Volume 4 Number 2, July-December 2022: pp. 81-90.
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 makes it easier for humans to access everything without being limited by time, space, and distance so that they are connected in one space. Given cyberspace's borderless and anonymous characteristics, it encourages the emergence of criminal activities, namely cybercrime. Therefore, as a measure to prevent future damage, it requires not only regulatory laws and regulations but also international cooperation between countries is needed. These cooperation efforts can be implemented through the forum of regional organizations, namely ASEAN. Until now, many efforts have been made to encourage the improvement of cybersecurity through its various programs. Therefore, it is hoped that this increase in cooperation will further strengthen cybersecurity in the region to maintain security stability.

A. Introduction

The increasingly widespread digitalization era has made the world community increasingly accustomed to computerized activities connected online, which can be seen from the large number of people who access smartphones, laptops, computers, and even internet of things (IoT) devices. The development of information and communication technology makes it easier for humans to access everything without being limited by time, space, and distance so that they are interconnected with each other in one space where these activities are facilitated by media called cyberspace.[1]

The characteristics of cyberspace, among others, are not limited by regional boundaries (borderless), and when communicating between users, they can disguise their identity (anonymous). Given the characteristics of cyberspace, it encourages the emergence of criminal

[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.

activities, namely cybercrime. *Cybercrime* is an unlawful act using information and communication technology targeted at networks, systems, data, websites, and technologies.[2] In addition to being carried out with digital media, cybercrime is also connected to digital communication networks, so connectivity problems make cybercrime more complex to handle. Therefore, as a measure to prevent future damage, it is necessary to have laws and regulations governing cybercrime to prevent it.[3]

Criminals indeed target regions or regions with a certain level of vulnerability. For example, in the ASEAN region, based on the International Telecommunication Union (ITU) report entitled Global Cybersecurity Index (GCI) in 2020, Singapore was ranked first in the level of cybersecurity in Southeast Asia with a score of 98.52, then successively followed by Malaysia 98.06, Indonesia 94.88, Viet Nam 94.59, Thailand 86.5, Philippines 77, Brunei Darussalam 56.07, Myanmar 36.41, Lao P.D.R. 20.34, and Cambodia 19.12.[4] The assessment of this index is based on five main components, including legal, technical, organizational, capacity development, and cooperation measures. So, it should be a common concern for ASEAN member states to improve the quality of each component.

Based on an analysis conducted by ATKearney shows that first, ASEAN countries, especially Indonesia, Malaysia, and Vietnam, are at risk of becoming the main targets of blockade of suspicious web activity; second, weak policy regulation in ASEAN related to management and capabilities in the field of cybersecurity; third, the suboptimal competence of the human resources of each member state; and fourth, the awareness of corporations or stakeholders is still minimal because it has not made it a business priority regarding the dangers posed by weak cybersecurity, so there is no holistic handling of cyber resilience.[5] In addition, cybersecurity is a significant challenge in this era of digitalization because today, we live in a world where data or information is stored in digital form, so data privacy and security will always be a priority for any organization.

The risk of suboptimal handling of cybercrime in the ASEAN region has the potential to negatively impact the region's stability, especially on economic growth. This is considering that the 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 and has a total population of 663.47 million, the third most populous market in the world.[6] In addition, it is considering the results of an analysis from ATKearney in 2018 that ASEAN's potential in the digital economy in 2025 is predicted to reach an increase of up to 1 trillion dollars to the state budget and even continue with the 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]

The current condition is all digital. Suppose the government is not quick to respond to the risks that exist results in the threat of stability of a country. Whereas a nation is said to be strong depends not only on how big the economy or how strong its military is but also on the values it offers to the world, one of which is mastery of technology. Muhamad Rizal and Yanyan M. Yani gave their opinions in the Journal of ASEAN Studies, which read: "A nation's power is

[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.
[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.

neither just about how big the economy is nor how strong the military is. However, it is also about the values it offers to the world, and one of them is its mastery of technology."[9]

Given that cybercrime is a transnational crime and the lack of handling of ASEAN member state governments in handling cybercrime, it reflects that there is a need for cooperation of law, politics, and security, as well as an increase in cybersecurity facilities to minimize the losses that will occur.[10] Therefore, the multilateralism approach is an effective solution, and this is in line with the results of III C 2000 millennium Congress and The Congress UN on The Prevention of Crime and The Treatment of Fugitives Offenders, which emphasizes that to prevent and overcome cybercrime that is transnational crime requires international cooperation efforts between countries in the world.[11]

Based on the background that has been stated, the author formulates a formulation of the problem, namely, how is ASEAN's strategy in dealing with cybercrime in the region? This study's method of approach is the literature review on cybercrime. Sources are obtained using secondary data through research results based on literature research.

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. With the APSC, it is hoped that ASEAN member states can coordinate well in facing the region's global challenges and emerging threats.

One of the global challenges and threats around security that is an essential issue in the region is cybersecurity-related. This issue is inseparable from the development of Information and Communications Technology (ICT) in ASEAN, based on the ASEAN ICT Master Plan in 2011. It contains details about how ASEAN wants to develop its ICT sector. Then in its development, ASEAN has made considerable progress in the development of the ICT sector by incorporating ICT development as one of the connectivity aspects in its current master plan for the building of ASEAN Community 2015, which contains encompasses physical, institutional, and people-to-people connectivity with ICT as an integral part of physical connectivity.[14] However, it turns out that an important aspect is not paid attention to, namely the security aspect, resulting in the fragility of the ICT security system.

Cyber security has become one of the priorities of leaders in the ASEAN region, especially after the disruption caused by the Covid-19 pandemic, which made all elements of society adapt

[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.
[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.

to the era of digitalization because cyber security plays a vital role in the development of a country's stability. This is in line with one of ASEAN's objectives contained in Article 1 of the ASEAN Charter, which aims to maintain and enhance peace, security, and stability and further strengthen peace-oriented values in the Region. Concerning cybersecurity, Piet Hein van Kempen says that: "security may be described as freedom from such phenomena as a 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 can be understood when there is no illegal intrusion into computer systems.[16] Based on the results of research conducted by the ASEAN Desk, several cyber threats stand out in 2020 and beyond, including:

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 ensure the openness of internet platforms to enhance innovation and the economy while maintaining security in cyberspace and protecting the personal information and privacy of their citizens from being misused. For example, in the three countries in ASEAN, firstly Indonesia, to protect information security in cyberspace, issued Law No. 11 of 2008 concerning Information and Electronic Transactions which is the basis for the formulation of regulations and policies related to information security, then related to the protection of personal data and privacy regulated in Ministerial Regulation No. 20 of 2016 which is now Indonesia as of September 20, 2022, the Personal Data Protection Law has been passed by House of Representatives.[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.

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

Furthermore, Singapore has also made efforts to improve cybersecurity through its various programs, which in 2005 began with the launch of planning in the form of a Cybersecurity Masterplan. Infocom Security Masterplan in 2007. Then continuing with the launch of the National Cyber Security Masterplan and the National Cyber Security Research and Development Program in 2013, in the same year also, 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 country. In its development, in 2015, a Cyber Security Agency was formed. Further on its regulatory aspects, 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.

As for the cybersecurity handling measures carried out by the Malaysian government through a series of existing developments, through the National Security Emergency Response Centre (NISER) 2006 was given the power to implement the National Cyber Security Policy (NCSP) policy to make Malaysia's IT System "safe, resilient and independent." Then NISER changed its name to Cyber Security Malaysia was parked under the Ministry of Science, Technology, and Innovation (MOSTI).[19] In its policy implementation, Malaysia implemented 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 is also active in organizing prevention programs, such as the Cyber Security Awareness for Everyone program. Considering the need for a forum to accommodate aspirations related to cybersecurity issues, the Malaysian government also provides email hotlines at (cyber999@cybersecurity.my) in the fight against cybercrime so that this can help local Law Enforcement Agencies.[21]

Nonetheless, another problem in a nation's handling of cybercrime is a global phenomenon. Every country would be unable to fight this crime without the cooperation of the whole world. Cooperation between countries must reduce and control these cybercrimes before they become out of control. In the face of cybercrime of a multi-jurisdictional nature, there must be a quality improvement, especially with the latest technology that continues to increase. It should be of particular concern for each ASEAN member state to prepare preventive measures for cybercrime.

1. ASEAN's Steps in Managing Cybersecurity

So far, cybercrime handling tends to bilateral relations whose implementation is still limited. In this case, it can be understood that the concept of bilateral relations is a traditional approach, so the scope of security is defined by geopolitical terms and limited to relations between countries that intersect with nuclear use and military strategy issues. In summary, traditional security interprets a threat related to the state and physical threats from outside. International cooperation can enhance cybersecurity.[22] Thus, its development will give rise to initiatives, and

[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.
[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

therefore when difficulties arise in the enforcement of cyber incidents, it should not be ignored.[23]

In line with this, according to the Coordinating Minister for Political, Legal, and Security Affairs of Indonesia, Wiranto, on the occasion of 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) the eradication of transnational criminal acts must be carried out immediately by a country.[24] Otherwise, this will damage the political process, weakening security, endangering society, hindering economic development, and hindering the government of a country that is already doing well.[25] International Law plays a role in the principle of regulating behavior among international actors, not least in the context of technological advances, therefore in also playing a role in the development or dissemination of emerging technologies in response to the need to protect the international community from excesses, possible disasters, even risks posed by technology.[26]

Realizing that the handling of cybersecurity must be done through international cooperation, ASEAN, as a regional organization with a basis or foundation in preparing activities or agendas, can determine the role of each member state. This can be seen from the existence of the ASEAN Charter, which is binding to provide legal status and institutional framework to compile values and regulations to set targets for ASEAN to present accountability and fulfillment. So after realizing that ASEAN has a vital role in the region, at a later stage, the question arises what challenges are faced by ASEAN in handling cybersecurity? Through several analyses of various problems in the region, it was found that the problem is contained in the ASEAN body itself and external ASEAN, especially in the coordination of problem-solving. One factor that hinders it is the inconsistency of member states in an effort to implement the framework that has been prepared through the institutions they have formed. On the other hand, the external challenges faced are increasingly complex, especially regarding transnational crimes.[27]

The commitment to maintaining cybersecurity in the region is seen at several meetings, such as 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, the implementation of the Cybersecurity Maintenance and Security Strategy within the framework of multilateral cooperation can be seen in the ASEAN Regional Forum (ARF) through the ASEAN Political-Security Community (APSC) blueprint in Sub Chapter B.4.1. It is about an agreement to increase cooperation in non-traditional threats, specifically addressing transnational and cross-border crime issues. The discussion of Cybercrime is contained 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, which aims 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

[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.

[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).

Asia-Pacific region.[29] In this case, there is a difference with the concept of security cooperation by the North Atlantic Treaty Organization (NATO), which is synonymous with using military force. At the same time, the ARF tends to 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 contained in ASEAN's Cooperation on Cybersecurity and against cybercrime. The ARF on cybersecurity initiatives began to be 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 realization of the joint statement is then implemented in the form of various training at the regional level, with one of the focuses being how a country responds and coordinates when cyber incidents occur.[31]

In order to follow up on this cooperation, various international meetings were held in addition to the ARF, 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 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 continue to increase ASEAN's capacity to address the growing number of cyber threats in the ASEAN region.

Then The ASEAN Ministerial Conference on Cybersecurity (AMCC) the meeting was held in Singapore on October 11, 2016. In its development, Singapore held the ASEAN Cyber Capacity Program to ensure that the ability of ASEAN member countries can be increased in dealing with cyber security issues. To that end, four ASEAN mechanisms look to aspects of cybersecurity and cybercrime, namely: 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). Starting from regional news, issues that are then analyzed will be discussed in various ASEAN forums to establish cooperation in transnational crime, including cybercrime. SOMTC then implements the AMMTC plan.[32]

The framework contained in the ASEAN Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies (ICT) document on May 7, 2015, contains several goals to be achieved through a work plan as a means 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. 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. So that ASEAN cooperation can strengthen the country's security against the dangers of cyber aggression. The framework contained in the ASEAN Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies (ICT) document on May 7, 2015, contains several goals to be achieved through a work plan as a means 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. In its development through the ARF, ASEAN continues to follow

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

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. So that ASEAN cooperation can strengthen the country's security against the dangers of cyber aggression.

C. Conclusion

ASEAN, as a forum for cooperation for member states, plays a critical role in realizing cybersecurity. Therefore, ASEAN must improve its holistic handling of cyber resilience by strengthening the framework and work plan conceived together. It is necessary to embrace countries that are still passive so that cybersecurity can improve positively. On the other hand, cooperation between dialogue partnerships such as Japan, China, America, and several other countries is not limited to agreements but also requires a review of the components needed to encourage the success of cybersecurity resilience in ASEAN. In addition, the cyber issue itself is still a struggle for ASEAN because it is a new issue, so extra efforts are still needed to attract member states.

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, 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.