ASEAN International Sandbox Conference 2023
http://aseansandbox.org

Regional Cooperation on Cybersecurity Challenges: An Assessment of ASEAN's Efforts to Promote Shared Cybersecurity

Sisco Kanampumbi Ilunga

Institute of Diplomacy and International Studies, Rangsit University, Pathum Thani, Thailand
E-mail : sisco.ik@gmail.com

Abstract

The study examines regional cooperation on cybersecurity in the ASEAN region between 2013 and 2023. The study is anchored in neorealist international relations theory, which postulates that states compete for power as a means to survival but that states may also ally and cooperate to counter shared threats. The research questions of the study are: (1) What are ASEAN's current cybersecurity initiatives and how does it cooperate in tackling the challenges of cyberattacks on critical information infrastructure? (2) What are the challenges and limitations affecting ASEAN in realizing regional cooperation on cybersecurity? (3) What improvements could be made to ASEAN's existing cybersecurity framework to combat the challenges of cyberattacks on critical information infrastructure? A qualitative descriptive analysis is used to analyze data collected from secondary sources. The secondary data are studied extensively to extract relevant results, which are categorized to achieve the research objectives. The major challenges to cooperation identified by the study are: technological gap among member states, lack of common response strategies, inadequate trust among member states, the dependency of ASEAN's Computer Emergency Response Team (CERT) on member states to share intelligence, lack of new common cyber norms, and the sophistication of recent cybersecurity challenges. The study recommends that ASEAN should formulate and implement regional cybersecurity norms, establish a cybersecurity taskforce to enforce these norms, and that ASEAN-CERT should regularly train and retrain the CERTs of member states on the best practices in sharing intelligence information.

Keywords: *ASEAN, cybersecurity, cyberthreats, regional cooperation, critical information infrastructure*

1. Introduction

1.1 Background and Significance of the Problem

The globalized world, with developing economies and fast-advancing technology, serves as a threat to many actors in the international community. Consequently, every individual living on earth is a potential victim of cybercrime, no matter their technological sophistication or know-how. Cybercriminals use globalized Internet resources and services to commit crime in cyberspace, which is unrestricted by physical boundaries, causing significant impact on the global digital economy. The International Monetary Fund (IMF) (2020) reported that cybercrime is a "new threat to financial stability" and to overcome this global threat cybersecurity infrastructures and frameworks must be developed in low and middle-income countries where there is proliferation of cybercrime, primarily due to poor cybersecurity infrastructures and frameworks.

Recently, the Association of Southeast Asian Nations (ASEAN) has witnessed remarkable advancement in Internet and computer connectivity with geometric improvement in the penetration rate of Internet users (ASEAN Secretariat, 2020). The ASEAN region has a total population of about 659 million and is regarded as the world's third most populous region. Out of a 663.47 million populations, Statista (2021) estimated that Southeast Asia has approximately 495.95 million total Internet users. This high cyberspace penetration has led many governments and private organizations to connect to cyberspace for ease of improving service delivery. The IMF (2020) has projected that in 2022 the ASEAN region will make over US$ 2.8 trillion from engaging in e-commerce. This opportunity comes with the danger of increased attacks on government and business information infrastructure, which over the years have remained targets of cyber criminals.

As cybercrime is an inherently transnational phenomenon the best way to effectively combat it is through sophisticated regional cooperation on cybersecurity frameworks. It is an established fact that a secured regional interconnected digital space will act as promoter of economic advancement, improved

regional interconnectivity and improvement of living conditions for all within the region, as there will be adequate communication of information as well as sharing of human resources (Portnoy & Goodman, 2009; ASEAN, 2021). This study sought to assess the efforts of the ASEAN to promote shared cybersecurity through regional cooperation on cybersecurity challenges, especially the protection of critical information infrastructure (CII).

Critical information infrastructure refers to computer networked systems that provide support for the effective delivery of fundamental services in a country, damage to which can cause harm to the well-being of her citizens. Cyber Security Authority (2021) defines critical information infrastructure as the entire interconnected network (physical or virtual) as well as the system, functions, processes, and information that are essential to the nation-state in such a way that its destruction would have grave consequences on the overall internal and external security of the country as well as the economic and social wellbeing of her citizens. Similarly, the Cybersecurity Act of the Republic of Ghana (2020) sees critical information infrastructure as a networked computer system that is vital for the security of the nation or the economic and social health of her citizens. Critical information infrastructure ranges from the public telephone system, the interconnection of networked computers, satellite wireless networks, databases of organizations such as a country's military defense intelligence information, and educational databases among others. Any damage of any type of critical information infrastructure would interrupt the economic or social health of the population of a country, hence, the urgent need to protect it from attack.

It is estimated that the top one thousand organizations in ASEAN, most especially private businesses, as well as governmental critical information infrastructure, are at high risk of losing US$ 750 billion in market capitalization due to existing cybersecurity threats in the region (Yaksha 2018). There was a cyber-conflict between Malaysia and the Philippines in 2013 over Sabah land dispute which led to defacement of government websites by hackers claiming to be members of Anonymous (Newsbytes, 2013). In 2017, APT32 group, which is believed to work for the Vietnamese government, hacked ASEAN's website during its annual summit (Thomas, 2019). It was also reported that the same group sponsored by the Vietnamese government launched attacks on websites of ministries and government agencies in Lao PDR, Cambodia, and the Philippines. It is believed that the Vietnamese government is using the APT32 group to attack other governments' critical information infrastructure with the aim of getting strategic intelligence information (Vijayan, 2019). In 2020, the Malaysia Armed Forces (MAF) reported that there was an attack on military networked data (The Straits Times, 2020). According to Saballa (2022), Singapore has continued to experience attacks on their military website in recent years. The report revealed that in 2021 alone, there were 9080 ransomware and botnet attacks on Singaporean military critical information infrastructure. This series of state related cyber conflicts between countries in ASEAN shows that the various member states are prone to state-related cyber conflict on their critical information infrastructure. It also implies that critical information infrastructure is often a target of cyberattacks and crimes within ASEAN. Thus, the focus of this study will be on protecting critical information infrastructures in ASEAN through regional cooperation and collaboration.

As postulated by ASEAN Cyberthreat Assessment 2021 (Interpol, 2021), no ASEAN member state or critical information infrastructure is free from the threat of cybercrime, especially when it is focused on attacking the critical information infrastructure of government institutions and private businesses. In terms of cyber vulnerabilities, a 2016 study reported that the critical information infrastructures of ASEAN member states are 80 percent more prone to be targeted by cybercriminals when compared to the rest of the world (FireEye, 2018), with the Philippines being one of the top targets in the world. The only way forward is a sophisticated and robust cybersecurity framework aimed at protecting critical information infrastructures through regional cooperation that will include timely and effective intelligence information sharing, sharing of technical human resources, and other technological infrastructures which are meant to secure and protect the critical information infrastructure from unauthorized access and cyberattacks by cybercriminals.

1.2 Theoretical Framework

The study is anchored in neorealist international relations theory, which was originally propounded by Kenneth Waltz in *Theory of International Politics* (1979). Neorealism emerged as a challenger to classical realism, reflecting a desire to develop a more scientific and less historical or psychological approach to state behavior. The basic assumptions of neorealism are: that great powers are the main actors in world politics;

that states operate in an anarchic international system, which means that there is no centralized political authority or ultimate arbiter that stands above states; and that all states possess some offensive military capability. The consequence of anarchy, together with the fact that each state has the power to inflict some harm on its neighbors and that states can never be certain of others' intentions, is that states must compete for power as a means to ensure their security and survival. Survival is the main goal of states, and as rational actors states are capable of formulating sound strategies to maximize their prospects of achieving it (Mearsheimer, 2013).

Although the quest for survival leads states to compete for power, it can also result in alliances and other forms of cooperation between states that aim to counter shared threats. Neorealism considers interactions between states as a reflection of the relative power distribution between them. A stronger state dominates smaller states, and smaller states tend to bandwagon with the stronger state. States that have a relatively equal power balance deter each other. But conflicts are inherent in the neorealist world, while peace and cooperation are merely considered temporary (Nugroho, 2011). Thus, neorealism proposes that cooperation is possible among states in the international system, but that many setbacks will likely threaten the sustainability of such cooperation.

ASEAN regional cooperation on cybersecurity challenges to critical information infrastructure is one form of cooperation among states in the international system that is fueled by individual state interest to fight common enemies through common policy, similar preparedness, and response measures, as well as sharing of intelligence information. Neorealism recognizes that states form alliances to push for common goals such as this at certain points. However, it also emphasizes that alliances are not more important than individual state interest and sovereignty, which as we shall see, is an obstacle to effective cooperation within ASEAN.

1.3 ASEAN's Initiatives and Previous Studies

Over the years, efforts towards regional cooperation on protecting critical information infrastructure have been initiated by ASEAN. For example, the popular Singapore Declaration in 2003 aimed to protect the cyber system and space against attack and to enhance interconnectivity and interoperability (Saravade, 2016). Moreover, ASEAN countries have made attempts towards establishing regional cooperation on cybersecurity through such efforts as: ASEAN Cyber Capacity Programme (ACCP), ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Ministerial Conference on Cybersecurity (AMCC), ASEAN Regional Forum (ARF) Inter-Sessional Meeting on ICT Security, ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), and the ASEAN Defence Ministers' Meeting (ADMM)-Plus Experts' Working Group Meeting on Cyber Security (Lung, 2018). Additionally, ASEAN created a Ministerial Conference on Cybersecurity (AMCC), with the goal to develop a common strategy to adopt at the regional level, addressing topics such as cybersecurity control and resilience protection (Raemdonck, 2021). Within the AMCC, a coordinating committee on cybersecurity (ASEAN Cyber-CC) was created with the role to work cross-sectorally with relevant stakeholders on cybersecurity-related issues (Raemdonck, 2021).

ASEAN Telecommunications and IT Ministers (TELMIN) played a key role in the formulation of ASEAN's Internet and cyber security policy. It focuses mainly on ICT capacity building and collaboration among ASEAN member states (Lung, 2018). In September 2003, the Singapore Declaration was adopted by TELMIN at its third meeting. The Declaration set up an "action agenda to harness technological advances in Information and Communications Technology" (Saravade, 2016). In the action agenda, TELMIN decided that all ASEAN member states should establish national Computer Emergency Response Teams (CERTs) by 2005, a platform to coordinate computer incident information reporting and sharing (Saravade, 2016; Candice & Miguel, 2018). The establishment of CERTs has been seen as the mutual agreed performance criteria among ASEAN member states. And, in the 2008 ASEAN Economic Community Blueprint, intensifying capacity building and training of national CERTs and strengthening cooperation and coverage of ASEAN regional cyber- security network was listed as a priority action for ASEAN member states in 2008-2009. Nonetheless, the goal of establishing national CERTs was not achieved until February 2012 when Lao CERT was launched.

Previous studies have shown that despite ASEAN's attempts at regional cooperation in combating cybersecurity challenges in Southeast Asia, the organization still suffers great difficulty in actualization of

effective and proactive regional cooperation in protecting critical information infrastructures. This challenge of effective regional cooperation on protecting critical information infrastructure is a joint result of unequal circulation of technological infrastructures, operational procedures, policy formulation and implementation, as well as legal capability of ASEAN member states (Ang, 2020). Similarly, Heinl (2014) found that lack or inadequate regional cooperation on protecting critical information infrastructure among ASEAN countries is a consequence of inadequate coordination of efforts geared towards structuring cyber capacity as well as low implementation of policies as well as measures agreed upon in meetings.

This gap has allowed for an increasing rate of cybercrimes in ASEAN as almost all the countries in Southeast Asia have experienced many cyberattacks in recent years, which cooperation among member countries could help to mitigate. Furthermore, Southeast Asian nations have limited sharing of threat intelligence, often because of mistrust and a lack of transparency (Raska, 2018). Over the years the dearth of competences and abilities to comprehend as well as remediate cyber threats and potential attacks contributes significantly to the vulnerability of not just individual member states of ASEAN but the whole ASEAN region (Sharma, 2016). In short, although ASEAN member states have made efforts towards securing their critical information infrastructure through enacting regional cyber security strategies and measures, these efforts have not been particularly fruitful and proactive in the actualization of a secured and protected regional critical information infrastructure.

From the above and since continuous increase in cyberattacks on government and private information infrastructures has a negative impact on the growth of the digital economy in the ASEAN region, it is imperative to assess the efforts of ASEAN to promote shared responsibility through regional cooperation on cybersecurity challenges. This assessment will contribute towards understanding the strengths and weaknesses of ASEAN's existing cooperation on cybersecurity, as well as suggest workable recommendations for its improvement.

2. Objectives

The research questions of the study are:

1) What are ASEAN's current cybersecurity initiatives and how does it cooperate in tackling the challenges of cyberattacks on critical information infrastructure?
2) What are the challenges and limitations affecting ASEAN in realizing regional cooperation on cybersecurity?
3) What improvements could be made to ASEAN's existing cybersecurity framework to combat the challenges of cyberattacks on critical information infrastructure?

The objectives of the study are:

1) To review ASEAN's current cybersecurity initiatives and cooperation in tackling the challenges of cyberattacks on critical information infrastructure.
2) To identify the challenges for ASEAN and its limitations in realizing cooperation on cybersecurity to combat cyberattacks on critical information infrastructure.
3) To recommend improvements to the existing cybersecurity framework on regional cooperation to combat cyberattacks on critical information infrastructure in ASEAN.

3. Materials and Methods

The study examines regional cooperation on cybersecurity in the ASEAN region between 2013 and 2023. Data for the study was collected from secondary sources. The secondary data was studied extensively to extract relevant results, which were in turn categorized in accordance with the research objectives. Key data was collected primarily from the ASEAN website, specifically the two most recent publications of ASEAN's cybersecurity cooperation strategy. Each of the strategies specified in these two documents was critically evaluated and discussed. In addition, supplementary data was collected from other secondary sources and was again critically evaluated and categorized to achieve the above research objectives.

The collected data was analyzed using qualitative descriptive analysis, which entails extracting meaning and making logical deductions from secondary sources. This method of data analysis is fundamentally the application of qualitative research technique in the thorough examination and interpretation of research data. In using the qualitative descriptive analysis method, logical meaning was

extracted from each secondary source, including official ASEAN documents, academic journal articles, conference papers, reports, and other secondary sources.

4. Results and Discussion

This section focuses on the presentation of results. The results are presented according to the three research objectives that guided the study.

4.1 ASEAN's Current Cybersecurity Initiatives

Objective 1: To review ASEAN's current cybersecurity initiatives and cooperation in tackling the challenges of cyberattacks on critical information infrastructure.

ASEAN's current cybersecurity initiatives have produced two published regional cybersecurity strategy frameworks. These are *ASEAN Cybersecurity Cooperation Strategy 2017-2020* and *ASEAN Cybersecurity Cooperation Strategy 2021-2025.*

The first official roadmap to regional cooperation on cybersecurity among the 10 ASEAN countries was published in 2017. The cybersecurity initiative was approved by TELMIN. The underlying focus of the first cybersecurity strategy is to strengthen the Computer Emergency Response Teams (CERT) of individual member states to enhance CERT-CERT cooperation and capacity building among the 10 ASEAN countries, through coordination of the individual cybersecurity initiatives of individual member-states (ASEAN, 2017; Raska, 2018; Candice & Miguel, 2018). To enhance the effectiveness of the regional cooperation on cybersecurity, the cybersecurity strength and capacity of each of the ASEAN member-states was assessed using "ASEAN CERT Maturity Framework", which is a self-assessed toolkit to measure the maturity level of their CERT based on a list of questions and checklist. After the assessment, a regional CERT was established to coordinate the CERTs of individual ASEAN member-states. The ASEAN regional CERT is expected to synergize the individual strengths and areas of expertise of the ASEAN national CERTs to bolster the overall effectiveness of regional incident response capabilities. The recently published *ASEAN Cybersecurity Strategy 2021-2025* is an updated version of the first strategy published in 2017 that lasted till 2020. The main overarching objective of developing a new ASEAN Cybersecurity Cooperation Strategy is to update ASEAN's approach, while continuing to build on existing achievements (ASEAN, 2021).

To tackle the challenge of cyberattacks on critical information infrastructure of ASEAN member-states, the regional cybersecurity framework mandates the CERT of each member state to share intelligence information on cyberthreats (ASEAN, 2021). Thus, intelligence sharing among ASEAN member-states is at the heart of the ASEAN Cybersecurity Cooperation Strategy. Also, to tackle the challenge of cyberattacks on the critical information infrastructure of member states, most especially against each other, all 10 ASEAN member-states were made to subscribe in-principle to 11 voluntary, non-binding norms of responsible state behavior in cyberspace contained in the 2015 UN Group of Governmental Experts report (Ang, 2020), making ASEAN the first region to do so. A working committee was set up immediately to oversee the implementation of these 11 voluntary, non-binding norms. This committee was co-chaired by Malaysia and Singapore.

Furthermore, to promote effective regional cooperation on cybersecurity challenges among ASEAN member-states a timely 'cyberattack incidence response' is necessary. This was a major reason for the establishment of ASEAN-CERT – to facilitate the timely exchange of threat and attack-related information among national CERTs. Effective and timely exchange of cyberthreat and cyberattack-related information among ASEAN member-states is a proactive approach to tackling regional cybersecurity challenges among ASEAN member-states.

Another way that the ASEAN's current cybersecurity strategy promotes cooperation in tackling the challenges of cyberattacks on critical information infrastructure is through capacity building initiatives, which aim to identify member-state(s) with low cybersecurity capacity for training, as the weakness of one member-state will affect the desired regional-level cybersecurity cooperation (Candice & Miguel, 2018; Ang, 2020). Prior to capacity building, the cybersecurity strength, capacity, and maturity of individual member-states was assessed using the earlier mentioned 'ASEAN CERT Maturity Framework'. This was conducted in 2020. It allowed for a systematic identification of gap areas among ASEAN member-states for appropriate training or capacity building efforts to be directed towards. To achieve an international standard of cyber capacity building among each ASEAN member-state, experts from cybersecurity sophisticated countries

such as China, Russia, Japan, and Canada, as well as the EU and cybersecurity sophisticated ASEAN member-states such as Singapore and Malaysia, were invited to provide cybersecurity capacity training.

In tackling the challenges of cyberattacks on the critical information infrastructure of ASEAN member-states through regional cybersecurity cooperation, the recent ASEAN Cybersecurity Strategy 2021-2025 seeks to enhance trust in cyberspace among the member states. In 2017, APT32 group, which is believed to be working for the Vietnamese government, hacked ASEAN's website during its annual summit (Thomas, 2019). It is believed that the Vietnamese government is using the APT32 group to attack other government's critical information infrastructure with the aim of getting strategic intelligence information (Vijayan, 2019). Trust is imperative as intelligence on cyberthreats and attacks is expected to be shared among the CERT of each member state through the ASEAN CERT. No country shares intelligence information with another country without adequate levels of trust. As discussed below, insufficient levels of trust between member states is a significant obstacle to ASEAN achieving effective regional cooperation on cybersecurity.

4.2 Challenges and Limitations in Realizing Regional Cooperation on Cybersecurity

Objective 2: To identify the challenges for ASEAN and its limitations in realizing cooperation on cybersecurity to combat cyberattacks on critical information infrastructure.

Despite formulating a regional cybersecurity cooperation strategy (ASEAN 2017), ASEAN member states have continued to experience attacks on their critical information infrastructures (CII). This is due to certain challenges affecting ASEAN in realizing regional cooperation on cybersecurity. The major challenges are technological gap among member states, lack of common response strategies, inadequate trust among ASEAN member states, most especially in areas of exchanging intelligence information on cyberthreats and attacks, the dependency of ASEAN-CERT on national CERTs sharing intelligence, lack of new common cyber norms among the member states, and the sophistication of recent cybersecurity challenges among others. Subsequent paragraphs will discuss each of these challenges.

4.2.1 Technological Gap Among Member States

One of the major challenges and limitations affecting ASEAN in realizing regional cooperation on cybersecurity is a wide technological gap among member states in terms of their cybersecurity capacity, strength and maturity (Luk, 2019; Dupont & Whelan, 2021; Corrado & Sakal, 2021). This discrepancy among the ASEAN member states has created a strong challenge to effective regional cooperation on cybersecurity as attacks on weaker member states might affect others (Candice & Miguel, 2018; Ang, 2020).

Kearney (2018) reported that there is disproportionate cybersecurity development among ASEAN member states. For instance, Singapore and Malaysia are more sophisticated in terms of cybersecurity readiness than Myanmar, Lao and Cambodia. This unevenness is perhaps partly due to varying perceptions of threats among ASEAN members. Some member states, such as Singapore and Malaysia perceive cybersecurity as a critical and urgent concern, recognizing the potential threats posed by cyberattacks, data breaches, and other malicious activities (Kearney, 2018; Tay, 2023). These countries have prioritized the development of robust cybersecurity measures and frameworks to safeguard their digital infrastructure and protect sensitive information. On the other hand, Myanmar, Lao, and Cambodia might view the cybersecurity challenge as relatively less severe or may have differing levels of awareness regarding the potential risks (Kearney, 2018; Tay, 2023). As such, they might prioritize other issues or have varying levels of readiness in terms of cybersecurity infrastructure and policies.

The recent Global Cybersecurity Index published in 2020 further exposes the discrepancy in the cybersecurity capacity and maturity of the 10 ASEAN member states (Global Cybersecurity Index, 2020). According to the report, while ASEAN member states such as Singapore and Malaysia are among top 5 ranked countries with high cybersecurity preparedness in terms of technological resources, legal framework and human resources among others, Myanmar, Lao and Cambodia were ranked among the lowest globally. Out of the 182 countries ranked, Singapore was 4th, Malaysia 5th, Indonesia 24th, Vietnam 25th, Thailand 44th, the Philippines 61st, Brunei 85th, Myanmar 99th, Laos 131st, and finally Cambodia was ranked 132nd (Global Cybersecurity Index, 2020). This gap will affect the collective effort at ensuring secured cyberspace in ASEAN.

4.2.2 Lack of Common Response Strategies

There is a lack of common response strategies among ASEAN member states in the event of a cybersecurity attack. Both ASEAN Cybersecurity Cooperation Strategy 2017 and 2021 are silent on how ASEAN member states should respond to incidents of cyberattack. This implies that individual member states can employ their own response strategy, which might conflict with the strategies of other member states. Cybersecurity incident response is a very critical issue in cybersecurity and hence, should be treated with importance. This omission from policy consideration is one of the challenges affecting ASEAN in realizing regional cooperation on cybersecurity to combat the challenges of cyberattacks on critical information infrastructure.

4.2.3 Inadequate Trust Among ASEAN Member States

Inadequate trust among ASEAN member states, most especially in areas of exchanging intelligence information on cyberthreats and attacks, is another challenge affecting ASEAN in realizing regional cooperation on cybersecurity. As discussed in the introduction, from a neorealist perspective states operate in an anarchic international system in which all possess some offensive capability and in which none can ever be certain of others' intentions. The main goal of states within such a system is to ensure their survival. This quest for survival results in competition for power, but it can also lead to alliances and other forms of cooperation between states that aim to counter shared threats. However, the sustainability of such alliances will likely be threatened by setbacks that have to do with states prioritizing sovereignty and self-interest over collective interest, as well as lack of trust.

ASEAN member states attempt to engage in cooperation, but the association's guiding principles of respect for sovereignty and non-interference make it challenging to cooperate on regional issues (Acharya, 2014; Tay, 2023). Moreover, as discussed below, because of mistrust and a lack of transparency, Southeast Asian nations have limited sharing of threat intelligence (Raska, 2018). Though *ASEAN Cybersecurity Cooperation Strategy 2017-2020* and *ASEAN Cybersecurity Cooperation Strategy 2021-2025* seek to initiate and enhance trust among the CERT of ASEAN member states to exchange intelligence on cybersecurity threats and attacks, the process through which this trust can be initiated and enhanced is still unclear.

4.2.4 Dependency of ASEAN-CERT on National CERTs to Share Intelligence

Another major challenge affecting ASEAN in realizing regional cooperation on cybersecurity is that the sole responsibility to share intelligence information on cybersecurity threats and perceived likelihood of attacks lies with the national CERT of individual ASEAN member states. This implies that if the national CERT of a certain member state decides to withhold intelligence, ASEAN-CERT is ignorant to potential or actual threats. In other words, the ability of ASEAN-CERT to function proactively depends on receipt of information shared by national CERTs, but national CERTs can decide whether to share information or not. Exchange of intelligence information is central to effective regional cooperation on cybersecurity. Hence, it should be controlled (or at least shared) through a centralized system, not by individual member states. Also, the CERTs of member states that are least cybersecurity ready, such as Laos and Cambodia, might not be sophisticated enough to share intelligence on cybersecurity threats.

4.2.5 Lack of New Common Cyber Norms

A lack of new common cyber norms among the member states is a significant obstacle to achieving effective regional cooperation on cybersecurity in ASEAN. Both of the official cybersecurity strategies (ASEAN, 2017, 2021) fail to formulate new norms that will guide the cyber conduct of ASEAN member states. Advancing the eleven (11) voluntary, non-binding principles that are defined in the 2015 report by the UN Group of Governmental Experts (UNGGE) is inadequate as they are global principles that might not be suitable for the specific circumstances of ASEAN (Raemdonck, 2021; Corrado & Sakal, 2021). Similarly, Sunkpho, Ramjan, & Ottamakorn (2018) reported that the biggest problem in the region is that ASEAN does not have strict regulations to combat any threat from the cyber world. Thus, it will be difficult to cooperate in the absence of a common regulation that will serve as a guide to all ASEAN member states.

4.2.6 Sophistication of Recent Cybersecurity Challenges

Trends in cybercriminal activities are developing with sophistication and so any cybersecurity strategy must follow the trend to be effective in securing critical information infrastructure (CII). Cyber criminals are deploying different sophisticated techniques of attack. This is a great challenge for the CERTs of individual member states that are supposed to identify potential cybersecurity threats and immediately share information with ASEAN-CERT for immediate and proactive action. The more the sophistication of cybersecurity challenges globally, the more difficult it is for national CERTs to identify potential cybersecurity threats and for ASEAN-CERT to coordinate collective action.

4.3 Improvements to Combat the Challenges of Cyberattacks

Objective 3: To recommend improvements to the existing cybersecurity framework on regional cooperation to combat cyberattacks on critical information infrastructure in ASEAN.

Although the existing cybersecurity framework on regional cooperation to combat cyberattacks on critical information infrastructure in ASEAN is an important step forward, the growing sophistication of recent cyberattacks has created gaps in the existing ASEAN Cybersecurity Cooperation Strategy that must be filled so as to improve and facilitate the realization of effective regional cooperation on the matter. The key areas that need addressing are: formulating and implementing ASEAN Cyber norms, establishing an ASEAN Cybersecurity taskforce to enforce the ASEAN Cyber norms, regulating cybersecurity budget of ASEAN member states, and regular cybersecurity capacity training among ASEAN member states to close the cybersecurity maturity and capacity gap.

4.3.1 Formulating and Implementing ASEAN Cyber Norms and Policies

One major improvement that can be made to the existing cybersecurity framework is the formulating and implementing of ASEAN cyber norms and policies. These norms and regulations will help to regulate the conduct and behavior of state actors in cyberspace. ASEAN should formulate regulations, procedures, and norms to guide the behavior of its members by strengthening forums and dialogue (Obet, Suharto & Mujoko, 2021). Similarly, Ramadhan (2020) suggested that ASEAN needs to formulate policy that addresses cyber incidents, cooperation between CERTs, and capacity building among ASEAN members to build cyber resilience.

4.3.2 Establishment of ASEAN Cyber Norm Taskforce

After formulating and implementing ASEAN cyber norms, an ASEAN cybersecurity taskforce should be established to enforce these norms. The ASEAN cyber norms taskforce should consist of 10 members, one from each member state. The task force should be vested with the power to penalize any member state that defaults. Supporting this strategy, Krisman (2013) suggested that ASEAN needs to develop strong regulations, establishing a task force to secure them from cyber-attacks.

4.3.3 Regulation of the Cybersecurity Budget of ASEAN Member States

Regulating the cybersecurity budget of ASEAN member states is another way of improving the existing cybersecurity framework. Since the discrepancy in the cybersecurity capacity and infrastructures among member states is a direct consequence of the investment of each member state in cybersecurity, one way to get everyone working together and closing the technological gap is for the ASEAN council of ministers to mandate each member state to invest heavily in cybersecurity, as the weakness of one nation affects the others.

4.3.4 Regular Cybersecurity Capacity Training Among ASEAN Member States

Regular cybersecurity capacity training among ASEAN member states is needed to close the gap in cybersecurity maturity and capacity. ASEAN should establish trend-based cybercrime workshops and training sessions to eliminate information gaps between countries by involving non-state parties such as professionals, cyber employees, and corporate agencies within the state, and students (Obet, Suharto & Mujoko, 2021). This is imperative as cybercrimes and attacks are getting more advanced and sophisticated. Hence, regular training should be organized to enlighten each of the member states on the current trends and

global best practices in cybersecurity. This training should be made compulsory for the national CERTs of ASEAN member-states.

5. Conclusion and Implication

The study investigated ASEAN's current framework for mitigating cybersecurity threats in the region as well as identified the shortcomings of ASEAN in promoting shared cybersecurity. Based on the findings of the study, it was concluded that it is essential to effective regional cooperation that intelligence information on cyberthreats is quickly exchanged between the Computer Emergency Response Teams (CERTs) of the member states. Though this is not adequate, it has prevented some cyberattacks on critical information infrastructure (CII) within ASEAN. To tackle the challenge of cyberattacks on the critical information infrastructure of ASEAN member states, the regional cybersecurity framework mandates that the CERT of each member shares intelligence information on cyberthreats. ASEAN-CERT was established to facilitate timely exchange of threat and attack-related information among national CERTs. Another way that the ASEAN's current cybersecurity initiatives tackle the challenges of cyberattacks on critical information infrastructure is through capacity building initiatives, which aim to identify member states with low cybersecurity capacity for training, as the weakness of one member-state will affect the desired level of regional cybersecurity.

The study also concluded that technological gap among member states, lack of common response strategies, inadequate trust among ASEAN member states, most especially in areas of exchanging intelligent information on cyberthreats and attacks, dependency of ASEAN-CERT on national CERTs to share intelligence, lack of new common cyber norms among the member states, and sophistication of recent cybersecurity challenges are the major challenges to ASEAN realizing effective regional cooperation on cybersecurity. Of all the challenges, the study concluded that trust and honesty between ASEAN member states to share valid and timely intelligence information on cyberthreats is fundamental to achieving regional cooperation that succeeds in combating the challenges of cybersecurity. Also, the study found that it will be difficult to establish formidable regional cooperation on cybersecurity with the existing technological gap among ASEAN member states, in terms of cybersecurity readiness, policy framework, infrastructures, and human resources. The study also concluded that ASEAN's regional frameworks are silent on how member states should respond to cases or incidents of cyberattacks, which is a great limitation to the actualization of effective regional cooperation.

Based on the assessment herein, the following recommendations are suggested to help facilitate formidable and resilient regional cybersecurity cooperation in ASEAN.

1. ASEAN should formulate and implement regional cybersecurity norms and minimum acceptable behavior of member states. This will serve as standard to all the 10 member states in their actions and inactions on cyberspace.
2. ASEAN should establish a cybersecurity taskforce to enforce the ASEAN cyber norms. The taskforce committee should be selected from each of the 10 member states. Rules and regulations guiding the conduct of the taskforce should be clearly stated and strictly implemented.
3. ASEAN should regulate the cybersecurity budgets of member states to reduce the technological gap between member states. This technological discrepancy in the cybersecurity capacity and infrastructures among the member states is a direct consequence of the investment of each member state in cybersecurity. Hence, to get everyone working together and closing the gap, the ASEAN council of ministers should mandate each member state to invest heavily in cybersecurity, as the weakness of one nation affects others.
4. ASEAN-CERT should regularly train and retrain the CERTs of individual member states on the best practices in sharing cybersecurity intelligence information within the region.
5. Efforts at establishing adequate trust and honesty between the CERTs of individual member states is indispensable for achieving formidable regional cooperation to combat the challenges of cyberthreats in ASEAN.
6. The cybersecurity maturity and readiness of each member state in terms of both preventing cyberattacks and recovering from incidents of cyberattack should be assessed periodically to understand the strengths and weaknesses of each member state.

6. Acknowledgements

First, I would like to express my appreciation and thanks to the Institute of Diplomacy and International Studies, Rangsit University for providing me with the opportunity to complete my master's degree in the field of diplomacy and international studies. Also, I would like to show my gratitude to all the teachers and staff of the MA Program for their support, encouragement, and assistance throughout the entire journey. The completion of this research paper could not have been accomplished without the tremendous support of my advisor, Dr Benjamin D. King. His advice has been highly valuable for my research.

References

Acharya, A. (2014). *Constructing a Security Community in Southeast Asia: ASEAN and the problem of Regional Order.* Routledge.

Ang, B. (2020). Singapore, ASEAN and international cybersecurity. In E. Tikk, & M. Kerttunen, *Routledge Handbook of International Cybersecurity* (pp. 218-226). Oxon: Routledge.

Association of Southeast Asian Nations (2017). ASEAN Cybersecurity Cooperation Strategy (2017-2020). Jakarta: ASEAN Secretariat.

Association of Southeast Asian Nations (2021). *ASEAN Cybersecurity Cooperation Strategy (2021-2025).* Jakarta: ASEAN Secretariat.

Association of Southeast Asian Nations Secretariat (2020), *ASEAN Economic Community Blueprint*, Jakarta: ASEAN Secretariat.

Candice, T. D. & Miguel, A. G. (2018). Challenges and opportunities for cyber norms in ASEAN, *Journal of Cyber Policy,* doi:10.1080/23738871.2018.1487987

Corrado, R. & Sakal, M. (2021). Cybersecurity in Cambodia: Awareness as a First Step. *Cambodia Development Center, 3*(11),1-8.

Cyber Security Authority (2021). *Critical information infrastructure*. Retrieved July 21, 2022, from https://www.csa.gov.gh/cii#:~:text=The%20Cybersecurity%20Act%2C%202020%20(Act,social%20well%2Dbeing%20of%20citizens

Cybersecurity Act of the Republic of Ghana (2020). *Critical information infrastructure*. Retrieved July 25, 2022, from https://www.csa.gov.gh/cii#:~:text=The%20Cybersecurity%20Act%2C%202020%20(Act,social%20well%2Dbeing%20of%20citizens

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1), 76–92.

FireEye. (2018). *Cyber Evolution: En Route to Strengthening Resilience in Asia-Pacific*. Retrieved July 26, 2022, from https://www.fireeye.com/offers/wp-cyber-evolution-apac.html

Global Cybersecurity Index (2020). *Measuring commitment to cybersecurity*. Report published by the International Telecommunication Union, Development Bureau.

Heinl, C. (2014). Regional cybersecurity: Moving toward a resilient ASEAN cyber security Regime. *Asia Policy*, *18,* 131-159.

International Monetary Fund (2020). *The Global cyberthreat to financial system*. Retrieved January 15, 2022, from https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber threat-to-financial-systems-maurer.htm

INTERPOL. (2021). *ASEAN Cyberthreat Assessment 2021*. INTERPOL Global Complex for Innovation. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts top-cyberthreats -in-Southeast-Asia

Kearney, A. T. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action*. http://www.southeast-asia.atkearney.com/documents/766402/15958324/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/ffd3e1ef-d44a-ac3a-9729-22afbec39364

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

Luk, S. C. Y. (2019). Strengthening cybersecurity in Singapore: challenges, responses, and the way forward. In *R. Abassi, & A. B. Chehida Douss, Security frameworks in contemporary electronic government*, 96-128. doi:10.4018/978-1-5225-5984-9.ch005

Lung, N. (2018). *ASEAN leaders issue statement on cybersecurity cooperation.* Retrieved

from Opengovasia: https://opengovasia.com/asean-leaders-issue-statement-on-cybersecurity cooperation/

Mearsheimer, J. (2013). Structural Realism. *International Relations Theories: Discipline and Diversity* (pp. 77-91). In T. Dunne, M. Kurki, & S. Smith (Eds). Oxford University Press.

Newsbytes. (2013). *Malaysia-Philippines cyber-war claims sites of both sides*. Retrieved March 5, 2022, from https://www.digitalnewsasia.com/digital-economy/malaysia-philippines-cyber-war-claims-sites-of-both-sides

Nugroho, G. (2011). Neorealism and ASEAN States' Cooperation in ASEAN Free Trade Area (AFTA): An Empirical Critique. *Jumal Kajian Wilayah, 2*(2), 200-224.

Obet, D., Suharto, H. & Mujoko, H. (2021). cyber cooperation in the framework of the ASEAN regime. *Jurnal Pertahanan, 7* (2), 254-261.

Portnoy, M. & Goodman, S. (2009). *Global Initiatives to Secure Cyberspace: An Emerging Landscape.* New York: Springer.

Raemdonck, N. V. (2021). *Cyber Diplomacy in Southeast Asia*. Vrije Universiteit Brussels. Retrieved from https://eucyberdirect.eu/wp-content/uploads/2021/05/dd-southeast-asia-nb-fb-nvr-09-05.pdf

Ramadhan, I. (2020). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). In: *Journal of Social and Political Sciences*, *3* (4), 983-995.

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

Saballa, J. (2022). Singapore to establish cyber military force. *The defense post*. Retrieved March 16, 2022, from https://www.imf.org/en/Publications/REO/APAC/Issues/2022/10/13/regional economic-outlook-for-asia-and-pacific-october-2022

Saravade, N. (2016). International and Regional Responses to Cybersecurity Challenges.*Securing Cyberspace: International and Asian Perspectives* (pp. 244-254). In C. Samuel, & M. Sharma (Eds). New Delhi: Pentagon Press.

Sharma, M. (2016). A South Asian Regional Cybersecurity Cooperation (SARCC) Forum: Prospects and Challenges. *Securing Cyberspace: International and Asian Perspectives* (pp. 255-267). In C. Samuel, & M. Sharma (Eds). New Delhi: Pentagon Press.

Statista (2021). *Internet usage in Southeast Asia: Statistics and facts*. Retrieved January 15, 2022, from https://www.statista.com/topics/9093/internet-usage-in-southeast-asia/#topicOverview

Sunkpho, J., Ramjan, S., & Ootamakorn, C. (2018). Cybersecurity Policy in ASEAN Countries. *Proceeding in Information Institute Conferences 2018, pp. 1-7. Las Vegas, USA. Retrieved from* https://www.researchgate.net/publication/324106226

Tay, K. L. (2023). *ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework.* The International Institute for Strategic Studies.

The Strait times (2020). *Malaysia's armed forces confirms cyberattacks on network*. Retrieved from https://www.straitstimes.com/asia/se-asia/malaysias-armed-forces-confirms-cyber-attack on-network

Thomas, N. (2019). Cyber Security in East Asia: Governing Anarchy. *Asian Security*, *5*(1), 3-23.

Vijayan, J. (2019). *Vietnam rises as cyberattacks*. Retrieved from https://www.darkreading.com/attacks-breaches/vietnam-rises-as-cyberthreat

Yaksha, D. (2018). Overview of Cybersecurity Status in ASEAN-EU. *Tech. Report,* 123.

Waltz, K. N. (1979). *Theory of international politics.* Reading, MA: Addison-Wesley Publishing Company.