Journal of Social and Political Sciences

Ramadhan, I. (2023). ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities. *Journal of Social and Political Sciences*, 6(4), 1-10.

ISSN 2615-3718

DOI: 10.31014/aior.1991.06.04.440

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Social and Political Sciences* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Social and Political Sciences, which include, but are not limited to, Anthropology, Government Studies, Political Sciences, Sociology, International Relations, Public Administration, History, Philosophy, Arts, Education, Linguistics, and Cultural Studies. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Journal of Social and Political Sciences* aims to facilitate scholarly work on recent theoretical and practical aspects of Social and Political Sciences.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Journal of Social and Political Sciences
Vol.6, No.4, 2023: 1-10
ISSN 2615-3718

DOI: 10.31014/aior.1991.06.04.440

ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities

Iqbal Ramadhan[1]

[1] Student of Doctoral Programme International Relations Department at Universitas Padjadjaran, lecturer of International Relations Department, Universitas Pertamina, email: iqbal.ramadhan@universitaspertamina.ac.id

Abstract
Southeast Asia's technological achievements and economic prosperity have become the key drivers of the development of both regional and worldwide dynamics. As an organisation that represents all Southeast Asian member countries, ASEAN, as one of the region's primary actors, plays an essential role. ASEAN's attempts to fulfil its objectives include engagement with important partners outside of the area, termed "ASEAN Plus." China is one of ASEAN's key regional allies. In this scientific essay, the author wishes to comment on the potential and problems that ASEAN-China face, notably in establishing cybersecurity collaboration. Cyber security is a serious concern in Southeast Asia. The expansion of the digital economy is assisting Southeast Asia's economic progress. On the one hand, China invests in artificial intelligence and profits from open commerce in Southeast Asia. However, ASEAN lacks policies and a framework to combat cyber threats, which are akin to non-traditional threats such as drugs, human trafficking, and terrorism. In this article, the author expands on cybersecurity challenges such as the lack of cyber threat mitigation policies and the Southeast Asian region's large technology disparity. The author also examines the opportunities for ASEAN and China to expand their cybersecurity cooperation. Cooperation between ASEAN and China can focus on developing cybersecurity rules, increasing human resource capability, and transferring technology.

Keywords: ASEAN, China, Cybersecurity, Cooperation

1. Background

The Southeast Asian region is one of the world's fastest-growing. Because of its tremendous economic expansion and prosperity, this region has garnered special attention. One measure of economic growth in Southeast Asia is the advancement of information technology. Finally, technology becomes a cornerstone for the growth of the region's digital economy. As these technologies advance, so does the growth of digital trade (e-commerce) and online transportation (Nengsi, 2019; Yuniar, 2017). As one of the primary drivers of economic growth, ASEAN (Association of Southeast Asian Nations) administers the Southeast Asia region. Economists predict that total trade in Southeast Asia will reach US$102 billion by 2025. With an estimated value of US$20 billion in 2018 (ASEAN-UP, 2019; E-Trade for All, 2018), the digital economy also adds to total trade. This economic expansion is intrinsically related to the ease with which Southeast Asians may connect to the internet.

Singapore leads the way in Southeast Asia, with 82 percent of its population having internet connection. Meanwhile, approximately 70 percent of Malaysians, Thais, Bruneians, Indonesians, and Filipinos have convenient access to the Internet (ASEAN-UP, 2019; Chang, 2017).

China regards ASEAN as a strategic partner, with many forms of collaboration. Because of its developing economy, China is one of ASEAN's strategic partners. One of the organisation's partnerships is ASEAN Plus, a strategic partnership cooperation plan comprising entities from beyond Southeast Asia such as China, Japan, South Korea, the United States, and India (Feraru, 2016). Several ASEAN countries, including Indonesia, Malaysia, and Singapore, are China's partners in establishing Belt Road Initiative projects (Ramadhan, 2018). According to He 2021, ASEAN and China account for more than half of entire global value chain commerce. Furthermore, the establishment of the 2015 ASEAN Economic Community urges China to contribute more to the economic expansion of Southeast Asia through the China-ASEAN Free Trade Agreement (CAFTA). Despite the fact that this cooperative plan was formed in 2000, both sides pushed for it to be more effective in 2015. One of the indicators is the decrease of trade tariffs. As a result, since 2010, 90 percent of ASEAN and China's trade goods have been tariff-free (Bi, 2021). Aside from economic collaboration, ASEAN and China work together on security issues. ASEAN utilises an ASEAN Plus Three policy at venues such as the ASEAN Defence Ministerial Meeting (ADMM), in which it asks China to collaborate in countering non-traditional threats such as drugs, piracy, human trafficking, and health (Wibisono, 2017). Furthermore, by implementing a South China Sea Code of Conduct, ASEAN involves China in the creation of a peaceful dispute settlement (Yang et al., 2022).

2. Cybersecurity Issues in Southeast Asia

ASEAN, as a vital partner of China, is still grappling with complicated cybersecurity challenges. First, ASEAN has urged its regional member countries to execute the 2015 ASEAN Economic Community by combining economic pillars with technical breakthroughs. One of the indicators is the creation of the ASEAN ICT Masterplan 2012 to create a technological cooperation framework to promote AEC 2015. The ASEAN technological cooperation framework, on the other hand, has yet to be systematically developed. What is the impact of technology? In addition to being a driver of economic growth, technology brings novel threats that may jeopardise ASEAN interests. This is a cyber threat that originated in cyberspace. Dunn-Cavelty categorises cyber threats as cybercrime, cyberterrorism, and cyberwar (Dunn-Cavelty, 2010). Regrettably, the organisation does not yet have ASEAN-level principles or cooperation agreements in place to combat cyber risks. Despite its agreements and multiple high-level discussions, ASEAN has only released a joint statement stating that cyber threats must be reduced (ASEAN, 2021c). ASEAN-level cybersecurity governance is one-of-a-kind. Southeast Asia's business processes are heavily reliant on technology.

Unfortunately, ASEAN, unlike other non-traditional dangers, is still looking for an appropriate structure to address cyber threats. ASEAN still requires a uniform mechanism, guide, or collaboration structure to mitigate these non-traditional dangers. ASEAN already has a framework of cooperation in place to combat terrorism, drugs, and people trafficking. To combat non-traditional dangers like as terrorism, ASEAN, for example, has a strategy known as the ASEAN Convention on Counter-Terrorism. The strategy governs counter-terrorism work methods, mainly those involving finance, money laundering, and collaboration in politics, security, and law (Sudirman & Sari, 2017). The ASEAN Convention against Trafficking in Persons, Particularly Women and Children (ACTIP) already has a cooperation framework in place to combat human and women trafficking. The mechanism even determines how ASEAN operates in the corridor Regional Consultation Process (RCP) on the framework for resolving human trafficking in accordance with the interests of ASEAN member nations (Yazid & Septiyana, 2019). In terms of drug abolition, ASEAN member states signed the Joint Declaration for a Drug-Free ASEAN in 1998 (Mok, 2020). The declaration was subsequently bolstered by the addition of China as a strategic partner through the implementation of programmes known as the ASEAN-China Cooperative Operations in Response to Dangerous Drugs (ACCORD). Through this collaboration, ASEAN and China are dedicated to eradicate drug trafficking, notably in the Golden Triangle, Laos, Cambodia, and Myanmar (Harper & Tempra, 2020). Given the phenomena of non-traditional risks outlined above, ASEAN still requires an integrated coordination structure for reducing cyber threats. The economic interests of ASEAN are heavily reliant on information technology. ASEAN's economic growth will suffer if it does not handle the cyber threat.

3. China Cybersecurity Overview

China is one of the developed countries in the field of cyber security, according to the International Telecommunication Union's (ITU) 2018 report. With 0.82 points, China ranks sixth in the Asia Pacific region and 27th overall in terms of cyber security maturity (ITU, 2018). China has deliberately focused on specific cyber security challenges, such as protecting key infrastructure from cyber assaults. To defend its cyber environment, China focuses independently on two contexts: network security and access control (Cai, 2015). China deploys The Great Firewall to secure cyber traffic entering its territory in terms of network security. The Great Firewall's aim is to protect its cyber environment from various cyberspace threats (Ramadhan, 2021). This policy was established to match with China's objective to maintain its independence in Internet administration, in addition to protecting the security of their cyber environment. What is China's official view on internet governance? In a speech delivered by President Xi Jinping in 2014 at the World Internet Conference 2014 in Wuzhen, China, the Chinese government emphasises the importance of cyber sovereignty. In his speech, President Xi Jinping stressed that each country has the power to manage cyber regulations. As a result, each country is bound to respect the development and governance policies of the other. According to President Xi Jinping, there is no national security without cyber security. Nonetheless, the Chinese government aspires to bolster its cyber capabilities while fostering secure cyberspace and upholding national sovereignty (Miao et al., 2020).

As a result, China's cyber policy is defensive rather than offensive. What is the reason for this? Because the major purpose of the Chinese government's Cyberspace Administration of China is to protect its critical infrastructure. To safeguard the safety of essential infrastructure, the Chinese government seeks economic, administrative, scientific, technological, legal, diplomatic, and military means (Jiang, 2019). The Chinese government thinks that it is the role of the state to safeguard cultural values that form the foundation of people's lives. One of the functions of the state in protecting its internet is to ensure that Chinese society's values are not damaged by external values (Cho & Chung, 2017). In terms of cybersecurity policy, the Chinese government is pretty well-established in seeing cybersecurity challenges similarly to its East Asian neighbours, especially South Korea and Japan. The Chinese government oversees and defends cyberspace through the Cyberspace Administration of China. The Chinese government's principal goal in defending its cyberspace is data protection, not just essential infrastructure (Belli, 2021; Jiang, 2019). The Chinese government considers information and data as precious commodities that must be better protected and managed by the state. China's National People's Congress passed the Personal Information Protection Law (PIPL) in January 2021. The law controls the implementation of data protection systems to satisfy the needs of Chinese enterprises and organisations. Meanwhile, in June 2021, the Chinese government enacted the Data Security Law (DSL), which categorises data security into three categories: essential, state core, and sensitive data. Article 21 of the DSL regulations requires every industry and organisation to categorise data types depending on its categorisation (Belli, 2021).

4. Challenges and China’s Interest in Southeast Asia

Southeast Asia as a whole is very exposed to cybercrime threats. The Cyber Security Agency of Singapore (CSA), Singapore's government agency, has provided data on cybercrime occurrences that happened in 2021. Singapore had 137 ransomware cases, marking a 54 percent rise. In terms of malware incidents, Singapore's CSA discovered 3,300 Singapore-based servers compromised with malware (CSA Singapore, 2022). Trend Micro, a worldwide technology company, has released information on cybercrime incidents in Indonesia. In 2021, Trend Micro examined 3,600 Indonesian firms. Around 81 percent of all businesses acknowledge the possibility of a data breach incident occurring. Approximately 61 percent of firms have reported a single data breach occurrence. In addition, hackers got Covid-19 medical data from the Indonesia Ministry of Health in 2021 (Chandra, 2021).

On the one hand, cybercrime cases in Malaysia have climbed dramatically. According to Malaysian Statistics Department data, cyber crime cases in Malaysia would rise from 283 to 400 by 2021. In Malaysia, the percentage of cybercrime climbed by 15.3 percent in one year (DOSM, 2022). With an average of 62 occurrences per year (STATISTA, 2022), ransomware remains Malaysia's most common case. In terms of the

frequency of ransomware assaults, the Philippines ranks third in the globe. Ransomware attacks cost the Philippines' businesses $1.6 million in 2021. Since 2020, this figure has more than doubled to USD 812,360 (SOPHOS, 2022). The most major challenge for China in building a cybersecurity cooperation framework with ASEAN is not merely addressing malware assaults or computer viruses. In-depth, China's most difficult problem is determining how to collaborate with ASEAN to close the Southeast Asian region's technology divide. Southeast Asia has a very substantial technology gap, according to data collected by the Portulans Institute for its report Network Readiness 2022. The report measures at least four indicators: technology, human resources, governance, and impact. The research examines 131 countries on six continents' readiness to create technology infrastructure. Singapore, according to the Portulans Institute, is the world's second best prepared country for technology adoption and development. Malaysia (36), Thailand (46), Indonesia (59), Vietnam (62), the Philippines (71), Laos (102) and Cambodia (104) were the countries that came next. In the meantime, China ranks 23rd in terms of technological readiness. Singapore ranks second as a result of its constant technology investment. Singapore is also constantly developing its human resource capabilities. Singapore has a long history of governance and robust cyber policies. Finally, Singapore makes good use of its technology skills, which are felt in the social, economic, and political sectors (Dutta & Lanvin, 2022).

How does this technical readiness stack up against other ASEAN strategic partners like Indonesia, Malaysia, and China? Indonesia, in particular, is dedicated to investing in technology to support economic growth. Indonesia's technology investment in the technology industry, in particular, focuses on cutting-edge technology, software development, and bandwidth Internet enhancements. In terms of individual digital technology adoption, Indonesia has proved its strength. On the other hand, Malaysia is ranked 36th in technological advancement, 39th in impact, 36th in human capital development, and 40th in governance. Malaysia is the world leader in technological product exports. Due to investment in telecommunications services and the pace of technology adoption in the business sector and individuals, the Chinese government is rated 23rd in the world (Dutta & Lanvin, 2022). China's most challenging problem, based on the preceding instances, is promoting a strategic alliance with ASEAN. Furthermore, ASEAN-China collaboration must bridge the technical barrier in the Southeast Asian region. China must recognise that the region's main difficulty is a lack of cyber security rules when expanding cyber security cooperation with ASEAN. The absence of regulation is intrinsically tied to the diverse decision-making systems when contrasted to similar organisations such as the European Union. ASEAN has a consensus-based decision-making framework. This process is distinct from that of the European Union, which functions on the principle of one person, one vote (Feraru, 2016). Prior to the approval of the 2008 ASEAN Charter, this consensus procedure was an impediment to obtaining a stable agreement in the Southeast Asian area. It is believed that the consensus procedure is too flexible to provide a decision. Following the passage of the 2008 ASEAN Charter, ASEAN developed the ASEAN minus X consensus method and the ASEAN X+2 formulae. ASEAN minus X denotes that nations can adopt ASEAN-agreed-upon policies based on their readiness and domestic circumstances. Whereas ASEAN X+2 refers to an agreement reached at the ASEAN level by more than two countries (Ramadhan, 2022).

Nonetheless, the ASEAN standard requires that no one be left behind. When an agreement is reached, the country that is ready to implement the policy must assist other member countries in order for them not to fall behind (Khoo, 2015). According to the author, one of the reasons for the lack of an ASEAN-level cybersecurity consensus is the unusually vast technology disparity. This gap is hampering cybersecurity consensus since technology readiness and maturity are continual processes. The Chinese government must recognise that the Southeast Asian region is a crucial strategic sector for its economic progress. China-ASEAN investment topped $340 billion in 2022 in July. This figure will rise in accordance with the development of the two parties' worldwide commercial relations (Global Times, 2022). Another important factor is that China is significantly investing in artificial intelligence. It has chosen Southeast Asia one of its investment goals, according to a research from the Centre of Security and Emerging Technology (CSET). The creation of this artificial intelligence began in 2016 with the passage of the 2016 Innovation-Driven creation Strategy Policy. This programme urged the Chinese government to acquire or invest in a wide range of firms. The policy grew into the 2017 State Council's New Generation Artificial Intelligence Development Plan, establishing China as a leading artificial intelligence powerhouse. China is aiming to construct a framework for Digital Silk Road economic

cooperation, with ASEAN as a strategic partner, in a shift from its AI development agenda. The Chinese government is investing $2.4 billion in artificial intelligence development in Singapore (Luong et al., 2022).

Meanwhile, China has committed at least $38 million to the development of artificial intelligence in the e-commerce sector in Indonesia. China, on the other hand, has committed $1.6 million in artificial intelligence research in drone technology. With a maximum of $1.6 million, Chinese investment in Vietnam is quite small. Meanwhile, with $53 million, the United States was the greatest investor in the Philippines. Similarly, the US government supported around 500 Thai startups. Despite this, the Chinese technology company has nine ASEAN branch offices. These technology businesses include Alibaba, Baidu, BeiDou, ByteDance, Dahua, Hikvision, Huawei, iFlytek, Inspur, Megvii, Meiya Pico, Ping An Technology, Tencent, and ZTE (Luong et al., 2022). The lack of cyber regulation might transform a challenge into a threat when it comes to China's technology investment in Southeast Asia. The lack of cyber regulation may jeopardise future Chinese technological investment growth. Cyber threats as previously noted, might appear as cybercrime, cyberterrorism, or cyberwar (Dunn-Cavelty, 2010). If there are no regulations or rules in place, it will be impossible for the state to overcome and reduce conflicts in cyberspace. ASEAN will struggle to prevent internal and external cyber warfare in the area due to a lack of cyber security administration. China's investment in Southeast Asia may be jeopardised if these three challenges are not addressed. As one of ASEAN's important partners, China must be ready to respond on an equal footing to these issues.

5. Room for Collaboration

Aside from Southeast Asia's varied cybersecurity challenges, the author sees a lot of space for improvement and capacity growth. One example of what can be done is the exchange of intelligence information between the ASEAN and Chinese governments. When assembling China-ASEAN strategic cooperation, we must take into account the characteristics of the ASEAN interaction pattern. Furthermore, the ASEAN member countries tend to be oriented towards the Westphalian structure. They preserve sovereignty and resist governmental intervention (Caballero-Anthony & Gong, 2021). This ideal is incorporated in the Treaty of Amity and Cooperation, which acts as the ASEAN organisations' moral compass. In essence, ASEAN member countries continue to cooperate with one another. They do, however, oppose non-interventionist initiatives that jeopardise their sovereignty In general, ASEAN prioritises the non-intervention standard, which is based on Article 2 of the Treaty of Amity and Cooperation in Southeast Asia, which was signed on February 24, 1976. According to the agreement's provisions, each ASEAN member country is obligated to respect each nation's freedom, sovereignty, equality, territorial unity, and national identity (Ramadhani & Mabrubah, 2021). Furthermore, ASEAN member nations have the right to control their country's administration without foreign influence and to promote the principle of non-intervention inside the internal organisation (Manopo & Sari, 2015). This attribute is congruent with China's non-interventionist foreign policy strategy, which respects each country's sovereignty. The idea of non-intervention is shared by ASEAN and China. China grounds its non-intervention principle on the 1954 Five Principles of Peaceful Coexistence norms. This norm explains how the Chinese government conducts in a way that respects the country's sovereignty and integrity, non-aggression, not interfering in a country's domestic affairs, equality and common interests, and peaceful coexistence (Mumuni, 2017).

Cooperation among intelligence agencies in cybersecurity is a concrete step that both players can take. What is the reason for this? The author believes that the problem of cyber security cannot be handled on its own. When national borders become ambiguous, internet becomes a no-man's land. Because of the vastness of internet, the problem of national borders is rendered moot. As a result, it covers every element of existence. Because cyberspace has no borders, cyber security coordination is a strategic step towards reducing non-traditional dangers. A pragmatic approach that encourages self-help is applicable to cybersecurity challenges. Every nation has the right to invest in technological progress.

However, each country can communicate information on cyber threat issues through bilateral cooperation structures. Of course, they cannot handle all of these difficulties on their own (Ramadhan, 2017). ASEAN must become the protector of its member countries' cyber security. According to the core neoliberal institutionalist concept, international organisations must be formed to serve common interests. When dealing with cyber

dangers, keep in mind that threats in cyberspace are asymmetric and proximal. It is difficult to detect the threat because it is anonymous. ASEAN, as Southeast Asia's sole regional organisation, must adopt information-sharing standards to address all cyber threats. Cyber dangers are not something that a country can deal with on its own. This threat requires cooperation among ASEAN member countries and their strategic allies. When one member country is paralysed by an attack, the effect extends to other countries. It promotes information sharing between ASEAN member countries and the Chinese government in order to address cyber threats collectively (Ramadhan, 2019).

Another area where ASEAN and China may engage is in the development of technological human resource capabilities. According to the author, improving human resource capability is crucial for three reasons. To begin with, the extent of the cyber environment is transnational, dissolving national boundaries. All government operations, however, are now connected with information technology platforms. All of these complexity, as well as digital innovation, necessitate collaboration in human capacity building. Second, ASEAN's economic progress has been intertwined with technological advancements, fueling the expansion of Southeast Asia's digital economy. Empirical evidence suggests that technology can help to stimulate economic growth. For example, data from 2017 revealed that the digital economy contributed 6.9 percent of United States' GDP growth, amounting to 1.4 trillion dollars (Solomon & van Klyton, 2020). Technology fundamentally transforms public communication medium, digitally transforms corporate businesses, and enables governments to organise digital-based government (Dhaoui, 2022).

Third, cybersecurity governance cannot be accomplished just through the participation of states; other players, such as industry, must be included (Watanabe, 2020). These three points can be met if ASEAN countries concentrate on strengthening human resource capability to facilitate regional collaboration. Human resource capacity development points are also included in the first dimension of the ASEAN Cybersecurity Cooperation Strategy 2021-2025, which is related to ASEAN's readiness to build cyber cooperation both formally and informally by involving the Southeast Asian CERT community (ASEAN, 2021b). Building human resource capacity can be done in a variety of ways, including independently, bilaterally, or multilaterally. Japan and Thailand, for example, participated in cyber cooperation in 2015 through a knowledge transfer mechanism and a workshop on human resource capability development (Noor, 2015).

Singapore's strategy to bridge the technical divide by sponsoring Singapore Cybersecurity Week 2016 is another instance in point. Singapore, as a country well-versed in cyber security, is interested in the programme to safeguard the digital economy's stability in Southeast Asia. The activities of Singapore Cybersecurity Week 2016 welcome other ASEAN countries to share knowledge and promote best practises in dealing with cyber threats. Singapore is interested in these activities in general due to the country's reliance on the digital economy (Anshori & Ramadhan, 2019). Singapore is a driving force in the development of cyber security capabilities, with three goals in mind: organising training and research, training CERT human resources in ASEAN countries, and fostering information exchange across the CERT community (CCDCOE, 2022). Malaysia is also enhancing cybersecurity collaboration through incorporating multilateral forums such as The Asia-Pacific Economic Cooperation (APEC), the British Commonwealth, the Organisation of Islamic Conference (OIC), the Global Forum on Cyber Expertise (GFCE), and the Asia-Pacific Computer Emergency Response Teams (APCERT) (National Security Council, 2020). Thailand also pioneered ASEAN-Japan collaboration by creating the ASEAN-Japan Cybersecurity Capacity Building Centre. The collaboration aims to develop cybersecurity capacity by training IT operators in key infrastructure, boosting cybersecurity cooperation among government agencies, raising awareness of information security, protecting personal data, and encouraging information sharing (ASEAN, 2019). Another example is Vietnam and Japan's collaboration in 2021 through the Vietnam-Japan Capacity Building for Cybersecurity. Since 2014, Vietnam has experienced losses as a result of distributed denial of service (DDoS) assaults that have left the government's information technology system ineffective. Through bilateral collaboration with Japan, the country aids Vietnam in building cyber security governance, cyber threat mitigation training, and strengthening the country's cyber resilience (JICA, 2021). Meanwhile, the Indonesian government and the United States reached an agreement to combat cyber terrorism. Through the BSSN (Indonesia Cyber Agency), the Indonesian government is working with the US government to develop cyber threat mitigation capabilities, notably in the context of terrorism (Putra, 2022). The Philippines increased

cooperation and coordination with the International Telecommunication Union (ITU) to improve cybersecurity capacity in terms of hardware standardisation and human resource development through technical seminars and vocational activities (Cabanlong & Macalinao, 2022).

Brunei participates in the ASEAN Network Security Council and APCERT to train cyber security personnel (Reksoprodjo & Zaelani, 2018). Brunei, on the other hand, implements the Brunei National Digital Strategy 2016-2020 policies at the school level through the deployment of a cybersecurity curriculum in conjunction with Microsoft. Finally, the Cambodian government and Japan decided to work together on the Project for Improvement of Cyber Resilience, which intends to improve cyber security capabilities, notably in the government sector (JICA, 2022). Only Laos and Myanmar have yet to begin cybersecurity capacity-building projects in their respective countries, according to the data shown above. ASEAN capacity building should involve a greater emphasis on vulnerability in Laos and Myanmar. The authors argue that ASEAN's principal focus in conducting sustainable capacity-building programmes is to close this technological gap. Implementing cybersecurity governance and combating cybercrime in Southeast Asia would become even more challenging if ASEAN does not solve this vulnerability gap. The study revealed that eight of the ten ASEAN countries have policies or strategies in place to build cybersecurity human resource capacities. As a result, ASEAN should capitalise on this momentum by encouraging human resource capacity-building programmes via pre-existing cooperation mechanisms such as ASEAN-Japan Capacity Building or capacity-building programmes initiated by ASEAN countries such as Singapore Cybersecurity Week (Anshori & Ramadhan, 2019; Watanabe, 2020).

ASEAN countries, on the other hand, must improve their cyber security capabilities as part of their overall national plan. According to the ASEAN Cybersecurity Cooperation Strategy 2020-2025 papers, every country must increase its cyber resilience as an indicator driving economic growth in Southeast Asia in the first dimension number 31 (ASEAN, 2021b). Building human resource capacity in cyber security will be beneficial if ASEAN member countries strengthen their technology skills bilaterally and multilaterally. One crucial aspect to emphasise is that ASEAN-China collaboration is still limited to a single statement. This declaration is contained in the ASEAN-China Joint declaration on Cooperation in Support of the ASEAN Comprehensive Recovery Framework. In the statement, ASEAN and China pledged to increasing digital capabilities in human resources, particularly in small and medium-sized firms. In order to develop cyberspace governance, ASEAN and China are aiming to establish an ASEAN-China Cyber Dialogue (ASEAN, 2021a). ASEAN and China must take advantage of every chance to strengthen their digital human resource skills. In addition to establishing a framework for ASEAN-China collaboration through human resource capacity building, the two sides can begin collaborating on technology transfer. The Agreement for Scientific and Technological collaboration between the European Community and the Government of the People's Republic of China, for example, is a technological collaboration agreement between China and the European Union. Through this technical cooperation, China and the European Union are dedicated to strengthening technology research and development through practitioner exchanges, collaborative research collaborations, and the interchange of technological gadgets and materials (EU, 2022). What about the ASEAN bloc? ASEAN and China have a framework for technology cooperation under the China-ASEAN Technology Transfer Centre (CATTC) agreement. The Chinese Ministry of Science and Technology and the Guangxi Autonomous Province began the collaboration to promote the integration of technology transfer, research collaboration, seminars, symposiums, business incubators, and human resource training in technology. 70 local and international technology transfer symposium activities, 1900 docking projects, and 491 cooperation agreements were launched successfully. So far, pharmaceuticals, medical devices, fisheries, and smart cities have dominated CATTC technology transfer (Zhou, 2020).The author believes that ASEAN and China may work on cybersecurity, particularly on technology transfer, through CATTC.

Cyber security, according to the author, is a spectrum of fields that must emphasise features of collaboration and cooperation. Asymmetric and anonymous non-traditional threats include cybercrime and cyberterrorism. To counter this threat, ASEAN and China must work together to create a technology transfer process that benefits both parties. Through symposiums and seminars, CATTC can become a venue for state actors, industry, and academia to share ideas in order to build a technology transfer mechanism in the field of cyber security. Aside from serving as a forum for idea exchange, CATTC can aid to bridge the technical divide. The author argues that future cybersecurity collaboration between ASEAN and China has enormous potential. Aside from being major

allies in Southeast Asia, ASEAN and China already have a number of agreements in place that can be utilised to maximise collaboration in cyber security. Southeast Asia has grown into a digital economy growth region. China has also made significant investments in artificial intelligence in Southeast Asia. As a result, in addition to increasing human resource capability, China can strengthen its relationship with ASEAN by cooperating on technology transfer to counter cyber threats.

6. Conclusions

Given the Southeast Asian region's cybersecurity phenomenon, the author suggests that China and ASEAN must enhance each other through strategic collaboration centred on cybersecurity. China, as one of the most technologically advanced countries, may be a strategic partner in building inclusive cybersecurity governance that all parties can execute. Furthermore, China may work with ASEAN to strengthen human resource capabilities in the technology industry. When employed by skilled humans, technology, regardless of its sophistication, is useful. China can close this gap by strengthening collaboration in human resource capability upgrading. Finally, ASEAN and China can strengthen cybersecurity technology transfer cooperation through the CATTC platform. Aside from improving the capabilities of its human resources, technology transfer intends to mutually refresh China's and ASEAN's technological capacities.

Conflict of Interest: The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding: The authors received no financial support for the research, authorship and/or publication of this article.

Informed Consent Statement/Ethics approval: Not applicable.

References

Anshori, M. F., & Ramadhan, R. A. (2019). Singapore's Cyber Security Interest in Southeast Asia through Singapore International Cyber Week. *Padjadjaran Journal of International Relations*, *1*(1), 39. https://doi.org/10.24198/padjir.v1i1.21591

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

ASEAN. (2019). *The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCC BC)*. https://asean2019.go.th/en/infographic/the-asean-japan-cybersecurity-capacity-building-centre-ajcc-bc/

ASEAN. (2021a). *ASEAN-China Joint Statement on Cooperation in Support of The Comprehensive Recovery Network*. https://asean.org/wp-content/uploads/2021/10/64.-Final-ASEAN-China-Joint-Statement-on-Cooperation-in-Support-of-ACRF.pdf

ASEAN. (2021b). *ASEAN Cybersecurity Cooperation Strategy*.

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

Belli, L. (2021). Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *The African Journal of Information and Communication*, *28*(28), 1–14. https://doi.org/10.23962/10539/32208

Bi, S. (2021). Cooperation between China and ASEAN under the building of ASEAN Economic Community. *Journal of Contemporary East Asia Studies*, *10*(1), 83–107. https://doi.org/10.1080/24761028.2021.1888410

Caballero-Anthony, M., & Gong, L. (2021). Security Governance in East Asia and China's Response to COVID-19. *Fudan Journal of the Humanities and Social Sciences*, *14*(2), 153–172. https://doi.org/10.1007/s40647-020-00312-4

Cabanlong, A., & Macalinao, G. (2022). *Capacity building: Creating the Philippines Cybersecurity Workforce*. Manila Bulletin. https://mb.com.ph/2022/03/15/capacity-building-creating-the-philippines-cybersecurity-workforce/

Cai, C. (2015). Cybersecurity in the Chinese context: Changing concepts, vital interests, and prospects for

cooperation. *China Quarterly of International Strategic Studies*, *1*(3), 471–496. https://doi.org/10.1142/S2377740015500189

CCDCOE. (2022). *ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone*. https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/

Chandra, G. N. (2021). *Indonesia at Highest Risk Level of Cyber Threat: TrendMicro*. Jakarta Globe. https://jakartaglobe.id/tech/indonesia-at-highest-risk-level-of-cyber-threat-trendmicro

Chang, L. (2017). *Cyber Crime and Cybersecurity in ASEAN*. https://www.researchgate.net/publication/318474107

Cho, Y., & Chung, J. (2017). Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity. *Pacific Focus*, *32*(2), 290–314. https://doi.org/10.1111/pafo.12096

CSA Singapore. (2022). *Ransomware and phishing attacks continued to threaten Singapore organisations and individuals in 2021*. https://www.csa.gov.sg/News/Press-Releases/ransomware-and-phishing-attacks-continued-to-threaten-singapore-organisations-and-individuals-in-2021

Dhaoui, I. (2022). E-Government for Sustainable Development: Evidence from MENA Countries. *Journal of the Knowledge Economy*, *13*(3), 2070–2099. https://doi.org/10.1007/s13132-021-00791-0

DOSM. (2022). *Crime Statistic, Malaysia, 2022*. Department of Statistic Malaysia. https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=455&bul_id=RnBiQjA1VHhmelZRVCszS3RiRXpNQT09&menu_id=U3VPMldoYUxzVzFaYmNkWXZteGduZz09#:~:text=Fraud cases were the highest,money cases (204 cases).

Dunn-Cavelty, M. (2010). Cyber Threats. In M. Dunn-Cavelty & V. Mauer (Eds.), *The Routledge Handbook of Security Studies*. Rouledge.

Dutta, S., & Lanvin, B. (2022). *The Network Readiness 2022*.

E-Trade for All. (2018). *ASEAN: E-Commerce Set to Dominate the Region in 2019*. https://etradeforall.org/asean-e-commerce-set-to-dominate-the-region-in-2019/

EU. (2022). *Scientific and technological cooperation between the EU and China*. https://eur-lex.europa.eu/EN/legal-content/summary/scientific-and-technological-cooperation-between-the-eu-and-china.html

Feraru, A. S. (2016). ASEAN Decision-Making Process: Before and after the ASEAN Charter. *Asian Development Policy Review*, *4*(1), 26–41. https://doi.org/10.18488/journal.107/2016.4.1/107.1.26.41

Global Times. (2022). *China-ASEAN two-way investment exceeds $340b by July amid active cooperation*. https://www.globaltimes.cn/page/202208/1274128.shtml

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

ITU. (2018). *Global Cybersecurity Index (GCI) 2018*.

Jiang, T. (2019). From Offense Dominance to Deterrence : China 's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Reviews*, *1*(2), 1–23. https://doi.org/10.1142/S2630531319500021

JICA. (2021). *Project on Capacity Building for Cyber Security in Vietnam*. https://www.jica.go.jp/project/english/vietnam/052/outline/index.html

JICA. (2022). *Signing of Record of Discussions on Technical Cooperation Project with Cambodia: Project for Improvement of Cyber Resilience*. https://www.jica.go.jp/english/news/press/2022/20221205_41.html

Khoo, N. (2015). The ASEAN Security Community: A Misplaced Consensus1. *Journal of Asian Security and International Affairs*, *2*(2), 180–199. https://doi.org/10.1177/2347797015586126

Luong, N., Lee, C., & Konaev, M. (2022). *Chinese AI Investment and Commercial Activity in Southeast Asia*.

Manopo, B. Y. W., & Sari, D. A. A. (2015). Asean Regional Forum: Realizing Regional Cyber Security in Asean Region. *Belli Ac Pacis*, *1*(1), 44–51. https://jurnal.uns.ac.id/belli/article/view/27366

Miao, W., Xu, J., & Zhu, H. (2020). From Technological Issue to Military-Diplomatic Affairs: Analysis of China's Official Cybersecurity Discourse (1994-2016). In J. Hunsinger, M. M. Allen, & L. Klastrup (Eds.), *Second International Handbook of Internet Research* (pp. 431–444). Springer.

Mok, S. Y. (2020). ASEAN and Transnational Crime: Gains and Challenges in Tackling Drug Trafficking. *Wimaya*, *1*(01), 31–38. https://doi.org/10.33005/wimaya.v1i01.13

Mumuni, S. M. (2017). China's non-intervention policy in Africa : Principle versus pragmatism. *African Journal of Political Science and International Relations*, *11*(9), 258–273. https://doi.org/10.5897/AJPSIR2017.0999

National Security Council. (2020). *Malaysia Cyber Security Strategy 2020-2024*.

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

Noor, E. (2015). 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* (pp. 150–163). JCIE.

Putra, B. A. (2022). Cyber Cooperation between Indonesia and the United States in Addressing the Threat of

Cyberterrorism in Indonesia. *International Journal of Multicultural and Multireligious Understanding*, *9*(10), 22–33.

Ramadhan, I. (2017). The Role of International Organization in Combating Cyber Threat. *Populis*, *2*(4), 495–508.

Ramadhan, I. (2018). China's Belt Road Initiative: In The Perspective of Classical Geopolitics Theory. *Intermestic: Journal of International Studies*, *2*(2), 139. https://doi.org/10.24198/intermestic.v2n2.3

Ramadhan, I. (2019). Cybersecurity Strategy in Southeast Asia: Self-help or Multilateralism?. *Jurnal Asia Pacific Studies*, *3*(1). https://doi.org/dx.doi.org/10.33541/japs.v3i1.1081

Ramadhan, I. (2021). *The Implication of Cyberspace Towards State Geopolitics*. *3*(2), 161–184. http://journal.uinsgd.ac.id/index.php/politicon

Ramadhan, I. (2022). ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia. In I. Kusumawardhana, E. Puspitawati, & R. Isnarti (Eds.), *Proceedings of the 1st International Conference on Contemporary Risk Studies (ICONIC-RS)* (pp. 1–15). EAI. https://doi.org/10.4108/eai.31-3-2022.2320684

Ramadhani, Z., & Mabrubah, M. (2021). The Influence of ASEAN's Non-intervention Principle through Indonesia's Negotiation for Managing Myanmar Coup Conflict. *Global Political Studies Journal*, *5*(2), 126–142. https://doi.org/10.34010/gpsjournal.v5i2.5952

Reksoprodjo, Y., & Zaelani, H. (2018). ASEAN Cyber Security Capacity Building in ASEAN: A Comparative Analysis in Brunei and Indonesia. *Jurnal Prodi Perang Asimetris*, *4*(1), 77–92.

Solomon, E. M., & van Klyton, A. (2020). The impact of digital technology usage on economic growth in Africa. *Utilities Policy*, *67*(January).

SOPHOS. (2022). *The State of Ransomware 2022*. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

STATISTA. (2022). *Number of ransomware incidents reported to CyberSecurity Malaysia through MyCERT* in 2018, by type of variants*. https://www.statista.com/statistics/1043328/malaysia-ransomware-incidents-by-variants/

Sudirman, A., & Sari, D. S. (2017). Building Regional Security in ASEAN for Combating The Threat of Terrorism. *Jurnal Wacana Politik*, *2*(1), 22–32. https://doi.org/10.24198/jwp.v2i1.11276

Watanabe, S. (2020). Strategic Analysis of Capacity Building for the Cyber Security of the United States in Asia. *Jurnal Asia Pacific Studies*, *4*(2), 100–111. https://doi.org/10.33541/japs.v4i2.2800

Wibisono, A. A. (2017). ASEAN-China Non-Traditional Security Cooperation and the Inescapability of the Politics of Security. *Jurnal GLobal & Strategis*, *11*(1), 39–54.

Yang, Z., Chandra, S. D., & Zhao, Y. (2022). ASEAN , China and South China Sea : Alternative approach for security cooperation. *Bussecon Review of Social Sciences*, *4*(2), 25–31.

Yazid, S., & Septiyana, I. (2019). The Prospect of ASEAN Migration Governance. *Journal of Indonesian Social Sciences and Humanities*, *9*(2), 95–112. https://doi.org/10.14203/jissh.v9i2.155

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

Zhou, X. (2020). *Case study from China on CATTC - China-ASEAN Technology Transfer Center*. https://stip.oecd.org/assets/TKKT/CaseStudies/38.pdf