**Jurnal Ilmiah Wahana Pendidikan, Oktober 2025, 11 (10.A), 50-56**
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/11685
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

# The Effort of ASEAN in Maintaining Cyber Threat in The Southeast Asia Region

**Batara Jeremy Chrisando Pasaribu[1] , Made Panji Teguh Santoso[2], Prilla Marsingga[3]**

[1,2,3]Universitas Singaperbangsa Karawang

Received: 05 September 2025
Revised: 17 September 2025
Accepted: 28 September 2025

**Abstract**

Cybercrime has developed over a long period of time and is caused by the rapid development of globalization. All activities in the Southeast Asia region today are filled with technology, not only that, every ASEAN community has also participated in cyber developments. Southeast Asia is a region that is vulnerable to cybercrime due to the low level of security among ASEAN countries. This journal will discuss how and what ASEAN's efforts are to fight and overcome cybercrime which is growing rapidly in regions that are still developing, such as Southeast Asia.

**Keywords:** Southeast Asia, ASEAN, Cyber Threat, Efforts

(*) Corresponding Author: 2110631260002@student.unsika.ac.id
made.santoso@staff.unsika.ac.id
prilla.marsingga@fisip.unsika.ac.id

**How to Cite:** Pasaribu, B. (2025). The Effort of ASEAN in Maintaining Cyber Threat in The Southeast Asia Region. *Jurnal Ilmiah Wahana Pendidikan*, *11*(10.A), 50-56. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/11685.

## INTRODUCTION

According to the Big Indonesian Dictionary, business can be defined as an activity that channels energy and thoughts towards a specific objective. Effort also entails striving for a goal, reasoning, endeavoring to achieve an aim, solving problems, or finding solutions. With this comprehension in mind, the endeavors of the Association of Southeast Asian Nations should have a clear target—namely preventing or combating prevalent cyber threats.

The initiation of the Association of Southeast Asian Nations dates back to August 8, 1967, when five Southeast Asian countries - Indonesia, Malaysia, the Philippines, Singapore and Thailand- came together to form this regional organization. At present, Asean boasts a membership of 11 countries with an additional six nations joining subsequently; these include Brunei Darussalam, Vietnam, Lao PDR, Timor Leste, Cambodia, and Myanmar. The motto "One Vision, One identity, One Community" aims at unifying member states in addressing regional challenges and fostering a shared identity towards realizing common goals. Reputed for its guiding principle known as the "ASEAN Way", which emphasizes non-interference and consensus decision-making among members in diplomatic matters. ASEAN has reinforced norms such as opposing violence, prioritizing peaceful solutions, respecting regional autonomy, and abstaining from intervening in other members' internal affairs by employing consultation and consensus-building as central tenets in its decision-making processes (Darmawan & Kuncoro, 2019).

Nowadays, the widespread use of the internet has significantly impacted

people's daily lives. The rapid growth of the internet has brought both positive and negative effects. With globalization, human activities increasingly take place in cyberspace, leading to various types of cybercrimes such as cyberattacks, botnets, financial institution breaches, dissemination of Multi-Purpose Malcode, state-sponsored cyber activities and hacking incidents. These crimes are facilitated by tools used by individuals in their everyday lives. As a result of these cyber threats/crimes there is a pressing need for cybersecurity which involves preventing and securing information technology resources to mitigate crime within the digital realm. Cybersecurity can be seen as an active endeavor to safeguard against attacks occurring on the Internet.(Rahmawati, 2019).

The entire Southeast Asian region still struggles to combat the escalating threat of cybercrime. This is attributed to inadequate security infrastructure in several countries, limited awareness and education on cybersecurity, and other factors. It is essential for ASEAN as a regional organization to take the lead in initiating efforts and providing assistance in addressing the persistent rise of cybercrime.

## METHODS

This journal employed qualitative descriptive research methodology, which can be utilized to offer a comprehensive and educational analysis of The Effort of ASEAN in Maintaining Cyber Threat in The Southeast Asia Region. Qualitative research seeks to comprehend the phenomena experienced by research subjects such as behavior, perception, motivation, action holistically through descriptions using words and language within a specific natural context and via various natural methods. One key characteristic of qualitative research is the use of case studies, making it easier to find and study an event, program, process or activity that serves as the basis for this type of inquiry.

The approach used secondary sources exclusively through library-based exploration encompassing books, notes scientific journals magazines newspapers, and preceding research findings. By searching literature relevant to the issue under investigation researchers find data objects pertinent towards finding viable solutions on how regional organizations like ASEAN are combating cybercrime.

## RESULTS & DISCUSSION

### *Results*

Cyberspace is not limited by regional boundaries (borderless), where people can opt for not to reveal their identity (anonymous). The anonymity in some extent opens the potential of criminal activities on the cyberspace referred to as cybercrime. Cybercrime is an unlawful act of using information and communication technology targeted at networks, systems, data, websites, and technologies.

Criminals often set regions with certain level of vulnerability as their targets. International Telecommunication Union (ITU) report entitled Global Cybersecurity Index (GCI) in 2020 showed that Singapore ranked first in the level of cybersecurity in Southeast Asia with a score of 98.52, followed by Malaysia with 98.06, Indonesia with 94.88, Viet Nam with 94.59, Thailand with 86.5, Philippines with 77, Brunei Darussalam with 56.07, Myanmar with 36.41, Lao P.D.R. with 20.34, and Cambodia with 19.12.4 This index was measured based on five main

components; legal, technical, organizational, capacity development, and cooperation measures. Therefore, ASEAN member states need to improve the quality of each component.

AT Kearney found that ASEAN countries, especially Indonesia, Malaysia, and Vietnam, are at risk of becoming the main targets of suspicious web activity blockage. The regulatory framework for cybersecurity management and capabilities within ASEAN is notably deficient, exacerbated by the limited expertise in human resources across member states. Additionally, the awareness among corporations and stakeholders about the significance of cybersecurity is minimal, often not recognized as a business priority, which impedes comprehensive and holistic approaches to enhancing cyber resilience. In the era of digitalization, where data and information are predominantly stored in digital formats, ensuring data privacy and security becomes paramount for any organization.5 This scenario underscores the pressing need for stronger regulatory measures and an increase in awareness, aiming to address the cybersecurity challenges effectively and safeguard digital assets in a world increasingly reliant on digital infrastructures.

Weak control over cybercrime in the ASEAN negatively impacts the region's stability, especially in terms of the economic growth. ASEAN region has a combined GDP of more than USD 3.11 trillion, making it one of the seventh-ranked largest markets in the world. ASEAN is also regarded the most populous market in the world with a total population 663.47 million.6 In addition, ASEAN's potential in the digital economy in 2025 is predicted to increase of up to 1 trillion dollars with stronger development of digital services such as the financial and commercial sectors.7 Cybersecurity experts project the net cost of cybercrime to grow by 15 percent per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015.

***Discussion***

The easy accessibility of communication and information has significantly influenced various aspects of a nation. In terms of national security, the internet has made threats to a country's sovereignty increasingly intricate. Nowadays, threats to national security involve not only military aspects but also non-military ones, such as cyber threats. Cybercrime is just one example among many negative consequences in this context. With these adverse effects rapidly expanding, it becomes crucial to address them effectively. The breadth of cybercrime presents a significant threat to countries as it can be utilized for activities like stealing information, propagating harmful ideas, or launching attacks on information systems across sectors such as banking data and military networks - with particular emphasis on nations in Southeast Asia region. The different forms of cybercrime are varied; they include bank embezzlement, pornography dissemination, data theft, hacking, and carding schemes.

Research conducted by the ASEAN Desk highlight a number of prominent cyber threats for 2020 and the subsequent years, including

1. Business E-mail Compromise, is a mode of fraud posing as the victim’s business partner company and aiming to obtain funds that should be directed to the actual business partner company.
2. Phising, is an attempt to obtain information about someone’s data by phising

techniques. The data targeted for phising are persona data (name, age, address), account data (username and password), and financial data (credit card information, accounts).

3. Ransomware, can be defined as a mass extortion of personal data or information stolen to seek profit from the victim in the form of money.
4. E-commerce data interception, is a threat to confidentiality in the form of information intercepted so that people who are no entitled can access the computed where the information is stored.
5. Crimeware-as-a-Service (CaaS), is malware software that encrypts files and documents from one of the computers to the entire network. The perpetrator will ask the victim for a ransom to be able to access the network that has been taken over again. Spyware phising kits, browser hijackers, keyloggers, and more are available to attackers through CaaS.
6. Cyber scams are fraudulent schemes by using fake websites to steal personal information and misuse it.
7. Cryptojacking is a type of cybercrime in which hackers use the victim's device secretly to take advantage of cryptocurrencies.

The ASEAN region has placed significant emphasis on cybersecurity, particularly due to the increased shift into the digital era following the Covid-19 pandemic. There are various factors that contribute to ASEAN's vulnerability to cyber threats. Firstly, this region represents a substantial portion of global internet users, with 922 million out of 2.1 billion originating from here—a number that is expected to increase further. Secondly, as the largest regional organization in Asia Pacific, ASEAN fosters extensive economic and market interactions within its borders. With most economic activities now being conducted online, it means that cyber transactions predominantly involve entities within ASEAN. Moreover, because it is a developing region, there is widespread use of ICT systems across diverse infrastructure sectors such as transportation, energy production and distribution networks, banking services, and expanding mobile telephone coverage even in remote areas. (Trisni , Isnarti, & Halim).

These growing threats should make countries in the Southeast Asia region more alert and increase cyber security, not only at the state level but at the regional level. There are several ASEAN Sectoral Bodies led by ASEAN on cyber security issues, namely the ASEAN Digital Ministers' Meeting (ADGMIN) and the ASEAN Digital Senior Officials' Meeting (ADGSOM) as subsidiary bodies, the ASEAN Regional Forum (ARF), AMMTC, the East Asia Summit (EAS), the ASEAN Defense Ministers' Meeting (ADMM)-Plus, and the ASEAN Ministerial Meeting on Social Welfare and Development (AMMSWD). In the field of cybercrime, ASEAN specifically increased its cooperation through its inclusion as one of the ten areas of cooperation under the ASEAN Senior Officials' Meeting on Transnational Crime (SOMTC) in 2001. The SOMTC Working Group on Cybercrime serves as a platform for discussion regarding practical cooperation in combating cybercrime among ASEAN countries.

ASEAN has undertaken significant efforts to improve security cooperation among its member countries, including the establishment of the ASEAN Political Security Community. This initiative aims to promote collaboration in political and security matters, ultimately contributing to regional peace, security, and stability.

In addition to traditional issues, such as cyber threats have also been addressed by APSC. ASEAN plays a critical role as a platform for its member states to work together in advancing cybersecurity. To effectively strengthen its overall cyber resilience, ASEAN must reinforce its core frameworks and jointly developed action plans. Member states should play an active role in driving progress in cybersecurity. Additionally, partnerships with countries like Japan, China, the United States, and others involve comprehensive assessments of the key factors necessary to boost cybersecurity resilience throughout ASEAN. Given that cyber challenges are relatively new to ASEAN's agenda, it is essential to make extra efforts to ensure the involvement of all member states in these cybersecurity endeavours.

In addressing political and security concerns in the Asia Pacific region, ASEAN organizes the ASEAN Regional Forum. The formation of ARF supports the integration and development process of the ASEAN Political Security Community. With a growing prevalence of cybercrime, an additional forum focused on cybersecurity was established within ARF known as "ASEAN Regional Forum on Cyber Security Initiatives." This development originated from discussions at a meeting held in Malaysia back in 2006 with aims to develop defence strategies that promote mutual trust between countries while minimizing potential external threats. These initiatives reflect ASEAN's commitment towards enhanced cooperation against cyber threats. (Fadilla, 2021). ASEAN has undertaken several initiatives to tackle cyber threats at the bilateral and regional levels, such as the ASEAN ICT Masterplan 2015, The ASEAN Cyber Capacity Program, Mactan Mebu Declaration Connected ASEAN: Enabling Aspirations, and other relevant documents. However, current measures implemented by ASEAN mainly focus on developing legal frameworks and enhancing collaboration in law enforcement. There is a necessity for more robust and practical efforts to effectively combat cyber threats instead of solely emphasizing document creation.

ASEAN member nations have formulated specific approaches to improve cybersecurity. These include the enactment of policies and laws to drive technological innovation and economic progress, while also ensuring the protection of individuals' personal information and privacy. In Indonesia, Law No.11 of 2008 on Information and Electronic Transactions contains provisions for cyberspace security, providing a foundation for related regulations and policies. Ministerial Regulation No.20 of 2016 addresses the safeguarding of personal data and privacy following approval by the House of Representatives. Furthermore, Indonesia has established a National Cyber and Encryption Agency aimed at proactively preventing cyber-attacks through prompt response strategies.

Singapore has also taken steps to enhance cybersecurity through various programs. In 2005, Singapore launched its Cybersecurity Masterplan followed by the Infocom Security Masterplan in 2007. Subsequently, the National Cyber Security Masterplan and the establishment of the National Cyber Security Center were initiated as a central body to supervise and coordinate all aspects of cybersecurity for the nation. In 2015, a Cyber Security Agency was formed, and in 2017 Singapore amended the existing Computer Abuse and Cybersecurity Act to address the increasing scale and transnational nature of cybercrime. A

comprehensive approach to improving cybersecurity in Singapore is evident in measures such as renewing the National Cyber Security Master Plan, establishing a Cyber Watch Centre, a Threat Assessment Centre, and instituting sector-specific agencies known as Private Sector-Critical Information Infrastructure partners across private and public sectors.

The Malaysian government has implemented a series of development plans, including the establishment of the National Security Emergency Response Centre in 2006. The purpose was to execute the National Cyber Security Policy and ensure the safety, resilience, and independence of Malaysia's IT System. Subsequently, NISER was renamed as Cyber Security Malaysia and operates under the Ministry of Science, Technology, and Innovation. Furthermore, Malaysia follows eight procedures outlined in the National Cyber Security Framework covering regulation and control, technology advancement, public-private cooperation, institutional collaboration as well as global aspects. Additionally, Malaysia has been proactive in organizing various programs aimed at promoting cyber security awareness. Recognizing the importance of addressing cybersecurity issues effectively, the Malaysian government also provides email hotlines at [cyber999@cybersecurity.my] (mailto:cyber999@cybersecurity.my) to assist local Law Enforcement Agencies in upholding cybersecurity measures.

## CONCLUSION

From the results and discussion above, it can be concluded that there have actually been efforts made by ASEAN as a regional organization to tackle the threat of cybercrime which is increasingly occurring in the Southeast Asia region. However, the efforts made are still in the form of legal documents and do not show much direct field action. This is what makes cybercrime continue to increase.

Furthermore, ASEAN as a regional organization must also understand the shortcomings of the Southeast Asian region so that the roots of the problems can be resolved slowly. ASEAN can also ask for help from its member countries so that this cyber threat can be resolved together, remembering that each country must have its own regulations regarding cybercrimes as explained above.

## REFERENCES

ASEAN. (2017, September 20). *ASEAN PLAN OF ACTION IN COMBATING TRANSNATIONAL CRIME (2016-2025).* Retrieved from asean.org: https://asean.org/wp-content/uploads/2021/01/ASEAN-Plan-of-Action-in-Combating-TC_Adopted-by-11th-AMMTC-on-20Sept17-2.pdf

Binsar , A. (2023, September 7). *Ini Dia 11 Negara ASEAN, Dari Nama Ibu Kota Hingga Mata Uang* . Retrieved from rri.co.id: https://www.rri.co.id/ktt-asean/349397/ini-dia-11-negara-asean-dari-nama-ibu-kota-hingga-mata-uang

Darmawan, A. B., & Kuncoro, H. R. (2019). Penggunaan ASEAN Way dalam Upaya Penyelesaian Sengketa Laut Tiongkok Selatan: Sebuah Catatan Keberhasilan? Andalas Journal of International Studies, 48. https://doi.org/10.25077/ajis.8.1.43-61.2019

Estiyovionita, K., & Sitamala, A. (2022). ASEAN's ROLE IN CYBERSECURITY MAINTENANCE AND SECURITY STRATEGY THROUGH AN

INTERNATIONAL SECURITY APPROACH. *Lampung Journal of International Law*. https://doi.org/10.25041/lajil.v4i2.2556

Fadilla, M. (2021). UPAYA ASEAN DALAM MENINGKATKAN CYBER SECURITY DI KAWASAN ASIA TENGGARA MELALUI ASEAN REGIONAL FORUM ON CYBERSECURITY INITIATIVES. 6.

Huang, H. (2024). UN Cybercrime Convention: Relevance to ASEAN. *RSIS Commentary*.

Interpol. (n.d.). *Supporting collective actions against cybercrime in Southeast Asia*. Retrieved from interpol.int: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk

Manopo, B. Y., & Sari, D. A. (2015). ASEAN REGIONAL FORUM: REALIZING REGIONAL CYBER SECURITY IN ASEAN REGION. *Jurnal Hukum Internasional UNS*. https://doi.org/10.20961/belli.v1i1.27366

Murti, G. (2016). ASEAN's "One Identity and One Community": A Slogan or a Reality? *Yale Journal of International Affairs*.

Putri, K. V. (2021). INDONESIA'S COOPERATION WITH ASEAN ON CYBER SECURITY AND CYBER RESILIENCE IN TACKLING CYBER CRIME. *Jurnal Hukum Lex Generalis*. https://doi.org/10.56370/jhlg.v2i7.90