ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia

Iqbal Ramadhan

{iqbal.ramadhan@universitaspertamina.ac.id}

Pertamina University, Jakarta, Indonesia

Abstract. Southeast Asia has emerged as one of the world's economic development zones. The advancement of information technology is undeniably driving economic growth in this region by the digital economy. Association of Southeast Asian Nations (ASEAN) member countries reap the benefits of the region's digital economy development. However, ASEAN itself still has significant problems related to cyber security regulations. Unlike other non-traditional security organizations, ASEAN already has a cooperation framework in place to combat security threats such as drugs, terrorism, and human trafficking. In reality, ASEAN does not yet have a framework for cooperation or regulation in dealing with cyber threats. This region is heavily reliant on the expansion of the digital economy. This scientific article will examine how ASEAN can maximize the organization's consensus mechanism in order to reach an agreement on cyber security regulations in the Southeast Asian region. The author analyzes cyber security issues using qualitative methods. As a data collection technique, the author employs a case study approach and secondary data such as literature studies. According to the author's discussion, a cybersecurity cooperation framework can be achieved through consensus if ASEAN can maximize the functions of the general secretariat and critical regional forums. As a result, the role of ASEAN sub organ will be very important in order to foster cybersecurity consensus in the Southeast Asian region.

Keywords: ASEAN, Southeast Asia, consensus, cyber security, international organization.

1 Introduction

The rapid development of information technology in this digital era influences the social, political, and economic dynamics of a region. According to Joseph S. Nye, the current state needs to make a breakthrough by increasing its capabilities in the political, economic, and technological fields [1]. Technology is important for economic growth, but it is also a political tool that can increase a country's bargaining power [2]. For example, under the governance of the European Union, the European region has already prepared regulations governing its digital world in the policy known as the "Cybersecurity Strategy 2013 [3]. The European Union believes that cyberspace has a positive impact on the digital economy's growth. This expansion has the potential to raise the income of EU member states. However, just like in the real world, the digital world must be protected from

ICONIC-RS 2022, March 31-April 01, DKI Jakarta, Indonesia

DOI 10.4108/eai.31-3-2022.2320684

unauthorized parties. One example is cybercrime, which includes hacking, money theft, and other illegal activities. As a result, the European Union regulates cyber security in order to benefit from the digital economy's growth while reducing the number of cybercrimes that can affect its member countries [3].

Not only is the European region experiencing digital economic growth, but the Southeast Asia region is also benefiting from the advancement of the digital world. The advancement of the digital world promotes economic growth in Southeast Asia. Digital trade (e-commerce) and online transportation contribute to the growth of the Southeast Asian digital economy [4][5]. Southeast Asia's total trade is expected to reach 102 billion US dollars by 2025, according to economists. In 2018, the digital economy alone contributed $20 billion to Southeast Asia's economic growth. This region exemplifies the evolution of information technology. Digital commerce is critical to the growth of the digital economy [6][7][8]. Singapore has the most total internet users in this region, accounting for 82 percent of the country's total population. Malaysia, Thailand, and Brunei Darussalam have approximately 70% of their citizens connected to the internet [9]. Cyberspace is accessible to approximately 132 million Indonesians and 67 million Filipinos [10]. The International Monetary Fund (IMF) predicted in 2018 that the total profit from digital trade in Southeast Asia could reach US$2.8 trillion [11].

Aside from the rapid growth of the digital economy, the Southeast Asia region continues to face critical domestic issues. This should be one of ASEAN's (Association of Southeast Asian Nations) top priorities to address right away. The issue is that ASEAN does not yet have a solid framework of cooperation in place to combat cyber threats that have the potential to disrupt the region's digital economy. ASEAN launched the 2015 ASEAN Economic Community, with the goal of integrating economic growth with the digital world. According to the "ASEAN ICT Masterplan 2012," the ASEAN Economic Community must be supported by a digital information security cooperation framework [12]. However, ASEAN has yet to establish a clear framework for formal cooperation or cybersecurity governance.

Unlike other non-traditional security forces such as drugs, terrorism, or human trafficking, ASEAN has previously established cooperation and conventions to combat these threats. ASEAN even has a framework for cooperation with China to combat the threat posed by drug cartels, as stated in "ASEAN and China Cooperative Operations in Response to Dangerous Drugs" (ACCORD) [13]. ASEAN is collaborating with the Chinese government through this mechanism to combat drug trafficking in the golden triangle region, which includes Laos, Cambodia, and Myanmar [13]. ASEAN already has a convention called the "ASEAN Convention on Counter-Terrorism" within the framework of cooperation to combat the threat of terrorism [14]. ASEAN has a threat mitigation guide in the form of the "ASEAN Convention on Trafficking in Persons, Especially Women and Children" (ACTIP) in the context of human trafficking [15]. Unfortunately, ASEAN does not yet have a stable framework for cyber security cooperation. This organization is only capable of issuing a joint statement in the form of the "ASEAN Leaders Issue Statement on Cybersecurity Cooperation" [16].

The lack of cyber security rules and regulations has a negative impact on politics, security, and the economy. In terms of politics, technology has the potential to be used to oppress or threaten other countries. A country's power capability can be enhanced by technology. If technology is not regulated, countries with greater technological power will use it as a tool of pressure [17]. Technology, like nuclear weapons, has the potential to be transformed into a weapon. This issue has the potential to drive countries into conflict in both the physical and cyber realms [18]. The worst-case scenario is that the state becomes involved in cyberwar. To further its political interests, the state will attempt to cripple another country's critical infrastructure [19]. In terms of security, technology has the potential to be exploited by non-state actors such as terrorist organizations. Many technologies are built on a "open source" foundation. As a result, terrorist groups can use technology to cripple a country's critical infrastructure, seek funding, and recruit new members [20][21].

Furthermore, ASEAN is currently working on a digitally connected gas pipeline. Energy infrastructure, such as gas pipelines, will become a primary target for terrorist groups if ASEAN does not adopt standard cybersecurity rules [22]. In terms of the economy, the lack of cybersecurity regulations will make it easier for non-state groups, such as criminal organizations, to commit crimes. In 2018, IBM Security disclosed 3.6 million US dollars in total losses due to cybercrime [23]. Cyber threats in the form of cybercrime use advanced technology to steal personal data, banking information, and even commit identity theft in order to profit financially [24][25]. This threat will undoubtedly harm ASEAN and the Southeast Asian region as a growing economic region. The most significant impact will be a reduction in the flow of money and investment because the region is not digitally secure.

The purpose of this scientific article is to examine ASEAN's stance on using the consensus mechanism to reach an agreement within the framework of cybersecurity cooperation. ASEAN's policy-making mechanism is guided by the principle of non-intervention. Each ASEAN member country may participate in the preparation of the cooperation mechanism as long as it does not interfere with its member countries' domestic policies [26]. Furthermore, ASEAN's regional forums, such as the ASEAN Summit, ASEAN Coordinating Council, or ASEAN Community Council, are regularly used to oversee the political, security, economic, and socio-cultural fields. Furthermore, ASEAN has a secretary-general who is elected from among the member countries. According to the 2008 ASEAN Charter, the secretary-general is responsible for overseeing the implementation of ASEAN programs in each member country [27]. The ASEAN consensus mechanism, on the other hand, has frequently been chastised. Some are agreements reached by ASEAN member countries that are frequently carried out bilaterally rather than multilaterally. Furthermore, consensus mechanisms are frequently viewed as merely informal forums. Another criticism is that ASEAN's non-intervention principle is viewed as a barrier to consensus. It is inextricably linked to a number of critical cases, such as humanitarian crises in Myanmar and the Philippines that have since vanished due to member states' reluctance to intervene [28][29][30]. This policy-making mechanism differs from the European Union's federal system, which is comprehensive and has clarity in formal legal aspects [31]. Aside from that, ASEAN is a critical organization in the Southeast Asian region. Organizations have a hierarchy and a set of priorities. The author intends to analyze how consensus

should be achieved, as well as ASEAN's potential in utilizing its organizational components and regional forums, in this paper.

2 Consensus

ASEAN's consensus mechanism is based primarily on the organizational norms that serve as the institution's foundation. ASEAN's consensus mechanism is based on the Southeast Asian community's culture of deliberation and consensus. Both mechanisms resolve problems without involving colleagues in conflict [32]. ASEAN later adopted the Malay culture, which is the source of the culture of deliberation and consensus, as the basic norm for policy-making and problem-solving [32]. The norm was then formalized in a treaty, namely the "Treaty of Amity and Cooperation," which emphasizes the principle of non-interference among ASEAN member countries [26]. In the early 1990s, ASEAN adopted the jargon "ASEAN Way" as the organization's moral compass, emphasizing constructive agreements and dialogue in resolving Southeast Asia's socio-political problems [33]. The ASEAN organization's policy formulation mechanism is unmistakably distinct from that of other organizations such as the European Union. The European Union, for example, has a policy formulation strategy that focuses on policy instrument adaptation, strategic bargaining, dialogue, argumentation, institutionalization, and capitalization [34]. This is unmistakably distinct from ASEAN's character, which is heavily influenced by Eastern culture. There are at least three main goals of ASEAN's consensus mechanism. The goal is to encourage regional consultation, facilitate problem-solving on a specific issue, and influence or shape an issue to align with ASEAN's vision and mission [28]. Is there any significance to the ASEAN consensus mechanism? Because ASEAN relies on its vision and mission in the context of non-intervention, the outcomes of the ASEAN consensus mechanism always result in the formation of solidarity. The goal of this solidarity formation is to avoid open conflicts between ASEAN countries [29]. The ASEAN consensus is, by definition, a flexible consensus. The meaning of this flexible consensus is that the agreement results do not have to be followed by countries that disagree with the organization's decisions. Furthermore, the flexible consensus is simple to apply to non-sensitive economic and political issues [29]. Following the 2008 ASEAN Charter, there are differences in the consensus mechanism for reaching an agreement within ASEAN. Following the ratification of the charter in 2008, ASEAN adopted the formulas "ASEAN minus X" and "X+2" [35]. This formula is used by the ASEAN organization to speed up integration among its member countries. In the "ASEAN minus X" formula, each country can adopt the agreement's results based on its own readiness and conditions. In the "X+2" formula, ASEAN policies can be implemented if more than two countries agree to them [35]. Following the 2008 ASEAN Charter, the mechanism for achieving ASEAN consensus is more formal than before. Prior to the adoption of the charter, ASEAN's consensus was more informal.

In contrast to the post-2008 period, ASEAN employs regional sub-organizations as a consensus-building mechanism [35]. The ASEAN Summit is an important ASEAN sub-organism for promoting consensus. This sub-organ serves as a forum for dialogue and agreement-making among ASEAN member-state leaders [27]. This organization prepared an agenda for the agreement at the

ministerial level, as regulated by the ASEAN Sectoral Ministerial Bodies, prior to discussing the agreement at the ASEAN Summit level (ASMB). This sub-primary organ's function is to coordinate agreements and discuss specific issues. Following the three ASEAN pillars of politics-security, economy, and socio-culture, agreements or policies discussed at the ministerial level will be discussed at the ASEAN Community Councils (APC) [27]. The Committee of Permanent Representatives (CPR) also assists the APC sub-organ in drafting agreements discussed at the ASEAN Summit [27]. The Secretary-General is one of ASEAN's most important sub-organs. Since the ratification of the ASEAN Charter in 2008, this function has played a critical role. The Secretary-General is in charge of overseeing the implementation of ASEAN policies that have been ratified by each member country [35]. This function is consistent with the concept of international organizations as confederation-based policymaking. In theory, a confederation of international organizations will appoint a specific agency within its organization to monitor policy implementation [36]. The secretary-position general's is autonomous and may not be influenced by other member states. In addition to overseeing the implementation of the agreement, the secretary-general serves as ASEAN's administrative center [27]. In theory, however, the secretary-general should be given more authority to set the agenda. The goal is to encourage member states to discuss a critical issue or to avoid sensitive issues that could jeopardize ASEAN solidarity [37]. So far, the secretary-general of ASEAN has been chastised for serving solely to regulate administrative tasks. Much more profoundly, the function of this sub-organ must be endowed with political authority in order to develop a critical agreement agenda in the best interests of all member countries [37]. Following common interests, the secretary-general can position himself to regulate the form of policy-making. Changing the organization's agenda to align the interests of a strong country and a politically weak country is one example [37].

3 Methods

This scientific article's author employs qualitative methods to investigate the phenomenon of international relations. When should a writer employ qualitative techniques? According to Hammarberg (2016), qualitative research analyzes or answers questions about experience, meaning, and perspective. Furthermore, a qualitative researcher can use language to interpret a phenomenon as a means of scientific thinking. One of them is a literature review, which employs a credible text or document to bolster the author's argument during the analysis stage [38]. Case study research is a type of research that is used by researchers as an alternative. According to Roselle and Spray, the case in the study of International Relations is a transboundary phenomenon involving both state and non-state actors [39]. This type of case study in International Relations generally discusses political, social, economic, and security issues [39]. The topics covered in this study are primarily concerned with security, particularly cyber security. The authors use secondary data to support their analysis, which is related to data collection.

The use of secondary data is common in qualitative research. According to Creswell (2014), researchers can use secondary data from reputable sources such as Dimensions, Scopus, or PubMed. Dimensions is used as a secondary data source by the author. Finally, the writer employs secondary

data to bolster the analysis and argument. The author employs a systemic approach technique, which entails bolstering arguments with data, journals, and other reliable secondary sources [40]. In qualitative research, the researcher's perspective or point of view is important. Reflectivism, or the researcher's point of view in qualitative analysis, is defined by Creswell [41]. This qualitative methodology concept allows researchers to use their own point of view as long as it is supported by credible sources [41].

4 Discussion

Before moving on to the analysis stage, the author first summarizes previous research on cyber security. The author conducts a bibliographic search using the VosViewer application to identify cybersecurity research topics that are frequently the focus of research. VosViewer mapping results are as follows:

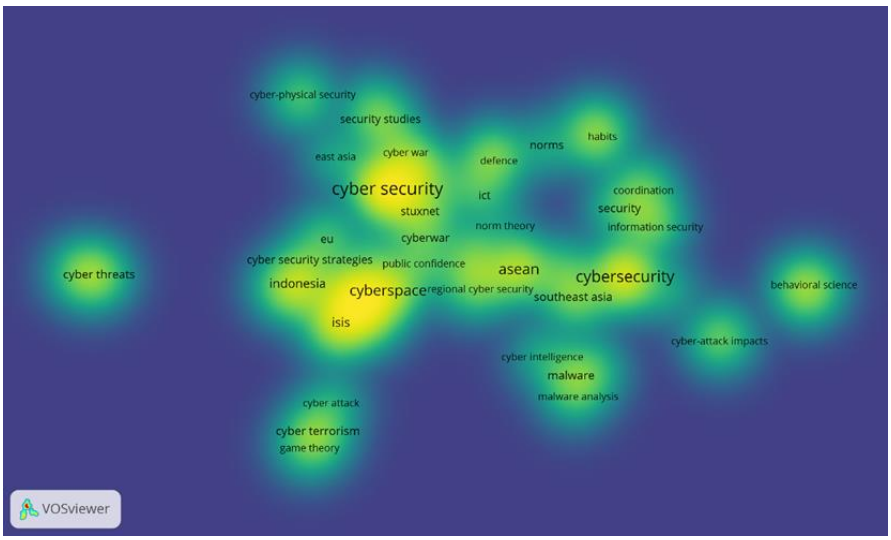

Fig. 1. Cybersecurity research density in Southeast Asia.

The density level of cybersecurity research downloaded from various sources is depicted in the image above. Secondary data in the form of scientific journals is used. The brighter the indicator color, as shown in the image above, indicates the density level of a study. If the indicator's color lightens, it means that the density of the research topic has been thoroughly investigated. At least 50 previous studies are used by the authors to determine the density of cybersecurity research. Previous research, for example, examined cyber security from the perspectives of international law and risk management [26][20]. Another study describes ASEAN's collaboration with actors outside the region to combat cyber threats [42][43]. Previous research has also demonstrated the significance

of norms as an important aspect of cybersecurity regulation in Southeast Asia [44][45][46][47]. Other studies, meanwhile, explain the role of multilateralism in cybersecurity issues, as well as the mapping of cybersecurity research in Southeast Asia [48][49]. However, the research presented above is still very limited in explaining how consensus is implemented as a policy-making mechanism at the ASEAN level. As a result, this scientific article will examine how a consensus mechanism can be implemented in Southeast Asia to reach an agreement in developing cybersecurity regulations.

At the ASEAN level, the cyber security agenda has not received the same level of priority as other security agendas. The organization does not yet have firm cyber security regulations, and regional agreements are still limited to joint statements [16]. The chairman is in charge of setting the agenda, which is coordinated by the secretary-general. The Chairman's role is to set the agenda and bridge the gap between the member countries' interests [37]. Furthermore, the secretary-role general's in ASEAN is frequently criticized for serving solely as an administrator. The ASEAN secretariat can establish lines of communication among member countries and monitor the implementation of organizational decisions [27]. The cyber security agenda must be determined by emphasizing the issue as a priority agenda for dialogue at the ASEAN level. As a result, the chairman is critical in ensuring that cyber security issues are included on the annual agenda. Discussion of cyber security issues could become the main agenda item if the chairman can push the issue to strengthen the member countries' national resilience [50].

On the one hand, the ASEAN secretariat's position must be strengthened. The secretariat's role is to establish coordination and facilitate information exchange [51]. It is important to note that ASEAN economic integration must be supported by the exchange of cybersecurity information [12]. Finally, the ASEAN secretariat can support the chairman's cybersecurity agenda. One method is to coordinate member countries' interests in cyber security issues. The issue was then elevated to the top of the agenda and became the center of attention at the multilateral level. As a result, the outcome of this consensus formulation process emerges from a multilateral, rather than a bilateral, process. Organizations such as ASEAN must optimize the tools within their institutions in order to dispel the myth that the mechanism for achieving consensus in Southeast Asia is bilateral [52]. Before concluding the discussion on how ASEAN's consensus mechanism should be implemented, we must examine the Southeast Asian region's cybersecurity situation and condition. For starters, ASEAN is heavily reliant on the growth of the digital economy. Organizations must integrate economic growth with the digital world in order to benefit their member countries economically, according to the mandate of the ASEAN ICT Masterplan 2012. Furthermore, in order to welcome the 2015 ASEAN Economic Community, this organization must strengthen its commitment to fostering information security cooperation in the digital environment [53][12]. Building cyber security regulations through a consensus mechanism, on the other hand, is a difficult task. The author describes the argument in this second point as the mechanism's preparation must be in accordance with ASEAN Way norms. This norm is enshrined in the Treaty of Amity and Cooperation (TAC), which emphasizes non-intervention, mutual respect, and a commitment to peaceful conflict resolution [32]. Although the norm has received harsh criticism for being too informal, Amitav Acharya explained that by adhering to the norm, ASEAN as a political security organization is relatively stable [53]. As a

result, the goal of reaching consensus on cyber security regulations must not violate the basic rules of the ASEAN Way. The outcome of ASEAN's cybersecurity consensus must be non-interventionist, respect the principle of sovereignty, and be non-confrontational [54][26]. Furthermore, the ASEAN Way is being implemented in the context of cybersecurity cooperation not only within ASEAN countries, but also among the organization's strategic partners outside the Southeast Asian region [34].

ASEAN should maximize the consensus formula of "ASEAN minus X" or "ASEAN X+2" in order to reach a common agreement. This cybersecurity issue, however, is linked to infrastructure development and people's maturity in cyberspace. Singapore and Malaysia are the most mature countries in terms of cybersecurity, according to an index published by the International Telecommunication Union (ITU). They obtained a Singapore index of 0.898 and a Malaysia index of 0.893 [55]. Meanwhile, Thailand received a cyber maturity index of 0.796, while Indonesia received a score of 0.776. These four countries meet the criteria for Asia-Pacific countries with the highest cyber maturity [55]. Vietnam (0.693), the Philippines (0.643), and Brunei are the countries with the modest level of cybersecurity maturity (0.624). According to the ITU data, there is a significant gap in cybersecurity maturity among ASEAN member countries, both in terms of infrastructure and human resource development. Meanwhile, Laos (0.195), Myanmar (0.172), and Cambodia (0.161) have low levels of cybersecurity maturity [55]. This is a difficult issue for ASEAN to resolve in order to reach a cyber security consensus.

Although there is a significant cybersecurity maturity gap among ASEAN member countries, this should not dampen the spirit of these regional institutions in managing cyberspace in Southeast Asia. In order to reach an agreement, ASEAN must consider at least two factors: benchmarking and capacity building. ASEAN member countries with low indexes can conduct comparative studies with ASEAN member countries with higher levels of cyber security maturity. Countries with a higher cyber maturity index, on the other hand, can be a key driver for other Southeast Asian member countries to finalize cyber security regulations. Singapore accomplished this by hosting the *Singapore Cybersecurity Week*, to which all ASEAN member countries were invited [56]. The main goal is for Singapore to be the economic center of Southeast Asia and to have a leading technology system in comparison to other countries. Singapore intends to be a forerunner in creating a safe cyber environment, both domestically and regionally, through this event [56]. Because its technological infrastructure and human development are more established, Singapore's position is suitable as a benchmark for driving cybersecurity governance in Southeast Asia [57].

However, using one or two countries as benchmarks is insufficient. The reached consensus will not work unless ASEAN commits to closing the technological gap between its member countries. The main goal is to prevent attackers from exploiting the weakest chain. As a result, ASEAN must optimize its capacity-building program to ensure that the cyber maturity index among its member countries is not too disparate [58]. By adhering to the principle of non-intervention, capacity building can increase trust among member countries [26]. This capacity building is in line with ASEAN's consensus. ASEAN, for example, could use Singapore or Malaysia as model countries for developing cyber security regulations. Furthermore, Singapore or Malaysia can serve as a driving

force in the development of these regulations. Developing the cybersecurity capacity of ASEAN member countries is critical, despite the fact that the ASEAN consensus is flexible. Regulations and cyber security governance can be implemented if ASEAN uses the "ASEAN X+2" formula and two countries agree. Meanwhile, other member countries will only implement the decision if they have the necessary technological infrastructure and human resources in place. There is a flaw in this consensus formula: cyber security regulations will only be effective for countries that agree to them. As a result, ASEAN must encourage capacity-building programs to close the technological gap [58]. As a result, ASEAN can benefit from all types of policy formulation formulas without overriding or overemphasizing one of its member countries. The fundamental principle of flexible consensus is solidarity, and no country appears to be falling behind in implementing policies that were initiated collaboratively [35].

On the one hand, ASEAN's sub-organizations can be used to reach a cybersecurity consensus. The ASEAN Ministerial Meeting is one of them (AMM). ASEAN can maximize preventive diplomacy and build trust through the AMM [59]. The primary goal of reaching an agreement is to avoid open conflict. By maximizing AMM, particularly the ministry in charge of information technology, ASEAN can encourage ministers to develop prevention plans in the event of cyber conflicts, as well as how to build trust among member countries in order to mitigate cyber threats themselves. At the very least, AMM is responsible for reducing knowledge gaps between countries, organizational norms gaps, policy gaps, organizational, operational gaps related to implementation and resources, and gaps related to regulatory commitment compliance [60].

First and foremost, AMM must address cybersecurity regulations governing data and scientific research. The data or research should be used as a guideline when developing cyber security governance based on scientific principles [48]. Cybersecurity governance is designed to manage an unbounded virtual space. The Treaty of Amity and Cooperation governs ASEAN's non-intervention policy [26]. As a result, cyber security governance must be tailored to norms that do not infringe on each country's sovereignty. The third point to make is that each ASEAN member country has a unique cybersecurity policy. One of the AMM's primary responsibilities is to synergize these regulations in accordance with each country's national interests.

One thing to keep in mind when it comes to AMM coordination is that cyberspace is a world without borders. As a result, ASEAN requires governance that can accommodate all interests. At the very least, ASEAN has regulations that take cybersecurity into account [61]. AMM can coordinate cyber security prevention efforts with its member countries and countries outside the region in order to reduce organizational resource gaps. One of them is the creation of the ASEAN Cybercrime Desk as part of the ASEAN-Interpol cooperation scheme [62]. Because not all information technology ministries have adequate infrastructure and human resources, this scheme is quite adequate. Finally, the AMM-adopted consensus oversight mechanism should be overseen by a specific agency. The operational pattern of ASEAN is confederation rather than federal. The institution will assign a specific agency to oversee the implementation of organizational agreements in each of its member countries in a confederation organizational pattern [36]. In the context of ASEAN, this organization can maximize the ASEAN secretariat's function as a supervisory executor. As a result, ASEAN can

reach a common position at the ministerial level before discussing it in a regional security policy forum.

Cyber security issues can be elevated in security politics community at the regional forum level. The ASEAN consensus agreement must emphasize the principle of non-intervention, the use of technology for peaceful purposes, cyber security regulations that can be tailored to each country's needs, the development of technological capabilities, and mechanisms for peaceful cooperation in cyber conflict issues [63][26][64][49][58]. Similarly, at the ASEAN Regional Forum (ARF), ASEAN must continue to pay attention to the non-intervention norms that have become the organizational reference. In order to achieve consensus at the ARF level, ASEAN must follow the agenda control principle. Each member country is free to consider, study, and adjust the ARF meeting agenda to suit their own national interests [65]. As a result, reaching a consensus on cyber security regulations at both the ministry and ARF levels can be tailored to the needs of each country. As a result, regardless of the ASEAN formula used, the consensus reached must be able to accommodate all interests.

Furthermore, the ASEAN consensus contains consultative content [28]. ASEAN must optimize this consultation function for capacity building in the context of ARF consensus formulation [26]. When ASEAN develops a consultation scheme to increase cyber security capabilities and capacities, cyber security regulations will be able to function properly. According to the ITU data, the technological gap between ASEAN member countries is very wide. A mature country in terms of technological infrastructure and human resources can adapt to the regulations that must be met. However, what about countries with less developed technological infrastructure, such as Laos, Myanmar, or Cambodia? ASEAN can bridge the technological gap through this consultation function. One of the strategies is for ASEAN to encourage mature technological countries to serve as mentors to other countries. Singapore, for example, can serve as a pioneer and mentor in bridging the technology gap because the country is well-established in cybersecurity [56][57]. Concerning this consultation, ASEAN should avoid bringing up sensitive issues that could jeopardize organizational solidarity. At the very least, ASEAN can concentrate on strengthening its member countries' technological capabilities in order to integrate the Southeast Asian region's economic interests [35][12]. Thus, the consultations emphasized the importance of improving human resources in technology, cooperating in infrastructure development, and exchanging information in cyber security [66][67][58]. Finally, the form of consensus on cyber security regulations that ASEAN seeks is one that is flexible and capable of strengthening the solidarity of each member country.

5 Conclusions

The most difficult challenge ASEAN faces is reaching a cybersecurity consensus. Nonetheless, by optimizing its sub-organizations, ASEAN can reach a cybersecurity consensus. The cybersecurity agreement reached must adhere to the organizational norms outlined in the TAC. Aside from that, the positions of chairman and secretariat are critical in pushing the cyber security agenda as the primary issue that ASEAN needs to discuss. Concerning the achievement of consensus, ASEAN

can use the formula agreed upon in the ASEAN Charter. The outcome of the consensus must include some degree of flexibility. Southeast Asia suffers from a significant technological gap. Thus, technologically mature countries can initiate and implement cybersecurity governance. The main principle of ASEAN, however, is solidarity. As a result, ASEAN must establish a mechanism for capacity building and cybersecurity cooperation among its member countries in order to implement the agreed-upon consensus as a whole.

References

[1] Nye Jr, J. The Future of Power. Perseus Group. New York; 2011.

[2] Dunn-Cavelty, M., & Egloff, F. J. The Politics of Cybersecurity: Balancing Different Roles of The State. St. Antony's International Review. 2019;15(1):37–57.

[3] Düll, A., Schoch, A., & Straub, M. Cybersecurity in the European Union. Central and Eastern European EDem and EGov Days. 2018;331:313–323. https://doi.org/10.24989/ocg.v331.26

[4] Nengsi, F. The Women's Participation in Digital Economy in ASEAN. Journal of Islamic World and Politics. 2019;3(1):516–536. https://doi.org/10.18196/jiwp.3128

[5]Yuniar, R. W. Uber Rival Grab Rolls Out Indonesia Investment Plan; 2017. https://www.wsj.com/articles/uber-rival-grabtaxi-rolls-out-indonesia-investment-plan-1486012764

[6]ASEAN-UP. Overview of E-Commerce in Southeast Asia [Market Analysis]; 2019b. https://aseanup.com/overview-of-e-commerce-in-southeast-asia/

[7]ASEAN Post. Strengthening Cybersecurity in ASEAN; 2019. https://theaseanpost.com/article/strengthening-cybersecurity-asean

[8]E-Trade for All. ASEAN: E-Commerce Set to Dominate the Region in 2019; 2018. https://etradeforall.org/asean-e-commerce-set-to-dominate-the-region-in-2019/

[9]Chang, L. Cyber Crime and Cybersecurity in ASEAN; 2017. https://www.researchgate.net/publication/318474107

[10]ASEAN-UP. Overview of e-commerce in Southeast Asia [market analysis]; 2019a. https://aseanup.com/overview-of-e-commerce-in-southeast-asia/

[11] Feng, J. On The Cusp; 2018. https://www.imf.org/external/pubs/ft/fandd/2018/09/pdf/aseandigital-economy-infographic-feng.pdf

[12] Ramadhan, I. Peran Institusi Internasional Dalam. Populis. 2017;2(4):495–508.

[13] Harper, N., & Tempra, N. Drug trafficking in the Golden Triangle: The Myanmar problem and ASEAN effectiveness. Jurnal Sentris. 2020;1(1):116–124. https://doi.org/10.26593/sentris.v1i1.4171.116-124

[14] Sudirman, A. Membangun Keamanan Regional Di Asean Dalam Menanggulangi Ancaman Terorisme. Jurnal Wacana Politik. 2017;2(1):22–32. https://doi.org/10.24198/jwp.v2i1.11276

[15] Subono, N. I., & Kosandi, M. The Regionalism Paradox in the Fight against Human Trafficking : Indonesia and the Limits of Regional Cooperation in ASEAN. Journal of Leadership, Accountability and Ethics. 2019;16(2):89–98.

[16] ASEAN. ASEAN LEADERS' STATEMENT ON CYBERSECURITY *COOPERATION*; 2021. http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf

[17] Dunn Cavelty, M., & Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy. 2020a;41(1):5–32. https://doi.org/10.1080/13523260.2019.1678855

[18] Papp, D. S., & Albert, D. Information Age: Anthology (eds). USA: CCRP; 2001.

[19] Robinson, M., Jones, K., & Janicke, H. Cyber warfare: Issues and challenges. Computers and Security. 2015;49:70–94. https://doi.org/10.1016/j.cose.2014.11.007

[20] Gultom, R. A. G., Supriyadi, A. A., & Kustana, T. A Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security

Framework. International Journal of Management & Information Technology. 2018;13:3288–3300. https://doi.org/10.24297/ijmit.v13i0.7624
[21] Ramadhan, I. Cyber-Terrorism in the Context of Proselytizing, Coordination, Security, and Mobility. Islamic World and Politics. 2020b;4(2):185–203. https://doi.org/10.18196/jiwp.4252
[22] Borelli, M. ASEAN Counter - terrorism Weaknesses. International Centre for Political Violence and Terrorism Research. 2017;9(9):14–20.
[23] IBM Security. Cost of Data Breach Record; 2019.
[24] Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity. 2018;4(1):1–15. https://doi.org/10.1093/cybsec/tyy006
[25] Bada, M., & Nurse, J. R. C. The social and psychological impact of cyber-attacks. In V. Benson & J. Mcalaney (Eds.), Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press; 2020. 73–92 p. https://doi.org/10.1016/b978-0-12-816203-3.00004-6
[26] Manopo, B. Y. W., & Sari, D. A. A. Asean Regional Forum: Realizing Regional Cyber Security in Asean Region. Belli Ac Pacis. 2015;1(1):44–51. https://jurnal.uns.ac.id/belli/article/view/27366
[27] Rattanasevee, P. Towards institutionalised regionalism: the role of institutions and prospects for institutionalisation in ASEAN. Journal of the Korean Physical Society. 2014;3(1):1–10. https://doi.org/10.1186/2193-1801-3-556
[28] Caballero-Anthony, M. Understanding ASEAN's centrality: Bases and prospects in an evolving regional architecture. Pacific Review. 2014;27(4):563–584. https://doi.org/10.1080/09512748.2014.924227
[29] Chiou, Y. hung. Unraveling the Logic of ASEAN's Decision-Making: Theoretical Analysis and Case Examination. Asian Politics and Policy. 2010;2(3):371–393. https://doi.org/10.1111/j.1943-0787.2010.01199.x
[30] Gerard, K. ASEAN as a "Rules-based Community": Business as Usual. Asian Studies Review. 2018;42(2):210–228. https://doi.org/10.1080/10357823.2018.1444016
[31] Keating, M. Europe as a multilevel federation. Journal of European Public Policy. 2017;24(4):615–632. https://doi.org/10.1080/13501763.2016.1273374
[32] Jong, K. H., & Ping, L. poh. The Changing Role of Dialogue in the International Relations of Southeast Asia. Asian Survey. 2012;51(5):953–970. http://www.jstor.org/stable/10.1525/as.2011.51.5.953
[33] Yukawa, T. The ASEAN Way as a symbol: an analysis of discourses on the ASEAN Norms. Pacific Review. 2018:31(3):298–314. https://doi.org/10.1080/09512748.2017.1371211
[34] Allison-Reumann, L. The Norm-Diffusion Capacity of ASEAN: Evidence and Challenges. Pacific Focus. 2017;32(1):5–29. https://doi.org/10.1111/pafo.12089
[35] Feraru, A. S. ASEAN Decision-Making Process: Before and after the ASEAN Charter. Asian Development Policy Review. 2016; 4(1):26–41. https://doi.org/10.18488/journal.107/2016.4.1/107.1.26.41
[36] Archer, C. International Organizations (3rd ed.). London: Routledge; 2001.
[37] Suzuki, S. Can ASEAN offer a useful model? Chairmanship in decision-making by consensus. Pacific Review. 2021;34(5):697–723. https://doi.org/10.1080/09512748.2020.1727553
[38] Hammarberg, K., Kirkman, M., & De Lacey, S. Qualitative research methods: When to use them and how to judge them. Human Reproduction. 2016;31(3):498–501. https://doi.org/10.1093/humrep/dev334
[39] Roselle, L., & Spray, S. Research and Writing in International Relations. Boston: Pearson Longman; 2012.

[40] Snyder, H. Literature review as a research methodology: An overview and guidelines. Journal of Business Research. 2019;104(August):333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
[41] Creswell, J. Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th Eds). London: SAGE; 2014.
[42] Noor, E. Strategic Governance of Cyber Security : Implications for East Asia. In R. Sukma & Y. Soeya (Eds.), Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance (Tokyo: Japan Center for International Exchange, 2015), JCIE; 2015. 150–163 p.
[43] Singh, S. INDIA-ASEAN COOPERATION ON CYBER CRIME. International Journal of Advanced Research in Computer Science. 2016;7(6):273–275.
[44] Tran Dai, C., & Gomez, M. A. Challenges and opportunities for cyber norms in ASEAN. Journal of Cyber Policy. 2018;3(2):217–235. https://doi.org/10.1080/23738871.2018.1487987
[45] Heinl, C. H. Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. Asia Policy. 2014;18(1):131–159. https://doi.org/10.1353/asp.2014.0026
[46] Maness, R. C., & Valeriano, B. The Impact of Cyber Conflict on International Interactions. Armed Forces and Society. 2016;42(2):301–323. https://doi.org/10.1177/0095327X15572997
[47] Noor, E. Positioning ASEAN in Cyberspace. Asia Policy. 2020;15(2):107–114. http://asiapolicy.nbr.org
[48] Mizan, N. S. M., Ma'arif, M. Y., Satar, N. S. M., & Shahar, S. M. CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. 8(October), International Journal of Advanced Trends in Computer Science and Engineering. 2019:113–119. https://doi.org/https://doi.org/10.30534/ijatcse/2019/1781.42019
[49] Van Der Meer, S. Enhancing International Cyber Security: A Key Role for Diplomacy. Security and Human Rights. 2015;26(2–4):193–205. https://doi.org/10.1163/18750230-02602004
[50] Katsumata, H. ASEAN's Diplomatic Tasks During the Pandemic. East Asia; May 2021. Available from: https://doi.org/10.1007/s12140-021-09366-x
[51] Heilmann, D. After Indonesia's ratification: The ASEAN agreement on transboundary haze pollution and its effectiveness as a regional environmental governance tool. Journal of Current Southeast Asian Affairs. 2015;34(3):95–121. https://doi.org/10.1177/186810341503400304
[52] Sari, S. Peran Indonesia Dalam Implementasi Asean Political Security Community. Jurnal Dinamika Global. 2019;4(01):24–65. https://doi.org/10.36859/jdg.v4i01.100
[53] Krisman, K. A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. JAS (Journal of ASEAN Studies). 2013;1(1):41. https://doi.org/10.21512/jas.v1i1.60
[54] Bangun, B. H. Pengaruh dari Kedaulatan Negara Terhadap Pelaksanaan Mekanisme Kerjasama ASEAN dalam Pemberantasan Terorisme. Pandecta: Research Law Journal. 2019;14(1):1–12. https://doi.org/10.15294/pandecta.v14i1.17777
[55] ITU. Global Cybersecurity Index 2018; 2018. Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[56] Anshori, M. F., & Ramadhan, R. A. Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week. Padjadjaran Journal of International Relations. 2019;1(1):39. https://doi.org/10.24198/padjir.v1i1.21591
[57] Raska, M., & Ang, B. Cybersecurity in Southeast Asia; 2018.
[58] Watanabe, S. Strategic Analysis of Capacity Building for the Cyber Security of the United States in Asia. Jurnal Asia Pacific Studies. 2020;4(2):100–111.. https://doi.org/10.33541/japs.v4i2.2800

[59] Agastia, I. G. B. D. Maritime security cooperation within the asean institutional framework: A gradual shift towards practical cooperation. Journal of ASEAN Studies. 2021;9(1):25–48. https://doi.org/10.21512/JAS.V9I1.6919
[60] Moon, C. I., & You, C. K. The ASEAN Regional Forum's Experts and Eminent Persons Group: Achievements, Limitations, Prospects. Global Governance. 2017;23(3):363–381. https://doi.org/10.1163/19426720-02303003
[61] Guarda, N. D. Governing the ungovernable: International relations, transnational cybercrime law, and the post-westphalian regulatory state. Transnational Legal Theory. 2015;6(1):211–249. https://doi.org/10.1080/20414005.2015.1042226
[62] INTERPOL. ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from The ASEAN Cybercrime Operations Desk; 2021. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia
[63] Dunn Cavelty, M., & Wenger, A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy. 2020b;41(1):5–32. https://doi.org/10.1080/13523260.2019.1678855
[64] Ramadhan, I. Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). Journal of Social and Political Sciences. 2020a;3(4). https://doi.org/10.31014/aior.1991.03.04.230
[65] Saputro, E. N. Beyond Consensus: Democratic Element in ASEAN Plus Three Economic Cooperation. Jurnal Global & Strategis. 2020;14(1):45. https://doi.org/10.20473/jgs.14.1.2020.45-62
[66] Isnarti, R. A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. Andalas Journal of International Studies (AJIS). 2016;5(2):151. https://doi.org/10.25077/ajis.5.2.151-165.2016
[67] Ramadhan, I. Strategi Keamanan Cyber Security di Kawasan Asia Tenggara: Self-help atau Multilateralism?. Jurnal Asia Pacific Studies. 2019;3(1). https://doi.org/dx.doi.org/10.33541/japs.v3i1.1081