Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
www.bircu-journal.com/index.php/birci
Budapest Institute

Japanese and ASEAN Security Strategies in Cyber Crime in 2021 - 2025

Elsa Alviyani[1], Made Fitri Maya Padmi[2]
[1,2]*International Relations Study Program, Universitas 17 Agustus 1945 Jakarta, Indonesia*
elsaalviyani6@gmail.com, made.padmi@uta45jakarta.ac.id

Abstract

Cybercrime cases have become an important issue in various countries, including Southeast Asia. This study discusses what ASEAN as an organization does to tackle cyber crime and develop cyber security by collaborating with other countries. This research is descriptive by using qualitative research methods through multilateral relations between Japan and ASEAN. The results of this study indicate that Japan has a contribution to help ASEAN countries strengthen cyber security by cooperating because both have the same interest in creating security and peace in Southeast Asia.

Keywords
cybercrime; cybersecurity; and cybersecurity strategies

I. Introduction

Development is a change towards improvement (Shah et al, 2020). Current technological developments produce a new innovation that is very useful for mankind. Technology will certainly continue to develop every day because there will be many new discoveries from researchers, and can simplify human life in the future.

In the past, humans communicated through newspapers, *short message services* (SMS), facsimile, and so on. But now humans only need to use a technology called the internet network, which can convey various news, make calls, make online transactions, and sell online.

But behind the advancement of technology that is increasing rapidly every year, there are various threats and security that are certainly very detrimental to someone. For example stealing and spreading someone's personal data, stealing state-owned confidential data, spreading viruses to disable information systems and asking for ransoms at unreasonable prices, and hijacking official government websites.

This happens because the internet, which is global and has no boundaries, makes cyber crimes difficult to identify because they are carried out in cyberspace and there are no clear laws regarding these crimes. Of course, this cyber crime is a challenge for all countries in the world, because crimes committed in cyberspace are not easy to find the perpetrators because they are anonymous.

Various countries in the world carry out security cooperation in preventing the rise of cyber crimes which are increasingly taking more victims, one of which is the cooperation between Japan and ASEAN.

Starting from a cyber attack in Japan that involved sites owned by the government and private companies, including: (Butar-Butar, 2022)

a. In September 2011, there was an attack on a site owned by Mitsubishi Healthiest Industries, Ltd.
b. June 2015, there was a leak of personal data belonging to 1.25 million people from a retirement service in Japan

c. In June 2016, an alleged leak of personal data belonging to 6.8 million people from JTBC Corp.
d. In January 2018, a Japanese company, Coincheck, suffered a hacking attack that cost them 58 billion yen.

The security of personal data is important for ASEAN members because there are indications that ASEAN is a target for cybercrimes. Actually, ASEAN does not yet have adequate digital security governance. Because several cyber crimes have also occurred in ASEAN, including: (INTERPOL, 2021)

1. In July 2018, a company from Singapore, Singhealth experienced a case of patient data theft of 1.5 million data.
2. July 2019, unauthorized access to Toyota Motor Corporation's network system detected by Thailand and Vietnam.
3. An e-commerce company from Indonesia, Tokopedia, experienced the theft of 91 million users' data.

Japan and ASEAN focus on strengthening cyber security in order to create a safe, peaceful, and stable environment to boost the economy and defense. This is a reciprocal relationship between ASEAN and Japan so that defense relations are getting closer. On the southeast Asian side, the events of the previous year have exposed cyber vulnerabilities, as well as how to overcome them is complicated. (Parameswaran, 2017)

From Japan's point of view, working with ASEAN is very logical because Japan is very vulnerable to cyber attacks. Japan is also investing in dealing with cybercrime cases through increasing expertise in Southeast Asia. Japan also plays an important role in the regional sector, and promotes Japan's economic, security and business interests. (Larasati, 2018) From this incident, in 2015 Japan created a cyber security institution called the *National Center of Incident Readiness and Strategy of Cybersecurity* (NISC). Some of the main principles that underlie Japan to maintain security in cyberspace, namely, have clear laws, open information, the role of the state in cyberspace, and guarantee correct information, and invite *stakeholders* to maintain security in cyberspace. This principle makes Japan cooperate with the Southeast Asian region. (Ramadhanty, 2021)

The reason ASEAN and Japan cooperate is because Japan is considered to have a good security system although it is not perfect, but both of them want to develop research on cyber security systems. Therefore, the two of them held a meeting to discuss improving cyber security. On 18 January 2019, a meeting was held in Brunei which was funded by *the Japan-ASEAN Integration Fund (JAIF)* which provided long-term efforts. That matter was carried out to increase expert resources in the field of cyber security so that they can create a safe cyber world. (Ramadhanty, 2021)

Japan initiates a regional alliance based on *Japan's Nikkei Newspaper report.* It aims to involve ASEAN members together with the ASEAN Regional Forum (ARF), which is a forum for political and security issues consisting of China, the European Union, India, Japan, Russia, the United States, and 13 other members. The plans are, offices to exchange information, cybersecurity laws, strategies, and practices, and research to study and prevent attacks especially on government infrastructure.

A dialogue on Japan-ASEAN cybercrime (AJCD) was put forward at the Japan-ASEAN Commemorative Summit in December 2013 to promote cooperation in tackling cybercrime and enhancing cybersecurity. According to AJCD, Brunei is undertaking cyber policies, trends and lessons learned to combat cybercrime, capacity building, and projects to be funded by JAIF. (Cybersecurity, 2022) From 2016 – 2018, the project trained 380

participants from each ASEAN country, enabling them to conduct national cyber reviews and cyber crime investigations. The occurrence of Japan-ASEAN cooperation in the cyber field because both of them need each other. Therefore, in increasing security in the cyber world, both of them can create regional cyber bodies and cyber security governance which are expected to strengthen security cooperation between the two regions. The ASEAN – Japan Exercise was successfully carried out on June 25, 2020, involving 11 countries, namely: Brunei, Cambodia, Japan, Indonesia, Laos, Myanmar, Malaysia, the Philippines, Singapore, Thailand, and Vietnam. This activity collaborates with Japan to deal with cyber issues such as incident handling, capacity building, information sharing, and building information security in ASEAN and Japan. (BSSN, 2021) This paper will discuss the strategies of Japan and ASEAN in the field of cyber crime, and the results that will be obtained by Japan and ASEAN.

II. Review of Literature

2.1 Cyberspace

has become a hot topic in society recently, both in Indonesia and abroad. The cyber world is a public space that is used to carry out various daily activities, both in conducting electronic transactions, online shopping, and connecting with relatives who are on different islands.

This becomes a convenience for the community because they can carry out various activities anywhere and anytime. Of course, behind all that there is a threat to important information, especially personal data owned by someone. A *hacker* is trying to find ways to access the devices that we have in various ways. If they find a loophole, of course, *hackers* will open someone's data.

Because of this incident, cyber security is certainly an important thing for the community and must be considered so that no one can access personal data, whether it is leaking personal data to public spaces, selling personal data on illegal sites, or misusing the data for personal gain.

Cybersecurity is a necessary process to protect computers, networks, and *smartphones* from malicious malware attacks. This is done to prevent any illegal access that leads to personal information.

According to Deibert, cybersecurity is a separate discourse with different reference objects, threats, policy options, and commands covering national security, state security, internal and external threats, network security, and private security.

This opinion is supported by Hansen and Nissenbaum where cybersecurity cases include network relationships and individuals and human objects so that there is no private security discourse which has individual security as the object of reference, but individual security is related to social and political matters. (Nissenbaum)

2.2 Cyber Diplomacy

According to Barrinha and Renard, cyber diplomacy is diplomacy carried out in the cyber realm where diplomatic performance is used to secure national interests related to cyber which is carried out in bilateral and multilateral cooperation. The agenda that becomes the issue is *cybersecurity, cyber crime, confidence building, internet freedom, and internet governance.*

Cyber diplomacy has evolved to define the ongoing efforts to resolve new conflicts occurring in the cyber world. Dialogue between actors in diplomacy is a way to gain profit, and the role of cyber diplomacy is to generate profits through cybersecurity dialogue. (CIRNU, nd)

III. Research Method

This paper uses a qualitative method that refers to previous research journals, books, and websites. Qualitative research was conducted by searching for data via the internet, magazines, books, and online news that are still relevant to cybersecurity issues and cyber diplomacy, as well as the role of Japan and ASEAN.

IV. Results and Discussion

4.1 Cybersecurity Conditions in ASEAN

Internet users always increase from year to year due to technological developments that continue to develop. Even in ASEAN itself the growth of the internet is very fast. Because anyone can access the internet and do various things easily. Freedom to use the internet can carry out illegal actions in seeking information and can be a crime in cyberspace. Currently, the issue of cyber security is important because it can threaten the security of a country. This happened because of very advanced technological developments and activities that usually use human power, slowly moved to using computers. The internet also makes human life easier because everything can be accessed anytime and anywhere.

Dependence on the internet can certainly trigger a cyber attack because the danger posed can paralyze a system. In ASEAN, awareness of using the internet is not evenly distributed and they understand the dangers that will arise from cyber attacks. Currently, children have understood the use of mobile phones which of course can have a bad impact and are not aware of the use of technology. Because many people provide personal information carelessly to others as well as in the form of social media and on websites. This can be used to commit data theft and do bad things in the future. ASEAN's vision is to build useful information technology to advance technology and be well connected. However, in its development, ASEAN has not included a security system. Therefore, ASEAN must be prepared to face cyber attacks that will occur in the future. (Klimburg, 2015)

ASEAN realizes that cyber threats are a negative impact of technological developments. Although cyber security was not a concern when ASEAN was founded, at this time cybercrime has become an important topic at several ASEAN meetings. At a meeting in 2004, ASEAN Ministers recognized cybercrime as a crime that could affect security in Southeast Asia, and were required to work together to combat transnational crimes such as cyberattacks. (ASEAN Secretariat, 2005)

In order to reduce the gap, ASEAN made a plan, namely promoting peace and security in the wider Southeast Asia region and tackling the problem of cyber crime. ASEAN and the Security Community (APSC) have the main objective of responding in a timely manner and in accordance with security principles against various forms of threats, state crimes and transnational borders. The actions noted by the APSC 2025 strengthen cooperation and assistance in the fight against cyber crime in collaboration with legal institutions that take into account the needs of countries regulated by law to deal with cyber crimes. Strengthen the judiciary to establish regulations in the field of cybercrimes

with electronic evidence, promote cybersecurity law enforcement, and strengthen cooperation with the private sector to increase information between the private sector and law enforcement to reduce threats and increase awareness of ASEAN members about cybercrime and world terrorism cyber (ASEAN Secretariat, 2016).

There are several important issues that must be addressed by ASEAN. First, ASEAN does not yet have a vulnerability infrastructure in each country because there is still a lack of understanding of the threats that will occur in various sectors. Second, ASEAN's cyber threat documents are still difficult to understand. Because the document has not described what solutions should be done by ASEAN. Of course, the documents made are still not perfect and only as a form of awareness that is the same as other regions. The weakness of ASEAN's actions makes it confusing when facing cyber attacks because there is no clear monitoring unit and procedures to take in the event of an attack and improve ASEAN's cyber security. (Kurlantzick, 2012) Third, ASEAN does not build awareness of cyber threats, because the largest internet users are civil society. However, ASEAN's efforts are only focused on the government and the military. It can be seen from the document that it only targets the governments of ASEAN countries, and only focuses on the military. Tackling cybercrime is centered solely on the military. Increased defense and cyber attacks in the military is a necessary effort to prevent cybercrime. However, more cyber attacks attack the public sector, not the military. This has not been done by ASEAN, and it can be seen if cyber attacks against ASEAN focus on the public sector, for example government websites, the spread of viruses on mobile phones and computers, espionage, and the theft of data and funds from the banking sector originating from personal savings and other attacks.

Cyberattacks cannot be confirmed by the military or the public, but the biggest target is the public. Indicates that the military cannot carry out cyber attacks in response to attacks in cyberspace. Fourth, inequality and technological capabilities in Southeast Asia. Some countries already have advanced technology and are developing evenly, but some ASEAN regions still do not have the same technology. This has an impact on the lack of awareness of cyber threats, because the perceived threat is not necessarily a threat to other countries because they do not have the same technology. Of course, this makes it difficult for ASEAN to develop a clear framework that can be implemented by all countries. (Larasati, 2018)

4.2 Cyber Security Index in ASEAN

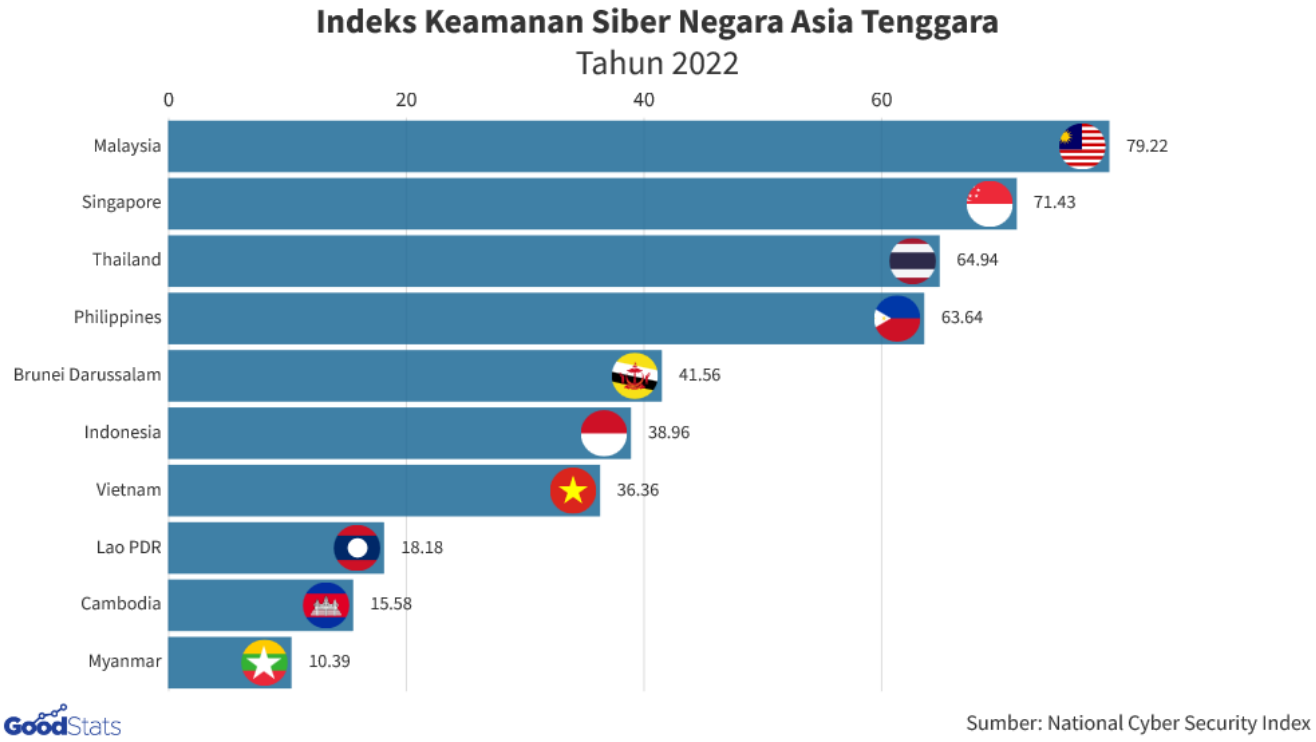

Figure 1. *Cyber Security Index in ASEAN 2022*

The case of data leakage is not the first time in Indonesia and other ASEAN countries. According to a survey *from the National Cyber Security Index* (NCSI) conducted in March 2022, it contains cyber security and conducts a survey based on several indicators, namely state laws relating to cyber security, government cooperation related to cyber security, and public evidence such as the official government website. Malaysia is in first place with a score of 79.22 points. Singapore is in third place with a score of 71.43 points, Thailand is 69.94 points, the Philippines is 63.64, Brunei Darussalam is 41.36, and Indonesia is in sixth place with a score of 38.96 points. While Vietnam is in 7th position with 36.36 points, Laos 18.18, Cambodia 15.58, and finally Myanmar 10.39. This marks Malaysia's progress on cybersecurity. This survey was conducted because of thousands of leaked government data due to malware infection which was uploaded by an account on Twitter called Dark Tracer on Friday, April 8, 2022. The account contains data as much as 878,319 of the 34,714 government property that was leaked. (ALIFAH, 2022) Cybercrime cases that have occurred in ASEAN: (Haibat, 2020)

1. On July 29, 2016, Vietnam Airlines experienced a hack that hijacked flight information screens and voice systems at Noi Bai, Hanoi and Tan airports Son Nhat in Ho Chi Minh City.
2. On August 31, 2016, Thailand experienced a cyber attack, namely the hacking of automated teller machines (ATMs) which cost the country USD 350 thousand THB 12 million.
3. In 2016, the Philippines experienced a cyber attack in which the election database was accessed by the whole world. The hacker group replaced the election image with another bad image.

4. In 2017, Indonesia experienced a cyberattack that cost domestic businesses USD 34 billion due to cash losses and long-term damage.
5. In July 2018, a company from Singapore, Singhealth, experienced a case of patient data theft of 1.5 million data.
6. July 2019, unauthorized access to Toyota Motor Corporation's network system detected by Thailand and Vietnam.
7. In March 2020, 310,000 credit card data issued by banks from Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam, committed a data breach.
8. An e-commerce company from Indonesia, Tokopedia, experienced the theft of 91 million users' data in 2020.
9. In May 2020, mobile network subscribers in Thailand suffered losses because their data was exposed to the general public.
10. In May 2020, 1.1 million accounts experienced a data breach in Singapore. (Bernadius Adi Pramudita, 2021)

4.3 Japan's Cybersecurity Policy

In 2017, according to a report by Japan's Kyodo news agency, the Ministry of Defense will set up a command center to tackle cybercrime that will increase its security personnel to 1,000 from the previous 110. This unit is responsible for maintaining cybersecurity, especially the assets of the Japanese Government, monitoring communication networks and responding to attacks 24 hours a day. They cooperate with the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) which aims to protect important assets belonging to Japan. NISC conducted a cybersecurity exercise that accumulated attacks on 21 ministries, and 10 industry associations. The exercise brings together 50 specialists who work in Tokyo and are engaged to prepare themselves to address cybersecurity issues related to the 2020 Tokyo Summer Olympics. (Abke, 2018)

On March 20, 2022, Japan launched a new cyber defense to respond to cyber attacks and important security domains in global conflicts. This unit consists of 540 personnel with duties to train human resources, support training, and manage information networks. The Japanese Ministry of Defense made a plan to tackle cybersecurity crimes by creating a new command center to oversee cyber defense in collaboration with private companies to deal with cyberattacks such as virus locking banking data, distributed denial-of-service (DDoS) attacks and ransomware. This attack signaled the Japanese government to know that the threat was very dangerous because the Japanese government made efforts to protect Japan's important infrastructure, namely cyber defense and intrusion. (Yabu, 2022)

The Japanese government has established several international cooperations related to cyber security with ASEAN. Such as the establishment of a *National Center of Incident Readiness and Strategy for Cybersecurity* (NISC) which will take control of campaigning for ministry activities, and promote cooperation between industry and academia, the public, and the private sector. The big office will cooperate with the Digital Agency that was formed to formulate development. (Cybersecurity, The National Security Strategy, 2013) They will collaborate and share information for terrorism emergency response. Headquarters also addresses national security issues with the Security Council. Collaborate with the Ministry to voice the strategy drawn up to government officials both at home and abroad to respond to cyber security risks, understand Japan's stance, and improve prevention by conducting international cooperation. Japan will make sure this plan will go well as they will make an annual plan to verify progress, summarize reports, and apply the annual plan for the following year. Plans should be discussed together and evaluate the

activities of the previous year and the following year. This plan should be organized so that the report will run clearly. (Japan TG, 2021)

ASEAN-Japan Cooperation Japan's commitment to the establishment of the 2015 ASEAN Community is marked by “The New Fukuda Doctrine” which states that Japan and ASEAN share a vision for the future. Because Japan is very concerned about the security of Southeast Asia. Therefore, Japan continues to strive to ensure the security of Southeast Asia in the political, economic, social and cultural fields. (Japan TG, 2021). Usually the relationship between Japan and ASEAN is centered on the economic and political fields, but currently the main focus of the relationship between Japan and ASEAN is in the field of cyber crime.

The 2021 – 2025 strategy supports the establishment of a cyber-ruled, secure, stable, accessible and peaceful operation. Created with non-binding norms responsible States, build trust, and build capacity that enhances cooperation with Japan. Built by CERT and capacity building cooperation, and considering cyber security that changes the cyber world and ensures security in Southeast Asia. Contains five dimensions, namely: (ASEAN Cybersecurity Cooperation Strategy, 2022)

a. Promoting cyber readiness cooperation
b. Regional cyber strengthening
c. Policy coordination
d. Increasing trust in the cyber world
e. International cooperation

4.4 ASEAN – Japan Cybersecurity Capacity Building Center (AJCCBC)

Discussions on the cyber world involving Japan and ASEAN continued with the ASEAN – Japan Cybersecurity Capacity Building Center (AJCCBC) in Singapore on 28 May 2014. The first dialogue on cyber crime discussed cooperation between ASEAN countries and Japan to increase and combat cyber crime, promote information to prevent cyber crime, promote international cooperation, cybersecurity development, and activities with JAIF. (Japan, 2014)

AJCCBC is a contribution from Japan to ASEAN in order to prepare capacity in fighting cyber crime. From the many efforts made by Japan and ASEAN, it is concluded that ASEAN countries must increase awareness of cyber security. Because ASEAN has become a victim of cyber attacks. Japan and ASEAN hope to be able to improve cyber security by exchanging information, training, and realizing cyberspace security. Japan is one of the countries that has made progress in the field of technology in collaboration with ASEAN to include the issue of cyber crime as an issue that needs to be discussed together. Japan also provides support through bilateral cooperation such as Official Development Assistance (ODA) or through multilateral organizations such as the United Nations. In October 2016, Japan issued a fund of USD 2 million which was implemented over 2 years and agreed to fund JAIF 2.0. The expected result is coordination in overcoming cyber crime, increasing the capacity of ASEAN countries, increasing cyber crime awareness among law enforcement, and increasing information exchange. (Larasati, 2018)

On March 17, 2022, AJCCBC expanded its training curriculum in collaboration with Switzerland in conducting “Secure Provision Training.” which is the first cooperation outside the ASEAN region and Japan. Which has the support of the Ministry of Home Affairs and Communications of Japan and the Swiss Embassy in Japan. The activity, which was held on March 14-15, 2022, totaled 22 participants. Focus on avoiding globally recognized cybersecurity risks. This training is very special because participants are able to investigate threats from different perspectives. Participants are expected to gain knowledge

that is useful for their work and cybersecurity in their area. AJCCBC as the organizer will expand the boundaries of cybersecurity training which is one of the important components in the digital economy and society. This activity is part of the Japan – ASEAN Integration Fund (JAIF) project, namely the ASEAN – Japan Cybersecurity Capacity Building Center. (JAIF Management Team, 2022)

4.5 Implementation of Japan-ASEAN Security Cooperation

Japan's involvement in overcoming cybercrime in increasing security capacity in ASEAN has led to several changes in ASEAN countries. For example, Brunei, Malaysia, Singapore, the Philippines and Thailand have implemented domestic laws and Myanmar has developed a legal framework. Cambodia carried out an investigation and prosecuted the relevant criminal law. A number of ASEAN countries have developed supporting frameworks such as national actions to eradicate cyber crime. Several countries have created authorities responsible for tackling cybercrimes. For example, Singapore which established a cyber security agency (CSA) in 2015. It is an agency that oversees cyber security strategy, cooperation, operations, education, outreach, and development managed by the Ministry of Communication and Information. CSA has implemented a cybersecurity scheme to prepare skilled experts. (Nandikotkur, 2018)

ASEAN representatives agreed on cyber security cooperation that focuses on the importance of cooperation in cyber fields such as cyber security policies, developing strategies, making laws, and increasing capacity. (CSAP, 2017) security cooperation will focus on rules for building a Computer Emergency Preparedness Team (CERT), increasing cybersecurity capacity. The proposals announced through the AMCC ceremony focus on three areas, namely building cybersecurity capacity, enhancing cybersecurity, and creating cyber awareness and environment and facilitating cyber norms. CERT collaborates to increase effectiveness in responding to cybersecurity incidents with the aim of developing a modular, flexible and multi-disciplinary framework to build ASEAN's cybersecurity capacity. Take a multinational approach, covering all areas. (CSAP, 2017)

V. Conclusion

Cyber security has not become a priority in ASEAN countries. In fact, the impact caused can suffer losses that are not small. As an organization, ASEAN must develop for member countries to fight and maintain cybersecurity. ASEAN members still have problems so they get different treatment. That's why ASEAN's role has not been stable because there are already developed member countries. ASEAN also cooperates with Japan, China and America. ASEAN needs to re-research ASEAN's role in cyber security issues. Because this issue is a new thing, efforts are needed to attract interest. ASEAN needs to invite countries that are still lacking in cybersecurity so that they can improve rapidly. They must consider data reporting and data breaches that occur in member countries. ASEAN must make a policy to fund and run the program so that it is beneficial for member countries. Japan has established cooperation in the economic field through multilateral cooperation, strategic partnerships and diplomacy in the economic, political, social and cultural fields. Japan's efforts to get attention in the international world by means of cooperation that adapts to the times. The relationship between Japan and ASEAN has a long history. The development of relations between Japan and ASEAN brings reciprocal relations in encouraging economic, diplomatic and socio-cultural cooperation. Japan's involvement in ASEAN political and security relations is built on an economic framework. Because Japan relocated their industry to Southeast Asia. Therefore, Japan

pays attention to reliable security conditions in the ASEAN region. The fundamental objective of Japan-ASEAN security cooperation is to call for peace, security and stability in the region.

There are many aspects that pose a threat in the Southeast Asian region, namely cyber crime which is a crime that crosses borders and crosses national borders. This can be seen from the access that is easily accessible by anyone and at any time. In ASEAN, there are many things that attract cybercrime, which causes ASEAN to have to improve cyber security because it is an important factor so as not to harm the country. Relations between Japan and ASEAN are focused on tackling cybercrime.

Japan has plans to call for communication between Japan and the agencies responsible for cyber crimes. For example the establishment of JAIF, funding the ACCP, and holding the ASEAN Japan Cybercrime Dialogue (AJCD). From this collaboration, ASEAN and Japan have succeeded in increasing cybersecurity capacity building in Southeast Asia. The relationship will continue to encourage economic activity. With diplomacy, Japan has succeeded in gaining ASEAN's trust, and is active in regional cooperation through multilateral cooperation to maintain peace, security and prosperity to support relations in Southeast Asia.

References

Abke, T. (2018, July 15). *Forum*. Retrieved from Jepang meluncurkan pusat komando baru untuk menghadapi ancaman siber: https://ipdefenseforum.com/id/2018/07/jepang-meluncurkan-pusat-komando-baru-untuk-menghadapi-ancaman-siber/

ALIFAH, N. N. (2022, April 08). *Keamanan Siber Negara Asia Tenggara 2022, Indonesia Peringkat Berapa?* Retrieved from GoodStats: https://goodstats.id/article/keamanan-siber-negara-asia-tenggara-2022-indonesia-peringkat-berapa-3RLgv

ASEAN Cybersecurity Cooperation Strategy. (2022, February 1). Retrieved from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122

ASEAN Secretariat. (2005). *Joint Communique of the 4th ASEAN Ministerial Meeting on Transnational Crime (AMMTC).* Jakarta: ASEAN Secretariat. Retrieved from https://asean.org/joint-communique-of-the-fourth-asean-ministerial-meeting-on-transnational-crime-ammtc-bangkok/

ASEAN Secretariat. (2016, March). *ASEAN Political Security Community Blueprint 2025.* Retrieved from https://www.asean.org/wp-content/uploads/2012/05/ASEAN-APSC-Blueprint-2025.pdf

ASEAN Secretariat. (2017). *Co-Chairs' Summary Report of the Second ASEAN-Japan Cybercrime Dialogue.* Kuala Lumpr, Malaysia: Adopted ad referendum on 17 May 2017.

Bernadius Adi Pramudita. (2021, January 04). *Rangkaian Kejahatan Siber Tahun 2020 di Asia Tenggara Versi Kaspersky*. (A. Dinilhaq, Editor, & Warta Ekonomi) Retrieved from https://wartaekonomi.co.id/read321161/rangkaian-kejahatan-siber-tahun-2020-di-asia-tenggara-versi-kaspersky

BSSN. (2021, February 25). *BSSN dalam Kegiatan ASEAN-JAPAN CYBER EXERCISE Tahun 2020*. Retrieved from https://idsirtii.or.id/berita/baca/457/bssn-dalam-kegiatan-asean-japan-cyber-exercise-tahun-2020.html

Butar-Butar, N. N. (2022, february 12). *Strategi Diplomasi Keamanan Siber Jepang dan Australia di Kawasan Asia Pasifik*. Retrieved from Linkedin:

https://www.linkedin.com/pulse/strategi-diplomasi-keamanan-siber-jepang-dan-di-asia-butar-butar/?trk=articles_directory&originalSubdomain=id

CIRNU, C. E. (n.d.). *Cyber Diplomacy –Addressing the Gap in Strategic Cyber Policy, No. 17*. Retrieved from http://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/

Consultation. (2017). *Adopted Joint Statement the third ASEAN plus Japan Ministerial on Transnational Crime* . Manila, Phiippines: Consultation.

CSAP. (2017, April 5). *7 CSAP Cybersecurity Workshop Conference Report. April 5, 2017*. Retrieved from 7 CSAP Cybersecurity Workshop Conference Report. April 5, 2017: http://www.cscap.org/uploads/docs/Cybersecurity%20Workshop/CyberWSReport5Apr2017.

Cybersecurity, N. c. (2013, December 17). *The National Security Strategy* . Retrieved from "cyberspace is necessary for promoting both economic growth and innovation: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf

Cybersecurity, N. c. (2022, January 31). *A Look Back on Cybersecurity for the Tokyo 2020 Games*. Retrieved from Commitment to a Free, Fair and Secure Cyberspace: https://www.nisc.go.jp/eng/index.html

Embassy, J. (2015). Japan-ASEAN Friendship and Cooperation. Mission of Japan to ASEAN 2015. *Japan-ASEAN Friendship and Cooperation. Mission of Japan to ASEAN 2015*.

Haibat, A. (2020). Proses Implementasi ASEAN Cybersecurity Cooperation Strategy. *Proses Implementasi ASEAN Cybersecurity Cooperation Strategy*, Retrieved from Perpustakaan Universitas Airlangga. https://repository.unair.ac.id/102829/4/4.%20BAB%20I%20PENDAHULUAN.pdf.

INTERPOL. (2021, January 5). *ASEAN Cyberthreat Assessment 2021*. Retrieved from www.interpol.int/en/News-and-Events/News/2021/INTERPOLreport-charts-top-cyberthreats-in-Southeast-Asia

Iyabu, A. F. (2022, March 20). *Antisipasi Ancaman Siber Global, Jepang Luncurkan Unit Pertahanan Siber Baru*. Retrieved from Antisipasi Ancaman Siber Global, Jepang Luncurkan Unit Pertahanan Siber Baru: https://voi.id/berita/147253/antisipasi-ancaman-siber-global-jepang-luncurkan-unit-pertahanan-siber-baru

JAIF. (n.d.). *Japan-ASEAN Integration Fund*. Retrieved from JAIF Management Team: https://jaif.asean.org/

JAIF Management Team. (2022). *ASEAN - Japan Cybersecuity Capacity Building Centre (AJCCBC) Conducted Secure Provision Training.* JAIF Management Team. Retrieved from https://jaif.asean.org/whats-new/asean-japan-cybersecurity-capacity-building-centre-ajccbc-conducted-secure-provision-training-on-14-15-march-2022/

JAIF Management Team. (2022, March 17). *ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) Conducted Secure Provision Training on 14-15 March 2022*. Retrieved from Japan-ASEAN Cooperation: https://jaif.asean.org/whats-new/asean-japan-cybersecurity-capacity-building-centre-ajccbc-conducted-secure-provision-training-on-14-15-march-2022/

Japan, M. o. (2014, May 27). *The Inaugural ASEAN-Japan Cybercrime Dialogue*. Retrieved from The Inaugural ASEAN-Japan Cybercrime Dialogue: https://www.mofa.go.jp/press/release/press23e_000019.html

Japan, T. G. (2021, September 28). *The Cybersecurity Policy for Critical Infrastructure Protection was decided by the Cabinet.* Retrieved from Cybersecurity Strategy: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf

Klimburg, A. &. (2015). Cyber Security Capacity Building: Developing Access . *Norwegian Institute of International Affairs*, 5.

Kurlantzick, J. (2012). "ASEAN's Future and Asian Integration. *Council on Foreign Relations*,, 142.

Larasati, A. I. (2018, March). Retrieved from http://repository.president.ac.id/handle/123456789/49

Nandikotkur, G. (2018, January). *Singapore to Open Cybersecurity Agency*. Retrieved from Singapore to Open Cybersecurity Agency: https://www.bankinfosecurity.com/singapore-to-open-cybersecurity-agency-a-7859

Nissenbaum, H. d. (n.d.). "Digital Disaster,.

Parameswaran, P. (2017, February 21). *Japan ASEAN Cyber Cooperation in the Spotlight*. Retrieved from https://thediplomat.com/2017/02/japan-asean-cyber-cooperation-in-the-spotlight/

Ramadhanty, S. A. (2021, November 4). Retrieved from Kerjasama Jepang-ASEAN dalam Meningkatkan Keamanan Siber: https://www.blog.iirs-center.com/2021/11/03/kerjasama-jepang-asean-dalam-meningkatkan-keamanan-siber/

Ramadhanty, S. A. (2021, November 4). *Indonesian International Relations Study Center dan IIRS Center*. Retrieved from Kerjasama Jepang-ASEAN dalam Meningkatkan Keamanan Siber: https://www.blog.iirs-center.com/2021/11/03/kerjasama-jepang-asean-dalam-meningkatkan-keamanan-siber/

Sekretariat. (17 May 2017). *Co-Chairs' Summary Report of the Second ASEAN-Japan Cybercrime Dialogue.* Kuala Lumpur, Malaysia: Adopted a referendum on 17 May 2017.

Shah, M. M., et al. (2020). The Development Impact of PT. Medco E & P Malaka on Economic Aspects in East Aceh Regency. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)* Volume 3, No 1, Page: 276-286.

Team, T. A. (2019, August 22). *Digital fraud on the rise in ASEAN*. Retrieved from The ASEAN Post Team: https://theaseanpost.com/article/digital-fraud-rise-asean?amp