TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 9, 2020

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

9 772668 779000

Indonesian Cyber Diplomacy: Asean-Japan Online Cyber Exercise

Dessy Permatasari Saputri¹, Surryanto D. W.², Helda Risman³

Defense Diplomacy Department, Faculty of Defense Strategy, Indonesia Defense University

dessypermatasarisaputri@gmail.com¹, surryantodw@yahoo.com²,
rismancan@gmail.com³

Abstract. The development of information and communication technology is growing both globally and regionally making it easier for everyone to access all information and communicate without knowing the limits even though many benefits can be obtained. The reality, in turn, gives a negative impact such as personal crime, theft, and data falsification to attack systems or forms of state infrastructure. Cyber threats that occur in Indonesia include racial riots in 1998 which Indonesia had to fight with hackers from China and Taiwan. Besides, the Indonesian government must also face espionage that done by Australia through its representative building in Jakarta. Therefore, cooperation is needed through the defense diplomacy process as a way to deal with all forms of cyber threats in Indonesia called cyber diplomacy. This study uses qualitative research methods through library research intending to analyze concepts and descriptions of cyber diplomacy. Cyber diplomacy conducted by Indonesia is involvement through the ASEAN-Japan Online Cyber Exercise program which is still at the level of developing the skills of cyber personnel, but has not touched on the policy domain to regulate program development. Then there needs to be further development by bringing this program to the ADMM forum.

Keywords. Cyberthreat, Cyber Diplomacy, Cyber Exercise

1. Introduction

The development of information and communication technology is progressing rapidly both globally and regionally. These developments ultimately made it easier for the world community to access all information and communication without knowing the boundaries of space and time so that the boundary lines of accessing information were lost. However, the development of information and communication technology not only brings positive impacts such as easy access to information or communicates freely but also brings negative impacts that can threaten the country's sovereignty. This can be illustrated through the many crimes that occur in cyberspace (cybercrime).

Cyber-based threats can be carried out by various state and non-state actors. This is due to the difficulty of identifying perpetrators of crime in cyberspace (cyber) for certain actions and actions in a place that has an effect or impact throughout the world (Coucri & Goldsmith, 2012). One of the countries facing impacts in the form of cyber threats in Indonesia. Indonesia is one of the largest internet user countries in the world as can be seen from the rapidly increasing number of internet users. Data on the development of internet users in Indonesia in the period

31 December 2000 amounted to 2,000,000 users and on 30 June 2019 it increased to 171,260,000 users. The percentage increase in internet users from 2000-2019 was 8.46% (Stats, 2019).

As one of the countries with the largest number of internet users in the world, Indonesia has faced various cyber threats. As in 1998 there were racial riots in cyberspace or cyberspace, namely Indonesia at war with hackers who allegedly came from China and Taiwan. Besides, based on research from Symantec (Sa'diyah. & Vinata, 2016) Indonesia is ranked second after Iran among 10 countries that have suffered a Stuxnet worm attack. Not only that, through a report from the Sydney Morning Herald that was quoted (Sa'diyah. & Vinata, 2016) Australia has tapped into the Indonesian government through its representative building. The number of cases of cyber attacks such as these examples is due to an increase in cyberspace or cyber dependence as explained in the following figure.

Figure 1. The Risk-Trends Interconnections Map (Forum, 2019)

Based on the picture above, it can be seen that the increasing dependence of the cyber world (rising cyber dependency) affects the occurrence of cyber-attacks (cyber attacks), fraud or data theft (data fraud or theft), damage to critical information infrastructure (critical information infrastructure breakdown). These three things are losses that are a consequence of the existence of the dependence of the cyber world. In the end, it does not rule out the possibility that the impact of the existence of the cyber world dependence will increasingly develop.

Cybercrime is an organized crime that can occur simultaneously in all countries. Cybercrime also has the potential to disrupt state sovereignty. Therefore, based on various cyber threats that occur in Indonesia and all kinds of cyber threats that will occur in the future, it is necessary to cooperate with other countries to increase protection against cyber threats. Through the

diplomatic process at the ASEAN regional level, ASEAN countries are working with Japan to develop the capacity of state actors to deal with cyber threats.

Cooperation between ASEAN countries and Japan is carried out through the ASEAN-Japan Online Cyber Exercise program. One of the points in the cooperation program is to provide training to government officials as actors who deal with cybercrime in the form of capacity building. This program is intended so that the government apparatus in ASEAN member countries and Japan can anticipate and be ready to face cybercrime if it occurs in their country. This cooperation has been carried out for more than a decade and in the course of the collaboration it will surely meet challenges and successes in the process. Based on the description above, the researcher formulates the problem of how Indonesian cyber diplomacy is in increasing the capacity of state actors to deal with cyber threats that have and will occur in the future.

2. Theoretical Framework

2.1. Diplomacy

Diplomacy according to Barston (Djelantik, 2008) is the management of relations between countries or relations between countries with other international relations actors. The development of globalization in the international world makes diplomacy develop into various types, one of which is in the field of information and communication technology. The evolution that occurs as a result of developments in technology and information ultimately creates new diplomacy that is used to deal with problems in cyberspace called cyber diplomacy. Barrinha and Renard (Chotimah, 2019) explained that cyber diplomacy is diplomacy carried out in the cyber domain or domain where diplomatic resources and diplomatic function performance are used to secure national interests related to cyberspace which are carried out bilaterally or multilaterally. The diplomatic agenda that is the focus of cyber diplomacy is the issue of cybersecurity, cybercrime, confidence-building, internet freedom, and internet governance.

The diplomatic agenda is in line with the objectives of defense diplomacy. The purpose of defense diplomacy according to Syawfi cited (Sinaga, 2017) has three main objectives, namely:

a As defense diplomacy for confidence-building measures (CBMs)

Acharya was quoted (Syawfi, 2009) explaining that defense diplomacy for confidence-building measures (CBMs) was carried out to build good relations with other countries where the main aim was to reduce tensions or eliminate misperceptions between parties using mutual openness in its policy, transparency in developing its military capabilities so that the notion of what is done by one country is not considered a threat to other countries.

b As defense diplomacy for defense capabilities

According to Matthews in (Syawfi, 2009) defense diplomacy for defense capabilities, aims to strengthen the capabilities of the country's defense materially. Enhancing defense capability can be carried out both internally and externally. In the external sphere, defense diplomacy instruments play an important role in making it possible for a country to fulfill its national interests.

c As defense diplomacy for industrial defense

Defense diplomacy for the defense industry (Amrullah, 2016) aims to develop and strengthen the defense industry.

Based on the description above it can be concluded that the existence of globalization affects the development of diplomacy. One of the evolutions of diplomacy is cyber diplomacy where this diplomacy is needed to deal with problems that exist in cyberspace as a result of the development of information and communication technology. One of the political agendas in cyber diplomacy is confidence building. This is in line with the objectives of defense

diplomacy. Therefore, cyber diplomacy can be used to strengthen defense diplomacy in cyberspace problems.

2.2. Internet Global Governance

Virtual world governance differs from global governance in several issues; it can even be said that cyberspace or cyberspace is a form of global governance. According to the Working Group on Internet Governance cited (Nursita, 2019) that internet governance can be interpreted as internet management carried out by the state, the private sector, community groups according to their respective roles, the existence of principles, norms, and joint rules and decision making and programs which contribute to the development and use of the internet. According to Glen quoted (Nursita, 2019) there are several universally agreed principles in cyberspace global governance. First, internet governance is directly related to several administrations that regulate how the internet functions. Second, internet governance is indirectly related to social, economic, and political phenomena and technical matters that ultimately affect public policy. Third, internet governance also depends on who has power over the rules. Fourth, the implementation of internet governance consists of several institutions, both public and private. Fifth, internet governance is bound by applicable rules or administration compared to the user or user experience.

Figure 2. Analysis Framework

3. Defining Cyber Development and Cyber Cooperation in ASEAN

3.1. Cyber Development in ASEAN

Cyber developments that occur in ASEAN can be seen from several aspects, namely the development of information and communication technology and the development of its user personnel. The development of information and communication technology tools in ASEAN is experiencing a gap. Singapore, as a developed country in Southeast Asia, has the most sophisticated internet access where 30 percent of the population can enjoy internet access smoothly. Whereas in Cambodia and Vietnam only 0.005 percent of the population can access the internet (Safril, Wardahni, Ponsela, & Tsauro, 2016). He further explained that the digital divide that occurred in the ASEAN region was due to three government policies that were not on target. First, the government policy related to the mastery of the telecommunications market which consists of three levels, namely (1) monopoly, (2) partial competition, and (3) full competition. Second, the government policy in working with the Internet Service Provider (ISP). The same agreement is intended to reduce internet costs through investment, both from foreign and local ISPs and thirdly, government policies related to equitable access to information and communication technology. Equitable digital access is closely related to

geographical conditions and infrastructure networks (Safril, Wardahni, Ponsela, & Tsauro, 2016).

As for the development of cyber personnel according to the ASEAN E-Commerce Database Project released in 2010, ASEAN accounts for 6% of internet users in the world (Andaya & Juban, 2010). Based on these data can give an idea of how the potential of creating regional communities that are interconnected due to the development of information and communication technology via the internet. Furthermore, the development of information and communication technology in ASEAN can be seen from the following table.

Table 1. ASEAN Internet Penetration

Rank	Country	Internet Penetration	Population	Internet Users
1.	Brunei Darussalam	81%	395.027	318.900
2.	Singapore	78%	4.701.069	3.658.400
3.	Malaysia	65%	26.160.256	16.902.600
4.	Philippines	30%	99.900.177	29.700.000
5.	Vietnam	27%	89.571.130	24.269.083
6.	Thailand	26%	66.404.688	17.486.400
7.	Indonesia	12%	242.968.342	30.000.000
8.	Lao PDR	8%	6.993.767	527.400
9.	Cambodia	1.30%	173.675	13.800.000
10.	Myanmar	0.20%	110.000	53.414.374
ASEAN			123.146.458	604.308.830

Source: ASEAN *e-Commerce Database Project* (ASEAN, 2010)

From the table above it can be seen that the development of technology and information occurs evenly across all ASEAN member countries. Indonesia is the first largest country as the most internet users in the ASEAN region with 30,000,000 users. Then the Philippines ranked second with a total of 29,700,000 users, and Vietnam ranked third with a total of 24,269,083 users. Therefore, as the first largest country of internet users in the ASEAN region, Indonesia cannot escape from various cyber threats.

3.2. ASEAN-Japan Online Cyber Exercise

One of Indonesia's cyber diplomacy engagements is joining the ASEAN-Japan Cyber Online Exercise program. The program was attended by 10 members of ASEAN and Japan. The activity is a manifestation of collaboration with ASEAN countries and Japan in dealing with various issues in the cyber realm such as incident handling, capacity building, information sharing, and building information security awareness and building information security of each ASEAN member country and Japan (BSSN, ASEAN-JAPAN Online Cyber Exercise, 2019). The ASEAN-Japan Cyber Online Exercise program has been running for more than a decade where the program aims to provide training to government apparatus through working group meetings, online cyber exercises, tabletop exercises and workshops to prepare for the possibility to face cyber threats that will occur. The objectives of this program are to increase capability and readiness in coordinating the response to cybersecurity incidents at the national level in each ASEAN country, developing communication methods for sharing information securely between participants and between ASEAN countries, and establishing good cooperation and communication between ASEAN countries and Japan in cyber security (BSSN, 2019).

The training is an effort to develop employee capacity and is motivated by several problems. As mentioned by Hasyim Gautama quoted (Midhio, Reksoprodjo, & Zaelani, 2018), among others, are as follows:

- a Weak understanding of the state administrators of cybersecurity requires restrictions in the use of services whose servers are located overseas so that a secured system is needed.
- b Legality in the process of handling cyber attacks.
- c The rapid pattern of incidence of cyber-attacks so it is quite difficult to handle.
- d Governance in cybersecurity institutions nationally.
- e The low awareness of cyber threats can paralyze a country's important infrastructure.
- f The still weak Indonesian industry in producing hardware related to information technology that can be a gap in cybersecurity.

The description of the implementation of the ASEAN-Japan Cyber Online Exercise is as follows.

Figure 3. Implementation of the ASEAN-Japan Cyber Online Exercise 2019 (BSSN, 2019)

From the picture it can be explained about the implementation of the ASEAN-Japan Online Cyber Exercise that the program is training for employees of government agencies in the form of improving skills in the field of information and communication technology. Increased skills in the field of information and communication technology are becoming important in handling cyber cases, this is because crimes that occur in the cyber world are getting more advanced with the development of the era. Therefore, employees of government agencies are required to be able to understand and master the cyber field so that they are better equipped to deal with various forms of cyber threats. Besides, with this program, the countries involved can share information and experience so that they can help one another. When employees of government agencies are better equipped to deal with cyber threats, they can contribute to defending the country's sovereignty from various cyber threats.

The ASEAN-Japan Online Cyber Exercise Program is still in the level of skills development of the cyber personnel itself. This is due to the absence of regulations or rules of cooperation between ASEAN and Japan. However, cooperation through the program for Indonesia as a developing country and other ASEAN member countries can attract a lot of information and knowledge sharing with other developing countries and developed countries such as Japan. As for Japan, it can increase its presence in the Southeast Asian region as a country that has advanced in technology and cyber problems.

4. Analysis

4.1. Indonesian Cyber Diplomacy

Indonesia as one of the ASEAN member countries adopted a policy to be involved in the program. This is because Indonesia views the cyber world as an asymmetrical and transnational world where it is an important part of diplomacy. After all, it can lead to diplomatic disagreements due to national interests and the country's political positions that rub against each other (Chotimah H., 2015). In this case the internet brings a new dimension to information and cybersecurity, which ultimately has implications for international relations where anything sent over the internet has the potential to be freely disseminated (Westcott, 2008). Based on this, the development of information and communication technology has an impact in the form of significant pressure on the country in developing a strong capacity to understand the potential of digital technology and design strategies that are tailored to short-term and long-term policy objectives (Bjola, 2017).

Citing the opinion of Indra Rosandry (2018) that cyber diplomacy in Indonesia can run effectively with several aspects, including the following. First, the existence of cyber threats that have complexity and cross country, requires a partnership or international cooperation with other countries because of Indonesia's strategic position as one of the largest internet user countries in the world which ultimately becomes an attraction for major power countries in the cyber field. Secondly, cooperation does not only involve actors from other countries, but also needs to involve various elements at the national level such as the public and the private sector. Third, to emphasize the orientation of Indonesia's foreign policy and diplomacy, the strategy in the cyber field has a vital role. In this case, the role of institutions responsible for cyberspace as implementing cyber diplomacy and cybersecurity functions is a positive record in efforts to achieve cyber resilience, public service security, cyber law enforcement, cybersecurity culture, and cybersecurity in the digital economy. On the other hand, the existence of institutions that deal with cyber problems can be capital in dealing with power struggles between major countries in the field of global cyber governance.

Based on the description above, it can be analyzed that cyber diplomacy by Indonesia has not been carried out effectively where the aspects mentioned by Rosandry have not all been fulfilled. First, the presence of complex and cross-border cyber threats makes Indonesia and the ASEAN member countries and Japan enter into a partnership or partnership in dealing with cyber threats in their respective countries. Second, the cooperation between Indonesia and ASEAN member countries and Japan has not yet fully involved the public and the private sector. This is because in the ASEAN-Japan Online Cyber Exercise program the objects are employees of government agencies working in the field of information and communication technology. Third, the role of institutions responsible for cyberspace can be seen from the existence of the Siber Board and the State Code (BSSN). BSSN is responsible for implementing the ASEAN-Japan Online Cyber Exercise program. Therefore, it can be concluded that Indonesian cyber diplomacy has not been effective because there is one aspect that has not been fulfilled in the ASEAN-Japan Online Cyber Exercise cooperation program, namely the absence of public and private sector involvement in capacity development to deal with cyber threats.

Threats in the field of cyber which are increasingly complex in all countries in the world make cyber diplomacy a very important thing to highlight. This is because defense diplomacy can be a way out to solve cyber problems that increase from year to year. The importance of cyber diplomacy is motivated by several things including the absence of clear territorial boundaries in the cyber world. The formation of the cyber world began because of the increasing use of the internet in various parts of the world. Based on data from the International Telecommunication Union (ITU) cited (Cahyadi, 2016) explains that the number of internet users covers about 30-

40% of the world population. The internet and the cyber world are double-edged blades for governments in the world. On one hand, the cyber world has the characteristics of a government that manages a variety of facilities and provides comfortable conditions for its citizens. While on the other hand, the formation of the cyber world also raises new challenges in determining the jurisdiction of a country. Therefore, the question of how to understand the roles, functions, and characteristics as well as how to build sovereignty in cyberspace, is a topic that is often debated (Barcomb, Krill, Mills, & Saville, 2012).

One of the difficulties in establishing cyberspace governance is that there are no clear boundaries (territorial areas) regarding cyber sovereignty in each country. The main challenge in upholding sovereignty on governance issues, including cyber world security, is the increasing role of parties outside the government that make it difficult to implement traditional international law due to unclear rules of sovereignty in cyberspace (Krasner, 2001). In addition, the importance of cyber diplomacy is also motivated by the dependence on globally connected technology that also opens a gap for hackers to develop tools and methods that are increasingly sophisticated, efficient, and effective. These tools and methods can threaten cybersecurity. For example, it is used for misuse, illegal access, and theft of important data belonging to the state and non-state actors (Yunandar, 2019).

If it is related to the defense diplomacy strategy the importance of Indonesian cyber diplomacy is carried out as one of the forms of diplomacy carried out in the interests of Indonesia's cyber defense. In defense, diplomacy has the characteristics of defense diplomacy for confidence-building measures (CBMs) which according to Acharya in (Syawfi, 2009) is a diplomatic process aimed at building good relations with other countries to reduce tensions or eliminate misperceptions between parties by mutual means open in its policies, transparency in developing its military capacity so that what the state does is not seen as a threat. Stauffacher and Kavanagh cited (Chotimah, Iswardhana, & Pratiwi, 2019) mentioned that Military Confidence Building Measures consist of three categories, namely (1) Exchange of information and communication aimed at increasing mutual understanding; (2) Transparency and verification that allows countries to monitor the military facilities and activities of each country to ensure non-aggressive military action; (3) Military restraints to limit offensive military attacks. Thus the application of the concept of Confidence Building Measures in cyber diplomacy through the ASEAN-Japan Online Cyber Exercise is as follows.

- a First, exchange information. The process of exchanging information in cyber diplomacy cooperation through the ASEAN-Japan Online Cyber Exercise is carried out bilaterally or multilaterally. This information exchange is carried out within the scope of cybersecurity between the countries involved and the government agencies involved in this program. However, the information provided between countries is certainly not possible to reveal the entirety of the capabilities possessed in the cyber world in dealing with various kinds of cyber threats that occur. This is because it relates to the cyber sovereignty of each country. Despite exchanging information, each country must continue to maintain its cyber sovereignty. Likewise with Indonesia, despite sharing information with countries cooperating in the ASEAN-Japan Online Cyber Exercise program, the state actors involved must limit the information provided so that cyber sovereignty is maintained. This information exchange process is carried out through an information channel where the information channel is the ASEAN-Japan Online Cyber Exercise training program. The program is carried out routinely every year because it can become an information channel used for the process of exchanging information.
- b Second, transparency and verification. The process of transparency and verification in the cyber world can be done by making a joint exercise. The ASEAN-Japan Online Cyber

Exercise Program is a form of joint exercise created by ASEAN member countries and Japan. Transparency and verification in this case are realized through training in information and communication technology in solving cyber problems. With joint exercise, it can increase the awareness of employees of government agencies about the importance of cybersecurity because the employees involved will get a picture of readiness between countries and their level of capability in dealing with cyber threats that occur. This is the result of transparency and verification.

- c Third, military restrictions. In the ASEAN-Japan Online Cyber Exercise activities there are military restrictions, this can be seen from those directly involved in the program where more are employees of government agencies from ministries or government agencies. Besides, it can also be seen from the implementation process which uses a more soft power method by sitting together conducting discussions between the parties involved and learning together to find ways to solve cyber problems.

Thus it can be concluded that the importance of cyber diplomacy is because cyber diplomacy can act as confidence-building measures (CBMs). With the three characteristics analyzed and described above, good relations with ASEAN member countries and Japan will be built to eliminate tensions and misperceptions as a result of cyber-attacks threatening each country. Besides, the existence of cyber diplomacy between ASEAN countries and Japan can create transparency about developing the capacity of each country's military strength as well as non-military forces to deal with cyber threats. With the transparency process created by each country, they can carry out the process of exchanging information in capacity building so that mutual trust arises between the countries that work together.

The importance of cyber diplomacy can also be related to other defense diplomacy strategies, namely defense diplomacy for defense capabilities which according to Matthews in (Syawfi, 2009) aims to strengthen the capability of the national defense materially. Enhancing defense capability can be carried out both internally and externally. The process of cyber diplomacy undertaken by Indonesia with other ASEAN member countries as well as Japan can be said as an effort to improve defense capability, especially in the external sphere of cyber. With this cyber diplomacy, Indonesia can exchange lessons on how to effectively deal with various cyber threats that are and will attack Indonesia. This is because Japan which has more advanced technological sophistication than Indonesia can provide information and knowledge to Indonesia regarding incident handling from each ASEAN country and Japan.

Capacity building in the ASEAN-Japan Cyber Online Exercise cooperation can be realized through joint training conducted and participated by all countries involved. This training can prepare the parties involved in this matter, namely the apparatus of ministries and institutions to be better prepared in facing cyber threats in their respective institutions. With the training the apparatus can better understand all kinds of threats that are developing in the world of berries and how the world in the regional scope, namely ASEAN and Japan, prepare each apparatus to overcome cyber problems in each country. Different cyber threats in each country can be important information to be shared with each country that is working together so that the parties involved can know what needs to be improved when faced with the same threat.

Based on the description above, it can be simplified that the importance of cyber diplomacy is currently motivated by cyber problems that do not yet have clear boundaries in the cyber world and because of the dependence of all people in each country in the world of information and communication technology. Therefore, cyber diplomacy is very necessary to realize the principles of defense diplomacy, especially in terms of Capacity Building Measures through the process of exchanging information, transparency, and verification, and military restrictions

to build mutual trust between the countries involved and can increase awareness and readiness of government agency employees to deal with cyber threats.

Indonesia's involvement in cooperation with the ASEAN-Japan Online Cyber Exercise program can also be a stepping stone for Indonesia to become the initiator of the development of the program in the ADMM (ASEAN Defense Minister Meeting). As mentioned above, the program is still at the level of developing cyber personnel skills not at the level of regulation or policymaking. Therefore, by being brought into the ADMM forum a clear regulation will be created to regulate the program, which in turn can be an inspiration for other countries in conducting cyber diplomacy.

5. Conclusion

The development of technology and information causes the boundary lines in accessing information to be lost. This can eventually lead to various threats that occur in the cyber world. Threats that occur in the cyber field can attack various kinds of parties both the state and non-state actors. As one of the countries with the most internet users, Indonesia cannot avoid various kinds of cyber threats. Therefore, Indonesia conducts defense diplomacy in the form of cyber diplomacy, namely establishing cooperation with ASEAN member countries and Japan with the ASEAN-Japan Online Cyber Exercise program in which this program aims to exchange information about cyber threats and provide training to the state apparatus to increase capacity in dealing with cyber threats. The importance of cyber diplomacy is done for several reasons, among others, because there is no clear sovereignty limit in the world of cyberspace so that all kinds of positive and negative information can be accessed easily and because of the dependence on the use of technology.

The ASEAN-Japan Online Cyber Exercise Program is still implemented at the level of increasing the skills of the cyber personnel themselves in dealing with the problems of the cyber world in their respective countries. This can be seen from the agenda of activities in the program in the form of workshops, seminars, training, and other skills development. As for the policy level, there are still no clear rules or policies governing the program. Besides, the objectives of cyber diplomacy that are in line with national defense diplomacy in this program can be realized in two ways, namely Capacity Building Measures (CBMs) and Defense Capability. CBMs aim to build trust between the countries involved to create transparency between countries regarding various cyber threats and activities carried out by each country to deal with cyber threats or can be said to be information sharing activities. Besides, it is also one of the efforts to increase the capability of each country in increasing preparedness to face various cyber threats that occur as well as a stepping stone for Indonesia to become an initiator in developing the program to the level of regulation of foreign cooperation policy by bringing the program to the forum. ADMM (ASEAN Defense Minister's Meeting).

References

- [1] Amrullah, M. R., (2016). Diplomasi pertahanan Indonesia terhadap Turki: Studi kasus kerja sama industri pertahanan. *Jurnal Pertahanan* , VI, 40.
- [2] Andaya, D. B., & Juban, A. M., (2010). *The ASEAN e-commerce database project*. Jakarta:ASEAN.
- [3] ASEAN., (2010). *ASEAN e-commerce database project*. Retrieved Desember 30, 2019, from Association of SouthEast Asian Nations: <https://www.asean.org/>
- [4] Barcomb, K. D., Krill, R., Mills, R., & Saville, M., (2012). Establishing cyberspace sovereignty. *prosiding 7th international conference on information warfare and security*. Academic Conferences Limited.

- [5] Barston, R. P., (2014). *Modern diplomacy*. New York: Pearson Education.
- [6] Berg, d., (2001). *Qualitative research methods*. 15.
- [7] Bjola, C., (2017). Trends and counter trends in digital diplomacy. *Working paper project, diplomacy in the 21st century, No. 18* , p. 8.
- [8] BSSN., (2019). *ASEAN-Japan online cyber exercise*. Retrieved Desember 25, 2019, from BSSN: <http://www.bssn.go.id>
- [9] BSSN., (2019). *ASEAN-Japan online cyber exercise*. Jakarta: BSSN RI.
- [10] BSSN., (2019). *BSSN Berharap Dubes Menjadi Mata dan Telinga Indonesia*. Retrieved Desember 30, 2019, from BSSN: <http://bssn.go.id>
- [11] Cahyadi, I., (2016). Tata kelola dunia maya dan ancaman kedaulatan nasional. *Jurnal Politika, VII*, 62 .
- [12] CATRA., (2016, September). Dari desk cyberspace nasional menuju badan cyber nasional. *Majalah Setjen Wantannas, Edisi VI* , p. 16.
- [13] Chotimah., (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. *Politika* , X, p.118.
- [14] Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S., (2019). Penerapan military confidence building measures dalam menjaga ketahanan nasional Indonesia di ruang siber. *Jurnal Ketahanan Nasional, XXV*, p. 35.
- [15] Chotimah, H., (2015). Membangun pertahanan dan keamanan nasional dari ancaman cyber di Indonesia. *Jurnal Diplomasi, VII*, p.114.
- [16] Cottey & Foster., (2004). *Reshaping defence diplomacy: New role for military cooperation and assistance*. New York: Oxford University Press inc.
- [17] Coucri, N., & Goldsmith, D., (2012). Lost in cyberspace: Harnessing the internet, international relation. and global security. *Buletin of the atomic scientist* 68 , p. 70.
- [18] Djelantik, S., (2008). *Diplomasi antara Teori & Praktik*. Yogyakarta: Graha Ilmu.
- [19] Forum, W. E., (2019). *The global risks report*. Geneva: World Economic Forum.
- [20] ICT, M., (2017). *Badan siber nasional akan cegah dan perangi cyber terorisme*. Retrieved Desember 26, 2019, from Majalah ICT: <http://www.majalahict.com/indonesia-butuh-badan-cyber-nasional/>
- [13] ID-SIRTII., (2017). *Pemantauan trafik internet*. Retrieved Desember 25, 2019, from ID-SIRTII/CC: <https://www.idsirtii.or.id/>
- [14] Krasner, S. D., (2001). Abiding sovereignty. *International Political Science Review, XXII*, 76.
- [15] Midhio, I. W., Reksoprodjo, Y., & Zaelani, H., (2018). Pembangunan kapasitas cyber security di negara ASEAN: Analisis komparatif terhadap Brunei dan indonesia. *Jurnal Prodi Perang Asimetris, IV*, p. 86.
- [16] Nursita, R. D., (2019). Cyberspace: Perdebatan, problematika, serta pendekatan baru dalam tata kelola global. *Dauliyah* , IV, 85.
- [17] Nutterlein, D. E., (1979). *The concept of national interest a time for new approach*.
- [18] Plessis, A. D., (2008). *Defence diplomacy: conceptual and practical dimensions with specific reference to South Africa*. Retrieved Januari 20, 2020, from UPSpace Institutional Repository: <http://repository.up.ac.za>
- [19] Rosandry, I., (2018). *Merajut diplomasi siber Indonesia*. Retrieved Desember 30, 2019, from Media Indonesia: <http://mediaindonesia.com>
- [20] Rudy, T., (2002). *Study strategis dalam transformasi sistem internasional pasca perang dingin*. Bandung: Refika Aditama.
- [21] Sa'diyah., N. K., & Vinata, T. R., (2016). Rekonstruksi pembentukan national cyber defense sebagai upaya mempertahankan kedaulatan negara. *Perspektif* , XIII, p.169.

- [22] Safril, A., Wardahni, A., Ponsela, D. F., & Tsauro, M. A., (2016). Problem dasar kesenjangan digital di Asia Tenggara. *Global & Strategis* , X, p.208.
- [23] Sinaga, T. H., (2017). Diplomasi pertahanan Indonesia melalui kerja sama intelligence exchange group (IEG) di Selat Malaka. *Jurnal Prodi* , p.44.
- [24] Stats., (2019). *Top 20 countries with the highest number of internet users*. Retrieved Desember 27, 2019, from Internet world stats: <http://www.internetworldstats.com>
- [25] Sumari, D. P., & Wahyudi, A. D., (2016). Diplomasi pertahanan Indonesia dalam pencapaian cybersecurity melalui asean regional forum on cyber security Initiatives. *Jurnal Penelitian Politik, XIII*, p.140 .
- [26] Syawfi, I., (2009). *Aktivitas diplomasi pertahanan Indonesia dalam pemenuhan tujuan-tujuan pertahanan Indonesia (2003-2008)*. Jakarta: Universitas Indonesia.
- [27] Westcott, N., (2008). Digital diplomacy: The impact of the internet on international relations. *Research Report 16* , p.14.
- [28] Yunandar, M. A., (2019). Kerja sama keamanan siber di ASEAN dalam menyambut industri 4.0. *masyarakat ASEAN, Edisi 22* , p. 12.