JURNAL TRANSBORDERS

THE IMPLEMENTATION OF REGIONAL CYBERSECURITY EFFORTS IN ASEAN TOWARDS A RESILIENT CYBERSECURITY AMID THE ASEAN MEMBER COUNTRIES' DIGITAL DIVIDE

Harryanto Aryodiguno
harry_anto@president..ac.id

Abstract

Technological development has brought changes to all aspects of life. Southeast Asia is a region with a large population and considerable economic potential. With the growth of technology, Southeast Asian countries have become highly dependent on the digital world, which in turn supports the region's developing digital economy. Therefore, cybersecurity and cyber resilience are essential to prevent cyberattacks and to limit their impact when they do occur. For this reason, Southeast Asian countries have joined a regional organization, ASEAN, committed to building regional peace and stability, including in the area of cybersecurity. However, in building resilient cybersecurity, ASEAN faces the digital divide among its member states as an obstacle that may hinder these efforts. This issue is raised because detailed discussion of cybersecurity in Southeast Asia remains limited. This research therefore examines how ASEAN builds resilient cybersecurity despite the digital divide among its member states, using a qualitative method, analyzed through liberalism theory, and closed with recommendations.

Keywords: *Southeast Asia, ASEAN, Cyber Threat, Secure and Resilient Cybersecurity, Digital Divide, Cooperation, Liberalism Theory*

INTRODUCTION

The world we live in today is largely a product of the development of the internet. The internet has touched nearly every aspect of human life. People anywhere and at any time can easily interact with each other simply by using devices connected to the internet, even holding large-scale online conferences. Through the World Wide Web, the internet has made possible access to an information space commonly known as cyberspace. Although it can only be

experienced through the use of computers and connected devices, cyberspace is increasingly substituting for ordinary human activities in cultural, economic, and other domains (Kalay & Marx, 2006).

Cyberspace is often described as a virtual world because it is intangible, yet in physical reality it is built from the electronics of communication technology (Jordan, 1999). Tim Jordan (1999) conceptualizes cyberspace as a matrix, a net, a metaverse, and, more generally, a place made out of information. Cyberspace resembles a non-place in that it both physically separates and connects humans, an idea made concrete in cyberpunk fiction. According to the United States Department of Defense (Computer Security Resource Center, n.d.), cyberspace is "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Cyberspace is usually described as borderless, while the underlying internet infrastructure is typically state-controlled (Cempaka Timur, 2017). Given cyberspace's importance to human life, improving trust, security, and stability within it is a shared duty across many different actors (Paris Peace Forum, 2018).

As internet use grows and becomes central to more aspects of human life, the threats present in cyberspace grow as well. Cyberattacks can target state or non-state actors, and can affect critical infrastructure, national security, the global economy, democratic processes, and personal privacy (Ibid). Several typologies of cybersecurity threats exist, including cyberwar, cybercrime, and cyberterrorism (Ramadhan, 2020b). Cyberwar is essentially a digital version of conventional war. Cybercrime refers to criminal activity in which groups exploit information technology to pursue economic objectives. Cyberterrorism, meanwhile, refers to the practice of terrorist organizations hacking into or disabling a state's information systems (Ibid).

The Council of Europe's Convention on Cybercrime divides these offenses into several categories: first, offenses against the availability, integrity, and confidentiality of computer data and systems (including illegal interception, system interference, misuse of devices, illegal access, and data interference); second, computer-related offenses such as forgery and fraud; third, content-related offenses such as child pornography; and fourth, offenses involving violations of copyright and related rights. These offenses are commonly known by terms such

as hacking, phishing, worm and trojan-horse transmission, malware, spyware, and unlawful downloading (Khanisa, 2013).

Because the digital world cannot be separated from the everyday life of nation-states, building resilient cybersecurity has become essential. Iqbal Ramadhan (2020b) draws on Joseph Nye's view that, in the digital era, cybersecurity must be a priority within security studies, since cyberspace plays a crucial role in every facet of a nation-state's existence, including the social order governed within it. Whether or not they wish to, nation-states must therefore treat cyber issues as a strategic national priority.

According to Salsabila et al. (2020), cybersecurity can be defined as "the form of technology, process, practice, and mitigation response, the measure of which is used to protect the network, computer, program, and data coming from the attack, damage or illegal access to ascertain confidentiality, integrity, and availability." While internet infrastructure is typically state-controlled, cyberspace itself is generally described as borderless. Because of its importance to national security, public safety, and international relations, cybersecurity has become a crucial component of social and political life; it aims to maintain the availability, integrity, and confidentiality of networks and infrastructure (Cempaka Timur, 2017). Cybersecurity alone, however, is not sufficient to guarantee safety in cyberspace; cyber resilience is equally necessary. Cyber resilience is the ability of a system to anticipate, respond to, recover from, and continually adapt in order to achieve its intended outcome despite unfortunate cyber incidents (Putranti et al., 2022). Resilient cybersecurity allows a system to defend against threats, withstand and reduce the impact of attacks, and continue to function even while under attack.

Building resilient cybersecurity, however, is complicated by the digital divide, a barrier that continues to challenge many nations, including those in Southeast Asia. The digital divide refers to the uneven distribution of opportunities to access and use information and communication technologies (ICTs) among people, businesses, households, and geographical areas at different socioeconomic levels (Evers et al., 2005). This gap is visible where some people within a country can use modern communication technology while others cannot access even basic telephone or internet services. Southeast Asia, meanwhile, is a region with a large population and considerable economic potential, positioned as an emerging market with a fast-growing digital economy. The region is home to more than 400 million internet users, with an internet penetration rate of approximately 75.6 percent (Ha & Chuah, 2023). Most internet

users in Indonesia, the Philippines, and Malaysia spend around four hours daily on their mobile devices accessing the internet, while users in Thailand, who log on for the longest time in the region, average four hours and 56 minutes per day (Obet et al., 2021).

From this, it is clear that cyberspace has become deeply integrated into ASEAN countries' economic and social life, and this integration has made them increasingly dependent on digital infrastructure. Southeast Asia is among the fastest-growing economic regions in the world, and advances in digital technology help drive that growth (Ramadhan, 2020a). As more people across ASEAN gain internet access, the region also becomes more exposed to cybercrime, since greater freedom to access information online can be misused for illegal purposes, which in turn threatens national security (Alviyani et al., 2022). Facing this shared challenge, Southeast Asian nations have united to seek a solution for building resilient cybersecurity through a regional organization called ASEAN.

The Association of Southeast Asian Nations, or ASEAN, was established by several founding members, namely Indonesia, the Philippines, Malaysia, Thailand, and Singapore, on 8 August 1967 in Bangkok, Thailand. Brunei Darussalam, Vietnam, Lao PDR, Myanmar, and Cambodia later joined, bringing ASEAN's membership to ten states (Association of Southeast Asian Nations, n.d.-b). With the aim of promoting regional peace and stability (Ministry of Foreign Affairs of the Republic of Indonesia, 2009), ASEAN prioritizes several efforts to build resilient cybersecurity: raising awareness of cybersecurity issues, building coordinated channels for cooperation and solutions, and making use of the capabilities of ASEAN member states and their external partners (Association of Southeast Asian Nations, n.d.-a). Even so, ASEAN's efforts to build resilient cybersecurity are hindered by the digital divide among its member states, since each faces a different phase of ICT development (Cempaka Timur, 2017; Chang, 2017).

This research addresses cybersecurity in Southeast Asia specifically because the region is one of the world's centers of economic development, yet ASEAN still faces numerous cyber threats that could undermine that growth. Cybersecurity is also an issue that tends to be overlooked and rarely receives sufficient attention within international relations discourse. Through this research, the author seeks to answer the following research question: "What steps has ASEAN taken to build resilient cybersecurity amid the digital divide within its member states?" This research aims to depict ASEAN's efforts to build resilient cybersecurity despite

this digital divide, and to offer several recommendations. To analyze this issue, the research uses liberalism theory as its theoretical approach, presented in the following section.

ANALYSIS FRAMEWORK

Liberalism is one of the most widely used theories in international relations. It emerged as a formal theory in the 1970s (Norwich University, 2017) and was shaped by the ideas of several philosophers, including Immanuel Kant, John Locke, and David Hume, among others. The pursuit of peace following World War I contributed significantly to the development of liberalism as a theory of international relations (Toprak, 2022). Liberal theories of international relations are influenced by humanism and the value placed on individuals, an ideology that places greater emphasis on concepts such as "international collaboration" and "conflict prevention" than on the use of force or violence.

Liberalism is often described as a rationalist framework that applies a rationalist perspective to events without necessarily adopting positivism outright; within the liberalism lens, positivism is considered first, and rationalism is applied to the extent that positivism fails to explain a given phenomenon. Liberal theory holds that power should be measured through a state's political freedoms and rights, its economy, and its potential for peace and cooperation (Norwich University, 2017). Liberalism further argues that peace and stability can be achieved by moving beyond a traditional, rigid conception of sovereignty and by fostering cooperation and participation among governments across political, cultural, economic, and other domains (Nejati & Hossein, 2021). Unlike neorealism, which treats states as the primary actors in international relations, liberalism also acknowledges the role of non-state actors, including individuals, organizations, and social movements (Isnarti, 2016). This emphasis on a plurality of global actors is arguably liberalism's most valuable contribution to theory-building in the digital age, as liberals seek ways to foster consensus and collaboration among states and other actors in pursuit of peace and stability (Ibid).

In cyberspace, many powerful actors operate alongside states, including terrorist groups and individuals who are equally capable of carrying out cyberattacks. Because of this, governments alone cannot secure cyberspace and instead require cooperation with other actors. Liberalism theory's recognition of non-state actors, including international organizations, makes it well suited to analyzing ASEAN's role as a regional organization pursuing cooperation

to achieve resilient cybersecurity among its member states despite the ICT gap that stands as a barrier.

RESEARCH METHOD

This research uses a qualitative method, which enables the researcher to develop a deeper understanding of the values, decision-making processes, and interactions involved in policymaking (Snape & Spencer, 2003). This method was chosen because it allows for an in depth understanding of ASEAN's efforts to build resilient cybersecurity within its member states. The data supporting this research come from secondary sources, including ASEAN's official websites, journal articles on cyberspace and cybersecurity in ASEAN, online news, official publications, and reports related to cybersecurity in the ASEAN region.

RESULTS AND DISCUSSIONS

Cybersecurity Condition in ASEAN

The increase in cross-industry technological advances suggests that Southeast Asia is catching up in information technology (IT). Even so, the cybersecurity condition and capacity of ASEAN member states vary considerably. Globally, countries were estimated to spend on average around 0.13 percent of GDP on cybersecurity in 2017, while ASEAN as a whole spent only around 0.06 percent, equivalent to roughly US$1.9 billion (Choudhury, 2018). This shows that ASEAN has historically under-prioritized cybersecurity spending relative to global benchmarks, a gap made more concerning given that digital trade accounts for a substantial share of ASEAN's economic growth (Obet et al., 2021). Underinvestment of this kind leaves the region more exposed should a major cyberattack occur.

Cyberattacks that have occurred in Southeast Asia demonstrate that the region's IT infrastructure often lacks adequate security, a vulnerability that has encouraged cybercriminals to target the region. An assessment by A.T. Kearney found that cybersecurity threats could result in losses of up to US$750 billion for 1,000 businesses across Southeast Asia, and recommended that ASEAN increase its cybersecurity spending to between 0.35 and 0.61 percent of its collective GDP (Nasir, Jamilah, & Halim, 2019). Singapore, Malaysia, Indonesia, and Thailand are among the ASEAN countries that invest the most in IT; in 2017, Singapore recorded the highest cybersecurity investment among ASEAN states, followed by Malaysia and Thailand (Ibid).

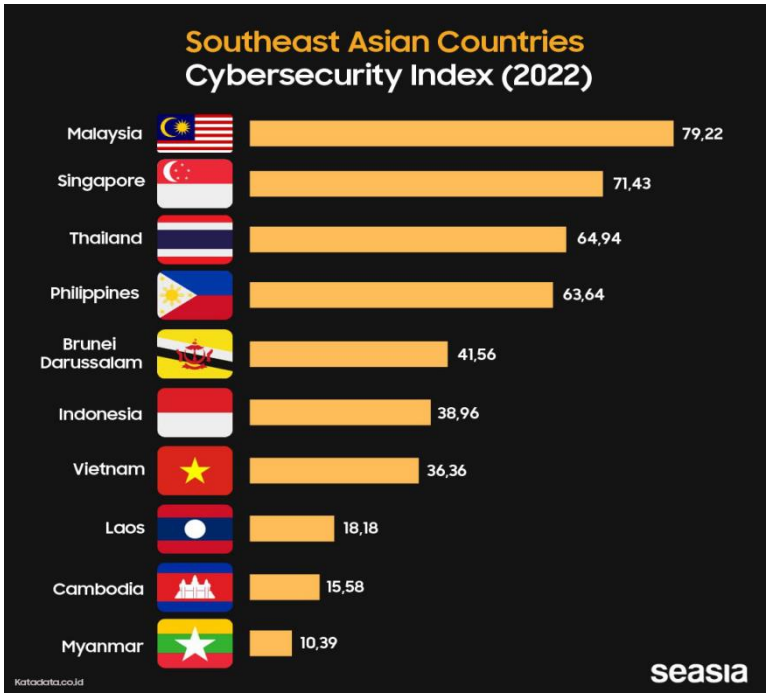

Figure 1: Southeast Asian Countries Cybersecurity Index 2022 (Seasia.co, 2022)

Based on the 2022 Cybersecurity Index of Southeast Asian countries (Seasia.co, 2022), Malaysia, Singapore, and Thailand rank among the top three in the region in terms of cybersecurity. This assessment is based on several indicators, including cybersecurity legislation and regulation, the presence of government agencies in the sector, government cooperation on cybersecurity, and the availability of open sources of information such as official websites and related programs.

Despite this relatively strong security index, ASEAN member countries remain vulnerable to cyberattacks. Data from INTERPOL member countries (2021) show that several types of cyber threats have consistently occurred in ASEAN since 2020, including business e-mail compromise, ransomware, phishing, cyber scams, e-commerce data interception, crimeware as a service, and cryptojacking. Several notable cyberattacks illustrate this vulnerability. First, in July 2018, hackers breached Singapore's healthcare institution group, SingHealth, stealing the personal information of 1.5 million patients, including that of Singapore's Prime Minister Lee Hsien Loong (Tham, 2018). Second, in 2020, the Indonesian start-up Tokopedia suffered a data breach affecting 91 million users, exposing user IDs, names, e-mail addresses, gender, dates of birth, phone numbers, and passwords; the stolen data was reportedly sold on the dark web for approximately US$5,000 (CNBC Indonesia, 2020).

In 2021, Vietnam recorded 2,916 cyberattacks, an increase of about 898 cases compared with 2020 (Vietnam Information Security Association, n.d.). Perpetrators took advantage of heightened public attention on the COVID-19 pandemic to expand their attacks, spread malicious software, and perpetrate hoaxes intended to steal or destroy user, organizational, and company information. These cases collectively illustrate how vulnerable ASEAN countries remain to cyberattacks, underscoring the need for resilient cybersecurity to prevent such incidents in the future and to minimize their impact when they do occur.

The Significance of Building Resilient Cybersecurity in ASEAN as a Region

Southeast Asia's exposure to cyberattacks carries direct economic risk, particularly as the region's digital economy continues to expand rapidly. According to a SEA economy report by Google, Bain, and Temasek, Southeast Asia's digital economy was projected to grow to US$363 billion by 2025, up from an earlier projection of US$300 billion (German-Indonesian Chamber of Industry and Commerce, 2021). ASEAN member states, in particular, have the potential to add as much as US$1 trillion to their combined GDP over a ten-year period through digital growth (Raska, 2018). This opportunity brings clear economic benefits, but it also exposes ASEAN member countries to greater cybersecurity risk.

ASEAN countries have become a prime target for cyberattacks for several reasons. First, several ASEAN countries have emerged as regional hubs for digital businesses (Chang, 2017): Southeast Asia is home to more than 7,000 digital start-ups, roughly 80 percent of which are based in Indonesia, Singapore, or Vietnam. Grab, the region's largest ride-hailing company, is based in Singapore, while four of Southeast Asia's ten most prominent tech start-ups, including GoJek, Traveloka, and Tokopedia, are based in Indonesia. Vietnamese tech companies are also attracting growing venture funding, exemplified by online gaming company VNG surpassing a billion-dollar valuation (Asialink Business, n.d.). Second, Southeast Asia continues to exhibit comparatively weak governance, policy frameworks, and cybersecurity capabilities (Chang, 2017), a gap discussed further in the following section. Given this combination of high digital potential and limited cybersecurity capacity, building resilient cybersecurity is essential both to maximize the region's digital opportunities and to minimize its cyber risk.

The Influence of the Digital Divide on ASEAN's Efforts to Build Resilient Cybersecurity

Unequal access to information and communication technologies (ICTs) is one of the defining features of the digital divide, visible for instance in the uneven distribution of mobile phones, fixed telephones, and internet access among ASEAN countries (Tsauro, 2016).

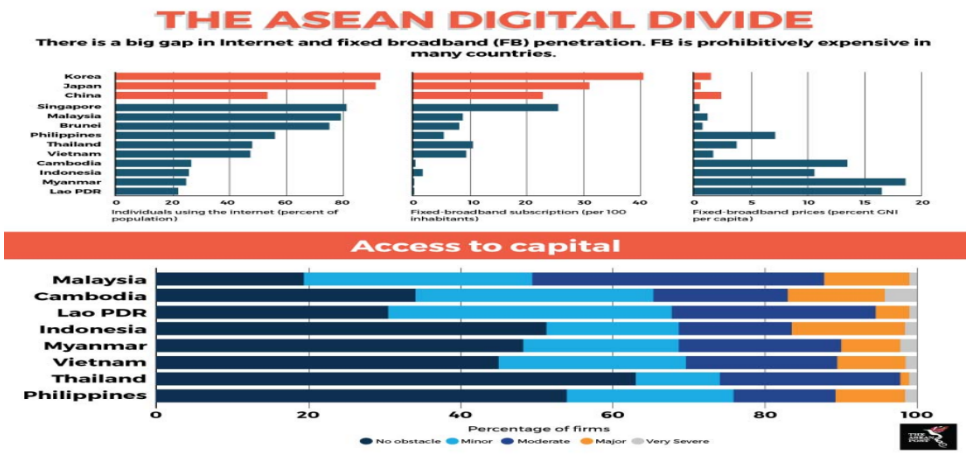

Figure 2: The ASEAN Digital Divide (ASEAN Post, 2019)

According to data compiled by the ASEAN Post (2019), Singapore, Malaysia, and Brunei have been the most successful ASEAN states in expanding internet access, each exceeding 80 percent of their total population, supported in part by comparatively lower fixed-broadband prices. By contrast, less developed member states such as Cambodia, Indonesia, Myanmar, and Lao PDR recorded penetration rates below 70 percent. More recent academic evidence confirms that this divide has persisted: internet penetration in Cambodia, Laos, and Myanmar remains close to 50 percent, compared with roughly 80 percent in Singapore, Thailand, and Malaysia (Kaushik, 2019, as cited in Ha & Chuah, 2023). Measured against the region's population of approximately 676.6 million people (ASEAN Secretariat, 2023) and more than 400 million internet users (Ha & Chuah, 2023), this gap remains substantial and continues to shape ASEAN member states' respective cyber capabilities.

Hanan Mohamed Ali argues that low cyber capabilities stem from several causes, including limited human-resource expertise and limited financial resources to subsidize ICT infrastructure (Ali, 2021). Cybersecurity Ventures projected a persistent shortage of cybersecurity expertise from 2021 onward (JAIF Management Team, 2021), and Dr. Chaichana Mitrpant, Chief Executive of Thailand's Electronic Transactions Development Agency, has argued that ASEAN needs hundreds of thousands of additional cybersecurity experts (Ibid). Financial constraints compound this problem, since the high cost of

infrastructure hinders member states from deploying high-speed fixed broadband, making cyber capability development critical to a country's overall cybersecurity awareness.

Low cybersecurity awareness partly stems from countries perceiving cyber threats differently depending on their level of technological development (Alviyani et al., 2022). According to Nasir et al. (2019), cybersecurity awareness in developing ASEAN countries remains relatively low; Myanmar, for instance, lacks cybersecurity awareness due to inadequate technology, infrastructure, and expertise (Ibid). Some ASEAN member states have advanced cyber technology supported by dedicated cybercrime-prevention units, while others have yet to reach that stage. As a result of this digital divide, ASEAN member countries are sometimes considered not fully ready for cybersecurity cooperation, which itself becomes a threat to building resilient regional cybersecurity (Cempaka Timur, 2017; Nasir et al., 2019). The digital divide is thus widely viewed as a threat to a country's ICT development and to regional connectivity more broadly (Tsauro, 2016).

Technological and cyberspace development in Southeast Asia continues to be dominated by Singapore (Ramadhan, 2020b), while other member states lag behind. This gap becomes a burden for less technologically advanced countries seeking to secure their own cyberspace, and because cyberattacks tend to have holistic, cross-border effects, an attack on one country can affect others within ASEAN (Ramadhan, 2020b). Even so, the ICT gap that has long been viewed as a barrier to resilient cybersecurity can instead be reframed as a new opportunity for ASEAN and its member states. Caitríona H. Heinl (2014) supports this view, arguing that regional cooperation need not be hampered by the digital divide between developed and developing states; on the contrary, ASEAN must strengthen its collective cyberspace against significant cyber threats and address common global cybersecurity concerns together.

This view aligns closely with liberalism theory's emphasis on cooperation as a path to peace and stability, including in cyberspace. Liberalism holds that actors in international relations extend beyond the state to include non-state actors such as regional organizations like ASEAN, and it emphasizes cooperation as central to achieving peace and security, in line with ASEAN's own objectives. Peace and security in cyberspace can therefore be pursued through ASEAN's role as a platform bridging the ICT gap among its member states, optimizing strategic cooperation through technology-sharing. Countries with lower digital capability can look to more digitally advanced member states as models, learning from their experience in combating

cyber threats and adopting best practices in policy and cyber law (Ibid). Singapore, given its comparatively advanced technology, is well positioned to lead this kind of cooperation, serving as a mentor in developing information technology capacity among member states.

During its term as ASEAN Chair in 2018, Singapore supported numerous cybersecurity initiatives and committed significant resources to developing operational, policy, and legal capacity (Salsabila et al., 2020). Reflecting this capacity, Singapore initiated the establishment of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in 2018, which became operational in October 2019 (Salsabila et al., 2020). The ASCCE was designed to strengthen cybersecurity across the region by building capacity for research, legislation, and the formulation of national cybersecurity strategies through training and the sharing of knowledge and best practices on open-source cyber threats (CSA Singapore, 2021). Singapore's Minister for Communications and Information, Josephine Teo, announced the opening of ASCCE's campus in Singapore as part of efforts to build cybersecurity expertise across the region (Chee Kenny, 2021). By expanding the pool of trained cyber experts, ASCCE has the potential to narrow the digital divide among ASEAN member countries and to make future technical cooperation on cyber issues easier to achieve. It also provides a platform and mechanism for information sharing, incident reporting, and collective response to cyberattacks.

The ASCCE can further be understood as a strategic implementation of the broader ASEAN Cyber Capacity Programme, since it helps close the gap between member states and address common obstacles such as weak infrastructure, limited human resources, tight budgets, and outdated technology. States with less developed cyber infrastructure stand to benefit from this disparity in development by learning directly from more advanced governments' expertise in handling cyber threats, policy design, and data security and privacy practices. To ensure ASCCE's continued operation, Singapore, as its initiator, committed approximately US$30 million in funding over five years (Baharudin, 2018), a commitment intended to encourage other member states to invest similarly in their own cyber-capacity building.

ASEAN has further reinforced this effort through the ASEAN Cybersecurity Cooperation Strategy 2021-2025, which prioritizes the development of a secure and resilient regional cyberspace (CSA Singapore, 2022). Under this strategy, ASEAN member states are working to establish the ASEAN Regional CERT, planned to become operational in 2023/2024. Singapore submitted the ASEAN Regional CERT Implementation Paper to the 2nd ASEAN Digital Ministers' Meeting (ADGMIN) in January 2022 for approval alongside the

ASEAN Secretariat and member states, and continues to collaborate with member countries on the CERT's operational framework, including its scope, goals, functions, partners, and procedures (Ibid). This collaboration offers ASEAN member states a valuable opportunity to exchange knowledge and information on cybersecurity and capacity building with states that have more advanced ICT infrastructure.

ASEAN Efforts through the ASEAN Regional Forum

Securing cyberspace cannot be achieved by any single country acting alone. ASEAN therefore collaborates with other countries through the ASEAN Regional Forum (ARF) to address cybersecurity issues, consistent with liberalism theory's view that states cannot manage security challenges through self-help alone and instead require global coordination and cooperation (Ramadhan, 2020b). The ARF's objective is to promote consultation and constructive dialogue on shared security and political challenges, contributing to mutual trust and preventive diplomacy across the Asia-Pacific region (ARF, n.d.). Unlike other security arrangements, the ARF does not rely on military force, instead emphasizing dialogue and engagement to prevent conflict. Cybersecurity has become an established component of ASEAN's strategy within the ARF since a joint declaration made at a 2006 meeting in Malaysia, which has since translated into numerous regional training programs, including training focused on how states organize their responses to cyber crises (Estiyovionita & Sitamala, 2022).

As a forum for discussing shared challenges, ASEAN engages several dialogue partners through the ARF, including Canada, China, Australia, the EU, Japan, New Zealand, India, Russia, the United States, and South Korea, alongside several observer states, including North Korea, Papua New Guinea, Pakistan, Timor-Leste, Bangladesh, Mongolia, and Sri Lanka (Australian Government Department of Foreign Affairs and Trade, n.d.). Over time, the ARF has had numerous opportunities to build cybersecurity work plans. The 28th ASEAN Regional Forum, held in 2021, set goals for advancing ICT security through cooperation in several areas: raising awareness of threats to the safe and proper use of ICT, improving incident response, and exchanging best practices important for preserving ICT security and regional peace and stability (ASEAN Regional Forum, 2021).

These goals have taken several concrete forms (ASEAN, 2020). First, information-sharing on national laws, best practices, policies, and strategies, co-led by Japan and the Philippines. Second, awareness-raising and information-sharing on emergency security

incident response, co-led by Singapore, Cambodia, and China. Third, workshops on building security principles in the national context, co-led by Singapore and Canada. Fourth, protection of critical infrastructure enabled by ICT, co-led by the EU and Singapore. The ARF thus benefits both ASEAN member states and their dialogue partners by enabling ongoing discussion, collaboration, information-sharing, and practical cooperation on cyber threats and cybersecurity. If fully utilized, this forum offers ASEAN a realistic pathway toward achieving resilient cybersecurity.

ASEAN Challenges

In carrying out these cooperative efforts, ASEAN's push for resilient cybersecurity faces several difficulties. First, although the digital divide can be reframed as an opportunity for technology-sharing cooperation, it also shapes how differently each country perceives cybersecurity as a national security priority (Khanisa, 2013; Nasir et al., 2019). Most ASEAN countries continue to prioritize economic growth over cybersecurity (Nasir et al., 2019): countries with advanced ICT, such as Singapore and Malaysia, treat cybersecurity as a critical priority, while countries with lower internet penetration and weaker ICT infrastructure, such as Myanmar and Lao PDR, tend to place it lower on their national agenda (Khanisa, 2013). It is therefore critical for ASEAN to encourage its member states to converge on a shared understanding of cybersecurity's importance.

Second, ASEAN member states still lack legal harmonization, particularly between national law and international cybercrime conventions (Ali, 2021). None of the ASEAN member states, for example, have signed or ratified the Budapest Convention on Cybercrime, which is designed to support the adoption of appropriate legal instruments against cybercrime through both substantive and procedural regulation, and to accelerate cooperation among governments in cybercrime investigation and prosecution (Ibid). Even so, eight of the ten ASEAN member states, excluding Lao PDR and Cambodia, have passed cybercrime laws broadly consistent with the Budapest Convention's requirements; Lao PDR enacted its own cybercrime prevention law in 2014 (Chang, 2017). Cambodia remains the only member state with cybercrime legislation still under review, its existing legal framework considered unclear relative to international standards (Nguon & Srun, 2020). Nevertheless, the general conformity of domestic laws across most ASEAN member states with the Budapest Convention provides a solid foundation for cross-border cooperation against cybercrime. Without ratifying the

Convention itself, however, ASEAN will still need to construct its own regional cooperation framework for transnational action against cybercrime (Chang, 2017).

CONCLUSION

Cyberspace and digital technology have become the backbone of ASEAN member countries' digital economic development. In pursuing resilient cybersecurity despite the digital divide among its members, ASEAN's situation, viewed through the positivist strand of liberalism, should be understood not merely as an obstacle but as an opportunity to deepen regional cooperation. This aligns with Caitríona H. Heinl's (2014) argument that regional cooperation need not be hampered by the digital divide between developed and developing states; rather, ASEAN must strengthen its collective cyberspace against significant cyber threats while addressing common global cybersecurity concerns together.

The most suitable steps for ASEAN are therefore cooperation through technology-sharing between more and less digitally advanced member states, and capacity-building cooperation with dialogue partners through the ASEAN Regional Forum (ARF). If pursued deliberately, these opportunities can become meaningful, if incremental, steps toward resilient regional cybersecurity. This also reflects liberalism theory's emphasis on cooperation and its recognition of non-state actors, both fulfilled through ASEAN's role as a regional organization cooperating with other states via the ARF. Together, these findings answer this research's central question regarding the steps ASEAN has taken to build resilient cybersecurity amid the digital divide among its member states.

Beyond these steps, several additional recommendations are worth considering. First, ASEAN can address the varying national priorities placed on cybersecurity by making fuller use of the ARF as a platform for synchronizing member states' understanding of cyber threats and priorities. Second, given the challenge of divergent national priorities, ASEAN member states need to commit to treating cybersecurity as a genuine top priority, so that regionally developed information and policy can be more easily implemented at the national level. Finally, rather than treating the digital divide as a permanent hindrance, ASEAN member states should expand the sharing of technology and knowledge through the ASCCE, including offering scholarships for students from each member state to study at the ASCCE campus, thereby attracting more people into the field and strengthening national human-resource capacity in cybersecurity. Ultimately, resilient cybersecurity cannot be achieved by any single country

alone; it requires sustained cooperation and active engagement from all member states if cybersecurity in the region is to move steadily toward greater resilience.

REFERENCES

BOOK

Jordan, T. (1999). Cyberpower: The Culture and Politics of Cyberspace and the Internet. Taylor & Francis. doi:https://doi.org/10.4324/9780203448632

BOOK CHAPTER

Chang, L. Y. C. (2017). Cybercrime and Cyber Security in ASEAN. In Comparative Criminology in Asia (pp. 135-148). Springer, Cham. doi:10.1007/978-3-319-54942-2_10

Snape, D., & Spencer, L. (2003). The Foundations of Qualitative Research. In D. Snape & L. Spencer (Eds.), Qualitative Research Practice: A Guide for Social Science Students and Researchers (pp. 2-10). London: Sage Publications.

JOURNAL ARTICLE

Ali, H. M. (2021). "Norm Subsidiarity" or "Norm Diffusion"? A Cross-Regional Examination of Norms in ASEAN-GCC Cybersecurity Governance. The Journal of Intelligence, Conflict, and Warfare, 4(1), 122-148. doi:10.21810/JICW.V4I1.2805

Alviyani, E., Fitri, M., & Padmi, M. (2022). Japanese and ASEAN Security Strategies in Cyber Crime in 2021-2025. Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 5(3), 23043-23054. doi:10.33258/birci.v5i3.6318

Cempaka Timur, F. G. (2017). The Rise of Cyber Diplomacy: ASEAN's Perspective in Cyber Security. KnE Social Sciences, 2(4), 244. doi:10.18502/kss.v2i4.893

Estiyovionita, K., & Sitamala, A. (2022). ASEAN's Role in Cybersecurity Maintenance and Security Strategy Through an International Security Approach. Lampung Journal of International Law, 4(2), 81-90. doi:10.25041/lajil.v4i2.2556

Ha, H., & Chuah, C. K. P. (2023). Digital Economy in Southeast Asia: Challenges, Opportunities and Future Development. Southeast Asia: A Multidisciplinary Journal, 23(1), 19-35. doi:10.1108/SEAMJ-02-2023-0023

Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. Asia Policy, 18(1), 131-159. doi:10.1353/ASP.2014.0026

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. Andalas Journal of International Studies (AJIS), 5(2), 151-165. doi:10.25077/AJIS.5.2.151-165.2016

Kalay, Y. E., & Marx, J. (2006). Architecture and the Internet: Designing Places in Cyberspace. First Monday, 5(SPECIAL ISSUE). doi:10.5210/FM.V0I0.1563

Khanisa. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. Journal of ASEAN Studies, 1(1), 41-53. Retrieved from https://journal.binus.ac.id/index.php/jas/issue/view/26

Nejati, M. H., & Hossein, M. (2021). The Role of Liberalism in International Relations of Nations. PalArch's Journal of Archaeology of Egypt / Egyptology, 18(6), 512-527. Retrieved from https://archives.palarch.nl/index.php/jae/article/view/8574

Obet, D., Suharto, S., & Mujoko, H. (2021). Cyber Cooperation in the Framework of ASEAN Regime. Jurnal Pertahanan: Media Informasi tentang Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity, 7(2), 254-261. doi:10.33172/jp.v7i2.1264

Putranti, I. R., Hanura, M., Alivia, S., Ananda, S., & Nura Nabila, G. (2022). Cyber Resilience Revisited: Law and International Relations. Journal of Social Studies (JSS), 18(1), 1-26. doi:10.21831/JSS.V18I1.39637

Ramadhan, I. (2020a). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). The Asian Institute of Research Journal of Social and Political Sciences, 3(4), 983-995. doi:10.31014/aior.1991.03.04.230

Ramadhan, I. (2020b). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. Jurnal Asia Pacific Studies, 3(2), 181-192. doi:10.33541/japs.v3i1.1081

Salsabila, A. S., Fikri, M. D., Andika, M. S., & Harahap, N. A. (2020). Potential and Threat Analysis Towards Cybersecurity in South East Asia. Journal of ASEAN Dynamics and Beyond, 1(1), 1-13. doi:10.20961/ASEANDYNAMICS.V1I1.46794

Tsauro, M. A. (2016). Digital Divide in ASEAN: Analyzing Regional Integration through Information and Communication Technologies Development. Retrieved from https://www.researchgate.net/publication/298348177

WEBPAGES

ARF. (n.d.). ASEAN Regional Forum. Retrieved 3 December 2022, from https://aseanregionalforum.asean.org/about-arf/

Asialink Business. (n.d.). Southeast Asia's Digital Boom. Retrieved 10 November 2022, from https://asialinkbusiness.com.au/news-media/southeast-asias-digital-boom

Association of Southeast Asian Nations. (n.d.-a). Cyber Security - ASEAN Main Portal. Retrieved 5 December 2022, from https://asean.org/our-communities/asean-political-security-community/peaceful-secure-and-stable-region/cyber-security/

Association of Southeast Asian Nations. (n.d.-b). Homepage - ASEAN Main Portal. Retrieved 23 October 2022, from https://asean.org/

Australian Government Department of Foreign Affairs and Trade. (n.d.). ASEAN Regional Forum (ARF). Retrieved 3 December 2022, from https://www.dfat.gov.au/international-relations/regional-architecture/asean-regional-forum-arf

Baharudin, H. (2018, September 19). Singapore to Spend $30 Million Over Next 5 Years to Fund New Regional Cyber Security Centre. The Straits Times. Retrieved 29 November 2022, from https://www.straitstimes.com/singapore/singapore-to-spend-30-million-over-next-5-years-to-fund-new-regional-cyber-security-centre

Chee Kenny. (2021, October 6). Asean-S'pore Centre for Training National Cyber-Security Teams Opens New Campus. The Straits Times. Retrieved 29 November 2022, from https://www.straitstimes.com/tech/tech-news/asean-spore-centre-for-training-national-cyber-security-teams-opens-new-campus

Choudhury, S. R. (2018, January 23). ASEAN Need to Increase Cybersecurity Spending, Says New Report. CNBC. Retrieved 7 November 2022, from https://www.cnbc.com/2018/01/23/asean-need-to-increase-cybersecurity-spending-says-new-report.html

CNBC Indonesia. (2020, May 4). Cerita Lengkap Bocornya 91 Juta Data Akun Tokopedia. Retrieved 3 December 2022, from https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia/1

Computer Security Resource Center. (n.d.). Cyberspace - Glossary | CSRC. Retrieved 27 October 2022, from https://csrc.nist.gov/glossary/term/cyberspace

CSA Singapore. (2021, October 6). ASEAN-Singapore Cybersecurity Centre of Excellence. Retrieved 29 November 2022, from https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence

CSA Singapore. (2022, October 20). Establishment of ASEAN Regional Computer Emergency Response Team (CERT). Retrieved 29 November 2022, from https://www.csa.gov.sg/News/Press-Releases/establishment-of-asean-regional-computer-emergency-response-team

German-Indonesian Chamber of Industry and Commerce. (2021, December 3). SEA's Digital Economy to Double in 2025, Nearly Half of It in Indonesia. Retrieved 10 November 2022, from https://indonesien.ahk.de/en/infocenter/news/news-details/seas-digital-economy-to-double-in-2025-nearly-half-of-it-in-indonesia

JAIF Management Team. (2021, November 3). Enhancing Cybersecurity Skills of Professionals in ASEAN. Japan-ASEAN Integration Fund. Retrieved 29 November 2022, from https://jaif.asean.org/beneficiaries_voice/enhancing-cybersecurity-skills-of-professionals-in-asean/

Ministry of Foreign Affairs of the Republic of Indonesia. (2009, September 5). About ASEAN. Retrieved 5 December 2022, from https://kemlu.go.id/portal/en/read/122/halaman_list_lainnya/about-asean

Nguon, S., & Srun, S. (2020, January 27). Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law. Konrad-Adenauer-Stiftung. Retrieved 28 November 2022, from https://www.kas.de/en/web/kambodscha/single-title/-/content/cambodia-v-hackers-balancing-security-and-liberty-in-cybercrime-law

Norwich University. (2017, October 2). 7 Components of Liberalism. Retrieved 12 November 2022, from https://online.norwich.edu/academic-programs/resources/7-components-of-liberalism

Paris Peace Forum. (2018). Paris Call. Retrieved 5 December 2022, from https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Raska, M. (2018, May 22). Cybersecurity in Southeast Asia. Retrieved 29 November 2022, from https://centreasia.eu/wp-content/uploads/2018/12/NotePre%CC%81sentation-AngRaska-Cybersecurity_180518.pdf

Seasia.co. (2022, September 19). Southeast Asian Countries Cybersecurity Index (2022). Retrieved 11 November 2022, from https://seasia.co/2022/09/19/southeast-asian-countries-cybersecurity-index-2022

Tham, I. (2018, July 20). Personal Info of 1.5m SingHealth Patients, Including PM Lee, Stolen in Singapore's Worst Cyber Attack. The Straits Times. Retrieved 3 December 2022, from https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

The ASEAN Post Team. (2019, March 9). A Digital ASEAN for Everyone. The ASEAN Post. Retrieved 26 November 2022, from https://theaseanpost.com/article/digital-asean-everyone

Toprak, B. (2022, January). Introduction to Liberalism in International Relations: Critical Approach to Liberalism and Covid-19. Retrieved 12 November 2022, from https://www.researchgate.net/publication/361590646

Vietnam Information Security Association. (n.d.). Vietnam Hit by 2,900 Cyber Attacks in First Half of 2021. Retrieved 3 December 2022, from https://www.vnisa.org.vn/en/vietnam-hit-by-2900-cyber-attacks-in-first-half-of-2021/

WORKING PAPER

Evers, H.-D., Gerke, S., & Solvay. (2005). Closing the Digital Divide: Southeast Asia's Path Towards a Knowledge Society. ZEF Working Paper Series, 1(1). Retrieved from http://hdl.handle.net/10419/88324

CONFERENCE

Nasir, P. E., Jamilah, M., & Halim, A. (2019). Proceeding of the 1st International Conference on ASEAN (IC-ASEAN) 'Towards a Better ASEAN' (pp. 1-547). Warsaw: Sciendo. doi:https://doi.org/10.1515/9783110678666

REPORT

ASEAN. (2020). ASEAN Cybersecurity Cooperation Strategy (2021-2025). Retrieved from https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

ASEAN Regional Forum. (2021). Chairman's Statement of the 28th ASEAN Regional Forum, 6 August 2021, via Videoconference. Retrieved from https://www.mofa.go.jp/files/100220807.pdf

ASEAN Secretariat. (2023). ASEAN Statistical Yearbook 2023. Jakarta: The ASEAN Secretariat. Retrieved from https://asean.org/wp-content/uploads/2023/12/ASEAN-Statistical-Yearbook-2023.pdf

Interpol. (2021). ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook From the ASEAN Cybercrime Operations Desk. Retrieved from https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia