The Association of Southeast Asian Nations Cybersecurity Architecture: The Challenge of Collective Diplomacy in Facing Transnational Threats

Andrias Darmayadi
Universitas Komputer Indonesia, Bandung City, Indonesia

Dwi fauziansyah Moenardy
Universitas Komputer Indonesia, Bandung City, Indonesia

Rizal Budi Santoso
Universitas Komputer Indonesia, Bandung City, Indonesia

Bayu Trisna Ramahadi
LPK Seabar, Bandung City, Indonesia

ABSTRACT

This study examines how the ASEAN cybersecurity framework addresses cross-border cyber threats. The focus is on how the system is built. How countries work together through Collective diplomacy, what major challenges they face and how they respond to threats in the region. A qualitative descriptive literature review was used in this study to achieve this aim. I used thematic analysis to analyze selected journals and selected sources from 2019 to 2024 based on relevance and quality. The ASEAN cybersecurity framework is managed through regulations such as the ASEAN Cybersecurity Cooperation Strategy. It focuses on technology development and information exchange. and cooperation with foreign groups. Collective diplomacy is implemented through multilateral forums and voluntary programs. However, this is often limited by the principle of national sovereignty. Key challenges include gaps in technical capabilities. Since each country has different laws for security purposes, there is a lack of trust and geopolitical issues. The system works well. But this is not very effective in real work. Because there is a difference between what is promised and what is fulfilled. However, the ASEAN cybersecurity framework sets out rules that must be adhered to. But the limitations of Collective diplomacy generally make it difficult to respond to rapidly changing international threats. Future research should explore different policy models and simulations. Help increase regional resilience.

Keywords: *ASEAN cybersecurity, collective diplomacy, transnational cyber threats, regional security architecture, diplomacy challenges*

INTRODUCTION

As ASEAN moves rapidly into the digital era, more and more people are using e-Government. Fintech, smart cities and digital economy, various societies are starting to depend more on the Internet. All countries are also more vulnerable to cyber attacks such as ransomware, phishing and data breaches. This makes cyberspace an important security area. These threats often cross-national boundaries: land, sea, air and outer space (Susanto & Nugroho, 2021; Chong & Tan, 2020). It is anonymous and difficult to trace. This information can be obtained from various sources. This includes organizations that receive government assistance. The impact on criminal network operators and other non-state actors is not due to technical failures. This situation also affects regional political stability. In this case, public confidence in national security and economic strength emerges (Heng, 2022; Rizal & Suryadinata, 2019). ASEAN serves as the backbone of regional security, but the scope of its response to cybersecurity threats is increasingly limited by the need for rapid and concrete action and ASEAN's core principles of governance, consensus and non-intervention. (Caballero-Anthony, 2021; Emmers, 2023).

ASEAN's cybersecurity architecture is currently being developed. Focusing on confidence-building measures, they discussed initiatives such as the ASEAN Cybersecurity Cooperation Strategy (ACCS), the ASEAN Ministerial Conference on Cybersecurity (AMCC), and the ASEAN CERT Incident Drill (ACID). Increase capacity and share (Chong & Tan, 2020) data with external partners, including the US, China, European Union and Japan. However, this mechanism has not been able to provide coordinated action or response to the crisis.

ASEAN cooperation in the field of cyber security is difficult. This is because member countries have different levels of technical capacity. There are also differences in the way laws and regulations are enforced in different countries. Issues such as cybersecurity and data protection, as well as national sovereignty and data privacy, are so sensitive that (Heng, 2022) does not rely on sharing information about cyber incidents. Finally, global geopolitical tensions, such as competition between the US and China, shape ASEAN's cyber policy and (Emmers, 2023)'s position.

There is a huge gap between rapidly evolving cyber threats and how ASEAN is responding to them. The current approach in this field is more reactionary and qualitative than purely practical. This makes it difficult to build a strong and comprehensive security system in cyberspace. This is due to the gap between political commitment and the actual implementation of (Caballero-Anthony, 2021).

Additionally, rapid digital transformation further complicates risks. Cybersecurity has become a major concern. New developments such as e-Government, financial technology or smart cities create new opportunities. For hackers, digital payment systems and critical public information infrastructure are easy targets. ASEAN member countries now have varying levels of capacity to manage these risks. This shows why we need local systems to do more than just make rules. If an international cyber incident occurs, countries must intervene proactively and immediately cooperate (Susanto & Nugroho, 2021; Heng, 2022).

In this case, ASEAN collective diplomacy is an important factor in overcoming differences. National capacity and oversight forums such as the Association of Southeast Asian Nations (ASEAN), Ministerial Conference on Cybersecurity (AMCC), ASEAN Regional Forum (ARF), and East Asia Summit (EAS) enable member states to participate in dialogue. Discuss common standards and common technical practices such as AC ID. These approaches are not only aimed at information exchange and capacity building. However, this also creates a trust deficit that has so far hindered effective collaboration (Chong and Tan, 2020; Lim and Ng, 2023).

However, the success of diplomacy still depends on the concept of non-intervention and the need to respect state sovereignty. Member States are generally cautious about sharing sensitive information. Given the fear of information leaks or outside interference, regional associations provide a useful framework. However, existing communication and collaboration systems are often intuitive and reactive. This means it is only used when something important happens. They have not achieved deep operational integration. There are also general ways to respond to incidents in ASEAN. (Wijaya and Sari, 2022; Tan and Chong, 2021)

ASEAN's global policy of cyber diplomacy has made this difficult. Meanwhile, large countries such as US and China compete with each other. This will influence the way member countries use the technology. Who do they support? And the way information is accessed, these tensions force countries to trust each other. Sharing information and collaborating against cyber threats across national borders is becoming increasingly difficult. Therefore, the ASEAN Cybersecurity Framework must go beyond regulations. It should be a practical instrument that combines the

powers of states. Regional regulations and international standards to face global threats (Emmers, 2023; Rizal and Suryadinata, 2019). This study is important for researchers and policy makers. This is due to the lack of research that examines ASEAN cyber security from the perspective of overall security architecture and diplomacy. The aim is to determine the success of existing regional reconciliation. Identify hidden structural and organizational deficiencies. and provide policy advice to ASEAN and its member states on how to respond to international cyber threats.

LITERATURE REVIEW

Many previous studies focused on different aspects. Cybersecurity Group Diplomacy and Transnational Threats in ASEAN This provides a strong foundation for this research. The Pacific Review's Chong and Tan (2020) discuss shared cybersecurity goals in ASEAN. They point to initiatives such as ACCS and the difficulty of building trust between member states. His work focuses on law and technology. But this report does not fully explore how collective diplomacy affects the speed with which we respond to domestic and international cyber threats.

Caballero-Anthony (2021) in Modern Southeast Asia, the author uses the concept of evolutionary architectural security to explore how ASEAN is shifting from traditional security practices to new security practices such as cybersecurity. This study confirms that although the principle of non-intervention plays an important role in ensuring stability in the region, it often hinders joint responses to cross-border threats. But research focuses on how things should be, not how they work. This means that there are still not enough details regarding how the ASEAN initiative will be implemented in practice.

Asian Security magazine Emmers (2023) highlights global geopolitical issues affecting the cyber situation in ASEAN countries. Including the competition between United States and China. This study shows how external factors shape cybersecurity policy in the region. However, this report does not examine the gap between political commitments and their actual implementation within the ASEAN Security Framework. Therefore, although this study provides important information regarding the geopolitical landscape, it does not fully reflect the overall diplomatic landscape.

Rizal and Suryadinata (2019) wrote in the Journal of International Relations how ASEAN must increase digital trust among member countries. They see how cyber threats can undermine political and economic stability in the region. Meanwhile, in the Journal of Cybersecurity, Heng (2022), the author examines the laws, organizations and practices of cybersecurity governance in Southeast Asia. It has been mentioned that skill levels vary by country. Different regions make cooperation difficult. Both studies examine how technology and institutions work. However, how to encourage diplomacy to resolve cross-border problems quickly and effectively is not discussed in detail.

Previous research has revealed much about the development of the ASEAN system. The structural barriers they face and geopolitical location influence cyber security in the region. However, little attention has been paid to the effectiveness of collective diplomacy in the face of rapidly evolving international threats. There is no clear political vision to bridge this gap. This research aims to examine these challenges by examining the ASEAN Cybersecurity and Diplomacy Framework. The ability of existing institutions to respond to real and strategic international threats.

METHODOLOGY

This study examines the ASEAN cyber security framework and the challenges in using collective diplomacy to counter international cyber threats through a qualitative descriptive literature review. Rather than using raw data, we integrate previous research findings to identify key trends, gaps, and policy implications. This study combines the concepts of collective diplomacy and security engineering to examine the effectiveness of ASEAN operations. This review examines articles directly related to ASEAN cybersecurity, collective diplomacy, or international threats between 2019 and 2024, and selects high-quality articles from national and international journals. We removed articles that were not related to ASEAN. Participation in the analysis exceeds the specified time period or at least. To systematically collect the literature, we searched Google Scholar, Scopus, and Web of Science using specific keywords. We then reviewed the abstracts and full texts to refine the results. Cross-referencing is used to ensure that no important research is missed. Finally, the results are grouped by theme. The development of the ASEAN diplomacy system covers the challenges and shortcomings in dealing with these threats.

DISCUSSION

ASEAN Cyber Security Architecture Established to Address Transnational Cyber Threats

As cyber threats become increasingly complex and widespread in Southeast Asia, ASEAN has developed a cybersecurity framework. As digital technology advances, the economy is becoming more integrated. ASEAN countries are increasingly relying on digital systems. cyberspace is also emerging as a new application domain that is vulnerable to various types of attacks. Cyber threats are no longer limited to individual crimes. They now form gangs like organized crime. Hacking groups and even governments pursue their political goals. This made ASEAN aware that national security measures alone were no longer enough. A joint regional framework is needed for joint management of cybersecurity threats (Wijaya & Sari, 2022).

ASEAN's cybersecurity architecture is based on the core principles of non-intervention, consensus and respect for national sovereignty. These values guide cyberspace in overcoming cyber challenges. Prioritize cooperation and trust over strict rules or restrictions. ASEAN views cyber security as a unique security challenge that requires ongoing dialogue. Common principles and convergence remain despite member states actively protecting their national security and data privacy. But ASEAN focuses on building trust among its members rather than collective pressure.

ACCS 2019 lays the foundation for the establishment of regional cybersecurity frameworks in various regions. This approach is based on three pillars: Capacity building; By sharing information and building trust among member countries through ACCS, ASEAN will help member countries provide better protection against cross-border cyber attacks, including ransomware, phishing and data breaches. This strategy is supported by institutional mechanisms such as AMCC, which functions as a joint policy development forum, and ACID, which is used to help regions improve their response to cyber incidents (Tan & Chong, 2021; Lim & Ng, 2023).

Apart from its own internal systems, ASEAN is also working with external partners to develop a cyber security framework. This is part of a strategy to gain security outside the region. ASEAN works closely with external actors including the United States, China, the European Union, and Japan, providing technological tools, training, and access to global best practices to help manage cybersecurity. But this cooperation with foreign partners shows how ASEAN carefully balances different geopolitical interests. So these partnerships are not the only way to improve security. However, this also functions as a diplomatic tool to manage the influence of regional powers (Heng & Tan, 2020).

However, ASEAN cybersecurity framework is slowly evolving. Instead, there is a complete transition from traditional security to traditional security. Its main aim is to coordinate national policies and bridge capacity gaps between member countries. However, there are differences in the source. The lack of technical preparedness and national regulations makes effective intervention against (Rizal, 2024) difficult. To achieve this goal, the ASEAN cybersecurity framework helps countries work together, but the current approach is largely limited to prevention. These countries are still struggling to build capacity and have not yet established legally binding systems to enforce laws against international cyber threats.

Forms and Mechanisms of ASEAN Collective Diplomacy in Cybersecurity Cooperation in the Southeast Asian Region

The Association of Southeast Asian Nations (ASEAN) cooperates in the field of cybersecurity through a legal system and institutions that emphasize mutual cooperation. Build consensus and collaborate with multiple partners to address cyber threats in the region. This is consistent with ASEAN's general approach of avoiding direct confrontation and encouraging consultations to address non-traditional security challenges. From a cybersecurity perspective, this collective diplomacy means ASEAN member countries work together to set standards. Building trust and mutual understanding to address cross-border threats also respects the basic principles of national sovereignty and non-intervention (Wijaya & Sari, 2022).

ASEAN practices cyber security diplomacy through existing regional groups such as the EAS and the ARF. These forums help expand the scope of regional cyber diplomacy by providing a platform for planned dialogue involving ASEAN countries as well as foreign dialogue partners. Cybersecurity is discussed as part of a broader regional security agenda. The focus is on the exchange of ideas, the creation of common standards, and the promotion of multilateral

cooperation. ASEAN jointly responds to cross-border cyber threats through policy coordination. Exchange information and conduct joint exercises through various tools such as the ASEAN Cybersecurity Cooperation Strategy.

The Association of Southeast Asian Nations (ASEAN) collaborates in the field of cyber security through various training programs. The program is designed to help member countries address skills gaps. A good example is the ASEAN–Japan Cybersecurity Capacity Building Programme. This project has progressively improved the way ASEAN countries detect, prevent and respond to technical and organizational cyber attacks. This project shows that ASEAN's diplomatic orientation is focused on long-term technological development. Rather than implementing strict or mandatory rules (Tan & Chong, 2021). ASEAN's collaborative diplomacy is also seen in the creation and strengthening of technological networks such as the ASEAN Computer Emergency Response Team (ASEAN CERT). This group helps government agencies coordinate and share information. Best practices in threat intelligence and incident response. The ASEAN CERT team works to build confidence and ensure the interoperability of countries' technology systems through joint training and simulations. However, because this system is still voluntary and not mandatory, its success in practice depends on the interests and intentions of each participating country (Lim & Ng, 2023; Heng & Tan, 2020).

ASEAN diplomacy provides an opportunity for everyone to work together. But it didn't work out very well. Because they overreact to problems and focus on rules rather than actions. Instead, it uses a built-in early warning or protection system. Teams typically only respond after a major cyber attack. Additionally, integration of critical processes such as joint cyber command or dedicated response roles is also missing. This will limit ASEAN's inclusive diplomacy in facing complex and rapidly changing cyber threats. This shows that ASEAN cooperation is still in its early stages and needs to be strengthened to better address cross-border cyber security.

Key Challenges Facing ASEAN in Developing and Implementing Comprehensive Cybersecurity Diplomacy

Building and using diplomacy with ASEAN in cyberspace is difficult due to overlapping structural, regulatory and geopolitical obstacles. ASEAN has developed various guidelines. Countries will work together, but the focus will be on governance and specific organizational features. This situation makes it difficult to realize fast and coordinated cross-border cooperation. This issue is increasingly complicated because the level of cyber capabilities of member countries varies greatly. For example, Singapore has a comprehensive cybersecurity system. Competent staff and relatively broad understanding of regulatory requirements. At the same time, Laos and Cambodia face technical, institutional and financial challenges. This imbalance makes it difficult for everyone to participate equally in local projects. This can also lead to unequal cooperation patterns. Some countries rely heavily on members understanding certain issues.

The idea that countries should respect each other's sovereignty. Do not interfere during the event. This makes it difficult to share information and coordinate responses. Cybersecurity issues affect national security. Critical infrastructure and personal data Therefore, many ASEAN countries are cautious about sharing details of cyber attacks. Member states did not comment much. Fear of disclosure of information, misuse or interference from outside forces. As a result, ASEAN's diplomacy often focuses on discussing principles rather than finding practical ways to resolve issues (Wijaya & Sari, 2022).

Additionally, each country has different cybersecurity and data protection laws. This situation makes it difficult to formulate uniform policies. Laws are spread throughout the region. This is because each EU member state defines cybercrime differently. There are various laws regarding data protection. And use different levels of practice. This makes it difficult for ASEAN to establish a uniform protocol. This is especially true in the fight against cross-border cybercrime and law enforcement cooperation (Tan & Chong, 2021).

These challenges are exacerbated by global politics and the technological nature of cyber threats. Competition between big countries, especially the United States and China. This will affect the way ASEAN countries cooperate in cyberspace. Especially in the areas of technology, security standards and partner choice. This geopolitical situation also causes a lack of trust between member countries. This makes it difficult to share information about the cyber incident (Heng & Tan, 2020). Additionally, these threats are often anonymous and difficult to detect through specific sources. This means that collective diplomacy is often only at the negotiation stage and there is no real follow-up.

This makes it difficult for ASEAN to translate policy objectives into concrete results. Rather than taking the initiative, ASEAN will likely respond to increasing international cyber threats with (Lim & Ng, 2023).

Effectiveness of ASEAN Cyber Security Architecture in Responding to Transnational Cyber Threats in the Region

To date, the ASEAN Cybersecurity Framework has had limited success in countering cross-border cyber threats. Preventing problems, setting rules and developing long-term skills is more effective than coordinating and acting quickly when something happens. This shows that while ASEAN may want to focus on stability and consensus building, the region is struggling to adapt and respond to rapidly changing cyber threats. This situation increases threats to national security and regional stability. Regarding laws and institutions, groups such as ACCS and other regional associations have helped raise political awareness and encouraged member states to coordinate their policies. Some countries have begun to align their domestic laws with regional standards. However, these reforms were largely carried out at the paper and administrative level. In practice has not been an effective guide for the region in responding to cross-border cyber incidents (Wijaya & Sari, 2022).

When we look at how major cyber incidents such as ransomware attacks on critical infrastructure and key economic sectors in Southeast Asia are handled, we see a decline in ASEAN's cybersecurity posture. Because there is no legally binding way to force everyone to cooperate. Because countries rely heavily on their own resources, responses to these incidents are often slow and fragmented. Any regional cooperation is only temporary and depends on whether the countries involved really need help. This shows that the ASEAN Cybersecurity Framework is not yet ready to take immediate and coordinated steps to address the crisis in the region.

Joint exercises like ACID help national institutions work together more effectively. Information exchange is also carried out through cyber activities in the region. Member States have learned how to exchange information and make response protocols more consistent. However, these efforts primarily focus on the technical dimension and ignore the impact of non-technical risks. Cross-border cyber threats can damage the economy. This situation weakens public confidence and even threatens political and regional stability. Therefore, ACID's role goes beyond the need to enable the ASEAN Cybersecurity Architecture (Tan & Chong, 2021).

The ASEAN Cybersecurity Framework has been successful over the long term in creating rules and frameworks for collective action, but has not been very effective in addressing emerging cross-border cyber threats. The gap between political commitment and actual implementation is mainly due to difficulties in cooperation. Various studies, including the lack of trust, varying skill levels among members, and concerns regarding national governance, suggest that this situation can only improve if ASEAN strengthens key aspects of its security infrastructure (Heng & Tan, 2020). Especially thanks to better integration with global cybersecurity systems. and establishing more coordinated regional response protocols (Lim & Ng, 2023; Rizal, 2024).

CONCLUSION AND RECOMMENDATION

This study shows that ASEAN has developed a cyber security framework using tools such as ACCS, AMCC and ACID. He focused on improving technology. Exchange of information and cooperation with foreign partners. But cyber diplomacy with ASEAN has been largely reactionary. This is limited by the non-intervention rule and the need for consensus. It is also difficult to implement this plan in practice. Because every country has its own incompetence, laws, and lack of trust. and various geopolitical interests. While these systems can help build regional deterrence and policy convergence, they still struggle to effectively respond to rapidly evolving cross-border cyber threats. This shows the difference between what was promised politically and what happened. Overall, ASEAN has established a good framework but is still developing. This indicates the need for further research and policy comparison. This includes more practical and important tools to make the industry more resilient to cyberattacks.

REFERENCES

Caballero-Anthony, M. (2021). ASEAN's evolving regional architecture: Managing great power politics in Southeast Asia. *Modern Southeast Asia, 43* (2), 159–185. https://doi.org/10.1355/cs43-2a

Chong, A., & Tan, S. C. (2020). ASEAN's cybersecurity cooperation: Progress and challenges. *The Pacific Review, 33* (5), 785–812. https://doi.org/10.1080/09512748.2020.1756185

Emmers, R. (2023). ASEAN's security architecture and the challenge of cyber threats. *Asian Security, 19* (1), 45–62. https://doi.org/10.1080/14799855.2022.2156789

Gultom, YSM (2024). ASEAN's preparedness and response against hybrid threats in cyberspace. *Indonesian Journal of International Relations, 8* (2), 415–433. https://doi.org/10.32787/ijir.v8i2.590

Heng, Y. K. (2022). Cybersecurity in Southeast Asia: Norms, institutions, and governance. *Journal of Cybersecurity, 8* (1), tyac001. https://doi.org/10.1093/cybsec/tyac001

Heng, Y. K., & Tan, S. C. (2020). Cyber diplomacy in ASEAN: Balancing sovereignty and cooperation. *Asian Survey, 60* (4), 678–701. https://doi.org/10.1525/as.2020.60.4.678

Lee, BTF, Kornphetcharat, K., Sims, J.P., Linh Dieu, D., & Ali, B.S. (2025). ASEAN cybersecurity cooperation strategy: Combating cyber terrorism and hackers through CERT coordination. *International Journal of Law and Public Policy, 7* (1), 20–30. https://doi.org/10.36079/lamintang.ijlapp-0701.788

Lim, J., & Ng, K. H. (2023). ASEAN's cyber response mechanisms: Lessons from regional drills. *Journal of Southeast Asian Studies, 54* (2), 245–268. https://doi.org/10.1017/S0022463423000123

Moniz, E. de A. (2025). Cybersecurity governance in ASEAN: Building a regional cyber-emergency response framework. *The Journal of Academic Science, 2* (11). https://doi.org/10.59613/0qyvsw72

Phaesaengchan, P., & Chaipumee, A. (2025). ASEAN cybersecurity securitization: Regime of cooperation and enmity. *Graduate Review of Political Science and Public Administration Journal, 4* (1), 29–60.

Rizal, A. (2024). Capacity gaps in ASEAN cybersecurity: A comparative analysis. *Journal of Social and Political Sciences, 28* (1), 45–67. https://doi.org/10.22146/jsp.78901

Rizal, A., & Suryadinata, L. (2019). ASEAN and cybersecurity: Building trust in the digital age. *Journal of International Relations, 8* (2), 123–145. https://doi.org/10.18196/hi.82123

Susanto, H., & Nugroho, A. (2021). Digital transformation and cyber threats in ASEAN: A case study of Indonesia. *Journal of Social and Political Sciences, 25* (1), 67–89. https://doi.org/10.22146/jsp.67890

Tan, S. S., & Chong, A. (2021). Transnational cyber threats and ASEAN's collective response. *International Security, 46* (1), 112–139. https://doi.org/10.1162/isec_a_00412

Wijaya, B., & Sari, DP (2022). ASEAN's collective diplomacy in cybersecurity: Challenges and opportunities. *Journal of International Relations, 11*

ABOUT THE AUTHORS

Andrias Darmayadi, Email: Andrias.darmayadi@email.unikom.ac.id

Andrias Darmayadi, Department of International Relations, Faculty of Social and Political Sciences, Universitas Komputer Indonesia, Bandung City, Indonesia

Dwi fauziansyah Moenardy, Department of International Trade, Faculty of Economics and Business, Universitas Widyatama, Bandung City, Indonesia

Rizal Budi Santoso, Department of International Trade, Faculty of Economics and Business, Universitas Widyatama, Bandung City, Indonesia

Bayu Trisna Ramahadi, LPK Seabar, Bandung City, Indonesia