HJIRS HASANUDDIN JOURNAL OF INTERNATIONAL AFFAIRS

Volume 6, No 1, February 2026
ISSN: 2774-7328 (PRINT), 2775-3336 (Online)

Singapore as A Norm Entrepreneur in Strengthening Regional Cybersecurity through the Development of ASEAN CERT

Muhammad Ismail Anshari
Department of International Relations, University of Gadjah Mada
Yogyakarta, Indonesia
muhammadismailanshar@mail.ugm.ac.id

ARTICLE INFO
Received; 5 November 2025
Accepted: 21 January 2026
Published: 18 February 2026

DOI
10.31947/hjirs.v6i1.48092

Abstract

This article examines the development of the ASEAN Computer Emergency Response Team (ASEAN CERT), which has shown significant progress shaped by Singapore's role as both an initiator and a technical norm entrepreneur in regional cybersecurity. Singapore's proactive engagement is closely linked to its domestic cybersecurity interests and to the broader demands of digital transformation, which remain highly vulnerable to cyber threats. Although ASEAN CERT was adopted by consensus among all ASEAN member states, its implementation continues to face challenges arising from differing perceptions of the importance of CERT mechanisms, as well as disparities in cybersecurity capacity and capabilities across the region. Drawing on norm entrepreneur and norm subsidiarity theories, this study explores Singapore's strategic position as a leading actor in mobilizing its resources to bridge technical gaps in CERT development, using the evolution of the ASEAN cybersecurity cooperation framework as a case study. Furthermore, the article assesses the potential of ASEAN CERT to enhance the technical capacity of ASEAN member states and to contribute to the consolidation and localization of existing international cybersecurity norms in the region.

Keywords: **Singapore, ASEAN, ASEAN CERT, Cyber, Norms**

1. INTRODUCTION

ASEAN is one of the regions that faces a high level of vulnerability to cyberattacks. Several ASEAN member states have become primary targets of malicious cyber activities, a situation exacerbated by weak policy frameworks and limited capacity for cross-border cyber incident response management among ASEAN countries (Putri, 2021). These limitations stem from the region's insufficient sensitivity to the need for a strategic framework in addressing cyber threats, despite the significant impact of such attacks on both public and business sectors (Salsabila et al., 2020). To accommodate the need for a regional strategic framework for coordinating cross-border cyber incident response, the ASEAN Computer Emergency Response Team (ASEAN CERT) Information Exchange Mechanism represents a key initiative to strengthen regional cybersecurity. This mechanism was adopted by consensus at the ASEAN Digital Ministers' Meeting (ADGMIN) in 2021, with Singapore acting as the proponent. The establishment of ASEAN CERT builds upon the ASEAN ICT Masterplan 2020, which was launched during the 15th Telecommunications and Information Technology Ministers' Meeting (TELMIN), reflecting the urgency of securing the rapidly expanding digital economy amid increasingly sophisticated cross-border cyberattacks.

Furthermore, ASEAN CERT aims to facilitate the timely exchange of information on cyber threats and incidents among the national CERTs of ASEAN Member States, while enhancing capacity-building and coordination related to CERT operations without undermining or duplicating the operational roles, mandates, and functions of individual national CERTs. This ASEAN CERT mechanism strengthens Singapore's training hub, namely the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), which was established in 2019 and is envisioned as a new platform and set of procedures for ASEAN to share information, report cyber incidents, and respond to them collectively (ASEAN, 2021). However, the absence of a clear and comprehensive operational mechanism within ASCCE has resulted in weaknesses in incident reporting procedures, thereby constraining the region's collective preparedness and its ability to mitigate cyber incidents due to limitations in information availability (Salsabila et al., 2020).

Although national CERTs across ASEAN Member States have long collaborated through various platforms such as the ASEAN CERT Incident Drill (ACID) and the Asia-Pacific Computer Emergency Response Team (APCERT), the establishment of the *ASEAN CERT Information Exchange Mechanism* marks a shift toward the formalization of information-sharing practices that were previously conducted primarily at the national CERT level. This development supports the region in building a more coordinated technical response to major cyber incidents (Tay, 2023). As part of its commitment to strengthening regional capacity, Singapore's earlier funding pledge of USD 30 million for cyber capacity building has been extended for an additional three years, from 2024 to 2026 (CSA, 2023). However, these initiatives often remain limited in scope and participation, with less-developed member states lagging behind in their ability to fully engage in such activities (Lee et al., 2025). Strengthening CERT capacity at the domestic level therefore remains essential, given persistent disparities in technical capability and institutional maturity that can lead to uneven incident responses and hinder effective regional coordination, particularly for states with limited resources and expertise (Sari, 2023). This suggests that, while ASEAN CERT was adopted by consensus among all ASEAN Member States, its implementation may encounter significant challenges arising from divergent national capacities and capabilities, which in turn shape domestic policy orientations toward the development of national CERTs.

According to the *Global Cybersecurity Index* (GCI) 2024, Singapore is ranked in Tier 1 (role-modelling), alongside Indonesia, Thailand, Viet Nam, and Malaysia. Tier 1 represents the highest level of performance, indicating a strong national commitment to government-led cybersecurity coordination through comprehensive mechanisms of evaluation, development, and implementation across five pillars: legal, technical, organizational, capacity development, and cooperation. Other ASEAN Member States, such as the Philippines, are classified under Tier 2 (advancing); Brunei Darussalam and Myanmar fall into Tier 3 (establishing); while Cambodia and the Lao PDR are placed in Tier 4 (evolving) (ITU, 2024). These findings underscore persistent disparities among ASEAN countries in fulfilling the five GCI pillars, disparities that directly shape each state's ability to strengthen national cybersecurity. Moreover, the five GCI pillars indirectly reflect the extent to which states have internalized international cybersecurity norms–particularly the United Nations Group of Governmental Experts (UN GGE) norms on responsible state behaviour in cyberspace.

Beyond its leadership in funding and the provision of technological infrastructure to support regional capacity-building initiatives, Singapore can thus be regarded as a norm entrepreneur of global cyber norms that are currently being internalized within ASEAN through the development of ASEAN CERT as a regional mechanism for technical CERT integration. This role is further reinforced by Singapore's strategic position in international forums, including its leadership as Chair of the United Nations Open-ended Working Group (OEWG) on ICTs in the context of international security for the period 2021-2025. This role enhances Singapore's reputation at the multilateral level as a key actor in the constellation of global cybersecurity norm discussions, while simultaneously advancing the collective interests of ASEAN member states in cybersecurity governance. Leveraging its resources and technical capacity, Singapore is well positioned to strengthen regional cyber resilience by engaging ASEAN member states in Tiers 2, 3, and 4 through targeted capacity-building activities that address evolving cyber threat trends. Against this background, this article examines how Singapore exercises its strategic role as a norm entrepreneur through the development of ASEAN CERT amid persistent capacity and resource gaps among ASEAN member states, which shape national policy priorities in the implementation of ASEAN CERT at the regional level. Furthermore, the article explores the potential of ASEAN CERT to address weaknesses in existing mechanisms for regional cyber incident coordination. It also analyzes the contribution of ASEAN CERT to regional CERT collaboration, particularly in sustaining cybersecurity stability in Southeast Asia through the adoption and localization of global cyber norms.

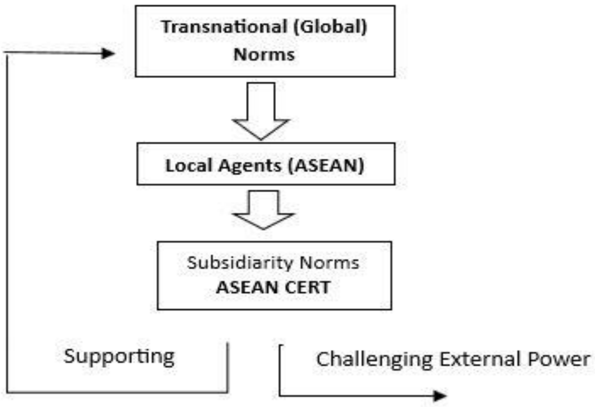
2. ANALITICAL FRAMEWORK

In an anarchic international system, neorealism views state survival as the primary objective, with states understood as rational actors capable of formulating strategies to maximize their chances of survival (Mearsheimer, 2013). Although efforts to ensure survival often drive states to compete for power, such dynamics can also lead to the formation of alliances and other forms of interstate cooperation aimed at addressing common threats. However, the dominance of stronger states over weaker ones may generate deterrence effects that, paradoxically, undermine the sustainability of such cooperation (Ilunga, 2023). Regime theory, by contrast, emphasizes the role of institutional structures in promoting compliance among member states by reducing uncertainty in interstate behavior and fostering trust in shared norms (Haggard & Simmons, 1987). In the context of ASEAN cybersecurity, compliance with norms remains difficult to achieve due to wide disparities in capacity and capability among ASEAN member states, as well as the entrenched principle of non-intervention, which constrains the extent of full compliance (Ramadhan, 2022).

Small states are no longer mere objects of great power competition; instead, they can play a significant role in shaping international norms in the cyber domain, reducing dependence on standards set by major powers (Adamson, 2019). This is why the concept of norm subsidiarity is particularly relevant in highlighting the role of small states in challenging and localizing global cyber governance frameworks at the regional level. Singapore, possessing advanced cybersecurity capabilities, meets the criteria to actively engage in global norm contestation and holds considerable potential to act as a norm entrepreneur, particularly within the ASEAN context. Despite its advanced capacity, Singapore remains committed to promoting norm entrepreneurship both within and beyond the region, while ensuring that other ASEAN member states are not left behind. This commitment is consistent with ASEAN's collective consensus to advocate for global cybersecurity norms while ensuring their alignment with ASEAN's core principles (Allison, 2017).

As a regional organization, ASEAN has developed its own approach to internalizing global norms in order to ensure their compatibility with existing regional principles and values, positioning states as local actors or agents in this process. Within a regional context, the role of a state as a norm entrepreneur is crucial to the diffusion of norms. A norm entrepreneur seeks to persuade other leaders–often referred to as norm leaders–to support and adopt new norms. According to Finnemore and Sikkink (1998), Two key elements contribute to the successful emergence of a new norm: (i) the presence of norm entrepreneurs and (ii) the availability of an organizational platform that can be utilized by these entrepreneurs. ASEAN, as a regional institution, functions as an effective platform for accommodating the diverse national interests of its member states, strengthened by the presence of local norm entrepreneurs who act as norm creators. Both ASEAN member states and the regional organization itself can serve as local agents in promoting norm diffusion by embedding new norms within pre-existing ones, thereby enhancing their legitimacy and fostering shared beliefs around the emerging normative framework (Finnemore & Hollis, 2016).

Figure. 1.1. Subsidiarity Norms



Source: modified by the author based on Acharya, 1998

Norm subsidiarity is defined as a process through which local actors create their own rules in order to preserve autonomy from domination, neglect, violation, or abuse by powerful actors possessing greater material and structural power (Acharya, 1998). ASEAN CERT was established as a regional effort to safeguard the sovereignty of ASEAN member states in cross-border CERT cooperation, reflecting ASEAN interests that are often marginalized within global cyber governance frameworks. In the process of norm subsidiarity, local actors may act as norm makers not by rejecting global norms outright, but by drawing upon them as sources of inspiration for formulating new, localized norms while maintaining regional autonomy from external influence. The concept of norm subsidiarity thus represents a crucial mechanism in the acceptance and localization of global norms. It highlights the capacity of states within a region to develop their own normative frameworks to address external challenges, rather than merely adopting global norms without accounting for the role of local actors (Acharya, 1998). ASEAN member states are currently practicing cyber norm subsidiarity in response to the adoption of global cybersecurity norms by prioritizing regional interests at the global level through ASEAN's consensus-based principles (Chen & Yang, 2022). This approach is consistent with the role of local actors in creating norms that support existing global norms while simultaneously securing their autonomy and counterbalancing the influence of more powerful actors (Acharya, 1998).

ASEAN CERT can also serve as a regional instrument to support the implementation of global cybersecurity norms, particularly those related to technical CERT operations and the protection of critical information infrastructure. Although classified as a small state within ASEAN, Singapore is able to play a strategic role as a local actor in the region by initiating ASEAN CERT and positioning itself as a norm entrepreneur through the effective use of its existing resources and capabilities. Norm entrepreneurs frame norms in ways that resonate with public understanding, drawing on established normative structures and shared collective meanings to generate legitimacy for the norms they promote and to strengthen the credibility of state authority in engaging relevant stakeholders (Qiao-Franco & Nadyatama, 2023). In line with the principle of subsidiarity, this mechanism ensures that incident response remains primarily at the national level, while ASEAN functions as a coordination platform that facilitates faster notification, information sharing, and mitigation of cross-border cyber incidents

3. RESEARCH METHOD

This study employs a qualitative approach using a case study method to analyze Singapore's role as a norm entrepreneur in the field of regional cybersecurity and its initiatives in advancing the development of ASEAN CERT, which was ultimately adopted by consensus among ASEAN member states. A qualitative approach is considered appropriate for examining the social dynamics involved in norm development at the regional level, particularly by highlighting the roles of key actors in the process of institutionalization (Acharya, 2017). This study also highlights the contribution of ASEAN CERT in responding to and localizing global cybersecurity norms that have been adopted within the region. Data collection is based on an analysis of official United Nations and ASEAN documents, complemented by a review of relevant academic literature. In examining official ASEAN documents, the author further analyzes Singapore's activities and initiatives within ASEAN's regional cybersecurity mechanisms, including the ASEAN Network Security Action Council, the ASEAN Cybersecurity Coordinating Committee, the ASEAN Checklist for the Implementation of Norms, the ASEAN Cybersecurity Cooperation Strategy 2021-2025, and other relevant frameworks. The analysis focuses on tracing the development of cybersecurity norms at both the global and regional levels, as reflected in agreed documents, and assessing their contribution to the region.

In addition to official documents, a literature review is conducted to deepen the theoretical understanding of norm entrepreneurship and norm subsidiarity, as well as the processes underpinning the formation of ASEAN CERT. This review draws on books, scholarly articles, academic journals, research reports, and publicly accessible news articles relevant to the research topic. Through an in-depth analysis of these documents, this study examines how ASEAN CERT has evolved as a mechanism to address regional needs for integrated cyber incident response, while taking into account the domestic policy dynamics of individual member states. It also evaluates the potential of ASEAN CERT to provide effective solutions to technical disparities among ASEAN countries through capacity-building initiatives facilitated by Singapore. In addition, the study investigates the contribution of ASEAN CERT to the implementation of global cyber norms, particularly within the technical pillar, which is currently being internalized across ASEAN.

4. RESULT AND DISCUSSION

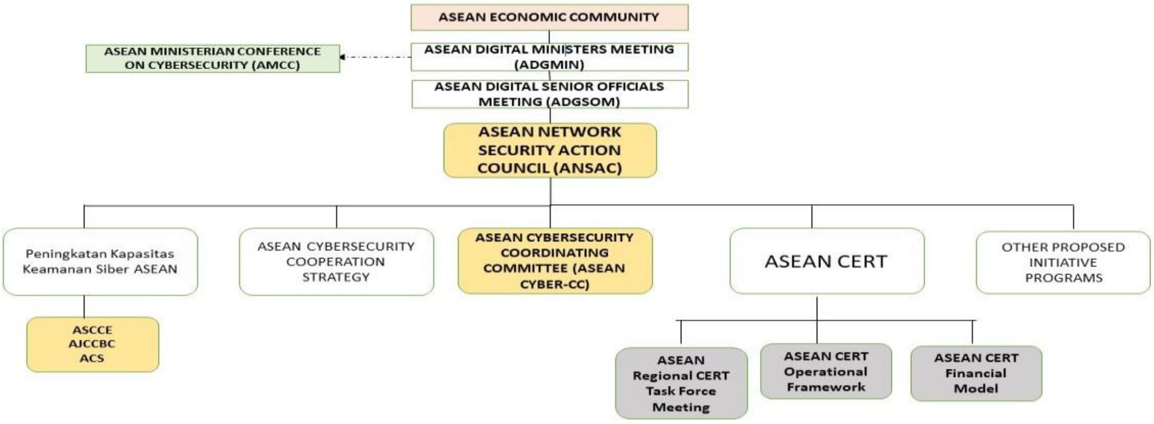
4.1 Singapore's Role in ASEAN Cybersecurity Cooperation

Singapore stands out as one of the ASEAN member states that views cybersecurity as a highly critical issue deserving significant policy attention. Singapore recognizes that the securitization of cybersecurity within ASEAN is essential for fostering regional cooperation aimed at achieving a harmonious partnership among ASEAN member states. This securitization is closely linked to Singapore's position as one of five countries in the Asia–Pacific region, including Australia, Japan, South Korea, and New Zealand that face cyberattack vulnerabilities estimated to be nine times higher than those of other countries, including most ASEAN states (Parameswaran, 2016). In response, Singapore has made substantial investments in the cybersecurity sector to enhance public awareness of the importance of cybersecurity (Permata & Nanda, 2019). To strengthen its strategic position at the global level, Singapore initiated Singapore Cybersecurity Week as an annual event beginning in 2016, inviting all ASEAN member states as well as non-ASEAN partner countries. Gradually, Singapore has consolidated its role as an economic hub in Southeast Asia and a regional leader in technological infrastructure by cultivating a secure cyberspace environment both domestically and regionally (Ansari & Ramadhan, 2019).

Since the adoption of the Singapore Declaration at the 3rd Meeting of Ministers of Telecommunications and Information Technology (TELMIN) in 2003, ASEAN has acknowledged the urgent need for systematic infrastructure and mechanisms to secure cyberspace amid rapid digital transformation. In response, all ASEAN member states developed early warning and cyber incident response systems through the establishment of national Computer Emergency Response Teams (CERTs) (Dai & Gomez, 2018). Over the following thirteen years, Singapore progressively built a robust organizational structure and policy framework to strengthen its national cybersecurity capacity, beginning with the Infocomm Security Master Plan (2005–2007), followed by the Infocomm Security Master Plan II (2008–2012), and subsequently the National Cyber Security Master Plan 2018 (NCSM2018), launched in 2013. To further consolidate these efforts, the Cyber Security Agency of Singapore (CSA) was established in April 2015 as a national body under the Ministry of Communications and Information, tasked with overseeing, coordinating, and strengthening Singapore's cybersecurity initiatives (Vu, 2016).

According to IBM's 2024 report, each ASEAN country suffered an estimated average financial loss of USD 4.8 million from cyber incidents, with data breach containment taking an average of 258 days (IBM, 2024). The significant economic and security risks posed by data breaches have reinforced Singapore's recognition of the need to securitize cybersecurity issues at the ASEAN level. This approach seeks to promote regional cooperation and establish a harmonized partnership among ASEAN member states in addressing cybersecurity challenges (Permata & Nanda, 2019). In the context of digital transformation, securitization elevates cybersecurity as a vital concern due to its potential impact on human security, particularly in safeguarding personal data and mitigating financial losses. Consequently, Singapore has positioned cybersecurity as a central agenda item in various regional forums and elevated it as a domestic policy priority. Within the ASEAN framework, cybersecurity has emerged as a cross-sectoral issue discussed across multiple ministerial-level bodies, including the ASEAN Foreign Ministers' Meeting (AMM), the ASEAN Defence Ministers' Meeting (ADMM), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), and the Telecommunications and Information Technology Ministers' Meeting (TELMIN), which was renamed the ASEAN Digital Ministers' Meeting (ADGMIN) in 2019. The ASEAN Ministerial Conference on Cybersecurity (AMCC), initiated by Singapore, serves as an informal platform for cross-sectoral dialogue and collaboration on regional cybersecurity cooperation. In parallel with the transformation of TELMIN into ADGMIN, the ASEAN Network Security Action Council (ANSAC) was established to provide a formal technical coordination mechanism, particularly for proposing and advancing cybersecurity-related initiatives within the ASEAN framework (ASEAN, 2018).

Figure 1.2. ASEAN Cybersecurity Cooperation Mechanism


ASEAN ECONOMIC COMMUNITY
ASEAN MINISTERIAN CONFERENCE ON CYBERSECURITY (AMCC)
ASEAN DIGITAL MINISTERS MEETING (ADGMIN)
ASEAN DIGITAL SENIOR OFFICIALS MEETING (ADGSOM)
ASEAN NETWORK SECURITY ACTION COUNCIL (ANSAC)
Peningkatan Kapasitas Keamanan Siber ASEAN
ASEAN CYBERSECURITY COOPERATION STRATEGY
ASEAN CYBERSECURITY COORDINATING COMMITTEE (ASEAN CYBER-CC)
ASEAN CERT
OTHER PROPOSED INITIATIVE PROGRAMS
ASCCE AJCCBC ACS
ASEAN Regional CERT Task Force Meeting
ASEAN CERT Operational Framework
ASEAN CERT Financial Model

Source: modified by the author based on https://asean.org/who-we-work-with/asean-sectoral-ministerial-bodies/

Within the ANSAC mechanism, the establishment of ASEAN CERT is incorporated into the ASEAN Cybersecurity Cooperation Strategy 2021–2025 as one of its key initiatives, with Singapore serving as the lead country. Since its endorsement in 2022, the ASEAN CERT has developed a comprehensive support framework to facilitate its implementation through the drafting of the ASEAN CERT Operational Framework, which was officially adopted by ASEAN member states during the 3rd ASEAN Digital Ministers' Meeting (ADGMIN) in 2023. This framework outline the purpose, scope, composition and partners, functions, and mechanism of the ASEAN CERT. In February 2024, ASEAN member states approved the ASEAN CERT Financial Model, based on Singapore's proposal to fund and host the ASEAN Regional CERT for a ten-year period, with an estimated operational budget of USD 10.1 million (CSA, 2024). Singapore further advanced the initiative by convening the first ASEAN Regional CERT Task Force Meeting, marking the transition of ASEAN CERT into its practical implementation phase through an action plan that actively involves other ASEAN member states. The process culminated in October 2024 with the official launch of ASEAN CERT at the Singapore International Cyber Week 2024 (CSA, 2024).

Table 1.1. Progress Update of Initiatives List Led by Singapore

Initiative List by Singapore	**Year**	**Progress Update**
ASEAN CERT Maturity Framework	2022	Adopted
ASEAN Regional Action Plan on the Implementation of Norms of Responsible State Behaviour in Cyberspace	2022	Adopted
ASEAN CERT Operational Framework	2023	Adopted
ASEAN CERT Financial Model	2024	Adopted
ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace	2024	Adopted
Launching of ASEAN CERT	2024	Launched
ASEAN Regional CERT Task Force Meeting	2024	Ongoing (annually)

Source: Modified the author based on www.csa.gov.sg

This progress reflects a positive trajectory in the development of ASEAN CERT as an instrument for CERT cooperation among ASEAN member states, while simultaneously reinforcing Singapore's position as a norm entrepreneur. Following the adoption of ASEAN CERT, a range of activities has been undertaken to promote the mechanism and engage a broader set of stakeholders. During several ASEAN cyber dialogues with non-ASEAN partner countries—such as the United States, India, Australia, Russia, and China—Singapore has promoted ASEAN CERT as a regional achievement in building mutual trust among ASEAN member states through coordinated CERT mechanisms. In the area of capacity development, Singapore has established partnerships with national CERTs of ASEAN member states in cooperation with INTERPOL, as well as facilitated the provision of industry-based cyber threat intelligence feeds to all ASEAN Member States (AMS). In October 2025, Singapore was organized the first physical iteration of the ASEAN CERT Incident Drill (ACID), inviting incident responders from all ten ASEAN member states and ASEAN Dialogue Partners. Participants use the ASEAN Regional CERT's Information Sharing Mechanism (ISM) for the first time to facilitate cross-border threat intelligence sharing. The ISM functions as a centralized communication channel that enables cyber threat information exchange, technical collaboration, and coordination of regional cyber exercises (CSA, 2025).

4.1. ASEAN CERT and Challenges

In implementing the ASEAN CERT, Singapore serves as both the host country and the principal funder of the project, while ASEAN acts as the facilitator overseeing the initiative. The overall coordinator, responsible for preparing the strategy and action plan of the ASEAN CERT, is designated based on the ASEAN member state holding the ANSAC chairmanship during that period. This country is tasked with reporting the progress of the ASEAN CERT to the ASEAN Secretariat, which subsequently places it on the agenda of ANSAC and ADGMIN meetings To strengthen regional partnerships and information sharing among ASEAN member states, the ASEAN CERT mechanism consists of eight core functions: (i) facilitating coordination and information exchange among national CERTs, (ii) developing and maintaining a point of contact (PoC) network comprising representatives from national cybersecurity agencies, (iii) organizing ASEAN cybersecurity conferences, meetings, and training for national CERTs, (iv) facilitating regional capacity-building programs, (v) cooperating with international and regional organizations to advance ASEAN's cybersecurity interests and objectives, (vi) developing partnerships with industry and academia, (vii) supporting national CERT capacity building and sharing best practices, and (viii) promoting cybersecurity awareness campaigns through collaboration with relevant ASEAN sectoral bodies and the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) (CSA, 2024). Each of these eight functions is led by one ASEAN member state, which serves as the lead country responsible for coordinating implementation among others.

Table 1.1. Global Cybersecurity Index 2024 Results

Country	Technical	Capacity Development	Legal	Organizations	Cooperation	Tier
Singapura	20	19,86	20	20	20	1 (Role Modelling)
Indonesia	20	20	20	20	20	1 (Role Modelling)
Malaysia	20	20	20	18,82	20	1 (Role Modelling)
Thailand	20	20	20	19,22	20	1 (Role Modelling)
Vietnam	20	19,74	20	20	20	1 (Role Modelling)
Filipina	19,11	17,17	20	19,51	17,7	2 (Advancing)
Brunei Darussalam	14,89	10,76	17,2	11,35	16,18	3 (Establishing)
Myanmar	10,9	14,42	15,34	13,06	20	3 (Establishing)
Kamboja	4,56	6,12	17,2	11,35	16,8	4 (Evolving)
Lao PDR	6,18	2,05	10,38	5,52	9,61	4 (Evolving)

Source: Global Cybersecurity Index 2024 (ITU, 2024)

According to the Global Cybersecurity Index (GCI) 2024, particularly regarding the technical and capacity development pillars both closely tied to ASEAN CERT implementation there remains a substantial gap among countries in tiers 1 to 4 in terms of infrastructure readiness, technical expertise, and the availability of skilled cybersecurity professionals. This disparity influences the uneven distribution of ASEAN CERT functions, which tend to be dominated by tier 1 countries, with some leading multiple functions simultaneously. Although all ASEAN countries have expressed their commitment to supporting ASEAN CERT implementation, differences in national capacity risk creating fragmentation among member states, potentially widening the regional divide in technological and institutional readiness. Differences in national priorities and understanding of the CERT concept also hinder the harmonization of regional objectives to establish an integrated CERT coordination mechanism. This challenge is compounded by the diverse social, political, and economic characteristics of ASEAN states, as regional cooperation has traditionally emphasized economic interests. In several ASEAN countries such as Myanmar and Lao PDR, CERT development remains a low policy priority due to limited human resources and infrastructure (Chang, 2017). The absence of autonomous national cybersecurity agencies also slows information flow and response time, as decision-making processes still involve multiple government stakeholders.

The uneven availability of adequate policy frameworks, particularly in Tier 2, 3, and 4 countries—has significant implications for domestic capacity to conduct effective cross-border coordination. This condition complicates the harmonization of legal frameworks, data protection laws, and technical standards among ASEAN member states, thereby impeding the timely exchange of information required for urgent and rapid incident response (Syahputra & Hidayati, 2024). Disruptions in information flows ultimately slow down incident handling and mitigation processes, resulting in substantial financial losses from cyber incidents. These domestic policy priorities reaffirm that ASEAN CERT lacks the legal authority to compel full participation from member states, as ASEAN itself operates strictly as a facilitator without jurisdiction over members' domestic affairs. However, this structural limitation may hinder ASEAN CERT's overall effectiveness and weaken regional cybersecurity resilience

To address this challenge, ASEAN with Singapore as a regional norm entrepreneur can collaborate to encourage greater participation from less active member states by assigning them co-lead roles in selected functions aligned with their domestic priorities and institutional capacities. Such an approach would enhance functional inclusivity, promote knowledge sharing, and foster mutual learning among member states with varying levels of cybersecurity capability. The development of a regional legal framework is therefore necessary to facilitate policy integration and harmonization across ASEAN member states, enabling faster and more responsive cross-border cooperation among CERTs in addressing cyber incidents. Capacity-building thus serves as a crucial foundation for strengthening ASEAN's cybersecurity ecosystem. Initiatives such as the ASEAN Cyber Capacity Programme (ACCP) and the ASEAN–Singapore Cybersecurity Centre of Excellence (ASCCE) enable Singapore to optimize its leadership role as a norm entrepreneur by supporting ASEAN member states in improving incident response capabilities, enhancing technical expertise, and building regional cyber resilience through targeted talent development and cooperative training programs (ACICE, 2024).

4.2. Contribution of ASEAN CERT to Global Cyber Norms

Singapore plays a dominant role in the contestation of ASEAN cybersecurity cooperation by serving as the lead country in several initiatives under both the ASEAN Network Security Action Council (ANSAC) and the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC). In addition to ASEAN CERT, Singapore also leads capacity-building initiatives through the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) based in Bangkok, Thailand. In the development of the legal and normative aspects, Singapore and Malaysia jointly initiated the ASEAN Regional Plan of Action

(RAP) on the Implementation of Norms of Responsible State Behaviour in Cyberspace, which was subsequently followed by the adoption of the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace in October 2024.

ASEAN CERT has indirectly contributed to the fulfilment of global UN cyber norms, particularly in the technical aspects related to CERT operations. The UN GGE 2015 Report highlighted eleven norms of responsible behaviour in cyberspace that were agreed upon by global consensus. These norms are categorized into two types: restrictive norms, which aim to prevent activities that could threaten cyberspace, and enabling norms, which encourage states to fulfil their obligations in maintaining cyber stability and security (CCAPAC, 2017). However, given the capacity gap among ASEAN states particularly between Tier 1 countries and Tiers 2, 3, and 4, ASEAN CERT is projected not only to serve as a mechanism for contributing to global cyber norms within the region, but also to bridge existing gaps through ASEAN's inclusive and participatory mechanisms that consider each country's readiness to engage. ASEAN CERT contributes to the implementation of preventive norms by optimizing coordination and collaboration mechanisms among member states to engage a broader range of relevant stakeholders, thereby enabling faster and more effective mitigation efforts. These efforts are closely linked to the protection of critical information infrastructure and the security of supply chains that are highly vulnerable to cyberattacks and pose significant risks to the continuity of public services.

The functions of ASEAN CERT reflect the region's need for integrated regional policies, secure and efficient cross-border coordination and collaboration, the enhancement of cybersecurity capacity, and the strengthening of confidence-building measures through regional cooperation. The norms related to these preventive measures include: (i) consideration of all relevan information, (ii) prevention of misuse of ICTs within national territories, (iii) cooperation in combating cybercrime and terrorism, (iv)prohibition of harmful ICT activities targeting Critical Information Infrastructure (CII), (v) protection of Critical Information Infrastructure (CII), (vi) Responding to requests for assistance, (vii) ensuring supply chain security, (viii) reporting ICT vulnerabilities, and (ix) protection of CERTs (ASPI, 2022).

Table 1.1. Contribution of ASEAN CERT to the Implementation of UN GGE Cyber Norms

Norm	Description	ASEAN CERT's Contribution to the Region
Consideration of all relevant information	This norm encourages states to consider all relevant information, including major events, attribution challenges at both regional and global levels, and potential consequences.	ASEAN CERT can serve as a platform for ASEAN member states to exchange information with other national CERTs, identify potential cyber threats, mitigate cross-border incidents, and determine which information should remain confidential to safeguard national sovereignty.
Prevention of misuse of ICTs within national territories	This norm urges states not to allow their territories to be used for internationally wrongful ICT activities.	– ASEAN CERT can expedite notification processes when ICT-related activities are suspected of using another state's territory. – ASEAN CERT can initiate regional guidelines and mitigation measures for cyberattacks, enhancing communication channels for notification and assistance

Norm	Description	ASEAN CERT's Contribution to the Region
		through both national CERT/CSIRT networks and regional frameworks. – In attribution processes, ASEAN CERT may act as a neutral party to ensure proportional responses that comply with international law.
Cooperation in combating cybercrime and terrorism	This norm encourages states to strengthen cooperation in information sharing, mutual assistance, and law enforcement against cybercrime and terrorism.	As the Point of Contact (PoC), ASEAN CERT can enhance coordination among relevant ASEAN sectoral bodies such as ADMM, AMMTC, and the ASEAN Regional Forum (ARF), ensuring that cyber incident information flows through ASEAN CERT to facilitate faster digital evidence collection and law enforcement.
Prohibition of harmful ICT activities targeting Critical Information Infrastructure (CII)	States should not engage in or support unlawful ICT activities that intentionally disrupt the operation of CIIs providing public services.	ASEAN CERT can promote the establishment of protection mechanisms for CIIs at both domestic and regional levels, prioritizing sectors with high societal impact.
Protection of Critical Information Infrastructure (CII)	States should take appropriate measures to protect CIIs from ICT threats.	– Some ASEAN states still lack proper CII protection mechanisms due to varying definitions of which sectors qualify as CII. – ASEAN CERT can stimulate the development of relevant domestic policies aligned with global norms and gradually provide regional-level CII protection guidelines.
Responding to requests for assistance	States should respond to assistance requests from other states whose CIIs have been targeted by harmful ICT activities.	ASEAN CERT can establish more efficient assistance mechanisms by integrating national CERTs, ensuring effective correspondence and coordinated incident responses.
Ensuring supply chain security	States should take concrete measures to ensure the integrity of ICT supply chains to enhance user trust.	To protect supply chains, ASEAN CERT can identify cyber threats and issue notifications through coordination between national CERTs and sectoral CERT/CSIRT entities from both the public and private sectors, preventing disruptions caused by cyberattacks.
Reporting ICT vulnerabilities	States should encourage ICT vulnerability reporting and share relevant information to	ASEAN CERT can provide periodic reports on ICT vulnerabilities across all ASEAN states—regardless of technical capacity—

Norm	Description	ASEAN CERT's Contribution to the Region
	limit or eliminate potential threats.	thereby creating an integrated preventive mechanism for cyber incidents.
Protection of CERTs	States should not engage in or knowingly support activities that endanger other states' incident response teams.	– ASEAN CERT is an integral part of CII and reflects ASEAN's commitment to establishing a coordinated CERT mechanism that respects state sovereignty. – ASEAN CERT embodies the principle of non-interference, ensuring political neutrality. – ASEAN CERT can serve as a catalyst to prevent potential conflicts of interest among ASEAN states that could jeopardize other CERTs.

Source: compiled by the author from Annual Progress Report (UNGA, 2024)

This demonstrates ASEAN CERT's potential to engage not only non-state actors but also corporations, the critical information infrastructure (CII) sector, and law enforcement agencies in the full implementation of ASEAN CERT mechanisms. The eight core functions of ASEAN CERT provide practical avenues for fostering multistakeholder cooperation. These strengths can help bridge capacity gaps among ASEAN member states in responding to cyber incidents and accelerate cross-border information sharing. In addition, ASEAN CERT also demonstrates ASEAN's commitment to actively localize and implement global cyber norms at the regional level, aligning with other regional CERTs, and promoting cooperation in capacity building, information sharing, strengthening regional cybersecurity resilience, and mitigating cross-border cyber incidents.

5. CONCLUSION

The securitization of cybersecurity undertaken by Singapore over the past decade has resulted in a robust domestic cyber governance framework and has even extended the securitization trend to the regional level. As a small state, Singapore has solidified its position as a cybersecurity hub in Southeast Asia by strategically leveraging ASEAN's regional cybersecurity cooperation frameworks to enhance its global image as a leading partner in cybersecurity initiatives. Decades of sustained investment have positioned Singapore as a regional leader in cybersecurity capacity and capability, enabling it to assume the role of a norm entrepreneur among ASEAN member states, particularly through its leadership in the development of ASEAN CERT. With its advanced infrastructure, technological resources, and financial capital, Singapore is well equipped to help narrow cybersecurity capacity gaps across ASEAN by facilitating pathways for partnerships and investment from ASEAN dialogue partners. Its objective is not only to ensure regional cyber stability but also to strengthen its own national cyber resilience. Despite significant progress in regional cybersecurity strategy and policy frameworks over the past five years, ASEAN states will require considerable time to reach comparable levels of capacity and capability.

This is understandable, given the many technical and non-technical challenges that remain unaddressed. Active participation and collaboration among ASEAN states in the operationalization of ASEAN CERT are therefore critical to creating spaces for dialogue and information sharing, particularly in bridging capacity gaps among national CERTs and enhancing the protection of critical information infrastructure. However, as ASEAN CERT remains in an ongoing developmental phase, its institutional mechanisms have yet to operate at an optimal level. Future research may further examine how ASEAN CERT can enhance the participation of ASEAN member states especially those classified as Tier 2, 3, and 4, in actively engaging with ASEAN CERT activities and initiatives, as well as the implications of such engagement for improving domestic cybersecurity capacity. Aside of that, with steadily increasing capacity, other tier 1 countries such as Indonesia, Malaysia, Thailand, and Vietnam are well positioned to emerge as the next norm entrepreneurs in the development of new cybersecurity norms in the region. As a strategically significant region in the Asia-Pacific, ASEAN CERT holds considerable potential to evolve into a regional CERT with a standing comparable to Asia-Pacific CERT (APCERT) or the Organization of Islamic Cooperation CERT (OIC-CERT), and to expand opportunities for inter-regional CERT cooperation in the future.

REFERENCES

Articles and Publications

ACICE (2024). Update on the Cyber Domain. ADMM Cybersecurity and Information Centre of Excellence. Retreived from https://www.acice-asean.org/files/cybersecurity%20centre%20reports/sep_24_cyber.pdf

ASEAN (2018). Leader’s Statement on Cybersecurity Cooperation Strategy. 32nd ASEAN Summit. Retreived from https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf

ASEAN (2021). ASEAN Security Outlook 2021. Retreived from https://asean.org/wp-content/uploads/2021/10/ASEAN-Security-Outlook-ASO-2021.pdf

ASPI (2022). The UN norms of responsible state behaviour in cyberspace. Retreived from https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace/

CCAPAC (2017). Norms for Cybersecurity in Southeast Asia. Access Partnership, Ltd. Retreived from https://ccapac.asia/wp-content/uploads/2022/03/Norms-for-Cybersecurity-in-Southeast-Asia.pdf

CSA (2023). Singapore Deepens Commitment to a Secure Cyberspace Through Capacity Building. Retreived from https://www.csa.gov.sg/news-events/press-releases/singapore-deepens-commitment-to-a-secure-cyberspace-through-capacity-building/

CSA (2024). Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region. Retreived from https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region

CSA (2025). CERTS From ASEAN Member States Gather in Singapore for the First Time to Participate in the ASEAN CERT Incident Drill (ACID). Retreived from https://www.csa.gov.sg/news-events/press-releases/certs-from-asean-member-states-gather-in-singapore-for-the-first-time-to-participate-in-the-asean-cert-incident-drill--acid-/

IBM (2024). Cost of Data Breach Report 2024. Retreived from https://www.ibm.com/reports/data-breach

ITU. (2024). Global Cybersecurity Index 2024 5th Edition. ITU Publication. pp.28. Retreived from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

UN General Assembly (2024). Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025. Retreived from https://docs.un.org/en/a/79/214#:~:text=At%20its%20eighth%20substantive%20session%2C%20on%2012,report%20of%20the%20open%2Dended%20working%20group%20(A/AC.&text=This%20third%20APR%20will%20be%20submitted%20to,the%20OEWG%27s%20mandate%20contained%20in%20resolution%2075/240

Vu, C (2016). Cyber Security in Singapore. Rajaratnam School of International Studies. Retreived from https://rsis.edu.sg/rsis-publication/rsis/cyber-security-in-singapore/

Journals

Acharya.A (1998). Culture, security, multilateralism: The ‘ASEAN Way’ and Regional Order. Contemporary Security Policy. pp. 97-98

Acharya, A. (2017). The evolution and limitations of ASEAN identity. Contemporary Southeast Asia: The politics of change, contestation, and adaptation. Palgrave. pp. 25-42.

Adamson, L (2019). Let Them Roar: Small States as Cyber Norm Entrepreneurs. European Foreign Affairs Review, Issue 2, pp. 217-234. https://doi.org/10.54648/eerr2019014

Allison-Reumann, L. (2017). The Norm-Diffusion Capacity of ASEAN: Evidence and Challenges. Pacific Focus 32(1): 5–29. https://doi.org/10.1111/pafo.12089

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

Chang, L (2017). Cybercrime and Cyber Security in ASEAN. Comparative Criminology in Asia pp 135-148. Retreived from DOI: 10.1007/978-3-319-54942-2_10

Chen, X & Yang, Y (2022). “Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance”. The International Spectator. Vol 57 (3). hlm. 57-58.

Dai, T., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. Journal of Cyber Policy, 3(2), 217–235. https://doi.org/10.1080/23738871.2018.1487987

Finnemore, M & Hollis, D.B (2016). Constructing Norms for Global Cybersecurity. The American Journal of International Law, Vol. 110, No. 3. pp. 425-479. DOI:10.1017/S0002930000016894

Finnemore, M & Sikkink, K (1998). International Norm Dynamics and Political Change. International Organization Vol 52 (4). hlm. 894-905. DOI: 10.1162/002081898550789

Haggard, S & Beth, A. 1987. Theories of international regimes. International Organization 41, no. 3: 491-517.

Ilunga, SK (2023). Regional Cooperation on Cybersecurity Challenges: An Assessment of ASEAN’s Efforts to Promote Shared Cybersecurity. ASEAN International Sandbox Conference. Vol 1.

Lee, et. All (2025). ASEAN Cybersecurity Cooperation Strategy: Combating Cyber Terrorism and Hackers Through CERT Coordination. International Journal of Law and Public Policy. Vol 7 (1). pp 20-30.

Mearsheimer, J. (2013). Structural Realism. *International Relations Theories: Discipline and Diversity* (pp. 77-91). In T. Dunne, M. Kurki, & S. Smith (Eds). Oxford University Press.

Parameswaran, P (2016). Singapore Among Most Vulnerable to Cyberattacks in Asia Report. Retreived from https://thediplomat.com/2016/02/singapore-among-most-vulnerable-to-cyberattacks-in-asia-report/

Permata, I & Nanda, B (2019). The Securitization of Cyber Issue in ASEAN. The International Conference on ASEAN 2019. pp. 90-97. DOI:10.1515/9783110678666-012

Putri, V (2021). Kerjasama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime", Malang: FH Universitas Brawijaya, Rewang Rencang Jurnal Hukum Lex Generalis. Vol.2 (7).

Salsabila, A, et. All (2020). Potential and Threat Analysis Towards Cybersecurity in South East Asia. Journal of ASEAN Dynamics and Beyond. Vol 1(1). Retreived from DOI:10.20961/aseandynamics.v1i1.46794

Sari, M.N. (2023). ASEAN's Regional Effort on Cybersecurity and Its Effectiveness. KEIO SFC JOURNAL, 23(1). Retreived from doi:10.14991/003.00230001-0026

Tay, Lin K (2023). ASEAN Cyber-security Cooperation: Towards a Regional Emergency-response Framework. The International Institute for Strategic Studies. Retreived from https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/06/asean-cyber-security-cooperation.pdf

Ramadhan, I (2022). ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia. Conference: ICONIC-RS. DOI:10.4108/eai.31-3-2022.2320684

Syahputra, R & Maslihati, H (2024). Implementasi Mutual Legal Assistance (MLA) untuk Perlindungan Data Pribadi Pengguna Layanan Komputasi Awan di ASEAN. Jurnal Ilmiah Universitas Muhammadiyah Buton. Vol 10 (3).

Tran Dai, C., & Gomez, M. A. (2018). Challenges and opportunities for cyber norms in ASEAN. Journal of Cyber Policy, 3(2), 217–235. Retreived from https://doi.org/10.1080/23738871.2018.1487987

Qiao-Franco, G & Nadyatama, R (2023). ASEAN as a Norm Entrepreneur in International Cooperation on Nuclear Non-proliferation: Bases, Pathways, and Challenges. Norm Diffusion Beyond the West. pp.165-182. Retreived from https://doi.org/10.1007/978-3-031-25009-5_10