Potential and Threat Analysis Towards Cybersecurity in South East Asia

Anna S. Salsabila, Muflih D. Fikri, Muhammad S. Andika, Nanda A. Harahap
Department of International Relations, Faculty of Social and Political Sciences, Universitas Sebelas Maret Surakarta, Indonesia
annasafira@student.uns.ac.id, muflihdwifikri@student.uns.ac.id, muhsinggiha@student.uns.ac.id, aziiz.harahap@student.uns.ac.id

Article Information

Submitted : January 21, 2020
Revised : May 1, 2020
Accepted : June 30, 2020

Keywords :
cybersecurity; cybercrime; ASEAN; ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)

Abstract

Cybersecurity is a very strategic issue in maintaining a state's stability, particularly in this modern era. The threats that can attack a state can no longer be physical or traditional threats but also cyber threat. In dealing with cases occurring related to the issue, Singapore initiated the establishment of ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) to ascertain cybersecurity stability in ASEAN region. However, it of course results in various speculations and potencies likely occurring when cybersecurity is concentrated and controlled on one country only. Therefore, this journal analyzed ASCCE-related potency and threat likely occurring in ASEAN using Speech Act, Securitization, Wideners, International Cooperation, and Information Technology Management theories. In addition, the author also discussed the effectiveness of ASCCE performance in coping with cybercrimes and cyberthreats in ASEAN and their effect on ASEAN states.

I. INTRODUCTION

Defense and security are two important aspects in maintaining a state's stability. Defense and security determine a state's strength in other countries' eyes. These defense and security are determined by a successful national development that will improve national resilience [1]. This national development includes, among others, information and technology (IT). Information and technology are closely related to defense and security, particularly in the term of cybersecurity. Cybersecurity, according to Amaroso (2006), is [2]:

> "Cybersecurity is closely related to mitigating the risk of cyberattacks and cybercrime attacking software, computer, and network. It includes the devices used to detect burglary, to cease virus, to block illegal access, to support originality, to provide access to confidential communication and etc."

Meanwhile, cybersecurity, according to Public Safety Canada (2015), is: "The form of technology, process, practice, and mitigation response, the measure of which is used to protect network, computer, program, and data coming from the attack, damage or illegal access to ascertain confidentiality, integrity, and availability". Very broad internet access inhibits the states to perform pacification and security measures over cybercrime conducted by certain groups. Therefore, there should be cybersecurity system that can expel cyberattack. Moreover, the state is often faced with such constraints as limited quality of technology, human resource, and infrastructure in dealing with cyberattacks. It indirectly forces the state to cooperate well with other states or non-state actors.

There is no doubt that the cybercriminals are interested in ASEAN's

economic growth and prosperity. The growth of an awareness of maintaining cyberspace and its IT infrastructure need collaborative attempts by ASEAN member states. There are four ASEAN's mechanisms of investigating cybersecurity and cybercrime aspects: ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications and IT Ministers Meeting (TELMIN), the ARF), and the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC). However, with all of these steps, it is difficult to keep one step ahead the cybercriminals. It seems to become a case that this criminal is always ready. Attack danger is always near, such as the dark cloud over the region, creating uncertainty in the government, whether or not they will be the next of attack target. Cyberattack will have serious consequence and broad coverage. Financial institution, defense center, central bank, hospital, and airport are some location likely suffering from such attack.

A good cybersecurity system should be supported with advanced technology. In ASEAN region, the state reputed to be the one with rapidly developing technology is Singapore. Singapore also achieve predicate as superior city in technology among Asian Pacific states. As the chair of ASEAN in 2018, Singapore has encouraged many cybersecurity agendas, invested substantial resource in building operational, policy, and legal capacities, and expanded partnership with United Nations and international multistakeholder's initiative such as Global Commission on Stability in *Cyber*space. It starts with a combined theme of Singapore's innovation and resilience leaderships. The most developed state technologically in this region has socialized continuously with its neighbors concerning debate on broader norms, international law implementation, and state's responsible behavior in cyberspace. Its effort can be seen in recent years and it seems to be fruitful gradually now.

Savills Tech Cities Index of 2019 shows that it is achieved due to business-friendly climate, superior human resource, and technology advance [3]. Because of its high reputation, Singapore initiates the establishment of ASEAN's Cyber Capacity Program initiated by Singapore in 2016 and the ASEAN-Japan ASEAN Cybersecurity Capacity Development Center newly launched in Bangkok is intended to deal with this using overlapping methods. The last location in Thailand capital, ASEAN entrance chair, may not ensure the same strategic and security focus in cyberspace agenda, but the founding of the center will at least institutionalize the sustainable attempt to build the capacity of cyberspace in the region.

Then, Singapore also initiates ASEAN-*Singapore Cybersecurity Centre of Excellence* (ASCCE) in cooperating with ASEAN as the more concrete step in cyberspace cooperation. ASEAN-Singapore Cybersecurity Centre of Excellence was born firstly from the statement of Singaporean Deputy of Prime Minister, Teo Chee Hean, in the opening of the 3rd annual event Singapore International Cyber Week. This ACCE establishment aims primarily to improve cybersecurity at regional level and to be the manifestation of ASEAN Cyber Capacity Programme development in which ASEAN countries cooperate to expel cybersecurity threats arising in this digital era. ASEAN *Cyber Capacity Programme* itself has cooperated with Japan as the state with high technology advance, thereby can encourage the quality. Singapore pays substantial attention to this cybersecurity issue following a series of cyberattack against South East Asia and Singapore in recent years. The first attack occurred in 2017 when there was *WannaCry* virus attack.

The latest attack targets Singaporean healthcare system, SingHealth, hacking the access and copying 1.5 millions patient recordings and 160,000 recordings of outpatient medication released, including the one belonging to the Prime Minister, Lee Hsien Loong [4].

ASEAN as a region with rapid economic development but without a qualified strategy to cope with cybersecurity issue also triggers the emergence of cyberattack itself. It is particularly weak in the term of strategic mindset, regulation alertness, and organizational or institutional negligence in dealing with cybersecurity. In addition, because this cyberattack risk is a security rather than business issue, business in the region does not have access to coping with this cyberattack risk [5]. Because of the region's sensitivity to national security, the cybersecurity measures supporting the objective of ASEAN Economic and Social-Cultural community is more likely achieved in short term. The comprehensive measures will be ASEAN members' joint interest, favorable to the broader Asia-Pacific initiative, and complementing the international cooperation in the future. Particularly, they will support the establishment of single market and production base, improve connectivity, and strategically improve ASEAN's position in global world. However, ASEAN-*Singapore Cybersecurity Centre of Excellence* (ASCCE) still generates some assumptions and speculations. They are, among others: whether or not ASCCE will be really effective in the future or instead will result in new problem related to data access in cybersecurity and ASEAN states' limited capability; In addition, whether or not Singapore itself has certain interest behind ASCCE. Therefore, the author attempts to prove whether or not this ASEAN-*Singapore Cybersecurity Centre of Excellence* (ASCCE) can run effectively in the future or instead have potential clash. In this case, ASEAN should be credited because it has taken a brave step forward. However, it should remain to cross information highway with agility, pragmatism, and particularly vision.

II. CONCEPTUAL FRAMEWORK

A. Speech Act Theory

Speech act theory is a theory stating that an action accompanying verbal communication has a distinctive message. Thus, communication can be done not only with language but also with action. The language we use daily is a language game because it contains rules. In other words, people follow the rule to do anything. Speech Act theory was constructed from the basic form by Wittgenstein and Austin [6].

In this theory, *Speech act* is a basic unit of language used to express the meaning, an utterance expressing an intention or purpose. *Speech act* is then not only used to refer to something but also to do something. That is why it is called *speech act*. As a result, speech act theory emphasizes not on individual reference of symbol but on the purpose of action entirely. If speech act is successful, the receiver will understand what the speaker wants to say. The meaning of speech act is illocution force (an interview about a power to influence the message receiver in order to achieve the speaker's objective). Searle fundamentally stated that speaking of language is to convince an individual with a rule of order to represent his/her conduct. Those two important rules are: constitutive and regulative. The constitutive rule actually creates game, that is, the game created or raised by these rules [7].

The theory can affect indirectly the states around the state implementing this theory. Included in this case is Singapore as the cyber-security center in ASEAN

that can influence other ASEAN states to conduct regional cooperation for cyber security in ASEAN region, of course favorable to Singapore because cyber data of ASEAN states can enter into Singapore easily so that it can "trace" the states potentially threatening in the future.

B. Securitization Theory

When we speak of securitization, it is inseparable from the effect of *The Copenhagen School* by Barry Buzan, Waever, Jaap de Wilde in *Security: A New Framework for Analysis* [8]. *The Copenhagen School* is a concept aiming to think critically of security conception. Securitization can be defined as extreme version of politicization. In securitization, actor expands national security into many areas so that all problems can be seen as national security through political process. As stressed by Constructivists, security is something constructed rather than something absolute in nature. The politicization of issue performed by the actor results in the issue formerly not security issue changes into the threatening one and needing national agenda to solve it. Through securitization, there is a shift of issue from usual political issue only into the issue assumed to be urgent and to need quick handling even without normal regulation or rules of other decision making. It is the essence of securitization.

There are some concepts in securitization showing how the actor performs securitization. Those concepts are: securitization actor, speech act, *existential threat, referent object,* and *audience*. As its name shows, the actor of securitization is the one attempting securitization. The actor will take some attempts of socializing idea or called *speech act*, by means of campaigning for *existential threat,* the existential threat issues discoursed. This securitization attempt is intended to audiences or those who want to be influenced by the actor to believe in the existential threat, and affects the referent object, the one to be threatened if the issue is not dealt with seriously. Then, how to measure the actor's success in performing securitization? In this case, it should be confirmed that securitization is said to be successful if only the audiences accept the attempt of socializing idea conducted by the actor. In other words, audiences agree to assume the issue voiced by actors as a security issue. Securitization practice will pass through some stages, from problem identification, politicization, debate, to action taking by the state.

All of these stages are highly dependent on *speech act* performed by the actor. The ability of socializing idea until the idea is accepted by audiences can be the key factor to securitization process, because finally the action taking by the state only occurs when the idea is acceptable. Otherwise, if *speech act actor* is not successful, or in other words audiences do not accept the existential threat from the actor, the securitization will not be successful. Therefore, as suggested by the Copenhagen School, a successful securitization will have three main components: *existential threat*, *emergency action*, and effect on inter-unit relationship. In analyzing the securitization process with speech-act approach, there are three important units to differentiate: (1) referent object, (2) securitizing actors, and (3) functional actors. The interaction between three actors does not occur directly but one actor affects another very significantly in presenting a comprehensive analysis. The three actors aforementioned, particularly referent object and securitizing actors, are very important to distinguish to prevent an overlapping analysis process from occurring. The referent object intended is any thing threatened by

existential threat and having legitimate claim over its survival.

The characteristics of this approach are: focusing on political power and symbolism of word 'security', the use of all resources in dealing with issue beyond ordinary politics, and then including it into security issue, and challenging the mindset of traditional security tending to zero-sum in nature [9]. For example, in ASEAN cyber-security case, the states in South East Asian region agree to take action for the sake of maintaining their regional security in cyber sector by building joint venture.

III. ANALYSIS

Some Heads of ASEAN member states, in 32nd ASEAN Summit one topic of which is cyber security, admitted that cyber security is a cross-sector issue requiring coordinated skill from many domains to solve effectively. They also admitted that cyber domain potentially represents the opportunity of significant regional economic and technology development, and also functions to be a significant job source. State sovereignty and norms as well as international principles of the responsible states are very important factor to grow the state's self-confidence and it highly affects the individual ASEAN members' regulation in their cyber development [10].

The heads of ASEAN member states also confirmed the need for ASEAN to speak up with a uniting voice in international discussion forum aiming to develop international policy and framework concerning the development of capacity related to cyber security in order to promote the regional interest more effectively. They also confirmed that the prevailing international law is very important to safeguard peace and stability, and to promote Information and Communication Technology environment that is opened, safe, stable, accessible, and conducive. They also discuss about the importance of knowledge on the expanding cyber threat considered as international issue for a long time, and urgency as well as the increased sophistication of cross-region cyber threat developing continuously in ASEAN region amid the expanding economic digitalization and the proliferation of internet-connected ware throughout ASEAN region [11].

ASEAN in the realization of speech act then created cooperation in anticipating the cyber attack by establishing *ASEAN Singapore Cybersecurity Centre of Excellence* (ASCCE*). ASEAN Singapore Cybersecurity Centre of Excellence* (ASCCE) is a program developed by Singapore aiming to be the form of defense to fight against cyber attack. Singapore brings this cyber security system into ASEAN domain as the form of cyber defense in South East Asia. Singapore invests US$ 30 millions for the next 5 years and is expected to develop cyber security in South East Asian countries. ASCCE was established to respond to the emergence of cyber attack issue and the increasingly sophisticated technology making the cyber security escalating in this 21st century. The cyber attacks occur recently in Singapore, one of which the one against Singaporean healthcare system. Singaporean healthcare system is hacked and as a result, about 1.5 millions data of patients have been copied, including the data of Singapore's Prime Minister, Lee Hsien Loong [4].

South East Asian region is the one dominated by the Third World states, in which they still need the big states' role as their alliance to maintain their sovereignty. Compared with superpower and majority European countries, the states in South East Asian region are still poor in coping with cyber attack. It can be seen from many large-scale terrorism

attacks in many states, particularly Indonesia. Terrorism attack intended is not the straightforward attacks such as bombing, but cyber attacks such as hacking, propaganda (hoax) dissemination, and hacking by hacker. The attacks do not result in visible impact, but the attack can gradually result in big damage due to dissolution such as internal conflict and system defect. It can be one of means of acquiring a state by recognizing the fissures obtained from information leakage and propaganda disseminate successfully.

As is known, everything may occur in this 21st century. South East Asia itself is preoccupied with the emergence of ISIS terrorist group in this region. The appearance of ISIS in South East Asia was due to the collapse of ISIS in Middle East and the news about the death of Abu Bakr Al Baghdadi or known to be the head masterminding the terroristic action or called *Islamic State of Iran and Syria* (ISIS). Having been collapsed, ISIS is known attempting to look for a region to reestablish its rule or power and to occupy and to take over the power of states in South East Asian region as their base. It can be seen from some attacks occurring in some South East Asian states such as Indonesia and Philippine, the appearance of symbols and the finding of ISIS flag ever flagging in a number of actions in a number of Indonesian cities, and then viral propaganda video made by a member and an official of ISIS in South East Asia. Therefore, cyber attack is likely an effect of terrorism issue prevalence in South East Asia. It is confirmed with the attenuating military power of ISIS, due to the collapse of its rule in Syria, Middle East. The reason making the South East Asian region the next jurisdiction is because most South East Asian states are the Third World states with less power when compared with other states in many regions throughout world, so that their state resilience and security are potentially harmed and threatened viewed from economic, political, social, and cultural aspects.

In addition, South East Asian region is the one rich of resources, including both human and natural resources. In Indonesia a cyber attack occurs, creating fake information (hoax) [12]. Hoax is false information fabricated deliberately. *Hoax* itself can be a means of creating opinion to be propaganda tool and to play off one against another that in turn can generate a problem in a state. Considering the result of security research in Kaspersky lab ICS CERT, it can be seen that South East Asia is a region with inadequate insight into security to fight against cyber attack. In some news contained in *The Diplomat* site, South East Asia region is mentioned to be the one unfamiliar with IT development, including some states: Philippine, Singapore, Vietnam, and Indonesia. Kaspersky Lab occupied Philippine on the 33rd rank out of 233 states evaluated to be the ones vulnerable to cyber attack during 2015. It can be seen from the cyber attack received from a Hacker community named Lulzsec containing the database of Philippine's election commission, and disseminating personal data of global community in cyberspace. Some South East Asian States rely on those in many regions throughout world for the cooperation in preventing cyber attack and for establishing cybersecurity cooperation, for example between Indonesia and Russia as the attempt of preventing terrorism and cybercrime [13].

ASCCE has an important program to build cybersecurity in South East Asia named *Cyber Think Tank*. Cyber Think Tank is a program held to conduct a research and training pertaining to international laws such as cyberspace strategy, conflict in cyberspace, law and norms prevailing within and for cyberspace. In implementing ASCCE

program, Singapore also devises to create a combined emergency team to prevent cyberattack in South East Asia named *Computer Emergency Response Team* (CERT). And to accustom the South East Asian states with this cybersecurity in the future, a massive training is held to be followed by South East Asian states called *Cyber Range Training Centre*. This *Cyber Range Training Centre* will provide defense training performed virtually later [14]. However, viewed from realism perspective, interstate cooperation also has an objective behind. Through the establishment of cyber cooperation throughout South East Asia, each of members involved will acquire more information on other states that can be utilized for the states' interest. In addition, through this cooperation establishment, each of members participating in ASCCE can find out other states' ability of preventing cyber attack and use it to attack those states.

Such cooperation is an evolution of national security. Just like, a joint military practice, the states are required to secure their sovereignty immediately from the visible attacks, potentially more harmful to the state system. While recently technology develops very rapidly, all of those technology developments are largely digital ones. It is in contrast to nuclear weapon and technology, the ownership of which should obey international regulations and is criticized by states in the world due to its known effect. It is because nuclear technology is something that can be seen for its shape and therefore is traceable and can be studied, and regulations can be made over the technology. Instead, digital technology is a hazardous innovation. Because it is difficult to detect information on its development, in the presence of invisible platform of cyberspace as its development and experiment places, it is more difficult to control and to follow its technology development.

ASEAN has some concentrations, one of which is to build regional cyber cooperation. It is based on ASEAN *Political-Security Community Council* (APSC) *Blueprint* 2015 stating that ASEAN members should strengthen cooperation in fighting against cybercrime, by means of sharing relevant information and best practices among law enforcers in real time, considering the need for developing or improving the appropriate law and ability of coping with cybercrime [15]. Moreover, such states as Malaysia, Indonesia and Vietnam are global hotspot for the blocked big suspicious web.

The score of 3.5 times higher than standard ration shows that these states are launching malware. *Botnet spam* also found ASEAN states to be an attractive house for their attack. For example, Vietnam registered 1.68 million IP blocks from December 2015 to November 2016, and this state is the fifth one among top world states from which attack against IoT or 2016 attack comes [5]. However, the cyber security industry newly born in this region faces inadequate ability and skill growing at home along with products and fragmented solution and some providers of comprehensive solution. Several vendor relations and product distribution create operational complexity and, in some case, increases vulnerability [5]. Thus, a variety of regional cooperation in cyberspace domain is performed to ensure regional security and stability.

ASEAN Cybersecurity cooperation is manifested, among others, into *ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)*, devised to be effective on October 2019 [16]. This cooperation is driven by Singapore, as the state with the best cyber ability and development, compared with other ASEAN member states [5], indeed having many positive

potencies in the future. ASCCE is devised to provide *think tank, Cyber Emergency Respond Team (CERT) center*, and *Cyber Range Training Centre* [16]. It is of course good news to collective security of ASEAN states in cyberspace domain. It is because to prevent and to respond to cyber attack, speed and good coordination at both national and international level are required. ASCCE program will be a new platform and procedure to ASEAN to share information, to report cyber events, and to respond to it collectively [17].

ASSCE indeed should be recognized as a strategic implementation of ASEAN *Cyber Capacity Programme*, in which it can reduce the gap between ASEAN members and the constraints usually encountered such as infrastructure, human resource quality, budgeting and technology. In reality, the gap of cyberspace development can indicate benefit to the states with less developing cyber infrastructure and less connected main infrastructure. Because the less developing states become connected digitally, the learning can be inspired with other states' experience with dealing with cyber threat, policy, and best applicable practice, and data security and privacy designed to be included into inception in cyber development and connected infrastructures [19. To ensure this successful ASCCE program, Singapore invests readily up to $30 millions within five years [20]. Although the budget is not a fantastic amount, it will of course stimulate the cyber advance in the region, recalling that some ASEAN states like Cambodia, Laos, and Myanmar have not allocated significant budget yet to cyber security. Moreover, this investment is projected to protect total income of ASEAN states up to $5,450 millions in 2025 [5].

In addition, ASCCE can also be the bridge for ASEAN to cooperate with the third party, for example INTERPOL. ASCCE has been devised to cooperate with *INTERPOL* Global Complex for Innovation (IGCI) based in Singapore [18]. IGCI will provide global training and coordinate international operation or cross-border operation, to prevent, to respond to, and to act on cybercrime particularly the international-scale one. Cooperation will also be conducted by Japan, from capacity building, technology aid, to international campaign [16].

Although *ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)* has many potentialities in the future, some constraints will be faced, thereby reducing the effectiveness of ASCCE itself.

Firstly, the constraint is diversity existing among ASEAN states. The diversity intended concerns disproportional technology development, along with the underlying social-political environment in each state. However, viewed from an organizational perspective, such dissolution seems to be inexistent. Through the establishment of ASEAN community, artifacts like ASEAN ICT Masterplan 2020 recommended the consistent conceptualization of cyberspace functioning to encourage social-economic development [20]. These varying technology developments very potentially result in bias among individuals cooperating to represent their own state, particularly in early years.

Secondly, policy made by ASEAN states is not synchronous with ASCCE's plan. The lack of specific-sector governance and policy is a domino-effect problem resulting in limited and the lack of various threat intelligences. For example, in Cambodia, not much developing yet, ASCCE is present as a solution, but Cambodia's policy discourages data sharing openly, so that ASCCE's original objective is impossible to achieve. Until today, only Philippine and Thailand have been well-established

with their national policy in cyber area, and only Malaysia and Singapore belong to advanced category [5].

Thirdly, there has been no clear and comprehensive mechanism in *ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE).* The consensus is achieved only pertaining to the establishment of ASCCE with its objective and function. There are not integrated strategy development, preparedness assessment, and incidence reporting, thereby restricting the region's collective preparedness and ability of utilizing knowledge jointly. Even there is no indicator or standard type of cybercrime that can be handled through ASCCE as to what and which their border is. It of course will result in bias with the authorized party in ASEAN states, particularly those having similar agencies like Indonesia with *Badan Siber dan Sandi Negara* (State Cyber and Code Agency), Malaysia with CyberSecurity Malaysia, Philippine with Department of Information and Communication Technology, and etc [5].

Moreover, viewed from a national security perspective, ASCCE can be a long-term threat to ASEAN states [21]. On the other hand, this cyber security cooperation is expected to be an output of securitization theory [22]. However, with ASEAN states' demand for opening themselves to information and need for cyber security, ASCCE then fills in the loophole existing with capacity building, technology and software improvement, and etc for short- and medium term (7-10 years), thereby resulting in the dependency on certain states because basically cyber technology always need renewal and certain states have no capability without aid. It is just like to submit a half of the state's cybersecurity sovereignty to the region that will be hazardous in the long term. If we assume that the state is anarchic and is not trustable completely, we also assume that certain states will utilize the weakness of other ASEAN states' cyber to take such undue actions as accessing the state's confidential data, spying, sector critical supervision, and etc. It can be actually avoided through a comprehensive framework related to data protection in ASCCE and national policy establishment in each state. However, one more time, the two points still become the weakness not solved yet by ASEAN states. Thus, acceleration is needed not only at regional level, but also in local (domestic) development.

ASCCE alliance cooperation gives an example to be analyzed using securitization theory. The attempt of socializing idea taken by some South East Asian states successfully makes other states feeling insecure from the problem occurring in some ASCCE member states, but it does not impact significantly on the state. For example, ASCCE was established originally when Singapore felt threat from hacking against its governmental sites, e.g. singhealth was successfully hacked and 1.5 millions patient data were obtained. From the sample case, it can be analyzed that originally the state feeling the effect of cyber attack really was Singapore. Then, Singapore invited other South East Asian states to enter into a cooperation in cyber security
by giving other states the awareness of cyber attack. It made the attack a national threat that can threaten the state securitization. Therefore, Singapore tries to compensate the problem by inviting the neighbor states in South East Asia region to participate in coping with cyber attack and to enter into cooperation agreement in the form of ASCCE. Cyber attack also occurring in Singapore is also a form of existential threat experience by the actor if it is not responded to seriously by Singapore clearly being the Referent Object. The attempt of socializing idea is also a form of speech act given by

Singapore by disseminating an understanding concerning the importance of safeguarding cybersecurity for the sake of a state's sovereignty. If Singapore is successful, the South East Asian states will be affiliated with ASCCE because they are aware of the idea expressed by Singapore, as such Singapore's sovereignty will survive. Although the cyber threat in its state is not substantial or has not been serious yet, ASCCE alliance states also attempt to prevent and to treat the cyber attack as the form of existential threat resulting from the socialization of idea made by Singapore. Thus, through this socialization, the South East Asia alliance states expect to prevent and to understand to cope with securitization problems encountered by Singapore, particularly cyber attack.

IV. CONCLUSION

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) is a form of cooperation initiated by Singapore for the collective defense of South East Asian states in cyber space. This cooperation in coping with cyber attack is very favorable to South East Asian states, due to the weak cyber security in this region. It can be seen from many attack cyber cases that can harm a state's sovereignty in the form of propaganda such as hoax and cyber attack divulging information. Moreover, hacking, spying, and large-scale cybercrime are very worrying to the state, even potentially resulting big financial loss.

Many constraints often occur in ASEAN states in dealing with cyber security. Limited infrastructure, technology, management, and limited fund are encountered by all ASEAN states. For that reason, the initiation to create collective security in cyber area is approved and implemented by ASEAN states, expectedly to reduce the constraints and to achieve the stability of cyber security in this region. The further vision is to protect the future potential projection of ASEAN region.

This cooperation in coping with cyber attack is very favorable to South East Asian states, due to the weak cyber security in this region. It can be seen from many attack cyber cases that can harm a state's sovereignty in the form of propaganda such as hoax and cyber attack divulging information.

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) cooperation offers a variety of intensive potentialities in the future, from capacity building, human resource development, to investment fund. However, some points should be noted in this cooperation project. They are: limited comprehensive cooperation framework, diversity of ASEAN states difficult to unite, gap between states, and policy in each state not synchronized yet with the ASCCE implementation plan. It can result in a domino effect in the future. Thus, this ASCCE cooperation requires mature planning before its actual implementation in ASEAN region. However, we recommend not to postpone the implementation of ASCCE by adjusting the legal base and supporting component with thee technical development in the field.

Finally, ASEAN region stands on the edge of unlimited potentialities. E-commerce companies such as Silicon Valley giant and even IT performers at home need safe cyberspace to utilize these potentialities. We may not lose it or be afraid of taking a forward step to pursue the digital agenda due to cyber security threat. Such a threat is inevitable because South East Asia keeps developing and ASEAN's bravery will be tested in fighting against the threat, so that we need an appropriate measure.

REFERENCES

[1] Bappenas. "Pertahanan dan Keamanan Nasional". Bappenas, 2019. http://bappenas.go.id (accessed on Jun. 3, 2019).

[2] Amoroso, E. "Cyber Security". New Jersey: Silicon Press. 2006

[3] NN. "Singapura Kota Paling Unggul dalam Teknologi di Asia". Koran Jakarta, 2018. http://www.koran-jakarta.com/singapura-kota-paling-unggul-dalam-teknologi-di-asia/ (accessed on Jun. 3, 2019).

[4] Prasanth Parameswaran. "What's Next for The New ASEAN-Singapore Cyber". https://thediplomat.com/2018/09/whats-next-for-the-new-asean-singapore-cyber-center/ (accessed on Jun. 3, 2019).

[5] A.T. Kearney. "Cybersecurity in ASEAN: An Urgent Call to Action". Seoul: A.T. Kearney Inc. 2018.

[6] Austin, J. L. "How to Do Things With Words. Cambridge, Mass". Harvard University Press. 1975.

[7] Ingber, Warren., Bach, Kent., Harnish, Robert M. "Linguistic Communication and Speech acts". The Philosophical Review. 1982.

[8] Buzan, Waever, de Wilde. "Security: A New Framework for Analysis". 1998.

[9] Wæver. "Securitization and Desecuritization". New York: Columbia University Press. 1995.

[10] ASEAN. "ASEAN Leaders' Statement on Cybersecurity Cooperation". https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/ (accessed on Jun. 3, 2019).

[11] Heinl, C. H. "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime". *Asia policy, (18), 131-160*. 2014.

[12] Bulelengkab. "Pengertian Hoax dan Ciri - cirinya. Pemerintah Kabupaten Buleleng". 2019. https://www.bulelengkab.go.id/detail/artikel/pengertian-hoax-dan-ciri-cirinya-41 (accessed on June 5, 2019).

[13] Baka P. "Southeast Asia Still Has Weak Information Security Against Cyber Threats". *The Diplomat*, 2019. https://thediplomat.com/2016/10/southeast-asia-still-has-weak-information-security-against-cyber-threats/ (accessed on Jun. 5, 2019).

[14] CNA. "Singapore to Pump In S$30m for New Regional Cybersecurity Training Centre". Central News Asia, 2019. https://www.channelnewsasia.com/news/singapore/singapore-to-pump-in-s-30m-for-new-regional-cybersecurity-10735308 (accessed on Jun. 3, 2019).

[15] ASEAN, APSC. "ASEAN Political-Security Community Council Blueprint 2025". Kuala Lumpur: ASEAN Secretariat. 2016.

[16] United Nations Initiative for Disarmament Research. "Cyber Policy: ASEAN". New York: Cyber Policy Portal. 2019.

[17] Singapore Government. "Cyber Security Agency of Singapore. Singapore's Cybersecurity Strategy". Singapore: Singapore Government. 2016.

[18] Caitriona Heinl. "Moving toward a Resilient ASEAN Cybersecurity Regime". pp. 131-159. 2014.

[19] Hariz Baharudin. *Singapore to Spend $30 Million Over Next 5 Years to Fund New Regional Cyber Security Centre*. Straits Times, 2018. https://www.straitstimes.com/singapore/singapore-to-spend-30-million-over-next-5-years-to-fund-new-regional-cyber-security-centre (accessed on June 3, 2019).

[20] ASEAN. "ASEAN ICT Masterplan 2020". Jakarta: ASEAN Secretariat. 2015.

[21] Mukhtar, Sidratahta. "Keamanan Nasional: Antara Teori dan Prakteknya di Indonesia". e-jurnal Universitas Kristen Indonesia Sociae Polites: Special Edition. 2011.

[22] Situmorang, Kara. "Teori Keamanan Internasional". Depok: Universitas Indonesia Publish. 2015

PENCEMARAN ASAP LINTAS BATAS DI ASEAN". p. 330. 2017.
[30] Greenpeace. "Data Terkini Kualitas Udara Kota-kota di Asia Tenggara". 2018.
[31] IQ AirVisual. "2018 WORLD AIR QUALITY REPORT". p.11. 2018.