia securitizes cyber security threats based on ego's conception and altered prescription and through the role carried out once, primarily as an initiator and host to improve cyber security. However, Indonesia could be a cyber protector in Southeast Asia with certain requirements.

First, apart from relying on regional cooperation relations, in achieving a cyber protector role Indonesia must strengthen bilateral diplomacy directly. ASEAN has made several of these efforts, such as Confidence-Building Measures to facilitate the flow of all information and the existence of Capacity-Building Measures to improve the skills of individuals working in the governments of Southeast Asian countries. From these things, Indonesia can also use these steps in approaching ASEAN countries, especially countries with an index below Indonesia which is reflected in the GCI, NSCI, and International Telecommunication Union (ITU) rankings. Because these countries' economic conditions are still lacking, Indonesia can invest or provide direct assistance, such as improving infrastructure on internet networks and building a business based on a digital economy so that the level of trust of these countries will increase in Indonesia. Then, suppose the people and the country benefit from digitalization. In that case, the government will ideally improve cyber security through organizational improvements, strengthening law enforcement, increasing skills, doing technical things more effectively and efficiently, and

expanding cooperation with various countries. But once again, it was emphasized that the alter prescription from ASEAN countries is non-interference, so Indonesia must be creative in approaching and influencing these countries. Especially in terms of perceptions from cybersecurity that technology and collaboration must be improved to maintain state sovereignty. Suppose governments in Southeast Asia, especially ASEAN, understand that there are common threats and concepts regarding cybersecurity. In that case, Indonesia can indirectly create norms and rules that all ASEAN countries can adopt.

Second, Indonesia must first fix its organizational structure, which tends to be under other aspects. The reason is that if collaboration between institutions is interconnected, it will be easy to carry out strategies at the national level and seek protection at the Southeast Asian regional group. Not only that, but also involvement with other actors such as private parties engaged in IT or other digital fields. Cyber diplomacy is needed that coincides with economic diplomacy from Indonesia to influence them to pay attention to the cybersecurity sector, which comes together with the increasing digital economic sector in their country. BSSN, as the agency dealing with cyber problems, has coordinated with various institutions such as the Ministry of Communication and Information, the State Intelligence Agency, the Ministry of Defense, the National Police, and other institutions. Its bureaucracy starts from making policies, developing and implementing SOPs, training and certification, security, monitoring, and auditing. Collaboration with other agencies has been created, but it is still not running effectively, and the lack of existence of the BSSN compared to the Indonesian National Police and the Indonesian National Armed Force (TNI or *Tentara Nasional Indonesia*) in handling cyber cases (Rizki, 2021). These agencies can collaborate with other ministries to improve protection against threats in cyberspace. In this context, Indonesia must strengthen its organizational bodies to achieve a role that will influence the actions and behavior of other countries regarding cyber security. In this study, the implications for Indonesia's thinking in ASEAN are that it should be able to become a cyber protector after previously succeeding as an initiator in several meetings at the ASEAN level so that Indonesia can build a more trustworthy image and can contribute to ASEAN in cyber security and bring national interests. to carry out digital diplomacy throughout ASEAN

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

With the development of technology, it will create a new threat to all humankind. At first, it was just a simple hardware problem, and now, it has expanded to threaten the sovereignty and security of a country. This impact is felt by governments in the Southeast Asian region, which are vulnerable to cyber threats. As one of the countries in this region, Indonesia sees that cyber threats are detrimental to its own country and other countries. Through the role performance approach, which is based on ego's conception, which is in the form of Indonesia's vision and mission towards cybersecurity and alters prescription, which is in the form of how intergovernmental organizations work, giving rise to roles such as being the initiator. With ASEAN, Indonesia conveyed various ideas to improve the security protection of personal data and cyberattacks or threats from an entity. However, this is still not enough to increase a substantial role in the Asia Pacific region because, in reality, there are still many Southeast Asian countries that still do not meet the standards. So, apart from being an initiator, Indonesia can play its role as a cyber protector in the Southeast Asian region. This is done by increasing bilateral relations through diplomacy, increasing investment and opening digital-based businesses, and providing guidance for maintaining cybersecurity by increasing Confidence-Building Measures and Capacity

building with other countries in ASEAN. To create an order of norms and rules that are intrinsic between Indonesia and the countries of the Southeast Asian region.

In the process, Indonesia faced several challenges. Like the case where BSSN as an Indonesian cyber institution only plays a coordinating role, the most basic thing that BSSN should do is formulate strategic policies regarding cyber security and its response and also standardize cyber security regulations. In the work scheme owned by BSSN, there is also no security consulting industry sector. The consulting industry plays a very important role with its technological capabilities and very adequate human resources. BSSN only carries out a consultative function with consulting companies to monitor the cyber ecosystem in the hope of creating security, cyber defense, and system recovery if at any time a cyberattack occurs. This is also a challenge for Indonesia in the absence of government regulations through BSSN that can take action like cyber agencies in other countries. However, despite this, Indonesia is still trying to improve and is optimistic that it can become a cyber protector in ASEAN. This is demonstrated by the position of BSSN which is a cyber institution under the coordination of the president and allows it to obtain a mandate to take action against cyber cases.

Indonesia, as the country with the most internet users in Southeast Asia, is expected to be able to position itself as a cyber protector, previously only as an initiator in Southeast Asian forums discussing cyber security, this is because it can carry out Indonesia's national interests in improving the quality of cyber security education and training. or the development of an innovative and trustworthy cyber security system in ASEAN countries in building collective cyber security that can work. The concept of non-interference which, if the consensus agrees regarding cyber security, is still not implemented well at the national level. This is a reflection of every decision and discussion made at the ASEAN Summit session, this occurs because of the diversity of countries' economic development which tends to be high and ultimately has an impact on the country's maturity in sectoral development information and communication technologies (ICT). Apart from that, the policies pursued by ASEAN countries are greatly influenced by the presence of large powers such as the United States and China, especially in the development of cybersecurity.

Limitations or weaknesses in research lie in the research process. Researchers realize that in a study there are bound to be many obstacles. One of the factors that is an obstacle in this research is the scale of the research. The limitation of this research is that it only discusses regional scale. Then it only arises from Indonesia's role in Southeast Asia in ASEAN. Meanwhile, Indonesia could have a more important role in its relations with other countries bilaterally and multilaterally. Based on the conclusions outlined, several recommendations can be made regarding cyber security. Indonesia as the largest internet user in Southeast Asia should be able to take a bigger role in maintaining cybersecurity in ASEAN, such as a cyber protector to improve critical infrastructure in Indonesia in building better cyber security and building trust in ASEAN by establishing cooperation to strengthen cyber diplomacy and transfer of technology.

REFERENCES

Abdullin, A. I., Davletgildeev, R. S., & Kostin, S. A. (2020). Organization for Defense and Cooperation in The Field of Collective Cyber Security in Europe. *Utopia y Praxis Latinoamericana*, *25*(12), 130–136. https://doi.org/10.5281/zenodo.4280100

Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology*, *15*(1), 79–94. https://doi.org/10.5281/zenodo.4766534

ASEAN. (2008). Piagam Perhimpunan Bangsa-Bangsa Asia Tenggara. Retrieved April 24, 2024, from https://www.asean.org/wp-content/uploads/images/archive/AC-Indonesia.pdf

Aulianisa, S. S., & Indirwan, I. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. *Lex Scientia Law Review*, *4*(1), 31–45. https://doi.org/10.15294/lesrev.v4i1.38197

Betz, D. J., & Stevens, T. (2011). Chapter One: Power and Cyberspace. *Adelphi Series*, *51*(424), 35–54. https://doi.org/10.1080/19445571.2011.636954

Bueger, C., Edmunds, T., & Mccabe, R. (2021). *Capacity Building for Maritime Security the Western Indian Ocean Experience*. New York: Springer International Publishing.

Buzan, B., Wæver, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. London: Lynne Rienner Publisher.

CCB. (2021). Cybersecurity Strategy Belgium 2.0 2021-2025. Retrieved January 23, 2024, from https://ccb.belgium.be/sites/default/files/ccb_strategie 2.0_uk_web.pdf

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles: Sage.

Crypto Agency and Regulation of the National Cyber and Crypto Agency Number 6 of 2021 concerning the Organization and Working Procedures of the National Cyber and Crypto Agency. (2021).

CSA Singapore. (2024). Cybersecurity Act. Retrieved January 23, 2024, from https://www.csa.gov.sg/legislation/cybersecurity-act

Dai, C.T., & Gomez, M. A. (2018). Challenges and Opportunities for Cyber Norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217–235. https://doi.org/10.1080/23738871.2018.1487987

Dai, C. T., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy*, *3*(2), 217–235. https://doi.org/10.1080/23738871.2018.1487987

Egloff, F. J., & Shires, J. (2022). Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies*, *7*(1), 1–18. https://doi.org/10.1093/jogss/ogab028

Fransiska, F. B., & Tobing, F. B. L. (2023). Securing Indonesia Cyber Space: Strategies for Cyber Security in the Digital Era. *Jurnal Studi Sosial Dan Politik*, *7*(1). https://doi.org/10.15294/lesrev.v4i1.38197

Gati, R. A., Rizki, M., & Posumah, R. Y. (2020). Artificial Intelligence and Indonesia Government Cyber Security Strategies. *International Conference on Public Organization*.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Melalui Badan Siber dan Sandi Negara. *Jurnal Dinamika Global*, *7*(2), 295–316. https://doi.org/10.36859/jdg.v7i02.1187

Hare, F. (2015). The Cyber Threat to National Security Why Can't We Agree. In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings* (pp. 211–226). Tallinn: CCD COE Publications. Retrieved from https://ccdcoe.org/uploads/2018/10/hare-the-cyber-threat-to-national-security-why-cant-we-agree.pdf

Holsti, K. J. (1970). National Role Conceptions in the Study of Foreign Policy Introduction. *In International Studies Quarterly*, *14*, 233–242. https://doi.org/10.2307/3013584

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society*, *33*(2), 224–242. https://doi.org/10.1080/13600826.2019.1569502

Intan, A. A., & Intan, R. (2023). Case Study: A Review of Cybersecurity Policies and

Challenges in Indonesia. In *International Conference on Intelligent Computing & …* (pp. 266–273). Springer. https://doi.org/10.1007/978-3-031-50327-6_28

International Telecommunication Union. (2020). Global Cybersecurity Index. Retrieved April 27, 2023, from https://www.itu.int/en/itu-d/cybersecurity/pages/global-cybersecurity-index.aspx

Iswardhana, M. R. (2021). Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia. *Journal of Islamic World and Politics*, *5*(2), 342–367. https://doi.org/10.18196/jiwp.v5i2.12242

Juncker, J.-C. (2017). Building Strong Cyber Security in the European Union. Retrieved April 20, 2023, from https://www.cyberwatching.eu/sites/default/files/building%20strong%20cybersecurity%20in%20the%20european%20union.pdf

Kaburuan, E. D., & Damayanti, A. (2022). The Effectiveness of Indonesian National Police Strategy in Cybercrime Eradication through ASEAN Ministerial Meeting on Transnational Crime (AMMTC). *International Journal of Social Science And Human Research*, *5*(8), 3649–3661. https://doi.org/10.47191/ijsshr/v5-i8-42

Kateryna. (2022). The Geography of Cybersecurity: Cyber Threats and Vulnerabilities. Retrieved May 26, 2023, from Intersog website: https://intersog.com/blog/geography-of-cyber-security/

Kim, Y. K., Go, M. H., Kim, S., Lee, J., & Lee, K. (2023). Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis. *Journal of Internet Technology*, *24*(2), 495–505. https://doi.org/10.53106/160792642023032402031

Kostyuk, N., & Gartzke, E. (2023). Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review*, *5*(3), 113–126. http://dx.doi.org/10.26153/tsw/42073

Kurta, N. C. L. (2023). *Cyber Security Stagnation in Indonesia and the Philippines: a Comparative Case Study of their Strategies*. (Thesis). Univerzita Karlova, Prague. Retrieved from http://hdl.handle.net/20.500.11956/187342

Law Number 11 of 2008 concerning Information and Electronic Transactions, (2008).

Llewellyn, A. (2022). Bjorka, the Online Hacker Trying To Take Down the Indonesian Government. Retrieved January 23, 2024, from The Diplomat website: https://thediplomat.com/2022/09/bjorka-the-online-hacker-trying-to-take-down-the-indonesian-government/

Lynch, M., Mcallister, J., Hurst, W. J., Gallagher, J. T., Sasdi, A., & Chow, J. T. (2005). ASEAN Counterterrorism Cooperation Since 9/11. *Asian Survey*, *45*, 302–321. https://doi.org/10.1525/as.2005.45.2.302

Marwan, A., Jiow, H. J., & Monteiro, K. (2022). Cybersecurity Regulation and Governance During the Pandemic Time in Indonesia and Singapore. *International Journal of Global Community*, *5*(1), 13–32. Retrieved from https://journal.riksawan.com/index.php/IJGC-RI/article/view/109

National Cyber and Crypto Agency Regulation Number 2 of 2024 concerning Cyber Crisis Management, (2024).

National Cyber and Crypto Agency Regulation Number 5 of 2020 concerning the Strategic Plan of the National Cyber and Crypto Agency for 2020-2024, (2020).

National Cyber and Crypto Agency Regulation Number 8 of 2023, (2023).

National Cyber Security Index. (2023). Archived data from 2016-2023 Indonesia. Retrieved January 23, 2024, from https://ncsi.ega.ee/ncsi-index/

Novitasari, I. (2017). Babak Baru Rezim Keamanan Siber di Asia Tenggara Menyosong

ASEAN Connectivity 2025. *Jurnal Asia Pasific Studies*, *1*(2), 220–233. https://doi.org/10.33541/japs.v1i2.624

Nugraha, L. K., & Putri, D. A. (2016). Mapping the Cyber Policy Landscape: Indonesia. In *London: Global Partners Digital*. Retrieved from https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf

Oosthoek, K., & Doerr, C. (2020). Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and Counterintelligence*, *34*(2), 300–316. https://doi.org/10.1080/08850607.2020.1780062

Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy*, *4*(2), 216–234. https://doi.org/10.1080/23738871.2019.1627476

Presidential Decree number 28 of 2021 concerning the National Cyber, (2021).

Presidential Regulation Number 47 of 2023 concerning National Cyber Security Strategy and Cyber Crisis Management, (2023).

Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure, (2022).

Rahardjo, B. (2018). The State of Cybersecurity in Indonesia. In E. Jurriens & R. Tapsell (Eds.), *Digital Indonesia Connectivity and Divergence* (pp. 110–124). ISEAS–Yusof Ishak Institute.

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Regulation of the Minister of Communication and Informatics Number 20 of 2016, (2016).

Rivera, J. (2015). Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. In M.Maybaum, A.-M.Osula, & L.Lindström (Eds.), *7th International Conference on Cyber Conflict* (pp. 7–25). Tallinn: NATO CCD COE Publications.

Rizki, M. (2021). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politea*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. *Journal of Government Science (GovSci)*, *1*(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Saputri, D. P., Surryanto D. W., & Helda Risman. (2020). The Indonesian Cyber Diplomacy: ASEAN-Japan Online Cyber Exercise. *Technium Social Sciences Journal*, *9*, 453–464. https://doi.org/10.47577/tssj.v9i1.911

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 157–178. Retrieved from https://scholar.ui.ac.id/en/publications/strategi-badan-siber-dan-sandi-negara-bssn-dalam-menghadapi-ancam

World Economic Forum. (2022). Global Cybersecurity Outlook 2022. Retrieved April 20, 2023, from https://www3.weforum.org/docs/wef_global_cybersecurity_outlook_2022.pdf