Volume 4 Number 2, July-December 2022: pp. 79-86.
Department of International Law, Faculty of Law, Universitas Lampung, Bandar Lampung, Indonesia.
p-ISSN: 1978-5186 E-ISSN: 2723-2603
http://jurnal.fh.unila.ac.id/index.php/lajil

ASEAN's ROLE IN CYBERSECURITY MAINTENANCE AND SECURITY STRATEGY THROUGH AN INTERNATIONAL SECURITY APPROACH

Khotimah Estiyovionita[1], Afandi Sitamala[2]
[1]Untirta Center of International Legal Studies (UCILS), Indonesia, E-mail : khotimahesti8@gmail.com
[2]Untirta Center of International Legal Studies (UCILS), Indonesia, E-mail: asitamala@untirta.ac.id

Submitted: Apr 05, 2022; Reviewed: Aug 08, 2022; Accepted: Sept 28, 2022.

Article Info

Keywords:
ASEAN, Cybersecurity, Cooperation.

DOI:
10.25041/lajil.v4i2.2556

Abstract

The development of information and communication technology allows easier interactions regardless of time, space, and distance. The borderless cyberspace and option to be anonymous are factors that can increase the criminal rates through cyberspace. Therefore, laws, regulations and international cooperation among nations need to be established. ASEAN is the forum of regional organizations that has successfully made the efforts to encourage cybersecurity enhancement through various programs. Stronger cooperation among the member nations will further strengthen cybersecurity in the region to maintain the safety and security of the nations.

A. Introduction

The digitalization accustomed the community to computerized activities on smartphones, laptops, computers, and even internet of things (IoT) devices. The development of information and communication technology enables easier access to communication regardless of time, space, and distance within cyberspace.[1]

Cyberspace is not limited by regional boundaries (borderless), where people can opt for not to reveal their identity (anonymous). The anonymity in some extent opens the potential of criminal activities on the cyberspace referred to as cybercrime. *Cybercrime* is an unlawful act of using information and communication technology targeted at networks, systems, data, websites, and technologies.[2] Cybercrime is also connected to digital communication networks, thereby cybercrimes are challenging to handle. To overcome this problem, it is necessary to have laws and regulations related to cybercrime as a means of prevention.[3]

[1] Wasisto Raharjo Jati, "Cyberpsace, Internet dan Ruang Publik Baru: Aktivisme Online Politik Kelas Menengah Indonesia", Jurnal Pemikiran Sosiologi Vol. 3 No. 1, Januari 2016, p. 26.
[2]UNODC, "University Module Series: Cybercrime", February 2020, https://www.unodc.org/e4j/en/cybercrime/module- 1/key-issues/cybercrime-in-brief.html, diakses pada 7 September 2022.
[3] Khanisa, "A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation", Journal of ASEAN Studies, Vol.1 No.1 (2013), p. 41–42.

Criminals often set regions with certain level of vulnerability as their targets. International Telecommunication Union (ITU) report entitled Global Cybersecurity Index (GCI) in 2020 showed that Singapore ranked first in the level of cybersecurity in Southeast Asia with a score of 98.52, followed by Malaysia with 98.06, Indonesia with 94.88, Viet Nam with 94.59, Thailand with 86.5, Philippines with 77, Brunei Darussalam with 56.07, Myanmar with 36.41, Lao P.D.R. with 20.34, and Cambodia with 19.12.[4] This index was measured based on five main components; legal, technical, organizational, capacity development, and cooperation measures. Therefore, ASEAN member states need to improve the quality of each component.

ATKearney found that ASEAN countries, especially Indonesia, Malaysia, and Vietnam, are at risk of becoming the main targets of suspicious web activity blockage. The regulatory framework for cybersecurity management and capabilities within ASEAN is notably deficient, exacerbated by the limited expertise in human resources across member states. Additionally, the awareness among corporations and stakeholders about the significance of cybersecurity is minimal, often not recognized as a business priority, which impedes comprehensive and holistic approaches to enhancing cyber resilience. In the era of digitalization, where data and information are predominantly stored in digital formats, ensuring data privacy and security becomes paramount for any organization.[5] This scenario underscores the pressing need for stronger regulatory measures and an increase in awareness, aiming to address the cybersecurity challenges effectively and safeguard digital assets in a world increasingly reliant on digital infrastructures.

Weak control over cybercrime in the ASEAN negatively impacts the region's stability, especially in terms of the economic growth. ASEAN region has a combined GDP of more than USD 3.11 trillion, making it one of the seventh-ranked largest markets in the world. ASEAN is also regarded the most populous market in the world with a total population 663.47 million.[6] In addition, ASEAN's potential in the digital economy in 2025 is predicted to increase of up to 1 trillion dollars with stronger development of digital services such as the financial and commercial sectors.[7] Cybersecurity experts project the net cost of cybercrime to grow by 15 percent per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015.[8]

In today's digital era, the importance of immediate response to cybersecurity risks cannot be overstated since it can threaten national stability. The strength of a nation is multifaceted, extending beyond the size of its economy and military. It also encompasses the values it contributes to the global stage, among which technological proficiency stands out. This perspective is shared by Muhamad Rizal and Yanyan M. Yani in the Journal of ASEAN Studies, where they argue that a nation's power is not solely defined by its economic scale or military strength. Instead, it also involves the values it presents to the world, including its command of technology. [9]

Since cybercrime is a transnational crime, a cooperation of law, politics, and security, as well as an increase in cybersecurity facilities are important to minimize the losses.[10] Hence,

[4] International Telecommunication Union (ITU), "Global Cybersecurity Index 2020", p. 25-27.

[5]Kristiani Virgi Kusuma Putri, "Kerjasama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime", Malang: FH Universitas Brawijaya, Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.2. No.7 (2021).

[6] James Tan et al., "ASEAN Cyberthreat Assessment 2021", p.10.

[7] Trisa Monika Tampubolon dan Rizki Ananda Ramadhan, "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara", Padjadjaran Journal of International Relations (PADJIR) Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197, p.272.

[8] James Tan et al., *Loc.Cit,* p. 8.

[9] Muhamad Rizal, Yanyan M. Yani, "Cybersecurity Policy and Its Implementation in Indonesia", Journal of ASEAN Studies, Vol. 4, No. 1 (2016), pp. 61-78, 2016 by CBDS Bina Nusantara University and Indonesian Association for International Relations ISSN 2338-1361 print / ISSN 2338-1353 electronic.

[10] Bima Yudha Wibawa Manopo, Diah Apriani Atika Sari, "ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region", Belli ac Pacis. Vol. 1. No.1 Juni 2015.

the multilateral approach emerges as an effective solution, as evidenced by the outcomes of the III C 2000 Millennium Congress and the United Nations Congress on the Prevention of Crime and the Treatment of Offenders. These gatherings highlight the necessity of international cooperation among countries worldwide to prevent and combat cybercrime, underscoring the importance of collective efforts to tackle this transnational challenge.[11]

Based on the background that has been stated, a research problem was proposed; How is ASEAN's strategy in dealing with cybercrime in the region? Literatures relevant to cybercrime were analyzed.

B. Discussion

The Association of Southeast Asian Nations (ASEAN) is a regional cooperation organization in the Southeast Asian region founded on August 8, 1967. ASEAN was established to maintain world peace and safety in the Southeast Asian region.[12] Currently, ASEAN consists of 10 countries: Indonesia, Malaysia, Singapore, Thailand, the Philippines, Brunei, Vietnam, Laos, Myanmar, and Cambodia. ASEAN has three pillars which include the ASEAN Political-Security Community (APSC), the ASEAN Economic Community (AEC), and the ASEAN Socio-Cultural Community (ASCC).[13] The discussion about cybersecurity intersects with one of the ASEAN pillars, APSC. APSC allows ASEAN member states to make more effective coordination in solving the region's global challenges and threats.

Global challenges and threats related to security need to be promptly addressed. particularly in the context of the Information and Communications Technology (ICT) sector's development within ASEAN. The ASEAN ICT Master Plan in 2011 contains details about the target related to ICT development set by ASEAN. ASEAN has made considerable progress in the development of its ICT sector by incorporating ICT development as one of the connectivity aspects in its current master plan for the building of ASEAN Community 2015, encompassing physical, institutional, and people-to-people connectivity with ICT as an integral part of physical connectivity.[14] However, such development needs to be balanced with establishing robust cybersecurity.

Cyber security has been set as one of the priorities in ASEAN region, especially after the Covid-19 pandemic which get the community adapted to digitalized era. One of ASEAN's objectives is stipulated in Article 1 of the ASEAN Charter, which states the necessity to maintain and enhance peace, security, and stability and further strengthen peace-oriented values in the Region. Concerning cybersecurity, Piet Hein van Kempen stated that security may be described as freedom from threat, danger, vulnerability, menace, force, and attack.[15]

Furthermore, according to Lucas Kello, cybersecurity has mechanisms for protecting computer operating systems from threats of danger. Therefore , cybersecurity is a condition when no illegal intrusion breaks into computer systems.[16] Research conducted by the ASEAN Desk highlights a number of prominent cyber threats for 2020 and the subsequent years, including:

---

[11] Bima Yudha Wibawa Manopo, Diah Atika Sari, "ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region", Belli ac Pacis. Vol. 1. No. 1 Juni 2015.
[12] Ahmad Syofyan, Achmad Gusman Siswandi, et al., "ASEAN Court of Justice: Issues, Opportunities and Challenges Concerning Regional Settlement Disputes", Journal of Legal, Ethical and Regulatory Issues, Volume 24, Issue 1, 2021, p. 1.
[13] ASEAN Political-Security Community Blueprint, 2009, p.1.
[14] Khanisa, "A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation", Journal of ASEAN Studies, Vol.1,No.1 (2013), p. 43.
[15] Piet Hein van Kempen, "Four Concepts of SecurityçA Human Rights Perspective", Human Rights Law Review 13:1(2013), 1-23, doi:10.1093/hrlr/ngs037, Downloaded from http://hrlr.oxfordjournals.org/ at Universidad de Costa Rica on July 15, 2013.
[16] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", International Security, Vol. 38, No. 2 (Fall 2013), pp. 7–40, doi:10.1162/ISEC_a_00138

1. *Business E-mail Compromise* is a mode of fraud by posing as the victim's business partner company and aiming to obtain funds that should be directed to the actual business partner company.
2. *Phishing* is an attempt to obtain information about someone's data by phishing techniques. The data targeted for phishing are personal data (name, age, address), account data (username and password), and financial data (credit card information, accounts).
3. *Ransomware* can be defined as a mass extortion of personal data or information stolen to seek profit from the victim in the form of money.
4. *E-commerce data interception* is a threat to confidentiality in the form of information intercepted so that people who are not entitled can access the computer where the information is stored.
5. *Crimeware-as-a-Service* (CaaS) is malware software that encrypts files and documents from one of the computers to the entire network. The perpetrator will ask the victim for a ransom to be able to access the network that has been taken over again. Spyware, phishing kits, browser hijackers, keyloggers, and more are available to attackers through CaaS.
6. Cyber scams are fraudulent schemes by using fake websites to steal personal information and misuse it.
7. Cryptojacking is a type of cybercrime in which hackers use the victim's device secretly to take advantage of cryptocurrencies.

In general, ASEAN member states have devised specific strategies for improving cybersecurity, such as implementing cybersecurity policies and laws to enhance innovation and the economy while protecting the personal information and privacy of their citizens.

Indonesia is an ASEAN member state which stipulated information security in cyberspace into Law No. 11 of 2008 concerning Information and Electronic Transactions. This law is the foundation of the formulation of regulations and policies related to information security. The protection of personal data and privacy are also regulated in Ministerial Regulation No. 20 of 2016 which has been passed by House of Representatives by September 22 2020[17] In addition, the Indonesian government also established a National Cyber and Encryption Agency (BSSN) responsible for preventing cyber-attacks and responding with an urgent strategy.

Singapore has also made efforts to improve cybersecurity through various programs. In 2005, Singapore launched its Cybersecurity Masterplan followed with Infocom Security Masterplan in 2007, and the National Cyber Security Masterplan and the National Cyber Security Research and Development Program in 2013. In 2013, Singapore pioneered the establishment of the National Cyber Security Center, which was established as a central body to supervise and coordinate all aspects of cybersecurity for the nation. In 2015, a Cyber Security Agency was formed and in 2017 Singapore amended the existing Computer Abuse and Cybersecurity Act to address the increasing scale and transnational nature of cybercrime.[18] A comprehensive approach to improving cybersecurity in Singapore is reflected in the renewal of the National Cyber Security Master Plan, Cyber Watch Centre, and Threat Assessment Centre. Singapore established Cyber Security Agencies (CSAs) in all sectors as private and public partners.

Malaysian government has set a series of development plans. The National Security Emergency Response Centre (NISER) was established in 2006 to implement the National Cyber Security Policy (NCSP) policy in order to make Malaysia's IT System "safe, resilient and

[17] Jirapon Sunkpho et al., "Cybersecurity Policy in ASEAN Countries", Information Institute Conferences, Las Vegas, NV, March 2018, p. 3.

[18] Muhammad Fikry Anshori, Rizki Ananda Ramadhan, "Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week", Padjadjaran Journal of International Relations Vol. 1 No. 1, Mei 2019, p. 38, doi: 10.24198/padjir.v1i1.21591.

independent." The name NISER was then revised as Cyber Security Malaysia which works under the Ministry of Science, Technology, and Innovation (MOSTI).[19] Malaysia implements the eight procedures in the National Cyber Security Framework which consists of regulation and control, technology, and cooperation between public-private, institutional as well as worldwide aspects.[20] In addition, Malaysia has been actively engaged in organizing various programs, such as the Cyber Security Awareness. Considering the need for a forum to accommodate aspirations related to cybersecurity issues, the Malaysian government also provides email hotlines at (cyber999@cybersecurity.my) to help local Law Enforcement Agencies to maintain its cybersecurity.[21]

Another significant challenge in addressing cybercrime is its global nature, underscoring that no single nation can effectively combat this issue in isolation. International cooperation is indispensable for mitigating and controlling cybercrimes before they escalate beyond manageability. Given the multi-jurisdictional nature of cybercrime, there's a pressing need for enhanced collaboration, particularly in leveraging the latest technological advancements. It is crucial for each ASEAN member state to prioritize the development of preventive measures against cybercrime.

1. ASEAN's Step in Managing Cybersecurity

To date, cybercrime has been handled based on bilateral relations with limited implementation. Bilateral relations represent a traditional approach, wherein the concept of security is primarily understood in geopolitical terms, focusing on the dynamics between nations, particularly in contexts involving nuclear capabilities and military strategies. In essence, traditional security frameworks are centered around threats to the state, emphasizing external physical threats. International cooperation can enhance cybersecurity[22] which will emerge more initiatives. Therefore, problems that arise in the enforcement of cyber incidents should never be ignored. [23]

According to the Coordinating Minister for Political, Legal, and Security Affairs of Indonesia, Wiranto, in the 6th Meeting of Attorneys General /Ministers of Justice and Minister of Law on the Treaty on Mutual Legal Assistance in Criminal Matters (Among Like-Minded ASEAN Member Countries) stated that the eradication of transnational criminal acts must be carried out immediately by every nation.[24] Failing to address these concerns can severely undermine the political process, compromise security, endanger society, disrupt economic development, and obstruct the governance of otherwise stable nations.[25] International Law regulates the behavior of international actors and in the development or dissemination of

[19] Jirapon Sunkpho et al., *Loc.Cit*, p. 3-4.
[20] Azian Ibrahim, Noorfadhleen Mahmud, et al., "Conference Paper: Cyber Warfare Impact to National Security - Malaysia Experiences", FGIC 2nd Conference on Governance and Integrity 2019, KnE Social Sciences, p. 211.
[21] Trisa Monika Tampubolon, Rizki Ananda Ramadhan, "Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week", Padjadjaran Journal of International Relations Vol. 1 No. 3, Januari 2020, doi: 10.24198/padjir.v1i3.26197 p. 219.
[22] Bedriansyah Zaini "Transformasi Keamanan Internasional", 30 Sep 2020, https://news.detik.com/kolom/d-5194202/transformasi-keamanan-internasional., diakses pada 15 November 2021
[23] Ian Yuying Liu, "State Responsibility and Cyber Attacks Defining Due Diligence Obligations", IV Indonesian Journal of International & Comparative Law 191-260 (April 2017) ISSN: 2338-7602; E-ISSN: 2338-770X http://www.ijil.org
[24] Afandi Sitamala, "Indonesia as Non-Permanent Member of United Nations Security Council, Guarding the Peace and Stability in ASEAN," *Lampung Journal of International Law* 2, no. 2 (August 13, 2020): 97–102, https://doi.org/10.25041/lajil.v2i2.2037.
[25] Kementerian Hukum Dan Hak Asasi Manusia Republik Indonesia, Menkopolhukam Ajak Negara ASEAN Tingkatkan Kerjasama MLA dalam Masalah Pidana, https://portal.ahu.go.id/id/detail/75-berita-lainnya/2234-menkopolhukam-ajak-negara-asean-tingkatkan-kerjasama-mla-dalam-masalah-pidana, diakses pada 22 September 2022.

emerging technologies in response to the need to protect the international community from excesses, possible disasters, even risks posed by technology.[26]

Upon the awareness of the significance of international cooperation, ASEAN can determine the role of each member state. For instance, the ASEAN Charter binds member states to provide legal status and institutional framework to compile values and regulations to set targets for ASEAN to present accountability and fulfillment. Upon recognizing ASEAN's critical role in the region, a question regarding the challenges faced by ASEAN in handling cybersecurity arises. Through analyses of various regional issues, it becomes apparent that challenges originate both within the ASEAN framework and from external sources, particularly in coordinating problem-solving efforts. The inconsistency of member states in implementing the framework appears as a major inhibiting factor. On the other hand, external challenges are increasingly complex, especially regarding transnational crimes.[27]

The commitment to maintaining cybersecurity in ASEAN has been discussed at several meetings, including the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications Regulators Council (ATRC), ASEAN Senior Officials Meeting on Transnational Crime (SOMTC), Senior dan Officials Meeting on Social Welfare and Development (SOMSWD). In addition, Cybersecurity Maintenance and Security Strategy within the framework of multilateral cooperation are explained in the ASEAN Regional Forum (ARF) through the ASEAN Political-Security Community (APSC) blueprint in Sub Chapter B.4.1. The chapter explains the agreement to increase cooperation in non-traditional threats, specifically addressing transnational and cross-border crime issues. The discussion on Cybercrime is presented in Article XVII.[28] In this regard, in 2006, ARF established ARF on cybersecurity initiatives related to the discussion of Cybercrime in ASEAN, which was then outlined in ASEAN's Cooperation on Cybersecurity and against Cybercrime.

The ASEAN Regional Forum (ARF) was established in 1994 to encourage constructive dialogue and consultation on political and security issues of common concern and interest, as well as positively contribute to confidence building and preventive diplomacy in the Asia-Pacific region.[29] In this context, the approach to security cooperation by the North Atlantic Treaty Organization (NATO), which is often associated with the use of military force, presents a stark contrast. At the same time, the ARF tends to set up dialogue and engagement as a way of preventing conflicts in the region.[30]

The ARF on cybersecurity initiatives is part of ASEAN's mechanism in dealing with cybercrime as stipulated in ASEAN's Cooperation on Cybersecurity and against cybercrime. The ARF on cybersecurity initiatives was first implemented in 2006 through a joint statement at a meeting in Malaysia and was reaffirmed in the ARF Statement on Cooperation in Ensuring Cyber Security in Phnom Penh on 12 July 2012. The statement was then implemented in the form of various training at the regional level, focusing on how a nation should respond and coordinate to cyber incidents.[31]

Follow up international meetings were held afterwards, including such as the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC), the ASEAN Ministerial Conference on Cybersecurity (AMCC), and the ASEAN Telecommunications and IT Ministers Meeting (TELMIN). ASEAN

[26] Emmy Latifah, Moch Najib Imanullah, "The Roles of International Law on Technological Advances", Brawijaya Law Journal Vol.5 No 1 (2018): Culture and Technological Influence in Regulation, DOI: http://dx.doi.org/10.21776/ub.blj.2018.005.01.07.
[27] Suwarti Sari, "Peran Indonesia dalam Implementasi ASEAN Political Security Community", p. 28.
[28] ASEAN Political Security Community (APSC).
[29] Michael Raska, Benjamin Ang, "Cybersecurity in Southeast Asia", Paris: Asia Centre & DGRIS, 2018, p. 2.
[30] David Putra Setyawan, Arwin Datumaya Wahyudi Sumari, "Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives", Jurnal Penelitian Politik Volume 13 No. 1 Juni 2016, p. 4.
[31] *Ibid*, p. 5.

SOMTC aims to implement the Comprehensive Partnership between ASEAN and the United Nations. On November 19, 2011, ASEAN leaders and the UN Secretary met to discuss the Joint Declaration in Bali, Indonesia. Regional meetings were also held to enhance ASEAN's capacity in addressing the growing number of cyber threats in the ASEAN region.

The ASEAN Ministerial Conference on Cybersecurity (AMCC) was held in Singapore on October 11, 2016. Singapore held the ASEAN Cyber Capacity Program to improve the capacity of ASEAN member countries in handling with cyber security issues. To address these challenges, ASEAN has established four key mechanisms focusing on aspects of cybersecurity and cybercrime: the ASEAN Ministerial Meeting on Transnational Crime (AMMTC); ASEAN Telecommunications and IT Ministers Meeting (TELMIN); the ASEAN Regional Forum (ARF), and the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC). The implementation commenced from analyzing regional news and issues in various ASEAN forums to establish cooperation in transnational crime, including cybercrime. SOMTC then implements the AMMTC plan.[32]

The ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICT), dated May 7, 2015, outlines a series of objectives aimed at fostering a peaceful, secure, open, and collaboratively beneficial ICT milieu. Through the implementation of this work plan, the goals include enhancing trust among ARF member states and bolstering their capacity, thereby preventing conflicts and crises. In its development through the ARF, ASEAN continues to follow up on cybersecurity cooperation using international global with China, Japan, the European Union, the United States, Australia, Canada, India, New Zealand, Russia, and South Korea to help ASEAN cooperation strengthen the country's security against the dangers of cyber aggression. Several goals have been outlined to promote a peaceful, safe, open, and mutually cooperative ICT environment and to prevent conflicts and crises by developing trust between ARF member states and capacity building. Through the ARF, ASEAN persistently pursues cybersecurity collaboration by engaging with global partners including China, Japan, the European Union, the United States, Australia, Canada, India, New Zealand, Russia, and South Korea. This international cooperation aims to bolster the security of ASEAN countries against the threats of cyber aggression.

C. Conclusion

ASEAN serves as a pivotal platform for its member states to collaborate towards achieving cybersecurity. To enhance its collective cyber resilience effectively, ASEAN needs to fortify its overarching frameworks and action plans collaboratively developed. Member states need to be actively engaged in generating positive advancement in cybersecurity. Moreover, collaboration with nations like Japan, China, the United States, and others goes beyond simple agreements, encompassing a comprehensive evaluation of the essential elements needed to enhance cybersecurity resilience across ASEAN. Considering that cyber challenges are a relatively new area of concern for ASEAN, it is crucial to undertake extra efforts to ensure the participation of all member states in these cybersecurity initiatives.

REFERENCES

Afandi Sitamala, "Indonesia as Non-Permanent Member of United Nations Security Council, Guarding the Peace and Stability in ASEAN," Lampung Journal of International Law 2,

[32] AH Kannaby, "Prospek Implementasi Asean Cybersecurity", https://repository.unair.ac.id/102829/4/4.%20BAB%20I%20PENDAHULUAN.pdf, 2020.

no. 2 (August 13, 2020): 97–102, https://doi.org/10.25041/lajil.v2i2.2037.
ASEAN Political-Security Community Blueprint, 2009.

Anshori, Muhammad Fikry, Rizki Ananda Ramadhan, "Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week", Padjadjaran Journal of International Relations Vol. 1 No. 1 (2019): 39-52. doi: 10.24198/padjir.v1i1.21591.

Ibrahim, Azian, Noorfadhleen Mahmud, et al., "Cyber Warfare Impact to National Security - Malaysia Experiences", Conference Paper: FGIC 2nd Conference on Governance and Integrity 2019, KnE Social Sciences. doi: 10.18502/kss.v3i22.5052.

International Telecommunication Union (ITU), "Global Cybersecurity Index 2020".

Jati, Wasisto Raharjo "Cyberpsace, Internet dan Ruang Publik Baru: Aktivisme Online Politik Kelas Menengah Indonesia", Jurnal Pemikiran Sosiologi Vol. 3 No. 1 (2016): 25-35. https://doi.org/10.22146/jps.v3i1.23524

James Tan et al., "ASEAN Cyberthreat Assessment 2021", https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia.

Kannaby, Ahmad Haibat. Prospek Implementasi Asean Cybersecurity Cooperation Strategy Dalam Menghadapi Ancaman Keamanan Siber Di Asia Tenggara. 2020.

Kello, Lucas "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", International Security, Vol. 38, No. 2 (2013):7–40, doi:10.1162/ISEC_a_00138

Kementerian Hukum Dan Hak Asasi Manusia Republik Indonesia, Menkopolhukam Ajak Negara ASEAN Tingkatkan Kerjasama MLA dalam Masalah Pidana, https://portal.ahu.go.id/id/detail/75-berita-lainnya/2234-menkopolhukam-ajak-negara-asean-tingkatkan-kerjasama-mla-dalam-masalah-pidana, diakses pada 22 September 2022.

Kempen, Piet Hein van "Four Concepts of SecurityçA Human Rights Perspective", Human Rights Law Review 13:1(2013): 1-23, doi:10.1093/hrlr/ngs037.

Khanisa, "A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation", Journal of ASEAN Studies, Vol.1 No.1 (2013): 41–53. https://ir.binus.ac.id/files/2013/08/4.pdf.

Latifah, Emmy, Moch Najib Imanullah, "The Roles of International Law on Technological Advances", Brawijaya Law Journal: Culture and Technological Influence in Regulation Vol.5 No 1 (2018): 102–116. http://dx.doi.org/10.21776/ub.blj.2018.005.01.07.

Liu, Ian Yuying, "State Responsibility and Cyberattacks Defining Due Diligence Obligations", IV Indonesian Journal of International & Comparative Law (2017): 191-260.

Manopo, Bima Yudha Wibawa, Diah Apriani Atika Sari, "ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region", Belli ac Pacis. Vol. 1. No.1 (2015): 44-51. https://doi.org/10.20961/belli.v1i1.27366.

Putri, Kristiani Virgi Kusuma "Kerjasama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime", Jurnal Hukum Lex Generalis. Vol.2. No.7 (2021): 542-54. https://doi.org/10.56370/jhlg.v2i7.90.

Rizal, Muhamad Yanyan M. Yani, "Cybersecurity Policy and Its Implementation in Indonesia", Journal of ASEAN Studies, Vol. 4, No. 1 (2016): 61-78.

Tampubolon, Trisa Monika and Rizki Ananda Ramadhan, "ASEAN Personal Data Protection (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara", Padjadjaran Journal of International Relations (PADJIR) Vol. 1 No. 3 (2020): 270-286. doi: 10.24198/padjir.v1i3.26197.

Raska, Michael, Benjamin Ang, "Cybersecurity in Southeast Asia", Paris: Asia Centre & DGRIS (2018): 1-9. https://centreasia.eu/wp-content/uploads/2018/12/NotePrésentation-AngRaska-Cybersecurity_180518.pdf

Sari, Suwarti "Peran Indonesia dalam Implementasi ASEAN Political Security Community", Dinamika Global : Jurnal Ilmu Hubungan Internasional, Vol. 4 No. 01 (2019), 24-65. https://doi.org/10.36859/jdg.v4i01.100.

Setyawan, David Putra, Arwin Datumaya Wahyudi Sumari, "Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives", Jurnal Penelitian Politik Vol. 13 No. 1 (2016): 1-20. https://doi.org/10.14203/jpp.v13i1.250.

Sunkpho, Jirapon, Sarawut Ramjan, Chaiwat Oottamakorn, "Cybersecurity Policy in ASEAN Countries", Information Institute Conferences, Las Vegas, NV (2018): 1-6.

Syofyan, Ahmad, Achmad Gusman Siswandi, Idris, Huala Adolf, "ASEAN Court of Justice: Issues, Opportunities and Challenges Concerning Regional Settlement Disputes", Journal of Legal, Ethical and Regulatory Issues, Volume 24, Issue 1 (2021): 1A-1F. https://www.abacademies.org/articles/ASEAN-court-of-justice-Issues-1544-0044-24-1-632.pdf

University Module Series: Cybercrime", February 2020, https://www.unodc.org/e4j/en/cybercrime/module- 1/key-issues/cybercrime-in-brief.html,.

Zaini, Bedriansyah, "Transformasi Keamanan Internasional", 30 Sep 2020, https://news.detik.com/kolom/d-5194202/transformasi-keamanan-internasional.