Hasanuddin Journal of Strategic and International Studies

ISSN: 2963-1394 (Online) Journal Homepage: https://journal.unhas.ac.id/index.php/hjsis/

Global Cyber Norms Subsidiarity (UN GGE and UN OEWG) within ASEAN’s Body

Feline Cloramidine, Ali Abdullah Wibisono

To cite this article:

Cloramidine, F., & Wibisono, A. A. (2024). Global Cyber Norms Subsidiarity (UN GGE and UN OEWG) within ASEAN’s Body. *Hasanuddin Journal of Strategic and International Studies (HJSIS)*, 2(2), 21-37.

To link to this article:

https://doi.org/10.20956/hjsis.v2i2.35313

HASANUDDIN JOURNAL OF STRATEGIC AND INTERNATIONAL STUDIES
VOL. 2 NO. 2 JUNE 2024: PP. 21-37
ISSN 2963-1394
DOI: 10.20956/hjsis.v2i2.35313

OPEN ACCESS: REGULAR RESEARCH ARTICLE

Global Cyber Norms Subsidiarity (UN GGE and UN OEWG) within ASEAN's Body

Feline Cloramidine[1,*], Ali Abdullah Wibisono[2]

[1] Department of International Relations, Faculty of Social and Political Science, University of Indonesia, Depok, Indonesia
[2] Department of International Relations, Faculty of Social and Political Science, University of Indonesia, Depok, Indonesia

Abstract
In the context of cybersecurity, ASEAN plays an important role as a normative extension that carries out norm subsidiarity of UN global cyber norms generated from UN GGE and UN OEWG processes. The subsidiarity of norms promoted by ASEAN serves to place any kind of global issues and global interest at the regional level, as well as regional issues and regional interest at the global level. This paper focuses on the implications of ASEAN as a regional institution in the context of cyber norm subsidiarity toward UN global cyber norms. This paper utilizes Acharya's norm subsidiarity to explain how ASEAN performs a norm subsidiarity of UN's cybersecurity norms. We argue that ASEAN's norm subsidiarity role is possible due to the fact that the UN's cybersecurity norms to regulate the responsible state behavior in cyberspace from the UN GGE and UN OEWG process were symmetrical to ASEAN Way's emphasis on prioritization member states' sovereignty and non-intervention principles. Furthermore, this article finds that the implication of ASEAN's norm subsidiarity to the region's own cybersecurity accomplishment is still unidentifiable. This article also finds that there are many factors affecting the process of norm subsidiarity in ASEAN, such as the heterogeneity within the institution and the lack of political will of the member states.

Key Words
ASEAN, norm subsidiarity, cyber norms, UN GGE, UN OEWG, cybersecurity

1. Introduction

The rapid development in Information, Communication, and Technology (ICTs) has contributed a lot of changes in the context of international security studies. Conflicts that initially occurred in the traditional ways and centered on wars between countries have now grown to be much wider and more complex. Today, technology is considered as one of driving factors of threat's emergence, specifically in terms of the huge potential technological influence to strategic relations (Buzan & Hansen, 2009, pp. 53-54). As one of domain for the use of ICTs, cyberspace which began to be used in 1985 (Leiner et al., 1997), has now become a source of risk that presents any kind of non-traditional threats with the broader of threat vectors that can come from state actors as well as non-state groups and individuals (Cha, 2000, pp. 393-394; Fjäder, 2016).

Cyberspace is known as one of five domains of warfare, namely air, land, sea, space, and cyberspace nowadays (Greiman, 2015, p. 1). As a new domain, cyberspace is closely related to national security and national interests of a state (Hansen & Nissenbaum, 2009, p. 1162; Stevens,

***CORRESPONDENCE** Feline Cloramidine I fcloramidine@gmail.com I Department of International Relations, Faculty of Social and Political Science, University of Indonesia, Depok, West Java, Indonesia

2012, p. 1). This domain is formed from a combination of physical and non-physical components and has become not immune to the insecurity, crime, and geopolitical components. In cyberspace, reports of crime cases often appear. This can be proven by the amount of media reports related to hacking, data theft, leakage of personal information, compromised networks, and also cyber espionage, both in the context of national level and transnational level (Chen & Yang, 2022, p. 1). That is why cyberspace is considered to be one of the most complex domains.

The inherent complexity in cyberspace makes this domain inseparable from the observations by studies other than security, including policies and laws that traditionally treat cybercrime as a new form of threat. Cyberattacks aimed against the national security stability are the important factors to examine the existing legal frameworks related to data protection, electronic communications, and access to public information (Tikk, 2011, pp. 120-121). To keep abreast of the evolving threats in the cyber domain, the UN produced two processes under United Nations Office for Disarmament Affairs (UNODA) aimed to monitor states' behavior in cyberspace.

The first process is based on the Russia's recommendation in 2004, namely United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, and US' Recommendation in 2018, namely United Nations Group of Governmental Experts (UN GGE) on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (UNGA, 2018; Broeders, 2021, p. 278). The UN GGE process took place in six rounds to provide proposals for the formulation of global cyber norms from 2010 to 2021. In 2015, the UN GGE process had successfully reached the consensus related to UN global cyber norms. It contains 11 points of the non-binding global cyber norms as the basis guidelines of all member states in the use of ICTs (Hogeveen, 2022, p. 8). However, in 2017, precisely in the fifth round of discussion, UN GGE failed to obtain any consensus (Broeders, 2021, p. 278). This happened because of several factors, such as disagreements between states, including Cuba, China, and Russia against the existing draft (Henriksen, 2019, p. 3).

The second UN process for global cybersecurity norms formulation is the United Nations Open-Ended Working Group (UN OEWG) on Development in the Field of Information and Telecommunication in the Context of International Security referred to Russia's recommendation in 2018. The UN OEWG process is considered to become more democratic, inclusive, and transparent compared to the UN GGE process. The UN OEWG process is important for all member states in supporting the process of the implementation and development of global cyber norms. Moreover, the UN OEWG report offers an additional layer of understanding to assist the government in the implementation of norms (Hogeveen, 2022, p. 8).

Both of UN's cybersecurity norms processes are observed closely by the international community, including Association of Southeast Asian Nations (ASEAN). In October 2016, when the ASEAN Ministerial Meeting on Cybersecurity (AMMC) took place, Singapore's Minister of Communications and Information and the Responsible Minister for Cybersecurity, Dr Yaacob Ibrahim underlined the need of the improvement for cyber norms that suit well to the characteristics of each state in various areas to behave in cyberspace (Dai & Gomez, 2018, p. 217). Amidst the UN GGE's inability to reach a consensus in 2017, many policy makers are seeking to find the answer on how multilateral and other regional activity can be used to increase the security and stability within cyberspace. ASEAN and ASEAN Regional Forum (ARF) are often identified as the platforms that can assist the implementation process of cyber norm, confidence building measures (CBMs), and so on in the Asia-Pacific region. In addition, several ASEAN member states, such as Malaysia and Indonesia, have championed some regional processes in the UN GGE forum to promote international cyber stability (Heinl, 2018). Then, in 2018, the leaders of ASEAN member states had shown their commitments to operate the UN cyber norms as the core element of ASEAN's approach in promoting its regional stability in cyberspace.

Previous studies have clearly explained about the issue of norm subsidiarity in ASEAN. Butler & Lachow (2012) found the important role of both regional and international institutions, organization, and alliances in promoting the formulation of a common understanding between the member states related to the acceptable terms, goals, responsibilities, and behaviour in cyber norms (Butler & Lachow, 2012). In line with Butler & Lachow (2012), Poetranto et al. (2021) underlined that regional institutions have a better insight against the states' priorities (Poetranto et al., 2021). Poetranto et al. (2021) reaffirmed the findings of Choucri et al., 2013 that, both international and intergovernmental institutions do not always have the same placement of the priority. The intergovernmental institutions' priorities are always closer to the states' priorities. Including the priorities related to cybersecurity (Choucri et al., 2013). In the context of ASEAN, Dai & Gomez (2018) contend that ASEAN faces obstacles in adopting the consensus related to cyber norms. Starting from the gaps between the member states, the heterogeneity among the member states, and the strict compliance towards ASEAN's historical principles, namely the non-intervention principles among the internal interests of the member states (Dai & Gomez, 2018). Therefore, Chen & Yang (2022) underlined that ASEAN has a very unique cyber governance. ASEAN is applicating the cyber norm subsidiarity towards the UN global cyber norms. Norm subsidiarity is necessary for ASEAN to place its regional priorities at the global level and vice versa by using the ASEAN's diplomatic culture, normative structures, and historical principles as the basis framework of its regional cyber governance (Chen & Yang, 2022).

In regard to the existing literature, there is a need to discuss how norm subsidiarity is possible and what implications it would bring to regional security. For that reason, this paper examines more about the role of ASEAN as a regional norm extension towards the UN global cyber norms (UN GGE and UN OEWG). By using the norm subsidiarity concept coined by Acharya (2011) as the conceptual framework, this article explains the implications of norm subsidiarity in the ASEAN's cyberspace. The following sections consist of five parts. First, the description of the general overview related to the issue, the previous studies about the role of regional institutions as a global cyber norm extension, and also the gap related to the topic. Second, the description about the concept of norm subsidiarity coined by Acharya (2011) as the conceptual framework used by the authors to answer the research question on this paper. Third, the description of the research method. Fourth, the discussion and the findings of this paper, specifically related to the process of ASEAN in subsidiarizing the UN global cyber norms, namely UN GGE and UN OEWG. For the last part, the authors will be reaffirming the findings of the research and conclude the whole points of the research.

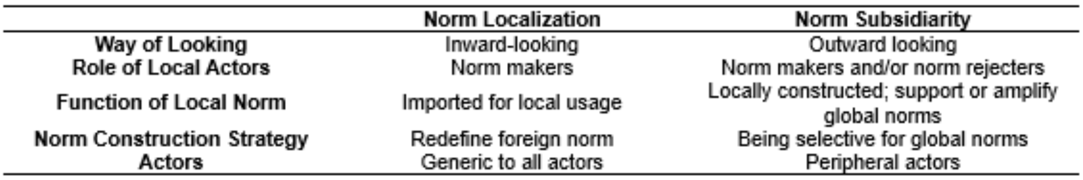
2. Analytical Framework

Norm is not a norm just because someone said so. Norm can be existing only when several of relevant groups agree and hold the collective certain beliefs related to expected behavior (Finnemore, Cybersecurity and The Concept of Norms, 2017, p. 1). Norms can be formed in the various ways, usually through habits and entrepreneurship. Sometimes, the expectations formed by repeated behavior within any regular interactions done by any group can also be contributed in the formulation process of norms (Finnemore, Cybersecurity and The Concept of Norms, 2017, p. 3).

Finnemore & Hollis (2016) disaggregate norms into four main ingredients. First is identity, which refers to the group where the norm is applied. Norm makes any kind of behavioral claims against the particular actor, either individual, the bigger groups, and the group of nation-state groups; Second is behavior, which refers to the particular actions required in the society. In this case, norms are usually regulative, either to regulate, to control, to prohibit, and to obligate the society. Norms are also constitutive when they play a role in creating the new rights for the particular actors; third is compliance, which refers to the basis where norms play a role to give any labels against the appropriate and inappropriate behaviors; and last is shared expectations, which refers to the intersubjective and social character within the norm itself (Finnemore & Hollis, Constructing Norms for Global Cybersecurity, 2016, pp. 438-443).

Furthermore, subsidiarity refers to the process where local actors formed the norm aimed to maintain their autonomy from the external dominations, neglects, violations, and abuses done by the central actors with the higher powers (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011, p. 95). Meanwhile, Acharya (2011) defined that norm subsidiarity is a process where the local actors can formulate new regulations and offer new understandings on the global regulations, and reaffirm the global regulations in the context of regional level (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011, p. 96). Norm subsidiarity is not only limited to the variation of norm diffusion. However, it also provides the understanding on how the third world countries play the roles to respond the existing norms, formulate the new norms, and spread the new norms (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011, p. 96). The concept of norm subsidiarity is often associated with the term of norm localization. There are indeed similarities between the two concepts, but both concepts are actually very different (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011, pp. 97-98). This can be seen at Tabel 1 below.

Table 1. Differences between norm localization and norm subsidiarity



	Norm Localization	Norm Subsidiarity
Way of Looking	Inward-looking	Outward looking
Role of Local Actors	Norm makers	Norm makers and/or norm rejecters
Function of Local Norm	Imported for local usage	Locally constructed; support or amplify global norms
Norm Construction Strategy	Redefine foreign norm	Being selective for global norms
Actors	Generic to all actors	Peripheral actors

Source: Processed by authors (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011)

According to Tabel 1, the concept of norm subsidiarity emphasizes on five aspects, first is outward-looking, which refers to interactions between local actors and external powers, in the situations where the first parties fear of the dominations from the other parties; second is in the context of norm subsidiarity, local actors play a role as norm makers and/or reject the existing norms; third is local actors can export and universalize locally constructed norms. This includes on how local norms are used to support and reinforce the existing global norms; fourth is local actors play a role to reject, borrow, and adopt the inappropriate external ideas in any forms; and last is the actors identified here are usually the peripheral actors who get more challenges from the external parties (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011, pp. 97-98).

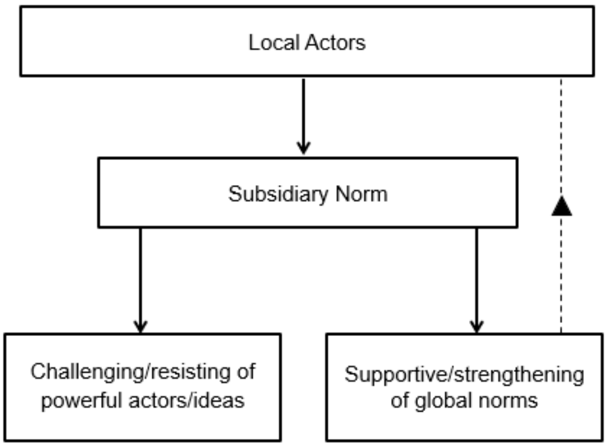

Local Actors
Subsidiary Norm
Challenging/resisting of powerful actors/ideas
Supportive/strengthening of global norms

Figure 1. Analysis model of local norm subsidiarity on the existing global norms
Source: (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011)

In regard to Acharya's (2011), the operationalization of the concept in this article will be begin with a clear identification of the local actors, which refers to the regional institution of Southeast Asia, namely ASEAN. ASEAN plays a role as normative extension and contributes to cyber norm subsidiarity. Authors will discuss ASEAN's regional cyber norms, namely ASEAN Way and ASEAN Centrality as the foundation for the subsidiarity of global cyber norms. In the next section, authors will discuss the position of UN GGE and UN OEWG endorsed and used by ASEAN as the standard in the formation of regional cyber norms. For the last section, the authors will identify the US-China relationship dynamics as the primary obstacles for ASEAN's cybersecurity.

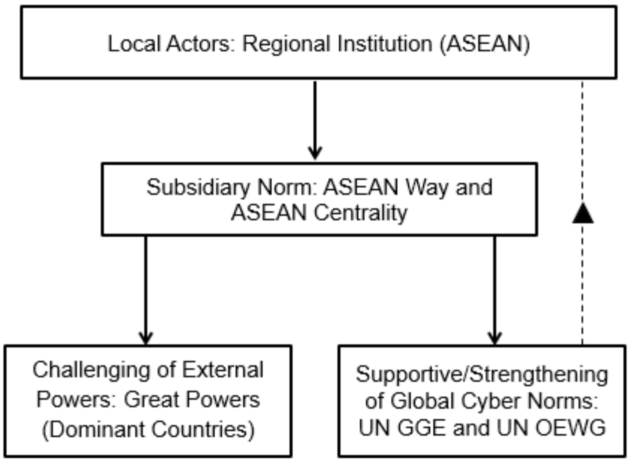

Local Actors: Regional Institution (ASEAN)
Subsidiary Norm: ASEAN Way and ASEAN Centrality
Challenging of External Powers: Great Powers (Dominant Countries)
Supportive/Strengthening of Global Cyber Norms: UN GGE and UN OEWG

Figure 2. Operationalization concept of norm subsidiarity in ASEAN on UN global cyber norms (UN GGE and UN OEWG)
Source: Processed by authors (Acharya, Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World, 2011)

3. Research Method

This paper will be using the qualitative-descriptive research method to facilitate the data collecting process and data analysis process. Qualitative research-based is usually a detailed explanation towards the research for ongoing phenomenon (Bryman, 2012, p. 402). Meanwhile, the descriptive research approach presents an overview of the specific details related to a situation, social settings, or relationship (Neuman, 2014, pp. 38-39). Qualitative research-based is usually using inductive logic. However, this paper will be following the deductive method. The deductive research based in this paper begins with the abstract concepts, evaluating those concepts with the existing facts, and the explanation about the ideas, theory, and the observation of empirical data.

This paper will be using the discourse analysis method. Discourse analysis is basically trying to cover all social phenomena involving individuals and institutions to understand the phenomena that occur properly. Discourse analysis, especially critical discourse analysis, not only examines the role language and text in social phenomena, but also learns the study of social context. For example, when the existence of certain institutions and the roles played by individuals allows them to be packaged through style and grammar (Hodges et al., 2008, p. 570). Referring to this, the type of data needed in this research is primary and secondary data, including the previous studies from the article journal, book, publications, and official websites.

4. Results and Discussions

4.1. ASEAN as A Normative Extension of UN Global Cyber Norms (UN GGE and UN OEWG)

The principle of non-intervention is pertinent to Southeast Asian states, and therefore their preference is geared towards non-binding norms. ASEAN emphasized the importance of cybersecurity through the establishment of the various dialogues and official meeting between all member states. In the fields of regional political defence and consultation, ASEAN defence officials have been involved in ASEAN Security Dialogue since 1996. Under the framework of ASEAN Regional Forum (ARF), ASEAN established a voluntary discussion related to regional political and economic development. ASEAN had also held some regular meetings to high-level defence officials under ARF Defence Officials Dialogue (DOD) and the ARF Security Policy Conference (ASPC) (ASEAN Secretariat, 2009, p. 8). ARF is an official government-level dialogue formed by ASEAN as ASEAN's endeavours in building the principle of mutual trust between the member states and other states in the Asia-Pacific region. The goal of ARF is to discuss any regional security issues (Manopo & Sari, 2015, p. 44).

ASEAN's commitment in the field of cybersecurity has also shown up on the existence of ASEAN sectoral bodies and other ASEAN mechanisms that also took up cybersecurity issues, such as ASEAN Digital Ministers' Meeting (ADGMIN) and ASEAN Digital Senior Officials' Meeting (ADGSOM) as its subsidiary bodies, ASEAN Ministerial Meeting on Transnational Crime (AMMTC), East Asia Summit (EAS), ASEAN Defence Minister's Meeting (ADMM)-plus, and ASEAN Ministerial Meeting on Social Welfare and Development (AMMSWD). Then, in the field of cybercrime, ASEAN has been improving its performance of cooperation through its adoption as one out of ten cooperation fields under Senior Officials Meeting on Transnational Crime (SOMTC) since 2001. SOMTC has become a discussion platform for ASEAN member states and its dialogue partners related to cybercrime (The ASEAN Secretariat, n.d.).

At the 31st ASEAN Summit held in Manila, Philippines, ASEAN reaffirmed the importance of the harmonization of laws related to cybercrime and the electronic evidence. This summit also encouraged all the member states to explore the possibilities of accessing regional and international instruments related to cybercrime (The ASEAN Secretariat, 2017). Furthermore, at the 32nd ASEAN Summit held in Singapore in 2018, ASEAN underlined the importance of promoting non-binding and voluntary international cyber norms related to states behavior in cyberspace. In this context, the leaders of ASEAN member states agreed to adopt and implement the existing practical norm in the field of cybersecurity which refers to the voluntary norms, recommended in the report UN GGE's consensus in 2015. This aims to improve mutual trust and common beliefs between ASEAN member states. The existence of the UN Charter is also very essential to become the global basis for ASEAN in maintaining peace and stability, as well as supporting the open, safe, stable, peaceful, and accessible environment of ICTs (The ASEAN Secretariat, 2018).

ASEAN is the first, one and only regional institution that has committed to adopt and implement 11 points of cyber norm initiated by UN GGE in 2015. Singapore has also contributed in the process of norm formulation and norm implementation in UN GGE (Kim, 2022, p. 40). Singapore collaborated with Malaysia to host a workshop on a regional action plan to promote any discussions related to those 11 points of cyber norm and translate them into practices (CSA Singapore, 2021). The other member states, such as Malaysia and Indonesia are also actively participating in any UN GGE's official meetings (Heinl, 2018). In the UN OEWG process, Singapore and Indonesia are considered to become the most active ASEAN member states in the UN OEWG process. Meanwhile, member states with less internet penetration, such as Myanmar and Cambodia, didn't participate or even gave any statements in both processes (Poetranto et al., 2021, p. 327).

In the process of UN OEWG, both Singapore and Indonesia agree to underline that the main problem in the context of cybersecurity is the misuse of ICTs. For that reason, all actions and legal frameworks related to the use of ICTs must be formulated, in order not to disrupt the improvement of new technology and innovations in the future (Indonesia, 2020, p. 2). Through their statements, both Singapore and Indonesia acknowledged that cyber threats cannot be mitigated simply by improving domestic capacity. However, there is also a necessity to help each other, especially to the less developed countries which are more vulnerable and potential to become a target for cyberattacks (Poetranto et al., 2021, p. 327). Still in the UN OEWG process, Singapore and Indonesia said that ASEAN plays an important role in the building and adapting cyber trust and capacity, either within the region and between other regional institutions (Poetranto et al., 2021, p. 327).

4.2. ASEAN's Subsidiary Norms: ASEAN Way and The Principle of ASEAN Centrality

ASEAN doesn't have any regional cyber norms to regulate the responsible behavior in cyberspace, but ASEAN has become a mediator in adopting and implementing global cyber norms into the regional level. As a regional institution, ASEAN is trying to offer several advantages that can be used to advance 'rules of the road' in cyberspace (Poetranto et al., 2021, p. 322). In regional institutions, the obstacles can be minimized by the negotiation processes from a smaller number of member states (Henriksen, 2019, p. 6; Madnick et al., 2023, p. 6). In addition, the legitimacy within regional institutions can be maximized because they usually operate based on regionally inherited social and political norms. In addition, the regionally inherited social and political norms within regional institutions can be used to encourage the maximum level of legitimacy. Therefore, regional institutions have better insight in reaching the national priorities of each state and advancing the governance of regional cyberspace (Poetranto et al., 2021, p. 322). cyberspace has now become a dimension where the states are trying to reflect the uniqueness of their visions and strategies inside it (Dai & Gomez, 2018, p. 225).

ASEAN's norm subsidiarity depends on the uniqueness of ASEAN's diplomatic culture and normative structures in promoting norms related to regional cyber governance (Chen & Yang, 2022, p. 61). In regard to the analysis of institutional structure and key documents related to ASEAN's cyber and digital policies, the approaches used by ASEAN as the basis for its cyber governance have two distinct characteristics: first, the principles and norms served as guidelines and adopted by ASEAN are in line with ASEAN's conventional foundation, namely ASEAN Way; and second, the principle of ASEAN centrality is always displayed in the vision of cyber governance implemented by ASEAN, especially those which related to the digital cooperation between ASEAN and its external parties (Chen & Yang, 2022, p. 58).

Acharya (1998) stated that ASEAN Way is a form of ASEAN's security culture. The emergence of ASEAN Way can be seen through four interrelated terms: first, the close interpersonal relationships among ASEAN's founding leaders; second, as an expression of cultural similarities; third, norm and regulation for ASEAN; and lastly, the process of interaction and socialization that marked up the evolution of ASEAN since 1967 (Acharya, Culture, security, multilateralism: The 'ASEAN way' and regional order, 1998, p. 56). In the context of security, the goal of ASEAN Way is to prevent and handle intra-regional conflicts (Acharya, Culture, security, multilateralism: The 'ASEAN way' and regional order, 1998, pp. 57-58). ASEAN Way contains a set of norms that respect the state sovereignty, the principle of non-intervention, informality, the minimalism of organizations, and intensive consultations leading to consensus opposed to legally binding agreements and regulatory frameworks (Solingen, 2005, p. 11; Haacke, 2013; Chen & Yang, 2022, p. 58). Rather than relying on legally binding agreements and highly institutionalized power initiatives, ASEAN regional cyber cooperation is defined by the strict adherence towards inter-governmental approach. Therefore, ASEAN appears to become a passive norm recipient from UN global cyber norms for the governance of cyberspace (Chen & Yang, 2022, p. 58). To encourage progress at the global level, ASEAN needs to make sure that its achievements can continuously influence another process, such as UN GGE and UN OEWG (Poetranto et al., 2021, p. 328).

In order to formulate the properly respected cyber norms, there must be a viable regional mechanism in monitoring and ensuring the compliance and meaningful consequences for the norm violations. However, ASEAN's sensitivity to the principle of non-intervention and sovereignty becomes the obstacle for ASEAN in achieving any of ASEAN's goals regarding the establishment of regional cyber norms. Additionally, the UN GGE and UN OEWG's efforts to improve regional cyber norms formation had been hampered by the disagreements of member states over the best means of maintaining sovereignty while achieving cybersecurity and the necessity of a binding legal framework versus a non-binding one. Looking at the position of Singapore and Indonesia in those two processes, this problem has also a potential to hinder the process of ASEAN in achieving the formation of regional cyber norms (Poetranto et al., 2021, pp. 328-329). ASEAN's strict adherence to the principle of non-intervention in each other's domestic interests can also be a hinder for ASEAN to reach the equal position in the cyberspace (Dai & Gomez, 2018, p. 225). Moreover, ASEAN is historically formed from the various countries with the contrast of differences. ASEAN member states are basically having no common threats, not having the same political system, and not even having the same economic growth (Fitriani, 2017, p. 115). Those contributed in creating the different cyber perceptions, capability, and solutions to deal with the issue of cybersecurity (Dai & Gomez, 2018, pp. 226-227).

For the second characteristic, ASEAN emphasizes the principle of ASEAN Centrality. The goal is to maintain ASEAN's position to become the center of institutional architecture and to promote broader regional cooperation in the Asia-Pacific region. ASEAN Centrality helps ASEAN to manage its relations with the powerful external parties, such as the US, China, Japan, South Korea, European Union, as well as India (Chen & Yang, 2022, p. 50). The conception of ASEAN Centrality has been clearly explained through the ASEAN's official documents, such as ASEAN Charter (Tan S. S., 2012, p. 26). ASEAN Charter stated that ASEAN needs to maintain its proactive role and centrality as the main driving force in establishing the open, transparent, and inclusive relations and cooperations with its external partners in the regional architecture (ASEAN Secretariat, 2008). For example, ASEAN Plus Three (APT), ASEAN Regional Forum (ARF), and East Asian Summit (EAS) (Acharya, The Myth of ASEAN Centrality?, 2017, p. 274).

ARF has organized some seminars and workshops related to cyber issues since 2004. At that time, ASEAN focused on cyberterrorism, the response towards cyber incidents, the national capacity building, and the threats from proxy actors (ARF, 2012). ARF is mentioned to become one of the most interested ASEAN forums in building the cyber trust (Dai & Gomez, 2018, p. 224). APT has also placed any issues related to cyberspace as a priority within the ASEAN Plus Three Cooperation Work Plan (2018-2020). In that work plan, APT strives to promote cybersecurity cooperation to build a resilient and safe regional cyberspace (Chen & Yang, 2022, p. 59).

The third characteristic of ASEAN's regional cyber governance is a discrepancy in the cyber capacity and governance of cybersecurity in ASEAN countries. Malaysia and Singapore tend to carry out institutional and legal development in a relatively more comprehensive manner. Apart from establishing special agencies in the field of cyber security, the two countries also present special departments handling cyber issues in various different ministries. This pattern is in contrast to that of Laos which prioritizes the role of the Ministry of Posts and Telecommunications and the national CERT agency. In terms of cyber security governance, there are also differences in the coordination flow between ASEAN countries. On the one hand, some countries choose to involve security authorities, such as the army, police, or both, in dealing with cyber threats. The differences between the three options are shown by Vietnam, Thailand, and Singapore, which involve the army, police and both army and the police, respectively. Differences in ownership of central bodies in the field of cyber security also reflect differences in coordination flows. Indonesia, Malaysia, Singapore and Thailand are countries that have bodies specifically tasked with handling cyber security. Meanwhile, other countries prefer to hand over this task to departments within various existing ministries.

ASEAN countries' cybersecurity budgets also reflect discrepancies in cybersecurity commitments. Although ASEAN has cumulatively increased its national cyber security budget periodically in the last five years (cumulatively the estimated cyber security budget for each ASEAN member country is 0.05% to 0.08% of Gross Domestic Product (GDP) since 2015 until 2018), there is a gap in the amount of national budget allocation that appears constantly. In this case, Singapore has always been the country with the largest budget, with a budget percentage of 45%, 44%, 42% and 42%, of the aggregate of all national budgets in ASEAN respectively from 2015 to 2018 (A. T. Kerney, 2018, p. 10). On the other hand, other countries tend to budget much smaller amounts than Singapore. This trend especially occurs in Cambodia, Laos, Brunei Darussalam, and Myanmar which, cumulatively, always disburse funds amounting to 1% of the aggregate of all national budgets in ASEAN from 2015 to 2018. Thus, there is a gap in the national security budget allocation among ASEAN member countries.

In the Telecommunications Union's assessment, ASEAN countries also achieved very different scores with a wide gap between the highest and lowest scores. Constantly, Singapore and Malaysia, as countries that occupy the top two rankings, always get scores that are far from the countries that get the lowest scores. Then, countries that occupy the lowest positions tend to overcome obstacles to improve or maintain their scores. This is especially demonstrated by Laos, Cambodia and Myanmar. On the one hand, the scores achieved by Laos and Cambodia have fluctuated, while Myanmar's scores continue to decline (International Telecommunication Union (ITU), 2019).

4.3. Supportive/Strengthening of Global Norm: The UN Global Cyber Norms (UN GGE and UN OEWG

Norms are usually formed as a result of the codification from the existing state practices. UN norms, as introduced in the resolution 70/237 of United Nations General Assembly (UNGA) are function to set the standards regarding what constitutes as a form of responsible behavior by the international community, based on the results of observations against the behavior done by the state actors either in the past until now (Hogeveen, 2022, p. 17). In the context of cyberspace governance, under UNODA, the UN established 2 processes related to the formation of global cyber norms, namely UN GGE and UN OEWG. UN GGE is aiming to create a basic framework to manage any kind of conflicts happening in the cyber domain, as well as possible ways to prevent and/or handle those conflicts. Besides that, the reports resulting from the consensus of UN GGE, can be functioned as legal and normative guidelines related to responsible state behavior in the cyber domain (Broeders, 2021, p. 277).

The consensus reports produced by UN GGE have their own key points to be presented: 1) In 2010, the report of UN GGE was marked as the success of the experts in reaching the first consensus on the nature of threats in the landscape of cyberspace (UN GGE, 2010); 2) The 2013 report was marked as the first time of the experts giving their proposals on the need for the implementation of international law in the cyber domain (UN GGE, 2013); 3) In 2015, there was a reaffirmation that international law can be used in cyberspace. Still in the same report, UN GGE was also presenting 11 points of voluntary and non-binding norm to regulate the states' behavior in cyberspace (UN GGE, 2015). Lastly, in 2021, the report of UN GGE contained the extensive elaboration regarding the previous 11 points of non-binding norm established in 2015, stating that "in line with the mandate to promote the responsible behavior, the UN has improved the additional layers to understand those norms […] provided the examples from any kind of institutional settings that can be applied by the states, either in the national and regional level (UN GGE, 2021; Kim, 2022, p. 33).

In 2017, the UN GGE failed to reach a consensus to provide explicit endorsement of the applicability of the right to self-defence, international humanitarian law and the use of countermeasures (Korzak, 2017). After the failure of UN GGE in reaching the consensus in 2017, United Nations formed a new process based on the resolution draft proposed by Russia in 2018, namely UN OEWG. Rather than UN GGE, UN OEWG is considered to be more democratic, inclusive, and transparent. Different from UN GGE which only involves 25 of states in its process, UN OEWG is actually involving the whole of UN member states (Kim, 2022, p. 33). The UN OEWG report didn't clearly explain the 11 points of norm which previously coined by UN GGE, but this process admitted the resolution 70/237 and 73/27 which refer to the UN GGE report and contain the emergence of those 11 points of norm, and also record the proposal of the states regarding their elaboration in relation to the rules, norms, and principles of the responsible state behaviour (Kim, 2022, p. 33).

The International community's ability in preventing and mitigating the effects of malicious cyber activities depends on the capacity of each member states in preparing the respond for the issues. This is pertinent for developing countries, particularly to enable the engagement and discourse about cyber capability within the framework of international security, as well as their capacity in mitigating risks and preserving the critical infrastructure (Tan & Ang, 2022, p. 158). As a regional institution focused on regional security and stability, ASEAN recognizes the significance of regional cyber norms. Consequently, ASEAN adopted and implemented the relevant global cyber norms, particularly those outlined by the UN GGE and UN OEWG. ASEAN is also promoting its domestic values, principles, and norms as the guidelines on the formation of global cyber norms. However, the implementation of the internationally agreed political agreements won't be free from any kind of challenges and obstacles. The documents may include the unclear language and terminology because they were formed through the negotiation between the governments. Because of this factor, as well as the lack of the blueprint, it is important for the states to build their own views and strategies in implementing the framework of UN global cyber norms (Hogeveen, 2022, p. 17).

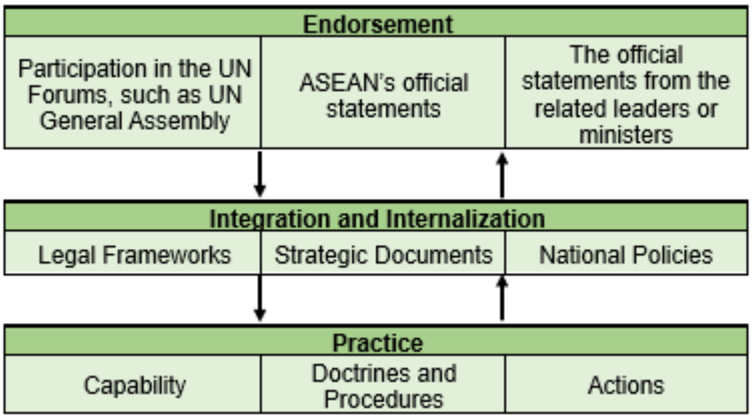

Endorsement
Participation in the UN Forums, such as UN General Assembly
ASEAN's official statements
The official statements from the related leaders or ministers
Integration and Internalization
Legal Frameworks
Strategic Documents
National Policies
Practice
Capability
Doctrines and Procedures
Actions

Figure 3. The implementations of UN global cyber norms related to responsible state behaviour
Source: (Hogeveen, 2022)

In regard with that ambiguity, states can demonstrate the application of the international behavioral norms through several ways. The implementation of global normw can be distinguished into three different levels, such as political endorsement, national laws and policies, and the action on the stages (practices). At the political endorsement level, states could be taking part at the UN General Assembly voting processes to support the pertinent resolutions. States might also collectively follow the ASEAN leaders and related ministers' statements participated in the UN forums. At the integration and internalisation level, the states could integrate and internalize the norms, both explicitly and implicitly into the national legal frameworks, as well as the national strategies and policies. Lastly, at the practice level, the states could demonstrate their implementations by referring to their governance practices in the form of institutional capabilities, doctrines and procedures, as well as the actions. These practices could provide clear evidence of the state's efforts in following the norms related to responsible behavior. The states could demonstrate their commitment on addressing the issues by cyber security through these practices (Hogeveen, 2022, p. 18).

4.4. Challenging of External Powerful Actors: Between US and China?

The historical goal for ASEAN has been to prevent the power of the external parties in achieving the great influence against the member states in the region or the region as whole. However, the ASEAN member states actually can't simply choose between the US and China (Acharya, The Myth of ASEAN Centrality?, 2017, p. 153). Historically, some ASEAN member states have been having close relations with the major powers. The close relations between the ASEAN member states and the major powers that existed even before the ASEAN member states got their independence, have contributed in creating the bigger internal gaps between the ASEAN member states themselves.

Rather than having the harmonious relationship within the internal ASEAN member states, they actually have a closer and harmonious relationship with their external parties (Mueller, 2019, p. 188). Those long-standing relationships then determined the position of ASEAN member states during the cold war. As a result, Thailand, Filipina, and Singapore were traditionally having closer ties with the US, while Vietnam could be considered as a part of the Soviet Union's alliance (Fitriani, 2017, p. 115). Those kind of polarization in Southeast Asia can be seen as a cluster of competing identities, especially between the interests of ASEAN and the interests of Indochina led by Vietnam (Acharya, Imagined Proximities: The Making and Unmaking of Southeast Asia as a Region, 1999, p. 68).

As a potential economic hub that connects the "west" with the "east", ASEAN has been involved indirectly in the trade war between the US and China. The digitalization of the ASEAN economy and other infrastructure within the region has created a more accessible environment. Therefore, the US-China trade war dynamics have had a major impact on ASEAN industries, starting from manufacturing, agriculture, and information technology. These industries are very vulnerable to any unprecedented state-sponsored cyberattacks These industries are very vulnerable to any unprecedented state-sponsored cyberattacks (CyberSecurity Malaysia, 2021). Regarding those matters, ASEAN is facing the challenges against its principle of neutrality adopted in ASEAN Centrality. ASEAN's alignment against the dynamics and competitions between two major powers is being questioned. For example, when the relations between US and China in the Southeast Asia region are suddenly heating up, both countries are putting any significant interest within the ASEAN member states (Acharya, The Myth of ASEAN Centrality?, 2017, p. 277). Some Southeast Asian countries are seeking the security guarantees of the US against China. Meanwhile, most of the countries in the region are taking a more balanced approach, as they rely on China for trade and investment (CYFIRMA, 2023).

In the context of cybersecurity, China is currently becoming one of the most feared countries by the ASEAN member states. China is actually presenting any serious threats and challenges in the Asia-Pacific region. China direct industrial cyber espionage against high-tech and advanced manufacturing companies in various countries, such as the US, Europe, Japan, and Southeast Asia (Segal, 2020, p. 61). According to the report released by a US-based private cybersecurity company, Chinese hackers are most likely state-sponsored hackers, they widely targeted governmental organizations and private sectors in Southeast Asia, including the countries with close ties to China. Particularly, they targeted the Thai Prime Minister's Office and the Thai Army, the Indonesian and Philippine Armies, the National Assembly of Vietnam and the Vietnam Communist Party Headquarters, as well as the Malaysian Ministry of Defence (Rising, 2021).

The Chinese organized criminal groups are now operating in the Southeast Asian countries bordering Cambodia, Laos, and Myanmar. These groups are spreading online frauds to all of the internet users in the world, so these can be considered as global security threat. ASEAN has basically tried to follow up the existing issues to maintain regional peace and security. However, Myanmar is a country with weak response capabilities, where there is almost no political will for Myanmar to handle this issue. Thus, it is a little difficult for ASEAN to handle the existing issues with the same threat perception between the member states (Naing, 2023). Meanwhile, in the perspective of China, Myanmar is being a development area for cybercrimes and often targeting China. For that reason, China is attempting to establish stronger cooperation and coordination with Thailand and Laos in order to overcome this issue. The Chinese government has urged Myanmar to put more effort in combating those criminal groups, moreover those groups are often colluded with Chinese criminal groups (Ziwen, 2023).

4.5. The Implications of Global Cyber Norms Subsidiarity in the ASEAN

Cybersecurity might not be one of ASEAN's concerns at the first time ASEAN was established. Even so, as time passed, several topics related to cybercrime and cybersecurity have taken place in ASEAN's meetings and dialogues. Since 2004, ASEAN has been starting to be more concerned with the issues related to cybercrime and cybersecurity (Chang, 2017). The attachment between the ASEAN member states and the improvement of ICTs has made this region become more vulnerable to any cyber incidents. The number of these incidents are significantly increasing, following the increasing number of the populations in the region. Even in between 2013-2014, ASEAN member states had experienced various kinds of cybercrimes, such as malicious computer activities, Automatic Teller Machines (ATMs) heists, Advanced Persistent Threat (APT), and etc

(Chang, 2017). The incident has now grown to be more varied, according to the annual assessment reported by the Interpol, in 2020, ASEAN had experienced any kind of cyberthreats, such as data breach and ransomware. These indicate that ASEAN needs to adopt and implement the UN global cyber norms. However, those norms are not yet effective to reduce the whole incidents in the region.

ASEAN member states are still becoming the main targets of cyberattacks. The large number of the incoming cyberattacks in the region proves that ASEAN member countries are having the vulnerable and unsafe infrastructure, so they can be infected easily on a larger global scale (A.T Kearney, 2018, p. 5). Although ASEAN's position as a regional institution is to promote a continuously increasing cybersecurity architecture, both the national and regional endeavors to adopt a comprehensive cybersecurity strategy are increasingly getting slow and fragmented (Manopo & Sari, 2015, p. 44). Cyber policies and governance are not yet well developed in the Southeast Asia region. However, several ASEAN member states, such as Singapore, Malaysia, Thailand, and Philippines have established their national cyber strategies. The other member states have also established the national bodies to consolidate and coordinate any cybersecurity agendas (A.T Kearney, 2018, p. 7).

In line with ASEAN, the establishment of UN global cyber norms is actually concerning the principle of non-interference and the principle of sovereignty. However, those two principles are not used in every kind of cyber incidents, they are used only after the detailed considerations about the effect that might be resulted from those incidents (digwatch). As long as ASEAN agreed to adopt and implement the two of UN global cyber norms, the member states have not yet questioned about the effects of the attacks, as well as doing things that could injure the principle of sovereignty by using the ICTs. Even so, ASEAN still shows its neutrality in adopting and implementing the global cyber norms, especially when both US and Russia proposed the parallel discussions, called UN GGE and UN OEWG and both are potentially competing to become a norm entrepreneur regarding the development of ICTs in the context of UN international security. Most ASEAN member states choose to support both proposals. Singapore stated that UN GGE and UN OEWG must go hand in hand and complement each other (Noor, 2020, p. 113).

In regard to that issue, recent analysis notes that, rather than choosing between a state-centric multilateral cyber governance approach adopted by non-western countries and a market-based multi-stakeholder approach adopted by western countries, ASEAN prefers to be a bridge between the two of cyber governance approach, adopted by China and US (Raemdonck, 2021; Chen & Yang, 2022). However, ASEAN has begun to embrace the idea of multi-stakeholderism in cyber governance. This can be proven through the policy released by ASEAN, titled "ASEAN Cybersecurity Cooperation Strategy 2021-2025", ASEAN seeks to implement a multi-discipline, modular and measurable cyber capacity building approach for the stakeholders (ASEAN, 2022).

5. Conclusion

ASEAN has confirmed its commitment to put cyber issues and cyber governance as one of their priorities. However, ASEAN doesn't have a single regional cyber norm that could clearly regulate the responsible behavior of ASEAN member states in cyberspace. ASEAN is still difficult to formulate its own regional cyber norm because of some factors, such as: first, the long-standing heterogeneity among the member states contributed in creating the bigger gaps in all sectors; and second, the closer relation between the member states and their external partners allowed the overlapping interests of the member states.

In order to maintain its regional cybersecurity, ASEAN committed to perform on the norm subsidiarity towards the UN global cyber norms, namely UN GGE and UN OEWG. It also refers to ASEAN's traditional principles, such as sovereignty, non-intervention, and neutrality. Several of the ASEAN member states, such as Singapore, Malaysia, and Indonesia, are actively participating in the official meetings coined by UN GGE and UN OEWG. The three of them are also actively giving their official statements as the representation of the national and regional interest. We find that the implication of norm subsidiarity in ASEAN is still identifiable. There is still no concrete literature proving that the process of norm subsidiarity is effective in reducing the number of cyberattacks in ASEAN.

In this research, the authors also find that the non-democratic and conflict-prone countries like Myanmar tend to be uncooperative to participate in the existing processes. This can be said that Myanmar is a state with the lack of political will. So, it is difficult to ensure Myanmar's steps and commitments in maintaining the security and stability of cyberspace, especially for the Asia-Pacific region.

References

A.T Kearney. (2018). Cybersecurity in ASEAN: An Urgent Call to Action. Seoul: A.T Kearney.

Acharya, A. (1998). Culture, security, multilateralism: The 'ASEAN way' and regional order. Contemporary Security Policy, 55-84. Retrieved from https://doi.org/10.1080/13523269808404179

Acharya, A. (1999). Imagined Proximities: The Making and Unmaking of Southeast Asia as a Region. Southeast Asian Journal of Social Science, 55-76.

Acharya, A. (2011). Norm Subsidiarity and Regional Orders: Sovereignty, Regionalism, and Rule-Making in the Third World. International Studies Quarterly, 95-123. Retrieved from https://www.jstor.org/stable/23019515

Acharya, A. (2017). The Myth of ASEAN Centrality? Contemporary Southeast Asia, 273-279.

ARF. (2012). Co-Chairs' Summary Report of the ARF Seminar on Confidence Building Measures in Cyberspace. Seoul.

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

ASEAN Secretariat. (2008). THE ASEAN CHARTER. Jakarta: ASEAN.

ASEAN Secretariat. (2009). ASEAN POLITICAL-SECURITY COMMUNITY BLUEPRINT. Jakarta: ASEAN Secretariat.

Broeders, D. (2021). The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment. Journal of Cyber Policy, 277-297. https://doi.org/10.1080/23738871.2021.1916976

Bryman, A. (2012). Social Research Method. Great Clarendon Street, Oxford: Oxford University Press.

Butler, B., & Lachow, I. (2012). Multilateral Approaches for Improving Global Security in Cyberspace. Georgetown Journal of International Affairs, 5-14. Retrieved from https://www.jstor.org/stable/43134333

Buzan, B., & Hansen, L. (2009). The Evolution of International Security Studies. United Kingdom: Cambridge University Press.

Cha, V. D. (2000). Globalization and the Study of International Security. Journal of Peace Research, 391-403. Retrieved from https://www.jstor.org/stable/425352

Chang, L. (2017). Cybercrime and Cyber security in ASEAN. Dalam J. Liu, M. Travers, & L. Y. Chang (Penyunt.), Comparative Criminology in Asia (hal. 135-148). Springer Cham. Retrieved from https://doi.org/10.1007/978-3-319-54942-2

Chen, X., & Yang, Y. (2022, August 24). Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. Italian Journal of International Affairs, 1-14. Dipetik July 24, 2023, dari https://doi.org/10.1080/03932729.2022.2101231

Choucri, N., Madnick, S., & Ferwerda, J. (2013). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 96-121. Retrieved from https://doi.org/10.1080/02681102.2013.836699

CSA Singapore. (2021, October 05). The Singapore Cybersecurity Strategy 2021. Retrieved from CSA Singapore: https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

CyberSecurity Malaysia. (2021). CYBER SECURITY OUTLOOK IN SOUTH EAST ASIAN REGION: FROM CYBERSECURITY MALAYSIA'S PERSPECTIVE. Selangor Darul Ehsan: CyberSecurity Malaysia.

CYFIRMA. (2023, November 17). The Changing Cyber Threat Landscape Southeast Asia. Retrieved from CYFIRMA: Decoding Threats: https://www.cyfirma.com/outofband/the-changing-cyber-threat-landscape-southeast-asia/

Dai, C. T., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. Journal of Cyber Policy, 217-235. Retrieved from https://doi.org/10.1080/23738871.2018.1487987

digwatch. (t.thn.). UN OEWG. Retrieved from digwatch: Geneva Internet Platform: https://dig.watch/processes/un-gge

Finnemore, M. (2017). Cybersecurity and The Concept of Norms. CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE.

Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. The American Journal of International Law, 425-479. Dipetik July 24, 2023, dari https://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425

Fitriani, E. (2017). Regionalism And Global Powers. Dalam N. Farelly, A. King, M. Wesley, & H. White (Penyunt.), Muddy Boots & Smart Suits: Researching Asia-Pacific Affairs (hal. 110-124). ISEAS-Yusof Ishak Institute.

Fjäder, C. O. (2016). National Security in a Hyper-connected World. Dalam A. J. Masys, Exploring the Security Landscape: Non-Traditional Security Challenges (hal. 31-58). Switzerland: Springer International Publishing Switzerland.

Greiman, V. (2015). Cybersecurity and Global Governance. Journal of Information Warfare, 1-14. Retrieved from https://www.jstor.org/stable/10.2307/26487502

Haacke, J. (2013). ASEAN's Diplomatic and Security Culture: Origins, Development and Prospects. London-New York: Routledge.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 1155-1175. Retrieved from https://www.jstor.org/stable/35139

Heinl, C. (2018, March 22). Can ASEAN Continue to Improve Cybersecurity in the Region and Beyond? Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/can-asean-continue-improve-cybersecurity-region-and-beyond

Henriksen, A. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. Journal of Cybersecurity, 1-9. https://doi.org/10.1093/cybsec/tyy009

Hodges, B. D., Kuper, A., & Reeves, S. (2008). Qualitative Research: Discourse Analysis. BMJ: British Medical Journal, 570-572. Retrieved from https://www.jstor.org/stable/20510756

Hogeveen, B. (2022). The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN. Australia: ASPI.

Indonesia. (2020). Indonesia's Response on the Pre-Draft Report of the UN OEWG on the developments in the field of ICT in the context of international security.

International Telecommunication Union (ITU). (2019). Global Cybersecurity Index (GCI) 2018. ITUPublications.

Kim, S. (2022). Roles and Limitations of Middle Powers in Shaping Global Cyber Governance. The International Spectator, 31-47. https://doi.org/10.1080/03932729.2022.2097807

Korzak, E. (2017, July 31). UN GGE on Cybersecurity: The End of an Era? Dipetik Oktober 15, 2023, dari The Diplomat: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., . . . Wolff, S. (1997). A Brief History of the Internet. Retrieved from Internet Society: https://www.internetsociety.org/internet/history-internet/brief-history-internet/

Madnick, B., Huang, K., & Madnick, S. (2023). The evolution of global cybersecurity norm in the digital age: A longitudinal study of the cybersecurity norm development process. Information Security Journal: A Global Perspective, 1-20. Retrieved from https://doi.org/10.1080/19393555.2023.2201482

Manopo, B. Y., & Sari, D. A. (2015). ASEAN REGIONAL FORUM: REALIZING REGIONAL CYBER SECURITY IN ASEAN REGION. Belli ac Pacis, 44-51.

Mueller, L. M. (2019). ASEAN centrality under threat - the cases of RCEP and connectivity. Journal of Contemporary East Asia Studies, 177-198.

Naing, I. (2023, Juni 28). Chinese Cybercrime Syndicates in Myanmar Now Target Victims Worldwide. Retrieved from VOA: https://www.voanews.com/a/chinese-cybercrime-syndicates-in-myanmar-now-target-victims-worldwide/7158750.html

Neuman, W. L. (2014). Social Research Method : Qualitative and Quantitative Approaches (7 ed.). Edinburgh Gate: Pearson Education Limited.

Noor, E. (2020). Positioning ASEAN in Cyberspace. Asia Policy, 107-114. Retrieved from http://asiapolicy.nbr.org

Poetranto, I., Lau, J., & Gold, J. (2021). Look South: challenges and opportunities for the 'rules of the road' for cyberspace in ASEAN and the EU. Journal of Cyber Policy, 318-339. Retrieved from https://doi.org/10.1080/23738871.2021.2011937

Raemdonck, N. V. (2021). DIGITAL DIALOGUE: Cyber Diplomacy in Southeast Asia. EU Cyber Direct. Retrieved from https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/2ZycxfN1/dd-southeast-asia-nb-fb-nvr-09-05.pdf

Rising, D. (2021, December 9). Report: Chinese hackers targeted South East Asian nations. Retrieved from The Associated Press: https://apnews.com/article/technology-business-indonesia-beijing-asia-bca3e5785c03cb4d7a1e3052f545a922

Segal, A. (2020). China's Pursuit of Cyberpower. Asia Policy, 60-66. Retrieved from http://asiapolicy.nbr.org

Solingen, E. (2005). ASEAN cooperation: the legacy of the economic crisis. International Relations of the Asia-Pacific, 1-29. Retrieved from https://www.jstor.org/stable/26156602

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy, 148-170. Dipetik Juli 24, 2023, dari https://doi.org/10.1080/13523260.2012.659597

Tan, E. E., & Ang, B. (2022). ASEAN Ambiguity on International Law and Norms for Cyberspace. Baltic Yearbook of International Law Online, 133-161. https://doi.org/10.1163/22115897_02001_008

Tan, S. S. (2012). ASEAN CENTRALITY. Council for Security Cooperation in The Asia Pacific .

The ASEAN Secretariat. (2017). ASEAN DECLARATION TO PREVENT AND COMBAT CYBERCRIME. Manila: ASEAN Secretariat. Retrieved from https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

The ASEAN Secretariat. (2018). ASEAN LEADERS' STATEMENT ON CYBERSECURITY COOPERATION. Singapura: ASEAN Secretariat. Retrieved from https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf

The ASEAN Secretariat. (t.thn.). Cyber Security. Retrieved from ASEAN: https://asean.org/our-communities/asean-political-security-community/peaceful-secure-and-stable-region/cyber-security/

Tikk, E. (2011). Ten Rules for Cyber Security. Survival, 119-132.

UN GGE. (2010). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201. New York: UNGA.

UN GGE. (2013). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98. New York: UNGA.

UN GGE. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. New York: UNGA.

UN GGE. (2021). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security. A/70/174. New York : UNGA.

UNGA. (2018). Resolution adopted by the General Assembly on 22 December 2018 on Advancing responsible state behaviour in cyberspace in the context of international security. A/RES/73/266.

Ziwen, Z. (2023, August 23). China teams up with Thailand and Laos to tackle cybercriminals in Myanmar who often target Chinese nationals. Retrieved from South China Morning Post: https://www.scmp.com/news/china/diplomacy/article/3232057/china-teams-thailand-and-laos-tackle-cybercriminals-myanmar-who-often-target-chinese-nationals