Journal of Social and Political Sciences

Ramadhan, Iqbal. (2020), Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). In: *Journal of Social and Political Sciences*, Vol.3, No.4, 983-995.

ISSN 2615-3718

DOI: 10.31014/aior.1991.03.04.230

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Social and Political Sciences* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Social and Political Sciences, which include, but not limited to, Anthropology, Government Studies, Political Sciences, Sociology, International Relations, Public Administration, History, Philosophy, Arts, Education, Linguistics, and Cultural Studies. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Journal of Social and Political Sciences* aims to facilitate scholarly work on recent theoretical and practical aspects of Social and Political Sciences.

Asian Institute of Research
Connecting Scholars Worldwide

The Asian Institute of Research
Journal of Social and Political Sciences
Vol.3, No.4, 2020: 983-995
ISSN 2615-3718

DOI: 10.31014/aior.1991.03.04.230

Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)

Iqbal Ramadhan[1]

[1] International Relations Department, Universitas Pertamina, Indonesia.
Email: iqbal.ramadhan@universitaspertamina.ac.id.

Abstract
For each nation-state, technology has become a new backbone. It links a range of critical infrastructures, including finance, banking, security, water, electricity, and transport. As Southeast Asia's dominant regional body, ASEAN enjoys privileges and benefits from emerging technology. In recent years, digital trade has enhanced the economic growth of ASEAN. Nßon-traditional threats such as a cyber attack are, however, the result of the modern world. Malware, malware, and advanced persistent threat (APT) lurk in every corner of cyberspace, seeking to cripple and shut down ASEAN's economic interest. The lack of rigorous regulation and a major technological gap among ASEAN members is the biggest challenge to strengthen cybersecurity in Southeast Asia. When conflict comes from the cyber world, the absence of control will jeopardize their interests. Using Archer's theory of international organization, the author aims to examine the policy in Southeast Asia to issue firm cybersecurity regulations. To improve the debate, the authors used the qualitative approach and secondary data. ASEAN needs to set the standard, aggregate and socialize the national interests of all members and enforce the unique legal formal process from the viewpoint of the authors. The Cybersecurity Regulation should certainly be consistent with the essential basis of the Treaty of Amity and Cooperation.

Keywords: ASEAN, Cybersecurity, Southeast Asia, Cyber Threat

Introduction

Emerging technology has moved every state, moving beyond its national boundaries. Today, nation-states can not be separated from the sophisticated digital world. They are integrating their political, economic, social and military systems into integrated information and technology (IT) systems. As a single dominant international institution in South East Asia, the Association of the South East Asian Nation or ASEAN is heavily dependent on the integration of the cyber world. Southeast Asia is the world's fastest-growing economic region, where the growth of economic digital technology can boost their growth (ASEAN-UP, 2019). Economic forecast that the region will achieve a trading profit of approximately US$ 102 billion in 2025 (E-Trade for All, 2018). In 2018, the region had a trade profit of US$ 20 billion from e-commerce (ASEAN Post, 2019). The growth of the digital economy is the result of an increasing number of Internet users in the region. Research conducted by Lennon Chang in his article, *Cyber*

Crime and Cyber Security in ASEAN, Singapore, was the highest internet user in Southeast Asia, with 82% of its population are active user (Chang, 2017, p. 2).

In the meantime, Malaysia, Thailand, and Brunei, Darussalam, were among the occupied countries, with 70 percent of their population highly connected (Chang, 2017, p. 2). This research was slightly different from other research mapped out by ASEAN. They concluded that Indonesia, Thailand, Malaysia, the Philippines, Singapore and Thailand were the most affiliated countries in Southeast Asia (ASEAN-UP, 2019). Approximately 132 million people were active users in Indonesia and there were 57 million internet users in Thailand (ASEAN-UP, 2019). On the other hand, 25 million Internet users were active in Malaysia, while 4.83 million Internet users in Singapore accounted for 5.25 million of the total population (ASEAN-UP, 2019). Last but not least, there were 67 million active users in the Philippines and 64 million internet users in Vietnam (ASEAN-UP, 2019). These numbers are likely to increase in the next year.

Southeast Asia is becoming a growing digital hub that can trigger the economic growth of the country that lives there. The birth of online transport has boosted the digital economic boom in this region (Feng, 2018). There are major players in online transport, such as Grab, a Malaysian tech-company and Indonesia's largest online transport company, Gojek Indonesia. In 2017, Gojek "successfully" expelled Uber from Indonesia, where most Indonesians were comforted by Gojek 's application (Yuniar, 2017). Online transport is emerging as a valuable contributor to the growth of digital economic growth in Southeast Asia (Feng, 2018). Based on *World Economic Outlook*, the International Monetary Fund (IMF) predicts that Southeast Asia will receive US$ 2.8 trillion from e-commerce (Feng, 2018). Online trading and transport will eventually contribute to South East Asia's economic growth, with a profit of approximately US$ 38 million (Thomas, 2019). Most of the 23 percent of ASEAN's economic growth came from internal trade among its members (Feng, 2018).

When Southeast Asia's region relies heavily on the digital economy, ASEAN should prepare for the challenges that lie ahead. Before ASEAN launched the *ASEAN Economic Community* (AEC) in 2015, the *ASEAN ICT Masterplan 2012* (Ramadhan, 2017, p.505) was organized. This master plan was designed to strengthen the ASEAN member partnership in the implementation of its economic community (Ramadhan, 2017, p.505). One of its clauses encourages ASEAN members to collaborate and share information on cybersecurity where they can use it to prevent cyber threats (Ramadhan, 2017, p.505). Unfortunately, the biggest problem in the region is that ASEAN does not have strict regulations to combat any threat from the cyber world (Sunkpho, Ramjan, & Ottamakorn, 2018, pp. 1-2). The lack of regulation could be a challenge for ASEAN, as it enjoys the economic advantage of e-commerce. If they are unable to address this challenge properly, ASEAN would be in jeopardy. It will shake the entire regional foundation and the states that benefit from the benefits of e-commerce (Ramadhan, 2017, p.506). Another critical issue is that the disparity or technological gap between ASEAN members is very large (Sunkpho, Ramjan, & Ottamakorn, 2018, pp. 1-2). If the attacker targets the weakest link in this system, the impact will engulf other members.

The cyber-world has become a backbone for every state to govern its nation. As far as ASEAN is concerned, the cyber world provides an opportunity for its members to thrive and prosper on digital trade, e-commerce and online business transport. Despite this opportunity, ASEAN still has a cyber threat that needs to be addressed. Myriam Dunn-Cavelty explained that cyber threats represented the complexity of the interconnected world where humans depended more on IT systems to make their lives easier (Dunn-Cavelty, 2014, p. 180). The birth of technological products, such as cloud computing and smartphones, makes them closer to human life (Dunn-Cavelty, 2014, p. 180). This can lead to problems, such as the evolution of malware and computer viruses (Dunn-Cavelty, 2014, p. 182). These types of threats can ultimately jeopardize both civil and state systems (Dunn-Cavelty, 2014, p. 182). In order to address this kind of problem, both states and international organizations should be prepared to ensure their cybersecurity. In his previous research, Roxana Radu pointed out that cybersecurity was a set of policies, tools, concepts, frameworks and technologies to protect the cyber environment from cyber threats (Radu, 2014, p. 11). Another definition came from Madeline Carr, who explained that cybersecurity was an integration of policy and technology to prevent cyber attacks from demolishing the nation's critical infrastructure (Carr, 2015, p. 8). When the state or region is more dependent on technology, they must defend it against cyber threats (Rizal & Yani, 2016, p. 62). Cyber threats can come and disrupt the system from the blue (Rizal & Yani, 2016, p. 62). This

means that the state needs to implement and develop cybersecurity policy implementation and capacity building (Rizal & Yani, 2016, p. 67).

The challenges that ASEAN will face are cyber threats can come in a different form. A cyber attack can be carried out by both state and non-state actors (Dunn-Cavelty, 2014, p. 182). For example, in his research, Jonathan D. Aronson identified three types of cyber threats that could be a hindrance in the future. These threats are intelligence gathering, hacking, and cyber warfare (Aronson, 2005, p. 540). In terms of definition, intelligence gathering is the ability of state or non-state actors to infiltrate their adversary's IT system to gather important data (Aronson, 2005, pp. 540-542). Hacking is often linked to activity in which hackers hack, disrupt, compromise and infiltrate IT systems to disrupt and destabilize IT system (Aronson, 2005, pp. 540-542). Cyberwar is a digital version of Von Clausewitz's concept of war, where two nations are engaged in a digital war trying to demolish their opponent's defense capabilities (Aronson, 2005, p. 542). Myriam Dunn-Cavelty also divided cyber threats into three types in another writing. Although, her argument was different from Aronson. Dunn-Cavelty argued that cyber-crime, cyber-terrorism, and cyber-war were the main problems for the state to overcome in the cyber world (Dunn-Cavelty, 2014, pp. 182-183). Cybercrime is an activity carried out by organized crime for economic purposes (Dunn-Cavelty, 2014, p. 181). On the other hand, cyber terrorism is a terrorist activity carried out by a terrorist group using malware to disrupt and cripple the IT system (Dunn-Cavelty, 2014, p. 181). As for cyber warfare, this type of threat comes from nation-states, where they build cyber defenses to destroy the enemy's defense capability (Dunn-Cavelty, 2014, p. 183).

An important cyber threat issue is that most countries do not know they are being attacked. There is a disparity and huge technological gap between ASEAN members (Sunkpho, Ramjan, & Ottamakorn, 2018, p. 2). Within the digital world, all ASEAN countries are becoming more interconnected. Their dependence on the digital world is critical because it plays a role in boosting and linking ASEAN's political, social and economic life (Gultom, Supriyadi, & Kustana, 2018). Cyber threat and cybersecurity issues will affect bilateral or multilateral state relations (Kshetri, 2014, p. 7). For example, US-Russia bilateral relations are often affected by cybersecurity issues such as cybercrime, with some Russian citizens targeting and stealing essential data from US banking and retail (Kshetri, 2014, p. 7). The cyber threat would be a key issue for ASEAN, given that its members have a domestic policy to deal with this threat (Khanisa, 2013, pp. 43-44). On the other hand, the technological gaps will be an obstacle because only developed countries can overcome cyber threats (Khanisa, 2013, pp. 43-44).

Literature Review

Analyzing how cyber threats can disrupt security and political stability in the region, this certainly requires previous research to support the novelty of a study. Scientific journals that discuss the importance of the role of institutions and international cooperation in addressing cyber threats have been published in a number of international journals. However, cybersecurity research in the International Relations Study, particularly in ASEAN, is still very minimal. One of the previous studies used in this study *was Enhancing International Cyber Security: A Key Role for Diplomacy*. This journal was written by Sico Van Der Meer, a researcher at the Clingendael International Relations Institute in the Netherlands. In this study, Van Der Meer (2015) explained that the cyber domain provides opportunities for state and non-state actors to act aggressively. Van Der Meer said that cyberspace interaction patterns are filled with anonymity. It may be an opportunity for a country that does not have too much power to cripple the more powerful state information system (Van Der Meer, 2015, pp. 193-195). He pointed to one empiric example, the cyberattack that paralyzed the Sony Pictures America data system by a suspected North Korean hacker as a form of protest against the film screening of The Interview (Van Der Meer, 2015, p. 196). According to the US government, this cyber attack is a protest because the film is considered to disapprove of North Korean President Kim Jong Un (Van Der Meer, 2015, p. 196).

This research seeks to compare two strategies to address cyber threats. Van Der Meer said that to overcome a cyberattack, the state could use cyber deterrence (Van Der Meer, 2015, p. 197). According to him, the term is taken from the notion of deterrence during the Cold War (Van Der Meer, 2015, p. 197). During the Cold War, two major powers, such as the Soviet Union and the United States, developed defense technologies to counteract their

respective influences. Van Der Meer argued that deterrence is still relevant to the modern world. The state may develop a cyber defense system, such as firewalls or intrusion detection (Van Der Meer, 2015, p. 197). Cyber deterrence is not the only way to prevent cyber attacks from occurring. Van Der Meer also explained that countries could develop multilateral cross-sector cooperation to mitigate cyber threats (Van Der Meer, 2015, p. 197). This strategy can be used if a country has a long-term vision of diplomacy. According to him, multilateral diplomacy will face difficulties if it is to keep pace with rapidly growing technology (Van Der Meer, 2015, p. 200). In Van Der Meer's view, this multilateral cooperation shows that cooperation between countries can refer to the establishment of international legal rules that can be applied to the cyber domain (Van Der Meer, 2015, p. 202). Multilateral cooperation in this article will be revealed in ASEAN, particularly in the context of the Southeast Asia region. According to the author, the strategy of cyber deterrence is not appropriate to be applied in Southeast Asia, as ASEAN itself adopts a non-intervention system, as stated in Article 2 of the *Treaty on the Friendship and Cooperation of Southeast Asia* (ASEAN, 2016).

Other previous research, which is very relevant to research articles, is the *ASEAN Regional Forum on Regional Cyber Security in the ASEAN Region*. This research was written by Bima YW Manopo and Diah Apriani Atika Sari to address the lack of cybersecurity regulation in Southeast Asia through an international legal approach (Manopo & Sari, 2015, p. 44). The research method written in this journal is based on an international legal approach. Manopo and Sari use international legal instruments to address cyber threats (Manopo & Sari, 2015, p. 44). The "Treaty of Friendship and Cooperation (TAC)" referred to the international legal instrument. The study stated that, by applying TAC standards, ASEAN member countries could maximize the ASEAN Regional Forum to address cyber threats (Manopo & Sari, 2015, p. 45). With reference to TAC standards, the ASEAN Regional Forum may make three decisions, such as *Confidence Building Measures* (CBM), *Preventive Diplomacy* and *Conflict Resolution* (Manopo & Sari, 2015, pp. 45-47).

According to Manopo and Sari's research, the three solutions refer to the TAC format itself. TAC standards emphasize cooperation, non-intervention and the promotion of friendship between ASEAN member countries (Manopo & Sari, 2015, p. 46). The ASEAN Regional Forum (ARF) can build trust and the principle of mutually beneficial cooperation between each member through TAC standards (Manopo & Sari, 2015, p. 45). In essence, the problem with Southeast Asia is that the legal principles of cybersecurity in each Member State differ (Manopo & Sari, 2015, pp. 45-46). Under the CBM concept, each country can promote mutual understanding in order to develop guidelines for cybersecurity (Manopo & Sari, 2015, pp. 45-46). Preventive diplomacy, which emphasizes the control of state behavior and encourages open communication in the formation of cybersecurity standards, is another output of the TAC (Manopo & Sari, 2015, p. 46). Finally, conflict resolution must be issued to deal with any cyber conflict in Southeast Asia (Manopo & Sari, 2015, p. 47). This research has similarities with the author's article, in particular with regard to security standards and cyber regulations in ASEAN. The difference is that the author does not use an international legal approach, but rather an international organization.

Another research group sees ASEAN as a strategic partner. Research entitled *India-ASEAN Cooperation on Cyber Crime* explains that India views ASEAN as a strategic partner in the maintaining of cybersecurity (Singh, 2016, p. 273). Sukhdeep Singh said that India and ASEAN's strategic partnership were inseparable from *The Look East Policy* of former Indian Prime Minister Narasimha Rao (Singh, 2016, p. 273). The study does not explain any specific framework for mitigating the threat of cyber terrorism between India and ASEAN (Singh, 2016, pp. 273-274). Research explains two issues related to cybersecurity cooperation. India and ASEAN member countries have a Computer Emergency Response Team (CERT) to detect anomalous activity on the Internet (Singh, 2016, p. 274). A member of CERT is a non-governmental organization (NGO) which is a non-profit organization. The group is made up of computer practitioners who voluntarily monitor cyber threats in their country (Singh, 2016, p. 274). India and ASEAN can work with these NGOs to monitor the flow of information on the Internet from cyber threats (Singh, 2016, pp. 274-275). Singh's point of view is indeed different from that of the authors. Singh focused on bilateral cooperation between India and ASEAN. The author sees ASEAN as a single actor, and this research does not discuss strategic cooperation between ASEAN and other IR actors. The author uses the theory of the international organization. Meanwhile, research issues discuss how ASEAN can accommodate the interests of each member state to overcome cyber threats.

The author also makes use of another research written by Caitríona H. Heinl. Her research is *Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime*. It explains that ASEAN, the largest international organization in Southeast Asia, is expected to strengthen its cyber resilience within member countries (Heinl, 2013, p. 1). Heinl explained in his quotation that ASEAN has three problems in alleviating cyber threats in Southeast Asia. These are the lack of cybersecurity regulation and the increasing cyber threat from non-state actors and the technological gap between ASEAN members (Heinl, 2013, pp. 3-4). She said that ASEAN did not adopt the Tallinn Manual on Cyber Security, as the European Union did (Heinl, 2013, p. 15). According to her, this may be dangerous as non-state actors, such as terrorist groups, can destabilize cybersecurity in Southeast Asia (Heinl, 2013, p. 26). She also saw that the technological gap between ASEAN member countries was very high. This gap could become the weakest link and could lead to a vulnerability to be exploited (Heinl, 2013, p. 32).

Heinl provides a number of analyzes to overcome existing problems. Heinl explained that it is necessary to develop strategic cooperation between ASEAN members (Heinl, 2013, p. 32). She said that ASEAN could not deny that it has emerged as one of the fastest-growing regions economically (Heinl, 2013, p. 32). The pattern of cooperation should be consistent with the non-intervention treaty (Heinl, 2013, p. 32). Heinl suggests that ASEAN should harmonize ICT rules and regulations that promote trade, investment and entrepreneurship (Heinl, 2013, p. 40). She explained that cybersecurity regulations must take into account the interests of each member without neglecting the spirit of economic growth currently being pursued by ASEAN (Heinl, 2013, p. 40). With regard to cyber threats arising from non-state actors, Heinl said that ASEAN must cooperate with the existing CERT community that has been formed among its member countries (Heinl, 2013, pp. 50-51). The research has similarities in this article, in particular the position of ASEAN as an institution responsible for protecting its member countries from cyber threats. However, Heinl's research has not theoretically shown how ASEAN, as an actor in international relations, can play a role in formulating cybersecurity regulations.

A Problem of Cyber Security in Southeast Asia

Preventing cyber threats in Southeast Asia is a hard work effort. All ASEAN members should support each other as the cyber attack is anonymous and comes out of the blue. The main question regarding cyber threats in Southeast Asia is how many cases have occurred in the region? According to AT Kearney, ASEAN has suffered from a number of malware attacks, notably *ransomware* and *cryptoware* that can encrypt and lock servers and computers (ASEAN Post, 2019). ASEAN spent US$ 1.9 billion, or 0.06 percent, from the Gross Domestic Product (GDP) region as an investment in the cybersecurity system (ASEAN Post, 2019). In order to protect the ASEAN cyber environment, at least 191 billion US dollars or 0.35% of GDP must be spent (Thomas, 2019). Ironically, ASEAN enjoys most of its economic growth from digital trade. On the contrary, they spent only 0.06 percent of their GDP, which was insufficient if they suffered cyber attacks (Thomas, 2019). Investment in cybersecurity is a major problem in Southeast Asia. Surprisingly, this corresponds to the emergence of an advanced persistent threat or APT. Stuxnet broke into the Iranian nuclear reactor cooling system in 2009. Suddenly, this APT shuts down its cooling system and destroys all industrial production (Ramadhan, 2017, p.496). Somehow, Stuxnet was a smart malware that could only target specific targets (Ramadhan, 2017, p.496). Without a doubt, the same problem would have occurred in Southeast Asia. IBM Security published its research that most states in Southeast Asia had a number of financial and reputational problems (IBM Security, 2019).

Based on research conducted in 2019, the Singaporean government tracked 850 missing medical records from the Singapore Ministry of Defense database (Mizan et.al, 2019, p.114). In the same year, the Malaysian government reported 45 incidents of ransomware attacks on its information system that encrypted a number of critical databases (Mizan et.al, 2019, p.114). The same thing was also reported by the Indonesian government. Badan Siber dan Sandi Negara (BSSN) or Indonesian National Cyber Agency tracked 513,863 malware attacks on their Internet backbone system (BSSN, 2019). They also shared the origin of cyber attacks, where most of the attacks came from Russia, China, and the USA (BSSN, 2019).

Thailand, on the other hand, reported that approximately 120,000 bank accounts from its national bank had been compromised (Nation Thailand, 2018). The situation worsened when Thailand lacked cybersecurity experts to

cover its national infrastructure (Nation Thailand, 2018). However, the Philippines was the most vulnerable country in Southeast Asia. Kasperksy Lab researched the most vulnerable countries around the world on cyberattacks, and the Philippines was one of them (Business World, 2019). The Philippines was crowned the most targeted state in Southeast Asia and ranked seventh in the world as the most vulnerable state in cybersecurity (Business World, 2019). Kaspersky argued that the citizens of the Philippines are well aware of the benefits of the Internet. Unfortunately, they have often ignored the security aspect of protecting their devices or personal information (Business World, 2019). As a result, Kasperksy had to put the Philippines on the cybersecurity issue as a vulnerable state in Southeast Asia. Organized crime or any unwanted party mostly uses various *malware* such as bot, trojan, *ransomware*, and newly developed advanced persistent threat or APT (Namanya et.al, 2018).

The key issue of cybersecurity in Southeast Asia is that ASEAN, as a pivotal organization, has no firm rule to protect its cyber environment. In his research, *The ASEAN Counter-Terrorism Weakness,* Marguerite Borelli argued that ASEAN was very vulnerable if the terrorist group attacked them from the cyber world (Borelli, 2017, p. 16). As a symbol of connectivity, ASEAN has undertaken a number of vital projects to connect members and provide for requirements such as the transport of natural gas (Borelli, 2017, p. 16). Trans ASEAN Gasline Pipes was predicted to be one of the successful ASEAN projects (Borelli, 2017, p. 18). However, Borelli explained in his research that ASEAN did not have a strong regulation on how to ensure its distribution from cyber-terrorist attacks (Borelli, 2017, p. 18). In the end, when there is no tight regulation, ASEAN members face an obstacle to the formation of strategic cooperation between them. ASEAN needs to develop robust regulations and set up a task force to protect them from cyber attacks (Khanisa, 2013, p. 46).

In the research called *A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation*, ASEAN was forced to adapt its "business process" due to fast-growing technology (Khanisa, 2013, p. 41). However, with this challenge, ASEAN would certainly face a new kind of threat (Khanisa, 2013, p. 44). ASEAN has the ASEAN Regional Forum or ARF to address cyber threats. Top government officials are holding a meeting and discussing daunting security, economics and social issues (Khanisa, 2013, pp. 48-49). Unfortunately, cybersecurity was not a top priority discussion in the ARF (Khanisa, 2013, p. 44). On the other hand, ASEAN has a tough homework to bridge a significant technological gap (Khanisa, 2013, pp. 48-49). Although ASEAN issued its *Statement on Cooperation in the Fight against Cyber Attack and Terrorist Misuse of Cyberspace* in 2006, it still faces difficulties in concluding a vigorous cybersecurity regulation (Nasu et.al, 2019).

The lack of a legal framework in ASEAN is the most urgent issue to address the cyber threat. Without any strict regulation or code of conduct, ASEAN will certainly need to work harder to address this challenge. The established regional institution, such as the European Union, has strict regulations to combat cyber threats and operational standards to protect its data (Khanisa, 2013; Ramadhan, 2017). The main problem is to analyze the capabilities and willingness of ASEAN to overcome cyber threats. Specifically, the aim of this article is to analyze the role of ASEAN as an international relations actor in coordinating, organizing and managing cybersecurity regulations or codes of conduct for the benefit of its member. The author therefore asks the research question in this article: **"How does ASEAN prevent cyber threats by formulating strict regulations in the South East Asian region and overcoming the forthcoming challenge?"**

International Organization as an Actor of International Relations

Dealing with cyber threats is certainly going to be hard work for ASEAN. Without a firm regulation and a code of conduct, as has already been mentioned, ASEAN will face difficulties in coordinating such an affair within its organization. International organizations such as ASEAN are theoretically involved in international relations (Archer, 2001, p. 68). In his *magnum opus*, Clive Archer mentioned that the international organization is an integral player in international politics, affecting the behavior of state interaction (Archer, 2001, p. 72). It divides the type of international organization into three forms: *an arena, an instrument* and *an actor* (Archer, 2001, pp. 72-79). The author will use and analyze ASEAN as an actor. On the basis of Archer's argument, the international organization as an actor can conduct its policy beyond the national borders and has the same role as the state actor (Archer, 2001, p. 79). Not only can its policy affect state actors, but the international organization also has the

legitimacy to push politically and to intervene in the name of human intervention, such as the North Atlantic Treaty Organization (NATO) or the United Nations (Archer, 2001, pp. 79-80). In addition, Archer explained that international organizations could be categorized as actors in international relations as long as they can formulate policies, manage and implement certain norms, values, and regulations (Archer, 2001, pp. 79-80). Although the existence of an international organization may have an impact on the behavior of the state's interaction, it still depends on the fidelity and commitment of its members (Archer, 2001, p. 87). However, international organizations are seen as reliable places to achieve common interest where it may be difficult to achieve if the state relies on itself (Archer, 2001, p. 87). With regard to cybersecurity, relying on a solitary movement within ASEAN members would have little positive effect. It comes from the nature of cyber threats that have anonymity, sporadic, and random attacks (Ramadhan, 2019, p.183).

Indeed, as an actor in international relations, the international organization has a function attached to it. These functions are *norms, articulation and aggregation, socialization, rule-making,* and *rule-making* (Archer, 2001, p. 92). In the context of norms, it is the responsibility of the international organization to establish norms for the management of interstate relations in the constellation of world politics (Archer, 2001, pp. 92-93). Standards are developed to lay down the necessary foundation for the organization and to set up as a vision (Archer, 2001, pp. 92-93). On the other hand, standards become a key set of guidelines for the formulation of any policy or decision (Archer, 2001, p. 93). As with the concept of articulation and aggregation, an international organization must be a place to accommodate any interest of its members (Archer, 2001, p. 94). The interest of the state is diverse, and none of them has any similarity. Archer explained that the diversity of interest and the gap between the international organization could be addressed (Archer, 2001, pp. 94-95). In order to achieve this objective, the international organization needs to understand the interests of its members and develop a strategy to achieve it (Archer, 2001, pp. 94-95). The state joins international organizations because there is a great deal of interest that they can not achieve on their own (Archer, 2001, pp. 94-95).

Archer also mentioned other functions such as socialization, rule-making, and rule-making. The international organization has a mandatory function to socialize the values of the organization and to emphasize the fidelity of its members to the institution (Archer, 2001, pp. 99-100). The international organization also socializes interest among state members and articulates each interest in socialization (Archer, 2001, pp. 99-100). Socialization also becomes another priority for an international organization to bridge its membership (Archer, 2001, pp. 100-102). In the meantime, regulation is the function of the international organization to establish a standard rule that needs to be complied with (Archer, 2001, p. 102). There are two types of legislation, such as the federal and the confederate (Archer, 2001, pp. 103-104). The type of federal regulation is governed by a supranational organization such as the European Union (Archer, 2001, pp. 103-104). This type needs a powerful organization where its position is above the level of the state-actor (Archer, 2001, pp. 104-105). As with the confederate type, rules are developed through the use of forum members to implement regulations on the basis of their domestic needs (Archer, 2001, p. 105). After establishing the basic rules for the institution, the regulation must be enforced even though Archer claims that there is no governing body (Archer, 2001, p. 105). In the case of a federal type, a supranational organization may apply the regulation among its members without exception (Archer, 2001, p. 105). On the contrary, the confederate type ensures that the application of the rule is complied with, depending on the assembly forum, in order to ensure that the regulation or code of conduct is complied with (Archer, 2001, p. 105). These concepts will be used to analyze the role of ASEAN in preventing any cyber threat.

Methodology

The author uses the qualitative method as an instrument for the resolution of research questions. A qualitative method is a form of scientific research that relies on text or language to analyze and understand social cases, phenomena or issues (Creswell, 2014, p. 42). This research highlights unique data collection, such as observation, interviews or audio-visual documents (Creswell, 2014, p. 42). In his book, John Creswell explained, "Research Design: Qualitative, Quantitative and Mixed Methods," that a researcher in social science had the role of *key instrument* and *reflexivity* (Creswell, 2014, p. 235). The key instrument highlights the researcher as the first person to collect primary data through observation and in-depth interviews (Creswell, 2014, p. 235). In the meantime,

reflexivity means that the researcher is allowed to provide an explanation or definition in a social case after conducting a number of data validation processes (Creswell, 2014, p. 235). As for the design of the research, the author uses case studies or case-based research. This approach is ubiquitous among scholars of international relations (Roselle & Spray, 2012, pp. 32-33). A case may be identified as an issue, phenomenon or policy that would be addressed through a conceptual framework and analytical thinking (Roselle & Spray, 2012, pp. 32-33). In addition, this case is an integral part of the research question that needs to be analyzed (Roselle & Spray, 2012, p. 33). In case-based research, the author may collect primary data through interviews, observation, secondary data such as journals, scientific books, or accurate statistical data from official institutions (Creswell, 2007; Creswell, 2014). In this article, the author will collect secondary data from a respectable journal and from a previous study to strengthen the analysis.

Discussion

What kind of cyber threat is likely to threaten Southeast Asia? After the end of the Cold War, many scholars of international relations (IR) predicted that the world would face many unlikely challenges. Kenneth Waltz, one of the most outstanding IR scholars, argued in his writing that the United States would meet its challenger (Waltz, 1993, p. 44). He believed that the most important thing to win an anarchy-filled competition in the world was to improve the nation's capacity in political and military matters and in economic and technological power (Waltz, 1993, p. 45). Waltz seemed to understand that the world was changing, and states needed to adapt and evolve. On the other hand, Joseph Nye also explained that there was no longer a threat to a real asset but also to an intangible asset (Nye, 2011, p. 114). He shared (2011) his view on his book *The Future of Power*, which Nye argued was that there were three powers that the state should have. The first was hard power, soft power, and cyber power (Nye, 2011, p. 115). The state could achieve hard power through the exercise of military and political aspects, while soft power should be achieved through the implementation of cultural and economic sectors (Nye, 2011, p. 115). In the meantime, cyber power can be achieved by producing and harnessing technological capabilities (Nye, 2011, pp. 115-116).

Before carrying out the primary tasks of international organizations, ASEAN should define and identify the main threats to cybersecurity. Many types of research explain and examine cyber threats. In his research, Andree Bendovschi, *Cyber Attacks – Trends, Patterns, and Security Counter-Measures* identified a number of cyber-world threats. Based on her research, *middle-attack man, brute force, distributed denial of service* (DDoS), *malware, phishing*, and *social engineering* are major threats that could harm the IT system (Bendovschi, 2015, pp. 3-4). Bendovschi conducted her research by examining her pattern over the last three years (Bendovschi, 2015, p. 5). Eligible data were collected worldwide and concluded what kind of cyber threats were likely to occur (Bendovschi, 2015, p. 5). Meanwhile, Harry Katzan Jr. also analyzed the type of cyber attacks in his research. Although his research was likely similar to Bendovschi, he noted that *advanced persistent threat* (APT) could pose risks to key aspects of human life, such as trade, diplomacy, finance, health, energy, and transportation (Katzan Jr, 2016, p. 3). These cyber-threats should be addressed as they harnessed network protocols in our daily lives (Katzan Jr, 2016, p. 3). The type of cyber attacks may be similar to each other. It means that a cyber incident can happen elsewhere in one country. As a thriving region, Southeast Asia can not isolate itself and pretend that cyber-attacks will not threaten it.

Why is resolving this cyber threat a daunting challenge for ASEAN? First, a cyber attack can be a destructive force to cripple and bring down the entire nation. Many cyberattacks target critical sectors such as banking, finance, water supply, transport and energy (Marshall & Saulawa, 2015, p. 10). An anonymous hacker had once successfully brought down the Moscow Central Bank and halted its business process (Marshall & Saulawa, 2015, p. 9). A prominent international defense organization such as NATO has already seriously attacked cyber attacks since Russian hackers allegedly attacked the Estonian power grid due to conflicting relations between Estonia and Russia (Marshall & Saulawa, 2015, p. 9). Another cyber threat problem is access control to attack and crippling the nation as a whole (Abomhara & Koein, 2015, p. 70). *The Internet of Things* (IoT) has become a hotbed for attackers to attack. In the DDoS attack, the attacker is merely harnessing and infiltrating multiple IoT objects, such as smartphones, smart TVs, smart cars, and so on, to control massive cyber attacks to demolish the state's IT system

(Abomhara & Koein, 2015, p. 69). The simplicity and anonymity of cyberspace can be used by state actors and non-state actors, such as terrorist groups. Cyberspace has become a new terrorist site since it provides security and anonymity for the conduct of their hideous acts (Bieda & Halawi, 2015, p. 37).

Since the threat is imminent and ASEAN does not have a strict cyberspace regulation or code of conduct, they will be faced with another challenge. ASEAN can reflect on the 2015 United Nations Group of Government Experts (UNGGE) report to set a concrete standard. The United Nations has agreed to lay down thirteen rules on responsible state behavior to ensure that cyberspace is not misused (UN, 2015). One of the standards established by the UNGGE mentioned state should cooperate to improve the stability and security of internet communication and technology (UN, 2015). These norms regulate state behavior for not misuse of ICT to harm the interests of others (UN, 2015). As Zine Homburger explained in his research *The Necessity and Pitfall of Cyber Security Capacity Building for Standard Development in Cyberspace*, he said that UNGGE's norms are being discussed in selected countries such as China, Russia and the United States (Homburger, 2019, p. 228). They tended to disagree on the grounds of their dissimilarity as to how the standards could be implemented at the domestic level. Although the standards have stalled since 2017, it can be a simple guide for nations or international organizations to set up a cyberspace standard (Homburger, 2019, p. 229).

Theoretically, the development of norms has become a crucial task in dealing with specific problems. In the previous chapter, Archer has already emphasized the importance of norms in international organizations (Archer, 2001). Cybersecurity norms can be defined as a means or tool to reduce conflict (Raska, 2018, p. 5). Cyber norms will eventually be regulated to maintain state behavior in cyberspace (Raska, 2018, p. 5). In order to establish a strong norm in Southeast Asia, ASEAN can begin its first step on the basis of its basic *Treaty of Amity and Cooperation* (Manopo & Sari, 2015, p. 46). Why is this treaty central to the development of cyber norms in the ASEAN body? However, this Treaty is a set of guidelines for ASEAN countries to act in friendship and to have good faith among their members (Manopo & Sari, 2015, p. 46). *The Treaty of Amity and Cooperation* is a necessary foundation for an ASEAN non-interference policy (Manopo & Sari, 2015, pp. 45-46). From the author's point of view, this treaty has become an essential foundation for ASEAN if it is to issue guidelines or codes of conduct. At the end of the day, cyber norms must adhere to this treaty. On the other hand, ASEAN can not ignore the technological disparity gap between its members. The disparity can be enormous in trouble if organizations are unable to bridge it. An attacker is likely to infiltrate and shut down the weakest link in the organization (Homburger, 2019, p. 229). With this cyber norms, ASEAN can set a guideline to bridge the technological disparity in the Southeast Asia region.

Creating cyber norms can be implemented in a variety of ways. First, ASEAN can maximize existing important forums, such as the ASEAN Regional Forum, to add cybersecurity as their main priority (Noor, 2020, p. 112). Undoubtedly, ASEAN is providing a multilateral forum for Southeast Asian countries to negotiate their common problems (Noor, 2020, p. 112). By using this privilege, ASEAN members should listen and understand what others want about their cybersecurity. In 2018, the ASEAN Ministerial Conference on Cyber Security (AMCC) agreed with the UNGGE principle of enhancing regional connectivity and improving the digital realm (Noor, 2020, p. 112). In South East Asia, the basic cyber norms should be based on incremental approaches, capacity building and non-intervention policies (Noor, 2020, pp. 112-113).

On the other hand, ASEAN can also engage IT-based communities such as the Computer Emergency Rescue Team or CERT with multiple bases across Southeast Asia (Rizal & Yani, 2016, p. 67). Since CERT acts independently and has many talented members, ASEAN may gather information and input to build a robust standard (Rizal & Yani, 2016, p. 67). The last one, the creation of norms, can be triggered by the most sophisticated members of ASEAN. Singapore is the most advanced country in ASEAN, becoming a technology hub in Southeast Asia and chairing AMCC (Ang, 2018). The heavy burdens depend on Singapore and ASEAN to shape the perfect and appropriate standards to be implemented in Southeast Asia (Ang, 2018). Since the UNGEE standards have stalled, Singapore can set standards that are appropriate to its needs and context (Ang, 2018).

The most difficult part of creating cyber norms is the aggregation of national interest and socialization. ASEAN relies most of the time on its legal-rational norms (Narine, 2009, p. 372). Their legal-rational norms include a

prohibition against the use of force and a commitment to a peaceful settlement of disputes, regional autonomy, non-interference doctrine, and no military pacts, and a preference for bilateral defense cooperation (Narine, 2009, p. 372). Cyber norms would be useless if they did not escalate into regulation or code of conduct. Consensus must be reached before a regulation is made (Dai & Gomez, 2018, p. 2). The consensus-based process takes time because ASEAN must ensure that all members' interests are properly addressed (Dai & Gomez, 2018, pp. 2-3). Through important meetings such as the ASEAN Regional Forum or the ASEAN Ministerial Meeting, ASEAN, as a socio-political hub, can socialize and emphasize their interest, such as building national capacity in the IT system, mobilizing against cybercrime, and securing their national economic interest (Dai & Gomez, 2018, pp. 2-3). ASEAN should conduct fraternal consultations and reach a consensus on the adoption of norms (Yukawa, 2017, p. 2).

Fraternal consultation and consensus are challenges that ASEAN needs to overcome. Based on Archer's theory, aggregation and socialization are part of the organization's mission to bridge gaps and interest. In the context of consultation and consensus, these are the primary functions of aggregation and socialization. Diversity of national interest may be detrimental to the ASEAN objective (Feraru, 2015, p. 29). In order to reach an agreement between ASEAN members, they must ensure that the decision-making process is "a pace that is comfortable for all" (Feraru, 2015, p. 29). In a consensus-based decision-making process, each member has a veto to deny any proposals that threaten their national interests (Severino, 2006). In the meantime, ASEAN members will consult and recognize other interests in the context of consultation through the use of bodies such as the ASEAN Political-Security Community Council, the ASEAN Economic Community Council or the ASEAN Socio-Cultural Community Council (Feraru, 2015, p. 36). Each body has its related ministerial bodies, consisting of representative ministers from all members (Feraru, 2015, p. 36).

In the context of cybersecurity, what should ASEAN do to aggregate interest and socialize to prevent cyber threats? Norms are a set of guidelines for ASEAN to manage state behavior and to scale it up to issue a regulation or a code of conduct (Dai & Gomez, 2018, pp. 4-5). ASEAN can use existing bodies such as the ASEAN Political-Security Community (APSC) to do this. This division is essential for the development and establishment of robust cybersecurity regulations or guidance (Khanisa, 2013; Rizal & Yani, 2016). Inside APSC there are ASEAN Sectoral Ministerial Bodies, the Permanent Representative Committee (CPR) and the Senior Officer Meeting or SOM (Feraru, 2015, p. 36). These divisions are inseparable parts of the decision-making process (Feraru, 2015, p. 36). Escalating standards into regulations or codes of conduct can be implemented by aggregating and socializing the importance of cybersecurity within APSC. Each year, the ASEAN Ministerial Meeting or the AMM will hold a meeting to discuss important issues (ASEAN, 2007a). By focusing on these mechanisms, each member consolidates and discusses their interests and bridges the gap. One thing is certain: a norm can not be scaled to the ASEAN summit unless a consensus has been reached (Feraru, 2015, pp. 28-29). ASEAN needs to ensure that all member interests in cybersecurity are fully addressed. Furthermore, their interest should be aligned with the basic norms and the foundations of ASEAN itself. Once it has been submitted, the draft or proposal is ready to be discussed at the higher level of the ASEAN Summit.

There is a considerable difference between ASEAN and the EU in the development of policies, regulations or codes of conduct. The EU is much closer to federalism in order to establish and implement a rule (Keating, 2017, p. 616). Since the EU has an authority over its members, it is easier for them to impose and regulate the European region (Keating, 2017, p. 620). Unfortunately, the same regulatory and implementation mechanism is not similar to that of ASEAN. This organization is very relevant to the confederate system (Archer, 2001, p. 105). ASEAN must adhere to a "rule-based community" to implement cybersecurity policy or regulation (Gerard, 2018, pp. 210-211). What is a rule-based community? This means that the proposal for a policy or regulation must reach a consensus among ASEAN members and does not violate the *Treaty of Amity and Cooperation* (Gerard, 2018, p. 217). As a result, the draft of cybersecurity policy should first meet this requirement. Prior to the ASEAN Summit, the draft was discussed at the ASEAN Law Minister 's Meeting (ALAWMM). The organization entrusts them with the development of cooperation programs to strengthen the rule of law, the judicial system and the legal infrastructure (Gerard, 2018, p. 217). Without in-depth cooperation, ASEAN will face a challenge in the face of cyber conflict. Like any other conflict, cyber-attacks can bring an end to the interests of ASEAN. Strengthening cooperation between ASEAN countries' ministerial legislation is therefore important.

Although all ASEAN members fully accept the proposal for a cybersecurity regulation, there is still a need for enforcement to implement the policy. ASEAN can rely on its chairperson to implement the policy or rule (Suzuki, 2020, p. 3). The Chairman of ASEAN has always rotated on an annual basis. However, the chairman may include specific and key issues that need to be addressed (Suzuki, 2020, p. 12). With a strong agenda-setting, the chairman can focus his negotiations and discussions by assessing equality between Member States (Suzuki, 2020, pp. 12-13). As regards cybersecurity policy, the chairman of ASEAN could focus his annual agenda by discussing and implementing it at the ASEAN Summit (Suzuki, 2020, pp. 12-13). The chairman also set the agenda by prioritizing the *Code of Conduct on Cyber Security* as their primary agenda. The role of the chairman is crucial as it can encourage all members to avoid non-agreement (Suzuki, 2020; Feraru, 2015). When the proposal for a cybersecurity policy is accepted, ASEAN uses its bodies in the ASEAN Secretary-General to oversee the agreement (Feraru, 2015, pp. 28-30). Implementing cybersecurity policy at home can be a challenge. Consensus within ASEAN is exhausting. ASEAN is introducing the "ASEAN minus X formula" to enhance cooperation (Yukawa, 2017, p. 12). If cyber policy is formulated at the ASEAN meeting, even though several members are willing to agree, they can implement it immediately at their domestic level (Yukawa, 2017, p. 12). However, the outcome of the ASEAN meeting must result in an incremental approach. An approach where policy can be adopted on the basis of the need of a member. Cybersecurity policy, regulation or code of conduct must address specific issues such as the prevention of advanced persistent threats, the handling of cyber incidents, cooperation between CERT in Southeast Asia, cooperation and capacity building between ASEAN members to build cyber resilience (Ramadhan, 2017; Ramadhan, 2019; Dai & Gomez, 2018).

Conclusion

Formulating cybersecurity regulation in Southeast Asia is defying and graving. Although there is a dominant regional player like ASEAN, there is no robust regulation or policy to combat cyber attacks in this region. On the contrary, ASEAN is benefiting from digital commerce, which is boosting its economic growth. ASEAN should put in place robust regulations to manage its region from cyber threats in order to protect its interests. The first step in formulating this Regulation is the creation of norms. This organization can start from the *Treaty of Amity and Cooperation* with a view to establishing the guidelines for cyber norms. In line with the ASEAN Treaty, cyber norms must aggregate and socialize all member interests in order to avoid prejudice and bias. Indeed, ASEAN can involve not only a state actor, but also a community such as CERT. The role of the chairman of ASEAN can not also be ignored. It has a responsibility to bridge the interests of the members and to reach an agreement. Once an agreement has been reached, ASEAN's Secretary-General is committed to ensuring that cybersecurity regulations or policies are implemented among ASEAN members. The policy needs to be able to adapt quickly at national level and to prevent any cyber threats. On the other hand, the policy should address cyber incidents, cooperation between CERT, cooperation and capacity building among ASEAN members to build cyber resilience. The policy should, above all, be aligned with the *Treaty of Amity and Cooperation*.

References

Abomhara, M., & Koein, G. M. (2015). Cyber Security and The Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks. *Journal of Cyber Security Vol.4*, 65-88.

Ang, B. (2018). *Next Step for Cybernorms in ASEAN.* Retrieved from https://www.rsis.edu.sg/rsis-publication/cens/next-steps-for-cyber-norms-in-asean/

Archer, C. (2001). *International Organizations (3rd eds).* London: Routledge.

Aronson, J. D. (2005). Causes and Consequences of the Communication and Internet Revolution. In J. Baylis, & S. Smith, *The Globalization of World Politics: An Introduction to International Relations* (pp. 540-559). London: Oxford University Press.

ASEAN. (2007a). *Charter of The Association of Southeast ASEAN Nations (ASEAN Charter)*. Retrieved from http://www.asean.org/wp-content/uploads/2012/05/11.-October-2015-The-ASEAN-Charter-18th-Reprint-Amended-updated-on-05_-April-2016-IJP.pdf

ASEAN. (2016). *Treaty of Amity and Cooperation in Southeast Asia*. Retrieved from https://asean.org/treaty-amity-cooperation-southeast-asia-indonesia-24-february-1976/

ASEAN Post. (2019). *Strengthening Cybersecurity in ASEAN*. Retrieved from https://theaseanpost.com/article/strengthening-cybersecurity-asean,

ASEAN-UP. (2019). *Overview of E-Commerce in Southeast Asia [Market Analysis]*. Retrieved from https://aseanup.com/overview-of-e-commerce-in-southeast-asia/

Bendovschi, A. (2015). Cyber-Attacks-Trends, Patterns and Security Countermeasure. *Procedia Economics and Finance*.

Bieda, D., & Halawi, L. (2015). Cyberspace: A Venue for Terrorism. *Issues in Information System, Vol 6 (3)*, 33-42.

Borelli, M. (2017). ASEAN Counter Terrorism Weakness. *Counter Terrorist Trends and Analysis, Vol.9 (9)*, 14-20.

BSSN. (2019). *Honeynet Project: BSSN's Measure to Detect Cyber Threats*. Retrieved from https://bssn.go.id/wp-content/uploads/2019/06/PRESS-RELEASE-honeynet-project.pdf

Business World. (2019). *Philippines Fifth on Cyber-Attack List*. Retrieved from https://www.bworldonline.com/philippines-fifth-on-cyber-attack-list/

Carr, M. (2015). Crossed Wires: International Cooperation on Cyber Security. *Interstate Journal of International Affairs, Issue II*, 2-13.

Chang, L. (2017). *Cyber Crime and Cybersecurity in ASEAN*. Retrieved from https://www.researchgate.net/publication/318474107

Creswell, J. (2007). *Qualitative Inquiry & Research Design: Choosing Among Five Approaches (2nd Eds).* London: SAGE.

Creswell, J. (2014). *Research Design: Qualitative, Quantitative & Mixed Methods Approaches (4th Eds).* London: SAGE.

Dai, C. T., & Gomez, M. A. (2018). Challenges and Opportunities for Cyber Norms in ASEAN. *Journal of Cyber Policy Vol 3 (2)*, 217-235.

Dunn-Cavelty, M. (2014). Cyber Threats. In V. Mauer, & M. Dunn-Cavelty, *The Routledge Handbook of Security Studies* (pp. 180-189). New York: Routledge.

E-Trade for All. (2018). *ASEAN: E-Commerce Set to Dominate the Region in 2019*. Retrieved from https://etradeforall.org/asean-e-commerce-set-to-dominate-the-region-in-2019/

Feng, J. (2018). *On The Cusp*. Retrieved from https://www.imf.org/external/pubs/ft/fandd/2018/09/pdf/asean-digital-economy-infographic-feng.pdf

Feraru, A. S. (2015). ASEAN Decision Making Process: Before and After The ASEAN Charter. *Asian Development Policy Review, Vol 4 (1)*, 26-41.

Gerard, K. (2018). ASEAN as a "Rules-based Community": Business as Usual. *Asian Studies Review, Vol.42 (2)*, 210-228.

Gultom, R. A., Supriyadi, A. A., & Kustana, T. (2018). Strengthening ASEAN Cyber Cooperation. *International Journal of Management and Technology, Vol.13 (1)*.

Heinl, C. (2013). *RSIS Working Paper.* Singapore: NTU.

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society, Vol.33 (2)*, 224-242.

IBM Security. (2019). *Cost of Data Breach Record 2019.*

Katzan Jr, H. (2016). Contemporary Issues in Cybersecurity. *Journal of Cybersecurity Research, Vol.1 (1)*, 1-6.

Keating, M. (2017). Europe as Multilevel Federation. *Journal of European Public Policy, Vol.24 (4)*, 615-632.

Khanisa. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies, Vol.1 (1)*, 41-53.

Kshetri, N. (2014). Cybersecurity and International Relations: The U.S. Engagement with China and Russia. *FLACSO-ISA.* Buenos Aires: University of Buenos Aires.

Manopo, B. Y., & Sari, D. A. (2015). ASEAN Regional Forum: Realizing Regional Cyber Security in ASEAN Region. *Belli ac Pacis, Vo.1 (1)*, 44-51.

Marshall, B. J., & Saulawa, M. A. (2015). Cyber-Attacks: The Legal Response. *International Journal of International Law, Vol.1 (2)*, 1-18.

Mizan, N. S. (2019). CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. *International Journal of Advanced Trends in Computer Science and Engineering*, 113-119.

Namanya, A. P. (2018). *The World of Malware: An Overview*. Retrieved from https://www.researchgate.net/publication/327665678

Narine, S. (2009). ASEAN in The Twenty-first Century: A Sceptical Review. *Cambridge Review of International Affairs, Vo.22 (3)*, 369-368.

Nasu, H. (2019). *The Legal Authority of ASEAN as a Security Institution.* England: Cambridge Press.

Nation Thailand. (2018). *Attacks Highlights Shortage of Cyber Experts*. Retrieved from https://www.nationthailand.com/news/30351401

Noor, E. (2020). Positioning ASEAN in Cyberspace. *Asia Policy, Vol.15 (2)*, 107-114.

Nye, J. S. (2011). *The Future of Power.* USA: Perseus Book Group.

Radu, R. (2014). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In J. F. Kremer, & B. Muller, *Cyberspace and International Relations: Theory, Prospect and Challenges* (pp. 3-20). Bonn: Springer.

Ramadhan, I. (2017). Peran Institusi Internasional dalam Penanggulangan Ancaman . *Jurnal Populis, Vol.2 (4)*, 495-508.

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies, Vol.3 (2)*, 181-192. DOI: https://doi.org/10.33541/japs.v3i1.1081

Raska, M. (2018). *Cyber Security in Southeast Asia.* France: Asia Centre.

Rizal, M., & Yani, Y. M. (2016). Cyber Security and Its Implementation in Indonesia. *Journal of ASEAN Studies, Vol.4 (1)*, 61-78.

Roselle, L., & Spray, S. (2012). *Research and Writing in International Relations.* Boston: Pearson Longman.

Severino, R. (2006). *Southeast Asia in Search of an ASEAN Community: Insights from The Former ASEAN Secretary General.* Singapore: Institute of Southeast Asian Studies.

Singh, S. (2016). India-ASEAN Cooperation on Cyber Crime. *International Journal of Advanced Research in Computer Science, Vol.7 (6)*, 273-275.

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). *Cybersecurity Policy in ASEAN Countries*. Retrieved from https://www.researchgate.net/publication/324106226

Suzuki, S. (2020). Can ASEAN Offer a Useful Model? Chairmanship in Decision-making by Consensus. *The Pacific Review*, 1-27.

Thomas, J. (2019). *Southeast Asia's Internet Economy Booming*. Retrieved from https://theaseanpost.com/article/southeast-asias-internet-economy-booming

UN. (2015). *Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015*. Retrieved from https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf

Van Der Meer, S. (2015). Enhancing International Cyber Security. *Security and Human Rights Vol. 26*, 193-205.

Waltz, K. (1993). The Emerging Structure of International Politics. *International Security, Vol.18 (2)*, 44-79.

Yukawa, T. (2017). The ASEAN Way as a Symbol: An Analysis of Discourses on the ASEAN Norms. *The Pacific Review*, 1-17.

Yuniar, R. W. (2017). *Uber Rival Grab Rolls Out Indonesia Investment Plan*. Retrieved from https://www.wsj.com/articles/uber-rival-grabtaxi-rolls-out-indonesia-investment-plan-1486012764