©2024 Indonesian Journal of International Relations
Vol. 8, No. 2, pp. 414-432.
DOI: 10.32787/ijir.v8i2.590

ASEAN'S PREPAREDNESS AND RESPONSE AGAINST HYBRID THREAT IN CYBERSPACE

Yosua Saut Marulitua Gultom
Department of International Relations
Universitas Pembangunan Nasional Veteran Jakarta
Jakarta, Indonesia
Yosuagultom187@gmail.com

INFO ARTIKEL
Article History

Received
29 June 2024

Revised
3 August 2024

Accepted
4 August 2024

Kata kunci:
ancaman hibrid; ancaman siber; ASEAN; *keamanan regional; Tiongkok*

Keywords*:*
cyber threat; hybrid threat; ASEAN; regional security; China;

Abstrak
Penelitian ini mengkaji kesiapan dan respons ASEAN menghadapi ancaman di ruang siber. ASEAN sendiri merupakan kawasan yang memiliki pertumbuhan pengguna internet dan ekonomi yang berkembang. Sayangnya, pertahanan siber ASEAN dinilai rendah. Penelitian ini menggunakan konsep ancaman hibrida oleh Hoffman yang menyatakan bahwa konflik/perang di masa depan menciptakan strategi hibrid, di mana cara-cara konvensional dan non-konvensional disatukan untuk melihat kerentanan tersebut. Menggunakan studi deskriptif menggunakan data primer dan sekunder berupa dokumen resmi, artikel jurnal, berita, dan sumber internet. Artikel ini menemukan bahwa kebangkitan Tiongkok di bidang siber, serta aktivitas serangan yang pernah dilakukannya baik secara langsung maupun tidak langsung memberikan persepsi ancaman yang kuat bagi kawasan ASEAN. Untuk itu, artikel ini menyimpulkan bahwa ASEAN harus menggiatkan kolaborasi di dalam kawasan dan dengan mitra global sembari membangun strategi pertahanan siber yang komprehensif, termasuk potensi tentara siber di seluruh kawasan.

Abstract
This research examines ASEAN's readiness and response to threats in cyberspace. ASEAN is a region with growing internet users and a thriving economy. Unfortunately, ASEAN's cyber defense is considered low. This research uses the concept of hybrid threats by Hoffman which states that future conflicts/war create hybrid strategies, where conventional and non-conventional means are brought together to see the vulnerability. Using a descriptive study using primary and secondary data in the form of official documents, journal articles, news, and internet sources. This article found that China's rise in the cyber field, as well as the attack activities it has carried out both directly and indirectly, provide a strong threat perception for the ASEAN region. For this reason, this article concludes that ASEAN must intensify collaboration within the region and with global partners while also establishing a comprehensive cyber defense strategy, including a potential for a cyber army across the region.

ISSN: 2548-4109 electronic
ISSN: 2657-165X printed

INTRODUCTION

The world has entered the information age, succeeding the prehistoric, agricultural, and industrial eras. In this age, information is crucial in all aspects of life, becoming a fundamental necessity for both individuals and organizations. Information acts as the lifeblood of the information society, essential for human existence. One of the most significant advancements of this era is the invention of the internet. This technology has revolutionized communication and information access, making it an inseparable part of daily life and causing a profound leap in societal development. However, like all technologies, the internet, as part of the technology, is not value-neutral (Miller, 2021). Its effectiveness depends on its use in accordance with social and personal values, as well as adherence to government regulations designed to protect people from its negative impacts. By carefully managing its use, we can harness the internet's benefits while minimizing potential harm, ensuring that it serves as a positive force in the information age.

Since information and communication technology is used in various aspects of life, both social, economic, legal, organizational, health, education, culture, government, security, defense, and so on, efforts to secure the internet from the bad use of certain individuals are very important and have become a priority issue for all countries in the world (Chotimah, 2019; Ginanjar, 2019, 2022). Directly proportional to the high level of utilization of information and communication technology, the level of risk and threat of misuse of information and communication technology is also getting higher and more complex.

The risks of cyberspace have a profound impact on society. There is significant concern about various threats, such as those posed by hacktivists, criminals, and spies. To safeguard systems, data, and daily life, stakeholders such as users, experts, and governments are continuously striving to enhance cybersecurity measures. However, there is also concern about maintaining the opportunities and freedoms associated with cyberspace, such as freedom of speech and privacy. Unfortunately, increased security often compromises any modern society. Thus, it is crucial for security professionals, including those in the military, to be aware of these competing concerns and work to minimize the negative effects of new security solutions. Balancing the need for security with the preservation of civil liberties is essential to fostering a safe yet free digital environment (Gunneriusson & Ottis, 2013).

Cyberthreats that evolve from the perception of threats in cyberspace have their own volatility. This is generally about anonymity and the difficulty of tracking cybercriminal actors. This special nature makes cyber threats a tool that can be used by certain actors, such as states, in conducting hybrid warfare as well as by non-state actors to hide their activities. Even worse, the special nature of cyber threats will greatly impact countries whose cyber defenses are not yet adequate.

Cyber threats, stemming from the inherent volatility of cyberspace, pose unique challenges due to their anonymity and the difficulty in tracking cybercriminals (Gundur et al., 2021). This distinctive nature of cyber threats allows them to be exploited by various actors, including states engaging in hybrid warfare as well as non-state actors looking to conceal their activities. The ability to operate anonymously and elude detection makes cyber threats a powerful tool in modern conflicts and illicit operations. This is particularly concerning for countries with insufficient cyber defenses, as they are highly vulnerable to such threats. The impact on these nations can be severe, affecting national security, economic stability, and public safety. As cyber threats continue to evolve, it is crucial for all countries to strengthen their cybersecurity measures to protect against these pervasive risks. Developing robust cyber defenses, enhancing international cooperation, and fostering a culture of cybersecurity awareness are essential steps in mitigating the adverse effects of cyber threats. By addressing these challenges proactively, countries can better safeguard their digital infrastructures and ensure a more secure cyberspace for all.

Cyber threats further compound the complexity of hybrid warfare in Southeast Asia. State-sponsored cyber operations, non-state actors' activities, and critical infrastructure vulnerabilities contribute to the multifaceted nature of hybrid threats in the region. Southeast Asian countries navigate a landscape where traditional forms of conflict intertwine with cyber tactics, shaping regional security dynamics.

The concept of hybrid threats is relatively new, introduced by Hoffman in 2007. Research on hybrid threats and wars is still largely theoretical, as indicated by studies conducted by Raugh (2016), Reichborn-Kjennerud and Cullen (2016), and Steingartner and Galinec (2021). Some other studies such as Renz (2016) and Chivvis (2017) tried to provide a practical picture

through Russia's hybrid activities. However, there have been numerous studies discussing Russia's role as a hybrid war actor (Veljovski et al., 2017; Weissmann, 2019). The author in this case wants to look at non-western actors who may also have this capacity, or even already apply the hybrid war paradigm, which in this case the author finds China as a major actor who is active in their hybrid threat projection.

Even so, the study of hybrid warfare whether it takes the case of Russia or China always tends to focus on two things: First is the projection of internal capacity (Saalman, 2021), and second is strategic rivalry with America or NATO (Gaiser, 2022). However, studies that discuss their relationship with ASEAN are rare to none. Therefore, the author argued that there needs to be a study that tries to describe ASEAN's role in this regard. Understanding and addressing cyber threats is integral to comprehending and mitigating hybrid threats in Southeast Asia. The author formulates the question, "How does ASEAN handle the hybrid threat in cyberspace?"

ANALYSIS FRAMEWORK

Hybrid Threat

The concept of hybrid warfare, which later included hybrid threats, was proposed by Frank Hoffman (2007) in his work titled "Conflict in the 21st Century: The Rise of Hybrid Wars." In his initial work, the number of challenges for the state does exist. The challenges were various, including traditional, irregular, terrorist, and disruptive challenges. This diversity of challenges provides a dilemma for policy actors in determining resource allocation scenarios in dealing with existing challenges. However, Hoffman sees that the separation of threat types may no longer be necessary, given that some threat and war patterns are merging and blurring. Conflict will be more of a hybrid combination to target vulnerabilities in the country's defense and security systems, as well as threat perceptions.

The hybrid threat has been a subject of much debate in recent security studies, often centering on Russia's actions in Ukraine (Veljovski et al., 2017; Weissmann, 2019). However, it's essential to recognize that hybridity is not a novel concept exclusive to Eastern Europe. Throughout history, strategies in Asia have exhibited elements of hybrid warfare. Whether observed in security dynamics on the Korean Peninsula, Chinese security practices, or the activities of non-state actors in Southeast Asia, the region's strategic landscape has long displayed characteristics that align with the hybrid

warfare paradigm (Aoi et al., 2018; Hoffman, 2009).

Hybrid threats combine conventional military tactics with non-military methods such as cyberattacks, data theft, disinformation, propaganda, social media manipulation, foreign interference in elections, economic coercion, and lawfare. These tactics aim to weaken governments, erode public trust, and undermine regional security. By creating confusion and complicating decision-making processes, hybrid threats make it challenging for governments to respond effectively. The overarching goal of these strategies is to destabilize societies and achieve political objectives without engaging in full-scale warfare. Through a blend of direct and indirect actions, hybrid threats pose significant risks to national and international stability, targeting both the integrity of state institutions and the cohesion of societies. Addressing these multifaceted challenges requires comprehensive and coordinated efforts across various sectors, including the military, cybersecurity, media, and legal frameworks. Understanding and mitigating the impact of hybrid threats is crucial for maintaining regional security and protecting democratic processes (Talat, 2021).

Hybrid threats involve a blend of state and non-state actors working together or independently to achieve strategic objectives. These threats are characterized by their complexity, making them difficult to identify and counter effectively. They can involve a diverse array of actors, including state entities like governments or military organizations aiming for geopolitical goals, as well as non-state actors such as terrorist groups or criminal organizations pursuing their agendas. The blend of tactics used in hybrid threats allows adversaries to exploit vulnerabilities across multiple domains. Ambiguity is a key element, with adversaries often using proxies or covert operations to obscure their involvement and minimize the risk of retaliation. Hybrid threats are asymmetric, exploiting disparities in power and capabilities between adversaries by targeting vulnerabilities and weaknesses. They are also flexible and adaptive, with adversaries quickly adjusting their tactics and strategies in response to changes in the operational environment, technological advancements, or countermeasures employed by their opponents (Ball, 2023).

RESEARCH METHOD

This research employs a qualitative methodology to comprehensively assess the preparedness of ASEAN countries in facing hybrid threats in the cyber field and the efforts made to address these challenges. The study will use multiple data sources to ensure a well-rounded analysis. Firstly, institutional reports on ASEAN's digital capacity will be reviewed to understand the existing infrastructure, policies, and strategies related to cybersecurity. These reports provide an official perspective on the region's digital readiness and highlight areas of focus for each member country. Secondly, a thorough literature review of journal articles will be conducted to incorporate academic insights and theoretical frameworks. These articles will offer in-depth analyses of cybersecurity issues, hybrid threat dynamics, and proposed solutions. Thirdly, online newspapers and news articles will be analyzed to capture real-time data and case studies of cyber incidents within the ASEAN region. This will help in understanding the practical challenges faced by these countries and their immediate responses. Lastly, other official sources such as government publications, international organization reports, and policy documents will be examined to gather additional context and validate findings from other sources. Data will be analyzed thematically to identify common trends, strengths, and vulnerabilities in ASEAN's approach to cyber threats. The study will synthesize these findings to provide a comprehensive overview of the region's preparedness and the effectiveness of current efforts to tackle hybrid threats in cyberspace.

RESULTS AND DISCUSSIONS

ASEAN and the Hybrid Threat Activites in Cyber Domain

Defining threats originating from or utilizing cyberspace can be complex, as they are often considered a subset of hybrid threats. Cyber threats can emerge from various sources, including state actors, criminal groups, terrorist organizations, hacktivists, and mercenary professional hackers. The range of exploitable technologies is constantly expanding—from servers, personal computers, and laptops to smartphones, smart meters for electricity distribution, wireless-enabled pacemakers, and industrial control systems. This diversity encompasses just the hardware aspect. The potential impacts of cyberattacks vary widely, from playful publicity stunts to the destruction of critical infrastructure and even potential fatalities. Cyberattacks exploit design assumptions or implementation flaws. It is crucial to understand that while

cyberspace is the primary environment for these threats, their effects can extend to other realms. A notable example is StuxNet, where a cyberattack disrupted uranium enrichment in Iran, leading to the failure of several physical devices (Farwell & Rohozinski, 2011).

The scale of cyber-attacks conducted at a military level indeed suggests the involvement of state actors orchestrating or endorsing these operations. Cyberspace operates across multiple layers, including the physical layer represented by hardware infrastructure, the logical layer dictating how data is distributed and processed, and the human layer comprised of users. However, cyber threats are still difficult to understand. The ambiguity arises from questions surrounding the perpetrators of these attacks and their affiliations – whether they are criminal enterprises acting independently or backed by state agencies (Kello, 2013; Nye, 2016). This ambiguity creates a challenging landscape for addressing cyber threats, as it necessitates navigating complex jurisdictional issues and determining appropriate responses to attacks with potentially far-reaching consequences. As such, effective cybersecurity strategies require collaboration between public and private entities, as well as international cooperation to enhance defenses against state-sponsored cyber threats and mitigate the risks posed by cyber-attacks in the military domain.

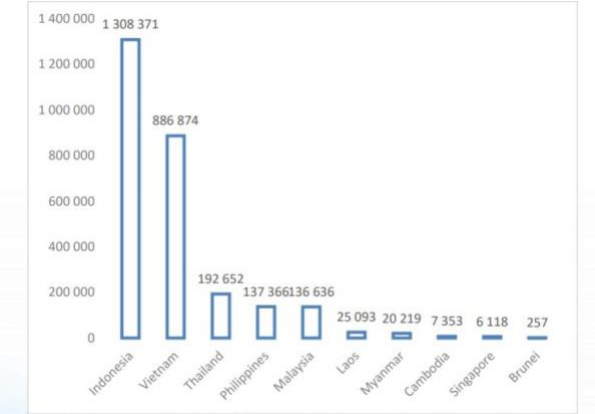
On the other side, digital development in Asia has grown significantly. This development is a result of reliable internet connectivity. According to research by Google, Bain, and Temasek, Southeast Asia, buoyed by some of the biggest and most rapidly expanding digital economies worldwide, is on course to generate US$100 billion in revenue by the end of 2023 (Knowles, 2024).

Due to ASEAN's strategic importance and geopolitical circumstances, the region faces significant threats in the form of Advanced Persistent Threats (APTs) (Noor, 2020). Cyber-attacks are becoming increasingly complex and destructive, with APT actors posing one of the most significant challenges. APTs are sophisticated, covert, and persistent, executing cyber-attacks based on well-coordinated plans and strategies aimed at achieving business and political objectives. As investments grow and economies diversify in the region, this progress also makes ASEAN more attractive to APT groups. These groups primarily target

critical services, which have a substantial impact on national and public security. Such services include telecommunications, banking and finance, transport, and energy (CyberSecurity Malaysia, 2020).

The likelihood of encountering a cyber incident is directly proportional to the number of individuals using the internet daily. To minimize this threat, significant interventions from various stakeholders are necessary. In countries such as Malaysia, Indonesia, the Philippines, and Vietnam, unsecured infrastructure has made it easier for hackers to successfully launch cyber-attacks (Borelli, 2017; Permata & Nanda, 2020; T-Systems, 2023).

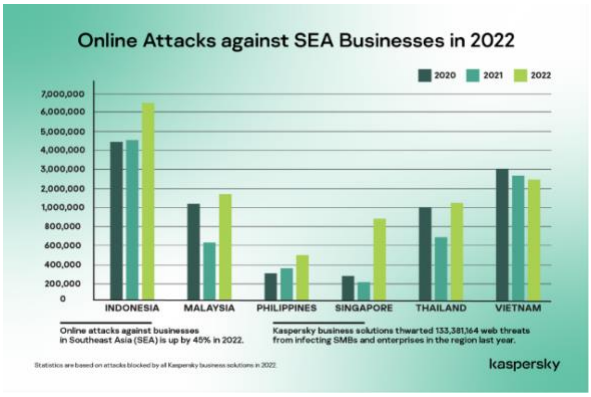
Figure 1. Ransomware detection in ASEAN from January to September 2020



Source: (INTERPOL, 2021)

Citing data from the figure 1. above, there were around 2.7 million ransomware attacks detected in Southeast Asian countries in the January-September 2020 period. Of that number, Indonesia topped the list with 1.3 million cases followed by Vietnam at 886 thousands cases, and the rest of ASEAN below 200 thousands cases. This shows the vulnerability of cyber defenses of countries in ASEAN in the face of cyber threats, especially the potential for hybrid threats sponsored by other countries to intervene in countries in Southeast Asia. The ransomware attacks, according to the data above mostly looking into highly populous and growth economy including Indonesia, Vietnam, Thailand, Malaysia, and Philippines.

Figure 2. Online Attacks against SEA Businesses in 2022



Source: Kaspersky (2022 in Digital Watch Observatory, 2023)

Cyber-attacks do not only occur through ransomware, but also online attacks on the websites of business institutions in

ASEAN countries. Based on the [Figure 2.] data, there is a 45 percent increase in online attacks by 2022. These online attacks not only damage businesses, but can also have a major impact on customers. Some of the most common types of web threats include data theft, phishing attacks, and computer viruses. Among those experiencing the most attacks is Singapore, increasing by 329 percent followed by Malaysia (197 percent), Thailand (63 percent), Indonesia (46 percent), and the Philippines (29 percent). Only Vietnam declines by 2022. However, consistently over the past three years, Indonesia and Vietnam have been the biggest targets of online attacks in ASEAN.

The vulnerability of ASEAN as a developing region to cyber threats underscores significant risks to national sovereignty. These threats, originating from both state and non-state actors, pose severe dangers to the digital infrastructure and security of each country within the region. State-sponsored cyber activities, particularly those attributed to China, alongside attacks by non-state actors, have disrupted digital operations across ASEAN communities. These malicious activities have not only compromised sensitive information but also undermined trust in digital systems, creating substantial economic and political repercussions. The region's lack of digital capacity development, coupled with diverse levels of cybersecurity readiness among member states, exacerbates this vulnerability. As a result, continuing threats demand a bold and coordinated response to protect national interests and maintain regional stability. Effective strategies must include enhancing cybersecurity frameworks, fostering international cooperation, and investing in advanced technology and skilled personnel.

China’s Hybrid Threat Projection in Cyberspace

China's rapid economic, military, and technological growth has significantly increased its power and influence on the global stage. This surge has seen China assert itself as a revisionist power, seeking to reshape the current international order to better align with its interests and values. The Chinese government has explicitly stated its ambitions to alter the status quo, aiming to establish a more dominant and influential position both regionally and globally. This includes territorial claims in the South China Sea, efforts to expand its Belt and Road Initiative, and increased military presence in key areas. As China continues to challenge

existing norms and power structures, it is clear that its strategic goals involve not only economic and technological leadership but also a redefined geopolitical landscape where China holds a central, commanding role.

Following its economic rise and international status, China has become a dominant power. China's dominance has been demonstrated through its activities in the South China Sea region. In the region, China carries out hybrid threats in the maritime sector through various policies. The first is through direct military contact at the border, creating friction between China and neighboring countries, especially ASEAN countries such as the Philippines, Vietnam, Malaysia and Indonesia. Then China also uses non-state assets such as militias and organized crime through piracy, ship incidents, and illegal fishing. Both of these are enacted one after the other (Agustiyan et al., 2022).

The Chinese threat does not stop at the maritime sector. Recently, China has been building its cyber capacity in a massive and structured manner. Chinese technical analysts from the Joint Operations College of the National Defense University have outlined strategies to enhance battlefield modelling and simulation. Their analyses highlight cyber means as a crucial component of hybrid warfare, stressing the importance of China leveraging its status as a major cyber power to bolster its cyber capabilities and defenses. This strategy includes manipulating social media to influence public opinion through information collection, propaganda, and psychological tools. Operationally, these support forces focus on border and maritime zones through reinforced strategic communications, psychological warfare operations, and military-civilian cooperative efforts. China is also advancing quantum communications to secure sensitive information channels and integrating coast guard and naval forces to protect maritime routes. To support these operations, it is essential for China to protect and strengthen media propaganda, communication networks, municipal security, civil society, social credit systems, and industrial and commercial networks (Saalman, 2021).

The China’s cyber threat projection not just a thing on paper-only. The China’s sponsored cyber attack has been used in the past, one of them is called Operation Aurora. It was an attack to the United States. In Operation Aurora, conducted in 2009, Chinese hackers breached Google's security to access the source code of Google's search engine (Read, 2014). Their goal was to replicate Google's success and develop a

more state-friendly search engine within China. While such cyber activities can harm national economies, they usually have a minimal impact on international security. However, during Operation Aurora, the hackers also obtained court documents from the United States Foreign Intelligence Surveillance Court and other judges nationwide. This provided a significant advantage to China's clandestine intelligence operations. The ability of Chinese intelligence to determine if their spies are compromised or under investigation before charges are filed is extremely advantageous. This capability has the potential to undermine the FBI's counter-intelligence efforts and significantly weaken national security. By the end of the year, 4.2 million personnel files had been stolen, including Social Security numbers and other sensitive information. Additionally, 5.6 million fingerprints were also compromised. The impact on U.S. national security was significant. This stolen information makes it easier to track down spies, hack into accounts, identify federal employees with security clearances, and pinpoint the best or most vulnerable targets for blackmail and bribery (Reilly III, 2020). The information can be used or shared in numerous other damaging ways, posing a serious threat to national security.

Despite being accused of conducting extensive and prolonged cyber espionage campaigns against the United States and several other countries, China has largely avoided significant punitive or economic repercussions. China's hybrid warfare strategy, aimed at influencing the international community, has been crucial in preventing a strong deterrence response (Iasiello, 2016). This strategy has enabled China to position itself as a viable partner in cyberspace while downplaying its rising threat. China has consistently denied the accusations to mitigate public perception of its actions.

Additionally, China has also established militia units, categorized as cyber-militias. While cyber-militias are fairly common for countries with strong cyber capacity, China's scale far exceeds that of other western countries. Its capacity competes with superpowers like the United States. China's cyber-militia structure aims to form informational warfare units. These militia units are spread throughout China, both State-Owned Enterprises and other civilian institutions, including higher education institutions (Klimburg, 2011).

Amid the ongoing tensions in the South China Sea, China has been conducting cyber espionage across Southeast Asia. Reports indicate that hackers affiliated with a Chinese state-linked security contractor have targeted government agencies throughout the region for years (Bajak & Kang, 2024; Kelliher, 2024). These cyberattacks have infiltrated state systems in Thailand, Vietnam, Malaysia, Indonesia, Myanmar, and Cambodia, as well as private companies. The hackers have specifically targeted high-level government departments in Southeast Asia, seeking information about each country's strategy regarding the contested South China Sea (Greig, 2024).

However, this is not the first-time incident related to China-linked hacking activities. In February 2022, hackers linked to China breached an email server operated by ASEAN, stealing a substantial amount of data. According to a cybersecurity alert, the hackers stole "gigabytes" of emails from ASEAN countries, with data being taken "on a daily basis." It is estimated that the attackers stole over 10,000 emails, resulting in more than 30 GB of data (Burgess, 2023). This incident disrupted correspondence and impacted all ASEAN members.

China's hybrid threat projection in cyberspace, particularly towards ASEAN countries, exemplifies its strategic use of cyber capabilities to influence regional dynamics. Amid South China Sea tensions, China has engaged in extensive cyber espionage, targeting government agencies and private companies across the region. These cyber activities are part of China's broader strategy to assert its dominance, disrupt regional stability, and gather intelligence to enhance its geopolitical standing. Facing these threats, ASEAN countries need to prepare themselves to avoid the destructive impact of hybrid threats.

Southeast Asia Countries Mitigation on Cybersecurity

Despite numerous cyberattacks, the Southeast Asian region struggles with relatively low cyber resilience (Curtis et al., 2022). Achieving robust cyber resilience demands a comprehensive approach involving governance, risk management, clarifying data ownership, fostering regional and international cooperation, and continually enhancing infrastructure and institutional capabilities. While the region has enhance its cybersecurity, persistent discrepancies in national cyber readiness and the lack of unified cybersecurity standards pose significant challenges.

Table 1. Cyber Capabilities of the 10 ASEAN Member States Compared[1]

Country[2]	Level of Cyber Readiness	NCSI Score	NCSI ranking	ADII score on Cybersecurity	ADI ranki
MY	Well-established	79.22	1	91.27	1
SG		71.43	2	89.70	2
TH	Developing	64.94	3	87.91	3
ID		63.64	4	78.43	4
PH		63.64	5	72.49	5
BN	Emerging	41.56	6	67.46	6
VN		36.36	7	63.05	7
KH	Limited	23.38	8	24.76	9
LA		18.18	9	32.58	8
MM		10.39	10	20.41	10

Source: (Cheng & Chow, 2023)

According to the Table 1 above, Malaysia and Singapore lead the region in cyber capabilities, having fortified their cybersecurity strategies through the establishment of dedicated agencies and the enactment of key legislation like the Cybersecurity Act and the creation of government agency specific to countering cyber threat, such as CyberSecurity Malaysia. Meanwhile, Thailand, Indonesia, and the Philippines are progressing in enhancing their cyber resilience, with each country implementing relevant laws and frameworks to bolster cybersecurity measures. Indonesia, in particular, is working on improving its legal framework and government coordination in addressing cyber issues. Brunei and Vietnam are categorized as "emerging" in cyber capabilities, with Vietnam making notable strides through legislation such as the Law on Cybersecurity, although it still faces challenges in certain areas like cyber threat analysis and data protection. Brunei, however, lags behind in policy development and global cybersecurity contributions. Cambodia, Laos, and Myanmar have limited cyber capabilities, primarily due to resource constraints, technological infrastructure challenges, and differing national priorities. Despite these challenges, efforts are being made across the region to strengthen cybersecurity

[1] National Cyber Security Index (NCSI) and ASEAN Digital Integration Index (ADII) score (0-100)

[2] ASEAN Countries abbreviation according to ISO 3166

frameworks and collaboration to mitigate cyber threats effectively.

Bold and decisive action needs to be taken by ASEAN countries. It is crucial for governments, cyber experts and business leaders in ASEAN to align their perceptions on cybersecurity issues and realize the urgency of a unified and coordinated approach. ASEAN has the opportunity to foster more cohesion for cyber resilience by promoting trust and transparency, supporting less developed economies, and integrating cyber resilience with the digital economy (Cheng & Chow, 2023).

ASEAN has initiated the ASEAN Digital Masterplan 2025 (ADM) in 2021 to realize ASEAN's vision supported by secure and transformative digital services, technologies and ecosystems. It also complements the existing ASEAN framework on Personal data Protection and Digital Data Governance by setting out desired outcomes, each with enabling actions to achieve the vision by 2025. This ADM is a common foundation for ASEAN in developing security, infrastructure, technology, standardization, human resource development, and policy frameworks (Abdurrohim, 2022).

Singapore independently also organized the Singapore International Cyber Week in order to strengthen ASEAN countries' focus on cybersecurity issues. At this cyber exhibition, Singapore consistently states that there is no country in Southeast Asia that is not threatened by cyber threats, be it by state or state actors. As such, Singapore is shaping the perception of an ongoing threat that ASEAN countries must remain vigilant and cooperate with each other to address. The Singapore International Cyber Week follows Singapore's efforts at the ASEAN level by holding the ASEAN Ministerial Conference on Cybersecurity, launching the ASEAN Cyber Capacity Programme, and establishing the ASEAN-Singapore Cybersecurity Centre of Excellence (Anshori & Ramadhan, 2019).

In the future, intensive collaboration in dealing with hybrid threats in the cyber sector in ASEAN needs to be encouraged (Krisman, 2013). Collaboration is not only among fellow countries in the region, but also needs to carry out cyber diplomacy and cooperation with other more advanced countries. There needs to be more coordinated and structured cooperation. In addition, the establishment of a comprehensive cyber army in the ASEAN region may be helpful in handling organized cyber attacks. The formation of a cyber army needs to synergize not only military agencies,

but also academia and the private sector (Setiawan, 2018).

CONCLUSION

ASEAN faces a significant challenge in addressing hybrid threats in the cyber domain, as cyber threats are increasingly sophisticated and come from a variety of actors, including state-sponsored groups, criminal organizations, and individual hackers. The expanding list of vulnerable technologies—from smartphones to industrial control systems—further complicates the cybersecurity landscape. The complexity and ambiguity of cyber threats, which can have far-reaching impacts beyond cyberspace, necessitate a multi-layered and coordinated response. Historical incidents like StuxNet and Operation Aurora illustrate the potential for cyberattacks to cause severe physical and national security damage.

The rapid digital development in Southeast Asia, driven by robust internet connectivity, makes the region a lucrative target for Advanced Persistent Threat (APT) groups. These APT actors, motivated by political and economic gains, often target critical infrastructure sectors, posing significant risks to national and public security. The scale of cyber incidents underscores the region's cyber vulnerability. High-profile incidents, including China's cyber espionage activities, reveal the strategic use of cyber capabilities to influence regional dynamics and gather intelligence, further destabilizing the region. Despite these challenges, Southeast Asia's cyber resilience remains relatively low, with significant discrepancies in cybersecurity readiness among ASEAN member states. While countries like Malaysia and Singapore lead in cyber capabilities, others like Cambodia, Laos, and Myanmar lag due to resource and infrastructure constraints. To mitigate cyber threats, ASEAN countries must enhance their cybersecurity frameworks, foster international cooperation, and invest in advanced technology and skilled personnel. The ASEAN Digital Masterplan 2025 and initiatives like the Singapore International Cyber Week demonstrate steps towards a more cohesive and resilient cyber environment.

Moving forward, ASEAN must intensify collaboration within the region and with global partners, promoting trust, transparency, and support for less developed economies. Establishing a comprehensive cyber defense strategy, including a regional cyber army and enhanced cyber diplomacy,

will be crucial in countering organized cyber threats and ensuring regional stability.

REFERENCES

Abdurrohim, M. (2022). ASEAN Digital Masterplan: Responding Cyber Security Dilemma in The Post-Covid Era. Global Focus, 2(1), 17–26. https://doi.org/https://doi.org/10.21776/ub.jgf.2022.002.01.2

Agustiyan, D. R., Mamahit, D. A., & Suwarno, P. (2022). Sea Lines of Communications (SLOC): Complexity of China's 21st Century Maritime Silk Road Threats. International Journal of Arts and Social Science, 5(2). https://www.ijassjournal.com/2022/V5I2/414659925.pdf

Anshori, M. F., & Ramadhan, R. A. (2019). Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week. Padjadjaran Journal of International Relations, 1(1), 39–52. https://doi.org/https://doi.org/10.24198/padjir.v1i1.21591

Aoi, C., Futamura, M., & Patalano, A. (2018). Introduction 'hybrid warfare in Asia: its meaning and shape.' The Pacific Review, 31(6), 693–713. https://doi.org/10.1080/09512748.2018.1513548

Bajak, F., & Kang, D. (2024, February 22). An online dump of Chinese hacking documents offers a rare window into pervasive state surveillance. AP News. https://apnews.com/article/china-cybersecurity-leak-document-dump-spying-aac38c75f268b72910a94881ccbb77cb

Ball, J. (2023, April 15). The Changing Face of Conflict: What is Hybrid Warfare? Global Security Review. https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

Borelli, M. (2017). ASEAN Counter-terrorism Weaknesses. Counter Terrorist Trends and Analyses, 9(9), 14–20. http://www.jstor.org/stable/26351552

Burgess, M. (2023, February 28). China Is Relentlessly Hacking Its Neighbors. WIRED. https://www.wired.com/story/china-hack-emails-asean-southeast-asia/

Cheng, J. H., & Chow, M. (2023, November 6). Strengthening Cyber Resilience in Southeast Asia. Fulcrum. https://fulcrum.sg/strengthening-cyber-resilience-in-southeast-asia/

Chivvis, C. S. (2017). Understanding Russian "Hybrid Warfare" and What Can be Done About It. https://www.rand.org/pubs/testimonies/CT468.html

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 10(2), 113–128. https://doi.org/10.22212/jp.v10i1.1447

Curtis, H., Hogeveen, B., Kang, J., Thu, H. L., Rajagopalan, R. P., & Ray, T. (2022). Digital Southeast Asia:

Opportunities for Australia–India cooperation to support the region in the post-Covid-19 context. https://www.orfonline.org/wp-content/uploads/2022/02/Digital-Southeast-Asia.pdf

CyberSecurity Malaysia. (2020). Cyber Security Outlook in South East Asia Region: From Cybersecurity Malaysia's Perspective. https://www.cybersecurity.my/data/content_files/26/2149.pdf

Digital Watch Observatory. (2023, April 27). Kaspersky: Online attacks against SEA businesses up 45% in 2022. Geneva Internet Platform.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Gaiser, L. (2022). Chinese hybrid warfare approach and the logic of strategy. National Security and the Future, 23(1), 67–77. https://doi.org/https://doi.org/10.37458/nstf.23.1.3

Ginanjar, Y. (2019). Hacker Sebagai Aktor Non-Negara : Cyber Warfare Sebagai Dampak Penyadapan Pejabat Negara Indonesia Oleh Intelijen Australia. https://doi.org/https://doi.org/10.36859/jdg.v4i02.138

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. Dinamika Global : Jurnal Ilmu Hubungan Internasional, 7(2), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Greig, J. (2024, June 5). Chinese hacking groups stole 'sensitive' intel on South China Sea from SE Asian government. The Record. https://therecord.media/chinese-hacking-groups-stole-from-se-asia

Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. CrimRxiv. https://doi.org/10.21428/cb6ab371.5f335e6f

Gunneriusson, H., & Ottis, R. (2013). Cyberspace from the Hybrid Threat Perspective. Journal of Information Warfare, 12(3), 67–77. https://www.jstor.org/stable/26486843

Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. https://www.comw.org/qdr/fulltext/0712hoffman.pdf

Hoffman, F. G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict (240; Strategic Forum). https://www.files.ethz.ch/isn/98862/SF240.pdf

Iasiello, E. (2016). China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. Journal of Strategic Security, 9(2), 45–69. http://www.jstor.org/stable/26466776

INTERPOL. (2021). ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk. https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

Kelliher, F. (2024, March 1). China data leak spotlights cyber-spying across Southeast Asia. Nikkei Asia. https://asia.nikkei.com/Politics/International-relations/China-data-leak-spotlights-cyber-spying-across-Southeast-Asia

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, 38(2), 7–40. http://www.jstor.org/stable/24480929

Klimburg, A. (2011). Mobilising Cyber Power. Survival, 53(1), 41–60. https://doi.org/10.1080/00396338.2011.555595

Knowles, C. (2024, January 5). Rising cyber threats challenge Southeast Asia's booming digital economy. SecurityBriefs: Asia. https://securitybrief.asia/story/rising-cyber-threats-challenge-southeast-asia-s-booming-digital-economy#:~:text=Rising%20cyber%20threats%20challenge%20Southeast%20Asia's%20booming%20digital%20economy,-

Krisman, K. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. JAS (Journal of ASEAN Studies), 1(1), 41–53. https://doi.org/10.21512/jas.v1i1.60

Miller, B. (2021). Is Technology Value-Neutral? Science, Technology, & Human Values, 46(1), 53–80. https://doi.org/10.1177/0162243919900965

Noor, E. (2020). Positioning ASEAN in Cyberspace. Asia Policy, 15(2), 107–114. https://www.jstor.org/stable/27023907

Nye, J. S. (2016). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44–71. https://www.jstor.org/stable/26777790

Permata, I. M., & Nanda, B. J. (2020). The Securitization of Cyber Issue in ASEAN. In P. E. Nasir, M. Jamilah, & A. Halim (Eds.), Proceedings of the 1st International Conference on ASEAN (IC-ASEAN) "Towards a better ASEAN" (pp. 90–97). Sciendo. https://d-nb.info/1254811931/34#page=100

Raugh, D. L. (2016). Is the Hybrid Threat a True Threat? Journal of Strategic Security, 9(2), 1–13. http://www.jstor.org/stable/26466774

Read, O. (2014). How the 2010 Attack on Google Changed the US Government's Threat Perception of Economic Cyber Espionage. In J.-F. Kremer & B. Müller (Eds.), Cyberspace and International Relations: Theory, Prospects and Challenges (pp. 203–230). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37481-4_12

Reichborn-Kjennerud, E., & Cullen, P. (2016). What is Hybrid Warfare? (1). http://www.jstor.com/stable/resrep07978

Reilly III, R. L. (2020). Strategic Competition and Escalation Management in the 21st Century: Russian Hybrid Warfare and China's Rise [University of Denver]. https://digitalcommons.du.edu/etd/1829/

Renz, B. (2016). Russia and 'hybrid warfare.' Contemporary Politics, 22(3), 283–300. https://doi.org/10.1080/13569775.2016.1201316

Saalman, L. (2021). China and its hybrid warfare spectrum. In M. Weissmann, N. Nilsson, B. Palmertz, & P. Thunholm (Eds.), Hybrid Warfare: Security and Asymmetric Conflict in International Relations (pp. 95–112). I.B. Tauris. https://doi.org/http://dx.doi.org/10.5040/9781788317795.0013

Setiawan, R. (2018). Indonesia Cyber Security : Urgency To Establish Cyber Army in the Middle Of Global Terrorist Threat. Journal of Islamic World and Politics, 2(1), 157–173. https://doi.org/10.18196/jiwp.2109

Steingartner, W., & Galinec, D. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica, 18(3), 25–48. https://doi.org/10.12700/APH.18.3.2021.3.2

Talat, D. (2021, January 8). Hybrid Threats & Warfare in South Asia. Modern Diplomacy. https://moderndiplomacy.eu/2021/01/08/hybrid-threats-warfare-in-south-asia/

T-Systems. (2023, March 9). Asia remains the epicenter of advanced persistent threats. Are you ready to take them on? https://www.t-systems.com/id/en/insights/newsroom/news/asia-remains-the-epicenter-of-advanced-persistent-threats-583682

Veljovski, G., Taneski, N., & Dojchinovski, M. (2017). The danger of "hybrid warfare" from a sophisticated adversary: the Russian "hybridity" in the Ukrainian conflict. Defense & Security Analysis, 33(4), 292–307. https://doi.org/10.1080/14751798.2017.1377883

Weissmann, M. (2019). Hybrid Warfare and Hybrid Threats Today and Tomorrow: Towards An Analytical Framework. Journal on Baltic Security, 5(1), 17–26. https://doi.org/10.2478/jobs-2019-0002