Title	ASEAN's regional effort on cybersecurity and its effectiveness
Sub Title	サイバーセキュリティに関するASEANの地域的取り組みとその有効性
Author	Sari, Monica Nila
Publisher	慶應SFC学会
Publication year	2023
Jtitle	Keio SFC journal Vol.23, No.1 (2023.) ,p.26- 42
JaLC DOI	10.14991/003.00230001-0026
Abstract	The speed of digitalization has accelerated further since the COVID-19 pandemic, making it one of the most significant growth engines for many developing nations. We are already seeing how digitalization is reshaping the Southeast Asia region. ASEAN now has an Internet penetration of over 77.6% which is above the global penetration rate (59.5%)1). As ASEAN experienced accelerated digitalisation which has helped to grow the region's digital economy, it has, on the other hand, also led to new challenges of cybercrime. In the past year, cybersecurity has been a priority on the ASEAN agenda. However, ASEAN is characterized by a high degree of heterogeneity in terms of economic development, which resulted in a notable gap in terms of cyber maturity and ASEAN countries' commitment and political will to engage with cybercrime policy. In this regard, this paper will analyse how effective the ASEAN's regional approach is in dealing with cybersecurity issues in the region.
Notes	自由論題 投稿論文：研究論文
Genre	Journal Article
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AA11671240-00230001-0026

［投稿論文：研究論文］

ASEAN's Regional Effort on Cybersecurity and Its Effectiveness
サイバーセキュリティに関するASEANの地域的取り組みとその有効性

Monica Nila Sari
Doctoral Program, Graduate School of Media and Governance, Keio University
サリ，モニカ ニラ
慶應義塾大学大学院政策・メディア研究科後期博士課程
Correspondence to: monica.nilasari@gmail.com

Abstract: The speed of digitalization has accelerated further since the COVID-19 pandemic, making it one of the most significant growth engines for many developing nations. We are already seeing how digitalization is reshaping the Southeast Asia region. ASEAN now has an Internet penetration of over 77.6% which is above the global penetration rate (59.5%)[1). As ASEAN experienced accelerated digitalisation which has helped to grow the region's digital economy, it has, on the other hand, also led to new challenges of cybercrime. In the past year, cybersecurity has been a priority on the ASEAN agenda. However, ASEAN is characterized by a high degree of heterogeneity in terms of economic development, which resulted in a notable gap in terms of cyber maturity and ASEAN countries' commitment and political will to engage with cybercrime policy. In this regard, this paper will analyse how effective the ASEAN's regional approach is in dealing with cybersecurity issues in the region.

COVID-19パンデミックが発生してからデジタル化はさらに加速し、多くの発展途上国にとって最も重要な成長エンジンの一つとなっている。私たちはデジタル化が東南アジア地域をどのように再形成しているのかをすでに目にしている。ASEANでのインターネット普及率は現在77.6％を超えており、全世界での普及率の約59.5％を上回る計算になっている。ASEANが経験したデジタル化の加速は地域のデジタル経済成長にも貢献しているが、サイバー犯罪という新たな課題にもつながった。この一年間で、サイバーセキュリティはASEANの優先順位の高い議題になった。しかし、ASEANは経済成長の面での格差に特徴があり、その結果、サイバーの成熟度やASEAN諸国のサイバー犯罪に関する取組政策、コミットメント等にギャップが生じている。そのため、本稿では、地域のサイバーセキュリティ問題に対処する上で、ASEANの地域的アプローチがどれほど効果的であるかを分析する。

Keywords: cybersecurity, ASEAN, policy, regional institution, data protection
サイバーセキュリティ、ASEAN、政策、地域機関、データ保護

1 Introduction

The Association of Southeast Asian Nations (ASEAN), is one of the fastest growing Internet markets in the world with 125,000 new users coming online every day. ASEAN has more than 440 million Internet users, and more importantly, 350 million, or about 80% of them, are digital customers[2]. We are already seeing how digitalization is reshaping the Southeast Asia region. ASEAN experienced a positive trend of GDP of more than USD 3.11 trillion in 2020, making ASEAN, collectively, the fifth largest economy in the world[3]. Moreover, ASEAN countries' Internet penetration is now over 77.6% which is above the global penetration rate (59.5%)[4]. With the ASEAN region seeing exponential growth in the digital technology sector, particularly financial technology and e-commerce, there is an increasing demand for Internet and broadband services.

However, this increasing reliance on the Internet has created a large number of security threats that can cause immense damage. As ASEAN experienced accelerated digitalisation, which has helped to grow the region's digital economy, it has also led to new challenges. ASEAN Cyberthreat Assessment 2021, produced by the INTERPOL ASEAN Cybercrime Operations Desk, suggests that ASEAN countries have become a prime target for cyberattacks considering their position among the fastest-growing digital economies in the world. According to IBM Security's 2020 Cost of a Data Breach Report, the average cost of a data breach in ASEAN in 2020 was estimated to be US$ 2.7 million. International Criminal Police Organization (INTERPOL) ASEAN Cybercrime Operations Desk reported that data breach is one of the highest cybercrimes in ASEAN countries in 2021.

As a regional organisation, ASEAN has an "ASEAN way" approach in the organisation's decision making process which is upholding the consensus principle based on ASEAN Charter. Some scholars[5] argued that this ASEAN way could limit the group of ten countries in accomplishing substantial achievement in finding common ground and mutually acceptable outcome. ASEAN respects the principle of territorial integrity, sovereignty, non-interference and national identities of ASEAN Member States[6]. The question arises whether this ASEAN way and principle of ASEAN regionalism are effective in dealing with cybersecurity in the region. Moreover, ASEAN is characterized by a high degree of heterogeneity in terms of economic development, which resulted in a notable gap in terms of cyber maturity and ASEAN countries' commitment and political will to engage with cybersecurity policy. In this regard, this paper will analyse how effective the ASEAN's regional approach is in dealing with cybersecurity issues in the region, taking into account the ASEAN way in forming consensus or making decisions and its non-interference principle. The conclusion of this paper will provide policy recommendation for strengthening ASEAN's cybersecurity framework.

2 Methodology

Data analyzed in this paper is drawn from two source types, namely: (i) data collected through the review of original documents of ASEAN's instruments, including meeting summaries relating to cybersecurity, and (ii) an interview[7] carried out with ASEAN Secretariat officials in Jakarta, Indonesia, through zoom meeting to receive updated information on the existing cybersecurity development in ASEAN.

3 ASEAN's efforts on cybersecurity

ASEAN leaders shared the vision of a peaceful, secure and resilient regional cyberspace that serves as an enabler of economic progress, enhanced regional connectivity and betterment of living standards, as stated in the ASEAN Leaders' Statement on Cybersecurity Cooperation[8].

3.1 ASEAN mechanism

Relevant ASEAN Sectoral Bodies and ASEAN-led mechanisms[9] have been working on cyber security issues, namely the ASEAN Digital Ministers' Meeting (ADGMIN) and the ASEAN Digital Senior Officials' Meeting (ADGSOM) as its subsidiary body, the ASEAN Regional Forum (ARF), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the East Asia Summit (EAS), and the ASEAN Defence Ministers' Meeting (ADMM)-Plus.

On the area of cybercrime, the ASEAN Ministerial Meeting on Transnational Crime (AMMTC) has the mandate to discuss the subject matter. Under this mechanism, ASEAN adopted ASEAN Declaration to Prevent and Combat Cybercrime in 2017. Recognising the need to address the rapid growth of cyber-security threats, the ARF established the ARF Inter-Sessional Meeting on Security of and in the Use of ICTs in 2017. It serves as a specific platform for ARF Participants to promote mutual understanding as well as to discuss and coordinate ARF's efforts on ICTs security, to implement the ARF Work Plan on Security of and in the Use of ICTs as well as to enhance trust and confidence through capacity building whilst ensuring that in the conduct of its activities. To guide the work of the ISM on ICTs Security, the ARF Work Plan on Security of and in the Use of ICTs was adopted in 2015. It serves to promote a peaceful, secure, open and cooperative ICT environment and to develop transparency and confidence-building measures to prevent conflict in cyberspace between states in the ARF region through capacity building. ARF recently adopted "ARF Terminology in the Field of Security of and in the use of ICTs" in September 2020 to encourage discussion among ARF participants on their domestic views and definitions of key ICTs related terminologies utilised in their respective countries.

Initiatives on cybersecurity under the ASEAN Economic Community pillar are under the mechanism ASEAN Digital Ministers' Meeting (ADGMIN). This mechanism was named ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN) before, and its name changed in 2019 to reflect the widening scope of work of the ICT ministries across ASEAN[10]. On cyber defence, in 2021 ADMM adopted concept papers on ASEAN Cyber Defence Network and the ADMM Cybersecurity and Information Centre of Excellence, as important milestones in promoting practical cybersecurity cooperation in ASEAN. These efforts serve as confidence building measures within the region, and ASEAN would like to encourage other regions to adopt similar measures, towards building trust and confidence at the global level. In order to reinforce the Leaders' intention to strengthen cooperation in cybersecurity, this issue has been increasingly featured under the ambit of the East Asia Summit (EAS). This mechanism has provided workshops regional cyber capacity building as well as Leaders' commitment to promote open, secure, stable, accessible and peaceful cyberspace.

ASEAN has various mechanisms dealing with cybersecurity with the aim to facilitate the deliberations of cybersecurity cooperation under the three pillars of ASEAN. In order to strengthen cross-sectoral coordination as cybersecurity is a cross-cutting issue, in 2020 ASEAN established the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) to tackle the coordination challenges and to promote cross-sectoral and cross-pillar cooperation and strengthen cybersecurity in the region. Under this new mechanism, ASEAN is now developing a Regional Action Plan on the Implementation of the Norms of Responsible State Behaviour in Cyberspace to assist with the prioritization and implementation of the 11 voluntary, non-binding norms of responsible State behaviour in the use of ICTs.

These ASEAN Sectoral Bodies and ASEAN-led mechanisms are not only aiming to produce Chairman's Statement or to adopt agreed documents. Its regular meetings among regional leaders and officials provide a diplomatic ecosystem where many informal and side-line engagements take place. ASEAN meetings engender a sense of familiarity and a give-and-take approach which in turn facilitate consensus-building on contentious issues. These mechanisms are also a forum for ASEAN countries and partners to discuss relevant issues related to cybersecurity.

3.2 Regional framework

Over the past few years, the ASEAN region has shown the way forward on how to build a regional cybersecurity cooperation framework. First, ASEAN has updated its cybersecurity cooperation strategy as reflected in the ASEAN Cybersecurity Cooperation Strategy for 2021– 2025, in response to the newer cyber developments to strengthen collective efforts in securing cyberspace for the region and promoting digital's economy and community to grow. The updated Strategy contains five dimensions of work: (1) advancing cyber readiness cooperation, (2) strengthening regional cyber policy coordination, (3) enhancing trust in cyberspace, (4) regional capacity building, and (5) international cooperation.

Second, ASEAN is the first and only regional organisation to have subscribed, in principle, to the United Nation's 11 voluntary, non-binding norms of responsible state behaviour in cyberspace[11)]. This is important to underpin ASEAN's active contribution to maintaining peace and security in the cyberspace. In this regard, ASEAN is developing ASEAN Regional Plan on the Implementation of UNGGE Norms of Responsible State Behaviour in Cyberspace, which are categorized into several focus areas including international cooperation, development of policy, awareness-rising, strengthening national cybersecurity and cybercrime laws, cybercrime cooperation, incident response cooperation and creation of a trustworthy ecosystem[12)]. This initiative has increased the understanding and awareness of ASEAN countries on key cybersecurity issues, and will act as useful guides in ASEAN's work on norms implementation.

Third, ASEAN is establishing ASEAN Regional Computer Emergency Response Team (CERT) and the ASEAN CERT Information Exchange Mechanism. ASEAN recognized the urgency to secure the growing digital economy in ASEAN in the face of increasingly sophisticated transboundary cyber-attacks, and therefore it would be valuable to establish ASEAN CERT to facilitate the timely exchange of threat and attack-related information among AMS (ASEAN Member States) National CERTs and foster CERT-related capacity building and coordination[13)].

4 Challenges in ASEAN

As one of the most successful regional organisation in the world, ASEAN has an "ASEAN way" approach in the organisation's decision making process, which is upholding the consensus principle based on ASEAN Charter. Some scholars argued that this ASEAN way could limit the group of ten in accomplishing substantial achievement in finding common ground and mutually acceptable outcome. Moreover, ASEAN respects the principle of territorial integrity, sovereignty, non-interference and national identities of ASEAN Member States[14]. The question arises whether this ASEAN way and principle of ASEAN regionalism are effective in dealing with cybersecurity in the region.

Furthermore, according to ITU's Global Cybersecurity Index (GCI) 2020, the gaps among ASEAN countries are ranging from number 4 to 131 among 194 countries in total (Table 1).

Table 1: Cybersecurity Maturity of ASEAN Countries

Country	Rank	Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
Singapore	4	98.52	20.00	19.54	18.98	20.00	20.00
Malaysia	5	98.06	20.00	19.08	18.98	20.00	20.00
Indonesia	24	94.88	18.48	19.08	17.84	19.48	20.00
Vietnam	25	94.55	20.00	16.31	18.98	19.26	20.00
Thailand	44	86.50	19.11	15.57	17.64	16.84	17.34
Philippines	61	77.00	20.00	13.00	11.85	12.74	19.41
Brunei Darussalam	85	56.07	14.06	14.19	10.84	12.85	4.12
Myanmar	99	36.41	9.39	3.64	4.71	8.92	9.75
Lao PDR	131	20.34	11.77	3.27	0.00	1.23	4.07
Cambodia	132	19.12	7.38	2.50	1.69	3.29	4.26

Source: ITU's Global Cybersecurity Index 2020

Moreover, the ASEAN countries have not spent enough budget for cybersecurity to secure a sustained commitment to cybersecurity and investment gap. A.T. Kearney report argued that to secure sustained commitment to cybersecurity and address the investment gap, ASEAN countries need to spend between 0.35 and 0.61 percent of their GDP – or US$ 171 billion collectively – on cybersecurity in the period spanning 2017-2025[15]. Based on the *State of Cyber Security in ASEAN* in 2020 by Palo Alto Networks, cybersecurity has risen to the top of the leadership agenda for many ASEAN businesses with a vast majority (92%) believing it to be a priority for their business considering growing volume of cyber threats in the region. As surveyed, most ASEAN organizations increased their security investments in 2019. In fact, 46% allocated at least half their total IT budget to cybersecurity. It is also mentioned that more than half (53%) of Singapore companies allocated over half their IT budget to cybersecurity and 84% of Indonesian companies increased their cybersecurity budgets between 2019 and 2020, which was the biggest jump in ASEAN[16]. For government allocated fund, Singapore, as the leading country in ASEAN in terms of cyber maturity, has allocated US$1 billion to build up the Government's cyber and data security capabilities for its 2020-2023 budget[17]. While Malaysia allocated US$6 million in 2021 to strengthen the nation's cybersecurity capacity[18], Indonesia allocated US$89 million in 2021 for ICT development[19]. However, other countries in ASEAN have not yet allocated the same proportion of their budgets for cybersecurity.

5 Data Protection in ASEAN

As of 2020, Malaysia, Singapore and the Philippines, and Thailand already have comprehensive general data protection laws in place. The other six countries do not have data protection laws. Thus, data protection is under general regulation such as Information and Electronic Transaction Law[20]. In October 2022, Indonesia enacted its first Data Protection Law, while other ASEAN countries do not have comprehensive data protection regulation.

ASEAN Digital Senior Officials' Meeting (ADGSOM) has adopted the ASEAN Framework on Digital Data Governance, which aims to align baseline principles and standards for data protection, advance digital innovation and the use of open and big data, and facilitate data flows[21]. In particular, the ASEAN Data Management Framework and the Model Contractual Clauses for Cross Border Data Flows were approved by the 1st ASEAN Digital Ministers' Meeting (ADGMIN) in January 2021[22]. In addition, the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) fully operationalized with the entry into force for the participating AMS that signed the Memorandum of Understanding (MOU) for Sharing of Information during Activities of Digital and Technology Network (DTN) on 1 February 2021, which allows information sharing to combat cybersecurity threats and to develop collaborative mitigation actions for ASEAN Central Banks.

However, data protection and cybersecurity are continuously ongoing processes.

In order to support the development of regional regulatory environment, ASEAN countries need to make sure their domestic data protection laws are updated regularly to remain relevant to the digital economy, such as enacting coherent and simple rules to both enable and protect cross-border data flows, clear obligations and responsibilities defined for data processors and data controllers, transparent data breach notification process, and others. In this regard, ASEAN may eventually create a regional framework on data protection in order to mitigate cybercrime in the region.

6 Analysis of ASEAN's Regional Approach to Cybersecurity

In order to analyse the effectiveness of ASEAN's regional effort on cybersecurity, this paper reviews it by measuring cybersecurity commitments across five pillars based on the toolkit from the ITU[23)].

6.1 Legal Measures

ASEAN is yet to develop a legal framework for cybersecurity. In the case of Indonesia, it demonstrated the urgency to have a legal framework for data protection. The EU has a legal umbrella for combating cybercrime with its Budapest Convention. The Budapest Convention was open for signature since 2001, and in 2018, one of the ASEAN countries, the Philippines, became a party to the Convention. Furthermore, although in the regional scope ASEAN is yet to develop a legal framework for cybercrime, nine ASEAN countries have enacted legislation to regulate cybercrime, and these cybercrime laws are aligned with the requirement of the Budapest Convention. Cambodia is by far the only ASEAN member country that has not passed a proper cybercrime law.

6.2 Technical Measures

ASEAN is focused on upgrading the technical capability of ASEAN's national CERTs. Based on the ASEAN Cybersecurity Cooperation Strategy 2021-2025, each ASEAN country shall assess the technical capability of their national CERT in the areas of cyber threat monitoring, incident handling, vulnerability handling, evidence handling, alerts and advisory drafting towards achieving a defined level of competency.

ASEAN is also establishing ASEAN CERT to facilitate the timely exchange of threat and attack-related information among ASEAN countries' national CERTs and foster CERT related capacity building and coordination.

6.3 Organizational Measures

ASEAN has a cybersecurity strategy as reflected in the document "ASEAN Cybersecurity Cooperation Strategy 2021-2025" which is updated from the 2017-2020 document. In this regard, ASEAN updates its cybersecurity regularly. Furthermore, ASEAN created a new mechanism in 2020 to strengthen cross-sectoral coordination in cybersecurity which is the ASEAN Cybersecurity Coordinating Committee. ASEAN countries have established their national CERT. To date, only Singapore, Malaysia, Indonesia, Brunei Darussalam and Myanmar have national cyber agencies, while other ASEAN counties are being represented by their relevant Ministries. ASEAN has also established ASEAN Critical Information Infrastructure Protection (CIIP) Coordination Framework, built upon the 2020 ASEAN CIIP Framework which is to provide strategic recommendations and coordinated approaches to create more resilient cybersecurity across ASEAN's critical information infrastructure.

6.4 Capacity Development

There are three ASEAN initiatives on regional capacity building, namely: (i) ASEAN-Japan Cybersecurity Capacity Building Centre which was established in 2018 in Bangkok, Thailand, (ii) ASEAN-Singapore Cybersecurity Center of Excellence, which was established in 2019 in Singapore, and (iii) ADMM Cybersecurity and Information Centre of Excellence, which was established in 2021 in Singapore. ASEAN-Japan Cybersecurity Capacity Building Centre conducts programs on technical hands-on computer simulation, digital forensics, and malware analysis, to improve cybersecurity and trusted digital services among ASEAN countries[24]. ASEAN-Singapore Cybersecurity Center of Excellence provides training in areas covering cybersecurity norms and policy and CERT-related technical training, and conducts virtual cyber defence training and exercise[25]. ADMM Cybersecurity and Information Centre of Excellence has three objectives, namely (a) function as a node for confidence-building measures, information-sharing and capacity building among regional militaries; (b) enhance regional cooperation and information sharing, focusing on cyber security, disinformation and misinformation threats including, among others, the dissemination of regular and timely reports; and (c) work with international experts to improve collective resilience against common security threats[26].

ASEAN has also developed a capacity development programme in order to strengthen its regional effort in combating cybercrime namely: ASEAN Cyber Capacity Development Project (2016-2019), ASEAN Cyber Capacity Development Project (2019-2021), Cyber Capabilities and Capacity Development 2021-2023, ASEAN-Japan Cybersecurity Capacity Building Centre, and ASEAN-Singapore Cybersecurity Center of Excellence (ASCCE).

6.5 Cooperation with External Partners

ASEAN has established a framework for ASEAN to widen and deepen its relations with external parties through the conferment of the formal status of Dialogue Partners with Australia, Canada, China, European Union, India, Japan, Republic of Korea, New Zealand, Russia, United States and United Kingdom. With these Dialogue Partners, ASEAN established ASEAN + 1 process to discuss and review the state cooperation between ASEAN and a Dialogue Partner as well as strengthening cooperation in a priority area such as cybersecurity. Through ASEAN+1 process, ASEAN has managed to enhance cybersecurity cooperation as reflected, for example, in the 2018 ASEAN-US Leaders' Statement on Cybersecurity Cooperation, the 2019 ASEAN-EU Statement on Cybersecurity Cooperation, inaugural ASEAN-Australia Cyber Policy Dialogue, ASEAN-Japan Cybersecurity Working Groups and Policy Meetings, the annual workshops on network security with China.

7 Key Recommendations

Based on the analysis above, ASEAN countries need to develop and strengthen the following measures. First, ASEAN needs to update its ASEAN cybersecurity strategy regularly by assessing current risks, prioritize cybersecurity interventions, track progress, and have a clear set of objectives on the protection of critical infrastructure. From the ITU’s GCI, we learn that the lack of adequate organizational measures can contribute to a lack of clear responsibilities and accountability in the national cybersecurity governance, and it can prevent effective intra-government and inter-sector coordination. If all ASEAN countries have established effective national cybersecurity, this will contribute to the development of ASEAN’s cybersecurity strategy. Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam have already developed national strategies related to cybersecurity and can do more to promote regional alignment and assist other ASEAN countries which have yet to craft their own cybersecurity roadmaps or implementation strategies.

Second, ASEAN needs to focus to strengthen its technical measures. While legislation and regulation are important, the actual implementation of cyber threat detection systems and the capability to handle cyber risks are more important. In order to improve its technical capabilities, ASEAN should enhance its capacity building programme.

Third, considering the huge maturity gap among ASEAN countries, the regional capacity building should focus on: (i) developing the technical ability of ASEAN countries’ CERT, (ii) developing policy, strategy, as well as technical aspects of cybersecurity for ASEAN countries’ officials and cybersecurity professionals, and (iii) improving the ability and preparedness of cybersecurity professionals within ASEAN region for cybersecurity and trusted digital services.

Fourth, ASEAN needs to establish a legal umbrella in combating cybercrime similar to Budapest Convention. However, taking into account the “ASEAN way” approach in the organisation's decision-making process which is upholding the consensus principle and the principle of non-interference, creating a legal document would be complex and lengthy. Cybercrime regulations generally define and detect criminal activities in cyberspace after they occur and provide powers to law enforcement to investigate the activities after they have occurred, to bring the offender to justice. Positive outcomes of cybercrime investigation can be contingent upon the successful collection, analysis and attribution of digital evidence. The term 'digital evidence' is used interchangeably with electronic evidence or e-evidence, and refers to information and data that is stored on, received, or transmitted by an electronic device. This includes evidence from digital devices or records obtained from online service providers[27)]. Therefore, the role of law enforcement is highly crucial in combating cybercrime.

Besides that, the national cybercrime strategy needs to be updated regularly by providing purpose, background and the reason why the strategy is necessary, information on cyber-related definitions, cybercrime statistics within the region, existing cybercrime authorities, existing legislation, and self-assessment and analysis summary. There is no universally accepted definition of cybercrime. The most common approach is to define the key terms used in cybercrime investigations. Examining frequently-used definitions will allow us to identify key concepts and use those definitions consistently in a country's cybercrime strategy.

Fifth, to narrow the gap among ASEAN countries, ASEAN can consider focusing on capacity building in the three Centers (AJCCBC, ASCCE, ACICE) in enhancing organizational measures and technical measures. The capacity building programme can be focused towards improving those two dimensions for ASEAN countries with the lowest cybersecurity maturity level by improving the capability of national CERT, training in areas covering cybersecurity norms and policy, and regular assessments of their cybersecurity commitments. At the same time, ASEAN countries with higher cyber maturity could provide their best practices in handling cybersecurity challenges regularly. ASEAN has experiences with its Initiative for ASEAN Integration (IAI) to provide a framework for regional cooperation by which the more developed ASEAN countries could provide assistance for ASEAN countries that most need it, with a view of narrowing the development gap and enhancing ASEAN's competitiveness in the region. This IAI has shown its effectivity through ASEAN's positive GDP trend and becoming the fifth largest economy in the world. With this experience, ASEAN could undertake a similar regional approach to cybersecurity by narrowing the gap among ASEAN countries to improve its cybersecurity framework.

8 Conclusion

Since the ASEAN Leaders' commitment to enhancing cybersecurity cooperation in 2018, ASEAN has made significant progresses. ASEAN has strengthened its cybersecurity effort in: (i) technical dimension by enhancing CERT cooperation, (ii) organization dimension by updating its Strategy and establishing the ASEAN Cybersecurity Coordinating Committee, (iii) capacity building with the three ASEAN initiatives and targeted capacity building training, and (iv) cooperation within ASEAN countries and also with ASEAN external partners in a way that is mutually beneficial and effective.

However, ASEAN as a regional organization has its limitation in finding mutually acceptable outcomes and implementing the agreed regional framework considering ASEAN's principle of non-interference and the ASEAN's way of consensus decision making process. In the case of cybersecurity, this limitation becomes more substantial since ASEAN countries have a high degree of heterogeneity in terms of economic development which resulted in a wide disparity of ASEAN countries' commitment and political will to engage with cybersecurity policy. This is shown in the notable gap among ASEAN countries in terms of cyber maturity. Therefore, ASEAN countries need to narrow their gap in cyber maturity. ASEAN has provided forums through various ASEAN mechanisms to discuss cybersecurity among ASEAN countries and with external partners. This regular interaction between relevant stakeholders subsequently serves to increase knowledge and understanding between relevant actors, and also strengthen the cybersecurity development. If trust-based relationships can be built, then solutions to cybersecurity challenges can be found.

There is no best cybersecurity standard or framework as new technologies and delivery mechanisms develop. Technology will continue to accommodate change and expand in order to address various fields of cybersecurity. However, there are already good examples of existing cybersecurity frameworks. Therefore, ASEAN still needs to learn from the best practices of other regional efforts and continue to strengthen its cooperation with external partners.

Endnotes

1) Statista (2021) "Internet penetration in Southeast Asia as of June 2021", Available at: https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/ (Accessed on September 07, 2022).
2) Digital customers are those who make purchases (of product or service) online. Digital purchases can be made via websites, mobile apps or social media (brand pages or paid advertising).
3) The ASEAN Secretariat (2021) "ASEAN Key Figures 2021", https://asean.org/wp-content/uploads/2021/12/ASEAN-KEY-FIGURES-Chapter-1-4-Rev-28-Dec-2021.pdf (Accessed on August 30, 2022).
4) Statista (2022) "Internet penetration in Southeast Asia as of June 2021", https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/ (Accessed on August 30, 2022).
5) Jones, D.M., and Jenne, N. (2016) "Weak states' regionalism: ASEAN and the limits of security cooperation in Asia-Pacific". *International Relations of the Asia Pacific*. 16(2), pp. 209-240.
6) "The ASEAN Charter", https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf (Accessed on September 5, 2022).
7) An interview was conducted on 23 May 2022 with Senior Officer for Cybersecurity and Digital Skills from the ASEAN Secretariat.
8) "ASEAN Leaders' Statement on Cybersecurity Cooperation", (2018) available at: https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf (Accessed on September 5, 2022).
9) ASEAN's constructive engagement with its external partners, through ASEAN-led mechanisms such as the ASEAN Plus-One, ASEAN Plus Three (APT), East Asia Summit (EAS), ASEAN Regional Forum (ARF) and ASEAN Defence Ministers' Meeting Plus (ADMM-Plus), in building mutual trust and confidence as well as reinforcing an open, transparent, inclusive and rules-based regional architecture with ASEAN at the centre.
10) ASEAN Secretariat, www.asean.org (Accessed on September 20, 2022).
11) "ASEAN Cybersecurity Cooperation Strategy 2021-2025", https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf (Accessed on May 10, 2022).

12) ibid.
13) ibid.
14) "The ASEAN Charter", https://asean.org/wp-content/uploads/images/archive/publications/ASEAN-Charter.pdf (Accessed on September 20, 2022).
15) Cisco and A.T. Kearney. (2018) "Cybersecurity in ASEAN: An Urgent Call to Action", p. 3, https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN—An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34 (Accessed on September 20, 2022).
16) Palo Alto Networks. (2020) "The State of Cybersecurity in ASEAN", https://www.paloaltonetworks.sg/apps/pan/public/downloadResource?pagePath=/content/pan/en_SG/resources/whitepapers/the-state-of-cybersecurity-in-asean-2020 (Accessed on November 2, 2022).
17) Lim Min Zhang. (2020) "Singapore Budget 2020: $1b over next 3 years to shore up cyber and data security capabilities", *The Straits Times*. February 18, 2020, https://www.straitstimes.com/singapore/singapore-budget-2020-1b-over-next-3-years-to-shore-up-cyber-and-data-security (Accessed on September 7, 2022).
18) Angelin Yeoh. (2020) "Budget 2021: RM27mil allocation for CyberSecurity Malaysia hailed by industry players", *The Star*. February 6, 2020, https://www.thestar.com.my/tech/tech-news/2020/11/06/budget-2021-rm27mil-allocation-for-cybersecurity-malaysia-hailed-by-industry-players (Accessed on September 7, 2022).
19) Indonesia Ministry of Finance, www.kemenkeu.go.id (Accessed on September 5, 2022).
20) TRPC (2020) "TRPC Data Protection Index 2020", https:/trpc.biz/old_archive/wp-contents/uploads/TRPC_DPI2020.pdf. (Accessed on September 20, 2022).
21) ASEAN (2018) "Framework on Digital Data Governance", https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-DataGovernance_Endorsedv1.pdf (Accessed on November 2, 2022).
22) ASEAN (2021) "ASEAN Data Management Framework", https://asean.org/storage/2-ASEAN-Data-Management-Framework_Final.pdf (Accessed on September 20, 2022).
23) ITU (2020) "Global Cybersecurity Index 2020", https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (Accessed on November 2, 2022).
24) ASEAN-Japan Cybersecurity Capacity Building Center, https://www.ajccbc.org (Accessed on September 7, 2022).
25) Cyber Security Agency Singapore website, https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence (Accessed on September 20, 2022).
26) "ASEAN Cybersecurity Cooperation Strategy 2021-2025", https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf (Accessed on May 10, 2022).
27) INTERPOL (2021) "National Cybercrime Strategy Guidebook", (Accessed on November 2, 2022).

References

ASEAN (2018) "Framework on Digital Data Governance", https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-DataGovernance_Endorsedv1.pdf (Accessed on November 2, 2022).

ASEAN (2021) "ASEAN Data Management Framework", https://asean.org/storage/2-ASEAN-Data-Management-Framework_Final.pdf (Accessed on September 20, 2022).

"ASEAN Cybersecurity Cooperation Strategy 2021-2025" (Accessed on November 2, 2022).

ASEAN-Japan Cybersecurity Capacity Building Center, https://www.ajccbc.org (Accessed on September 7, 2022).

ASEAN Secretariat, www.asean.org (Accessed on September 5, 2022).

ASEAN Secretariat (2021) "ASEAN Key Figures 2021", https://asean.org/wp-content/uploads/2021/12/ASEAN-KEY-FIGURES-Chapter-1-4-Rev-28-Dec-2021.pdf (Accessed on August 30, 2023).

Cisco and A.T. Kearney. (2018) "Cybersecurity in ASEAN: An Urgent Call to Action", p. 3, https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN—An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34 (Accessed on September 20, 2022).

Cyber Security Agency Singapore website, https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence (Accessed on September 20, 2022).

Heinl, C.H. (2014) "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime", *Asia Policy.* (18).

Indonesia Ministry of Finance, www.kemenkeu.go.id (Accessed on September 5, 2022).

International Telecommunication Union (2020) "Global Cybersecurity Index 2020", https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (Accessed on November 2, 2022).

International Business Machine (2020) "Cost of a Data Breach Report 2020", https://www.ibm.com/downloads/cas/QMXVZX6R (Accessed on September 7, 2022).

INTERPOL (2021) "ASEAN Cyber Threat Assessment 2021".

Jones, D.M., and Jenne, N. (2016) "Weak states' regionalism: ASEAN and the limits of security cooperation in Asia-Pacific", *International Relations of the Asia Pacific*. 16 (2), pp. 209-240.

Mahbubani, K. and Sng, J. (2017) *The ASEAN Miracle: A Catalyst for Peace*, Singapore: Ridge Books.

Palo Alto Networks (2020) "The State of Cybersecurity in ASEAN, 2020", https://www.paloaltonetworks.sg/apps/pan/public/downloadResource?pagePath=/content/pan/en_SG/resources/whitepapers/the-state-of-cybersecurity-in-asean-2020 (Accessed on November 2, 2022).

Statista (2021) "Internet penetration in Southeast Asia as of June 2021", https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/ (Accessed on September 7, 2022).

Sunkpho, J., Ramjan, S., Ottamakorn, C. (2018) "Cybersecurity Policy in ASEAN Countries", *Research Gate*. (March 2018)

TRPC (2020) "TRPC Data Protection Index 2020", https:/trpc.biz/old_archive/wp-contents/uploads/TRPC_DPI2020.pdf. (Accessed on September 5, 2022).

Yeoh, Angelin (2020) "Budget 2021: RM27mil allocation for CyberSecurity Malaysia hailed by industry players", *The Star*. February 6, 2020, https://www.thestar.com.my/tech/tech-news/2020/11/06/budget-2021-rm27mil-allocation-for-cybersecurity-malaysia-hailed-by-industry-players (Accessed on September 7, 2022).

Zhang, L.M. (2020) "Singapore Budget 2020: $1b over next 3 years to shore up cyber and data security capabilities", *The Straits Times*. February 18, 2020, https://www.straitstimes.com/singapore/singapore-budget-2020-1b-over-next-3-years-to-shore-up-cyber-and-data-security (Accessed on September 7, 2022).

〔受付日　2022. 11. 30〕
〔採録日　2023.　3. 11〕