Review of International Relations
(Jurnal Kajian Ilmu Hubungan Internasional)
Volume 8 Issue 1 (2026), pp. 169-192
doi: 10.24252/rir.v8i1.67087



INVESTIGATING SINGAPORE'S CYBER NORM ENTREPRENEURSHIP IN SOUTHEAST ASIA

Rifki Dermawan[1*], Diah Anggraini Austin[2]
Universitas Andalas[1,2]

Abstract

Global actors have been developing cyber norms in order to manage cyberspace. In the Southeast Asia region, Singapore emerges as a leading state in cyber cooperation. Its proactive participation has contributed to development of cyber joint efforts in the region. The city-state's central role raises the question of whether it can be considered a regional cyber norm entrepreneur. To answer this question, the study uses a constructivist approach and employs the analytical framework of small states as cyber norm entrepreneurs with three parameters, i.e., type of engagement, avenue, and Information and Communications Technology (ICT) capabilities. The research method is qualitative with a process-tracing mechanism. The data are based on archives or documents available online. The result of analysis indicates that Singapore can be labelled Southeast Asia's cyber norm entrepreneur. The island nation mainly relies on soft approaches in constructing and developing the norms. It also heavily depends on ASEAN as a platform for norms engagement. Its ICT development level is at an advanced level compared to other nations globally. This research contributes to the study of small states' role in norm entrepreneurship and exploration of the cyber landscape in Southeast Asia.

Keywords: *cyber norms; Southeast Asia; Singapore; small state; cyber norm entrepreneur*

Abstrak

Aktor-aktor global mengembangkan norma siber dengan tujuan untuk mengelola ruang siber. Di kawasan Asia Tenggara, Singapura muncul sebagai aktor yang memimpin kerja sama di ranah siber. Partisipasi aktif dari Singapura berkontribusi terhadap pengembangan kerja sama siber di kawasan. Peran penting dari negara-kota ini memunculkan pertanyaan apakah Singapura bisa dianggap sebagai norm entrepreneur *di bidang siber di kawasan. Untuk menjawab pertanyaan tersebut, penelitian ini menggunakan pendekatan konstruktivis dan mengaplikasikan kerangka analisis tentang*

*Corresponding Author: Rifki Dermawan, Departemen Hubungan Internasional, Universitas Andalas, Indonesia

P-ISSN: 2685-5879; E-ISSN: 2685-421X
Submitted: 16 April 2026; Revised Version: 8 June 2026; Accepted: 11 June 2026; Published: 15 June 2026

negara kecil sebagai norm entrepreneur *di ranah siber dengan tiga parameter yaitu bentuk pendekatan, wadah, dan kemampuan Teknologi Informasi dan Komunikasi (TIK). Metode penelitian adalah kualitatif dengan mekanisme proses penelusuran jejak. Hasil analisis menunjukkan bahwa Singapura bisa diposisikan sebagai* norm entrepreneur *bidang siber di Asia Tenggara. Negara pulau ini secara umum menggunakan pendekatan lunak dalam membentuk dan mengembangkan norma. Singapura juga sangat bergantung kepada ASEAN sebagai wadah untuk berinteraksi dengan norma-norma. Tingkat perkembangan TIK Singapura sudah berada di tingkatan maju dibandingkan dengan negara-negara lain secara global. Penelitian ini berkontribusi terhadap kajian peran negara kecil dalam* norm entrepreneurship *dan eksplorasi ruang siber Asia Tenggara.*

Kata Kunci: *norma siber; Asia Tenggara; Singapura; negara kecil;* norm entrepreneur *bidang siber*

Introduction

Cyberspace has become a platform for interaction, cooperation as well as competition among various international actors, including states and non-states actors. From 2015 to 2025, the number of internet users globally doubled from 3 billion to 6 billion, with high level of communication skills among them, regardless the level of internet development in their country (International Telecommunication Union, 2025). However, the fast pace of internet evolution is not in line with the creation of regulations in this area due to the non-existent comprehensive global rules (Yau, 2022, p.1).

It does make sense that governing cyberspace is not a simple task, given that it is a "fifth domain" of the global commons, alongside the ocean, air/atmosphere, the Antarctic, and outer space. Global commons can be defined as "naturally occurring domains or areas which are not governed by any single nation-state or political jurisdiction" (Burnay & Chaisse, 2020, p. 5). Several scholars viewed cyberspace in terms of its characteristics as global commons. For instance, Meyer (2016) compared cyberspace to the sea, and (Yau, 2022, p. 1) emphasized that the major difference between cyberspace and the other commons is its construction, since cyberspace is created by human beings. Looking at the features of cyberspace as global commons, it can be argued that some

challenging aspects of governing this area include highly competing interests among actors and the "unlimited" number of actors accessing the internet.

Despite complex dynamics in cyberspace, international actors have been seeking coordinated action to regulate it through various mechanisms, including the creation of norms. Primarily developed under the United Nations (UN) mandate, the UN cyber groups, i.e., the UN Group of Governmental Experts (UNGGE) and UN Open-Ended Working Group (UN OEWG) have actively pushed the process of building cyber norms (Hogeveen, 2022; Glen, 2021, p. 9). Other relevant actors serving as "norm entrepreneurs" in cybersecurity include the Shanghai Cooperation Organization (SCO), the European Union, the Council of Europe, France, and several non-state entities (Glen, 2021, p. 10). The works of UN cyber groups have resulted in the UN norms of responsible state behaviour in cyberspace, which are voluntary and non-binding in nature. The eleven norms aim to define which actions are deemed acceptable and unacceptable in cyberspace (Hogeveen, 2022; Glen, 2021).

Prior research on norms and cyberspace have examined the progress of cyber norms construction. Erskine & Carr (2016) re-examined the norms concept in the context of cyberspace as an attempt to understand the meaning of norms in cyberspace wholly and what could take us from there. Finnemore & Hollis (2016) focused on the cyber norms as the object of investigation through a process-centred analysis. Both works highlighted challenges and prospects in researching norms of cyberspace. Rapid advancement of the internet affects the approaches used by IR scholars to conceptualize and problematize cyber norms since they need to be aware of the latest developments of norms.

Exploration of cyber norms in the Southeast Asian context also drew the attention of many scholars. As a region with substantial increase in use of the internet, Southeast Asia has reached an almost 80% internet penetration rate with more than half

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

a billion users. Unsurprisingly, it can be considered as a "…dynamic and digitally connected region(s) in the world" (Statista, 2025). In terms of cyber norms, the Association of Southeast Asian Nations (ASEAN), as the regional organization, has shown commitment to adopt the 11-UN norms in cyberspace. In February 2025, the bloc released a document called the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace aiming to guide the members in the realization of the norms (Tran, 2025).

Previous literature regarding cyber norms in Southeast Asia are dominated by research on ASEAN as the key player. Cloramidine & Wibisono (2024) highlighted the norm subsidiarity process of global cyber norms by the regional grouping and found a correlation between global cyber norms and the basic principles of the ASEAN Way. This finding is in line with Chen & Yang's (2022) comparative research on the ASEAN and European Union (EU) approaches to cyber norms. They concluded that the Southeast Asian bloc followed a norm subsidiarity mechanism based on the ASEAN Way and ASEAN Centrality concept. On the other hand, the EU acted as a norm entrepreneur challenging the United States domination within the Western sphere. Other scholarly works focused more on the cybersecurity aspect of Southeast Asia governance rather than norms, for instance Hakeem et al., (2025), Ali et al. (2025), Lee et al. (2025), Ramadhan et al. (2024), and Ramadhan (2022).

Few studies specifically addressing cyber norms in Southeast Asia from the perspective of a member state. Even Singapore, a leading regional actor in digital technology, was less examined in cyber norms literature. Jones et al. (2024) in their piece argued that Singapore is a norm entrepreneur in the context of digital trade. The findings were based on a systematic comparison of trade agreements. Despite being supported with extensive data and a carefully structured methodological approach, this research did not engage much with norms as conceptual frameworks in IR.

Additionally, the paper was specifically limited to the issue of digital trade. Another relevant work analysing Singapore as the main actor in the cyber sphere of Southeast Asia is Prasodjo (2025). He found that Singapore has a significant influence in developing regional cybersecurity governance through initiatives, such as cyber dialogue, investments, and collaborations. Prasodjo also mentioned several workshops and discussions related to cyber norms proposed by the country, yet he did not delve deeply into Singapore's normative power.

To fill the lacunae, this paper attempts to investigate Singapore's "potential" role as a cyber norm entrepreneur at regional level. The city-state might appear as a primary actor in the regional cooperation in cyberspace; however, it cannot automatically qualify as a norm entrepreneur without critical scrutiny and further examination. Therefore, Singapore's pivotal role in ASEAN's cyber governance deserves scholarly attention.

The significant increase in global actors' reliance on the cyber world leads to the urgency of conducting this research. Cyberspace and contemporary international relations are also inseparable, as cyber has become a place of interaction and even changed the pattern of deterrence and war (Foulon & Meibauer, 2024, p. 427). This paper seeks to make several contributions. Firstly, to shed light on small states' normative power to influence other actors. Secondly, to expand the area of cyber norms studies in international relations by highlighting the role of cyber norm entrepreneurs. Thirdly, to unpack the dynamics of state relations in the context of cyber norms within the Southeast Asia region.

Analytical Framework

This research is in line with the constructivist tradition by emphasizing the significance of norms in the study of international relations. Constructivists argued that this approach provides a comprehensive analysis on post-Cold War era phenomena by exploring the combination of ideational and material factors in

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

international politics. (Fierke, 2013, p. 189). So, what are the norms? Finnemore (2017, pp. 1-2), a prominent constructivist scholar, explored the characteristics that define something as a norm. She emphasized that "norms are shared belief within a community". Why are some actors willingly following or subscribing to certain norms? She further argued that it happened because the actors identify that they are part of a group in which the norms are shared. Norms also refer to codes guiding states' behaviour in particular situations that can "constrain and compel" them at the international level. This means that norms determine what actions are deemed acceptable or unacceptable. They become standards of behaviour for states (Erskine & Carr, 2016, p. 90). For instance, in the human rights sector, the 1948 Universal Declaration of Human Rights (UDHR) is considered a global norm because plenty of treaties and declarations are derived from the document, international institutions also actively monitor the implementation of the norms, and it has motivated global social movements promoting and advocating human rights issues (Sundrijo, 2021, p. 28).

In constructing norms, including in cyberspace, norm entrepreneurs play a significant role as they are "…actively involved in defining and promoting cyber norms…". They may appear as individuals, corporations, nongovernmental organizations, and states (Finnemore, 2017, p. 3). Meanwhile, Kewalramani (2024, p. 7) specifically put the state as a norm entrepreneur who is able to alter current regional or global normative setting and push other states to behave according to their preferences. In short, norm entrepreneurs are influential actors in shaping global norms.

The framework of analysis for this research is particularly drawn from the work of Adamson & Homburger (2019) . The article puts small states as the main object for the investigation; thus, it can serve as a relevant theoretical basis for understanding Singapore's position as potential cyber norm entrepreneur at regional level. Adamson and Homburger specifically explored "…the process and

potential of small states to become norm entrepreneurs in cyberspace" in their research. They argued that the norm entrepreneur holds a crucial position in expanding or changing existing norms. Utilizing two case studies of European small states, Estonia and the Netherlands, the authors accentuate the possibility of small states behaving as cyber norm entrepreneurs (2019, pp. 217-218).

For the purposes of this research, the characteristics and behaviour of small states to qualify as a cyber norm entrepreneur are grouped into three different categories based on Adamson & Homburger's (2019) argumentations. The three categories become a parameter to analyse Singapore position in Southeast Asia's cyber norms development. The parameter guiding the discussion in answering the research question of whether Singapore is a regional cyber norm entrepreneur or not.

The first category is type of engagement. Cyber norm entrepreneurs are "…engaging in agenda setting, dramatizing, signalling their own commitment to change, creating coalitions…". These are some choices made by the cyber norm entrepreneur to influence other actors. Some key actions taken by the small states as norm entrepreneurs are based on "persuasion" and an act of "convincing". States that focuses more on coercion or using economic incentives to push other states to follow the norms cannot be considered norm entrepreneurs. This emphasized that the actions of norm entrepreneurs rely on soft approaches (p. 220).

Second, the avenue. Small states acting as cyber norm entrepreneurs consider the channels that they use to promote norms. "Niche diplomacy, multilateralism, or group diplomacy" are several media utilized by the norm entrepreneurs. There are at least three reasons why the small states believe that those channels are effective and efficient. Firstly, it helps them to build a high reputation among community members. Secondly, the multilateral mechanism puts the small states in a rather neutral position compared to the unilateral one. Thirdly, being in a multilateral

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

forum eases the process of creating an agreement since most forums focus on consensus (p. 221).

Niche diplomacy is often associated with middle power behaviour in international politics. Middle powers cannot be present in all global sectors; consequently, they have to choose a specific issue where they can play an influential role and engage with that niche space. They tend to select the area in which they possess "a high degree of resources and reputational qualifications". By doing so, the states will have a better bargaining position at the international level along with distinctive characteristics compared to great powers (Cooper, 1997, pp. 5-6).

Third, the level of ICT development. The capability of small states to act as norm entrepreneurs depends on their cyber power, such as "level of development (ICT maturity), level of e-governance, and ICT capacity". The level of influence (big or small) that they have also depends on this category. In addition, being an ICT-advanced country prompts a state to play a role as a norm entrepreneur (Adamson & Homburger, 2019, p. 224).

Methods

The main reference for the research design of this paper is Lamont (2015). Generally, I employed a qualitative approach to analyse Singapore as the case study in the analysis of regional cyber norm entrepreneurship. Lamont (2015, p. 79) defined qualitative methods in international relations as "data collection and analysis techniques or strategies that rely upon the collection of, and analysis of, non-numeric data".

The data utilized in this research relied on archives or documents available on internet consisting primary and secondary source documents. The main differences between these two sources are the authors and the content. The primary source is written or produced by a person who is directly involved or has access to a certain phenomenon being described. While the secondary source is a document created based on analysis or being referred to a

primary source (p. 80). The primary source in this research refer to statements, declarations, white papers, or any other official documents produced by the relevant actors, for instance, Singapore, ASEAN, and ASEAN member states. The secondary data are obtained from articles published in reputable journals, working papers, research reports, commentaries, op-eds, and websites relevant to this study.

I used the process-tracing mechanism to do the analysis. This method helps researchers to unpack the causal pattern inside a case under study. It follows the chain of events leading to the phenomenon that is being investigated (p. 135). The process-tracing is analogous to a detective trying to connect suspects and hints to a criminal activity (Bennett, 2002, p. 30). This method also brings certain benefits for the study of small states in international relations. Lutmar (2025, p. 9) argues that the process-tracing helps to reveal strategies applied by small states to spread their influence amidst the limitations that they have. In the case of Singapore, I traced policies, strategies, approaches, and choices made by the city-state in the context of its engagement with regional cyber norms. The outcome of the process-tracing is then linked to the three strategies based on Adamson and Homburger (2019). The answer to the research question is based on the compatibility of the process-tracing results with the analytical framework.

Discussion

Singapore External Relations

Singapore's external approach is based on two main concerns. First, limitations on geography and natural resources. Second, survival capability based on economic and political competitiveness (Yeo, 2019, p. 21). Despite having those limitations as a small state, it still actively engages in the international environment. It is proven by various institutions constructed under the city-state's initiatives. Since the 1990s, Singapore has strategically been building forums providing opportunities for small states to collaborate. Along with

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

Barbados and Cabo Verde, Singapore founded the UN group of small states known as the Forum of Small States (FOSS). The forum has been developed through programs such as the FOSS Fellowship Program and FOSS for Good, aiming to build the capacity of its members. Other than that, Singapore plays a significant role in the Alliance of Small Island States (AOSIS) and the Small Island Developing States (SIDS) (MFA, 2026). Its participation in international organizations reflects Singapore's foreign policy strategy.

Besides engagement with international forums, Singapore also maintains good relations with great powers, such as the United States and China. Literature describe that Singapore utilizes equidistant diplomacy and hedging in its approach to major powers. Equidistant diplomacy helps to create a perception of Singapore's neutrality for the receptors. It leads to less pressure to take a position on either side and the island nation can still get benefits from friendly relations with both actors (Teo & Koga, 2022, p. 26). Hedging is also evident in Singapore's behaviours through the development of economic and defence cooperation with Washington and Beijing (Lee, 2024, p. 79).

In the context of regional cyber development, Singapore plays a proactive role in relations with other Southeast Asian states. It leads the ASEAN members in cybersecurity field. It also established the ASEAN-Singapore Cyber Centre of Excellence (ASCCE), helping the regional grouping in capacity-building. Singapore is also considered a "key driver" in international law and norms for cyber activities (Ang, 2022). Again, these findings do not reflect Singapore's position as a norm entrepreneur in Southeast Asia. To dig deeper into this issue, the following sections will explore Singapore's role in detail.

Regional Engagement in Cyber Issues

The Cyber Security Agency (CSA) of Singapore, established in 2015, is the main institution responsible for managing the state's

cybersecurity and for building external cooperation in the cyber domain. It is under the office of the Prime Minister and administered by the Ministry of Digital Development and Information (MDDI) (CSA, 2025b). CSA actively interacts with relevant actors in the region, bringing the importance of acknowledging cyber issues. Its approaches reflect Singapore's attempts to popularize and strengthen cyber norms in Southeast Asia.

Adamson & Homburger (2019) stated that the engagement of small states acting as norm entrepreneurs relies on soft power rather than coercion. This aligns with several initiatives proposed by Singapore in the context of regional cybersecurity. Singapore has been involved in the agenda setting of cyber-attacks preparedness for a long period of time. Since 2006, the city-state has been coordinating the annual agenda of the ASEAN CERT (Computer Emergency Response Team) Incident Drills (ACID) (Tay, 2023, p. 6). ACID's goals are to strengthen ASEAN member states cyber defence during incidents and to enhance cooperation among them as well as with the organization's dialogue partners (CSA, 2025a).

Signalling commitment is another characteristic of a norm entrepreneur's engagement. Singapore's long-standing attention to regional cyber security is accompanied by its firm dedication, for instance, supporting the ASEAN Cyber Capacity Program (ACCP) with a USD 10 million budget. Funding was allocated for capacity building, technical training, and discussions on legislation and cyber strategies for Southeast Asian nations (Raska and Ang, 2018, p. 7). Regarding the establishment of ASEAN Regional CERT, Singapore has also committed to funding the development of its facilities. The government is willing to fund the ASEAN Regional CERT for USD 10.1 million over 10 years and to provide a physical location for the CERT in the country (Bernama, 2024). The regional CERT holds a crucial position since it serves as a platform of cooperation for cyber defence and the construction of a strong regional digital economy. The physical presence of regional CERT

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

in Singapore in October 2024 was a significant moment for the organization (ASEAN, n.d.). Prior to that, the national CERTs were central components of regional coordination responding to cyber-attacks. By 2005, eight member states had established their national CERTs, followed by Cambodia in 2008 and Laos in 2012 (Heinl, 2014). At that time, ASEAN's programs focused on the national level to achieve regional cyber resilience (Dai and Gomez, 2018, p. 7). The existence of regional CERT in Singapore around 20 years later signified the gradual shift in the regional organization's approach to cyber incidents. Indeed, its decision to cover the cost of ASEAN CERT and the ACCP was crucial in this context.

Small states also form coalitions when they play the role of norm entrepreneur. It is an example of a strategy they use to promote certain norms. Based on Singapore's policies, it can be seen that it tries to involve many actors in the cyber security field. For instance, in the recent ACID held on 21-22 October 2025, the island nation successfully attracted not only all ASEAN member states but also the organization's dialogue partners, namely Australia, China, India, Japan, and the Republic of Korea. In total, 36 incidents responders participate in the drilling. Singapore also took a transformative step in ACID 2025 since it was the first in-person meeting of the event since 2006 (CSA, 2025a) . Additionally, the ACID was conducted as part of the Singapore International Cyber Week (SICW) 2025, which entails participation by non-state actors, such as industry and scholars (ASEAN Tech & Sec, 2025). Hack The Box, a company providing services for cyber security training and development, was CSA's partner to support the incident drill practices (Vourlaki, 2025). This reflects Singapore's interests in including diverse entities into the area of cyber security and fostering broad collaboration.

Persuasion technique is an engagement method utilized by cyber norm entrepreneurs, as they do not rely on coercive actions. Based on Singapore's contribution for regional CERT, it can be seen how the island nation develops a soft approach to convince ASEAN

member states of the urgency of regional cyber security measures. Singapore also did not offer financial incentives to states that joined its initiatives. This mechanism corresponds to another feature of small states when it acts as a norm entrepreneur, i.e., not granting rewards to actors who subscribe to the norms being promoted. Furthermore, Prasodjo (2025, pp. 242-243) argues that Singapore encourages the ASEAN nations to be aware of the dangers of cyber-attacks. Through regular forums that emphasize dialogue and discussion, such as the SICW, Singapore endorses the importance of data protection and cyber security. These strategies are consistent with Singapore's interests in cyber power. Singapore is one of the most digitalized states around the globe. Consequently, it faces various types of cyber threats, such as data breaches and attacks on critical infrastructure and information systems (Internal Security Department, 2026). Thus, it is understandable that Singapore seeks to maintain a resilient cyber defence.

ASEAN as the Avenue

When it comes to promoting norms, cyber norm entrepreneurs consider platforms that are effective and efficient in the process. Multilateralism is a primary choice for those small states to be the avenue for popularizing norms. In the case of Singapore, it mainly relies on ASEAN to be a place for constructing and developing cyber norms as many interactions, discussions, and collaborations occur under the ASEAN umbrella. According to the Singapore Cybersecurity Strategy 2021, it engages with the regional body through at least three mechanisms. First, the SICW and ASEAN Ministerial Conference on Cybersecurity (AMCC). This annual flagship event hosted by Singapore has invited relevant actors in the field. It provides opportunities for them to have regional and international engagement on cyber issues. As a side event, the ASEAN Secretary General and ASEAN Ministers of Telecommunications and/or Cybersecurity can also have in-depth discussion on cybersecurity through the AMCC. Second, the

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). The institution was founded in 2019 with the purpose of integrating policies on cyber issues and improving the professional skills and capacities of the regional group's officers. Third, the ASEAN CERT. The CERT is an integral part of ASCCE programs. It aims to be a platform of coordination for national CERTs and technical skills development.

On the other hand, Singapore's bilateral relations with ASEAN members in cyber issues are limited. Among the ten states, strong cooperation and a clear collaboration framework are only evident in Malaysia. Both countries have been collaborating to address border issues for a long time and are expanding their joint efforts into cyber space. For instance, the agreement between Singapore's Maritime and Port Authority (MPA) and Malaysian shipping operator MISC Berhad concerning cyber issues and data exchange was signed in 2024 (Chan, 2025). In addition, in 2025, the neighbouring states signed a Memorandum of Understanding (MoU) related to the issue of data safeguarding, cybersecurity, and the digital economy (Bernama, 2023).

Meanwhile, the bilateral relations with other Southeast Asian nations seem unobservable. Last year, Indonesia held a top-level meeting on defence cooperation including cybersecurity. Singapore's Chief of Defence Force, Vice Admiral Aaron Beng and Indonesia's Minister of Defence, Sjafrie Sjamsoeddin attended this forum. Nevertheless, the execution plan for this collaboration is still in progress (Open Gov Asia, 2025). In 2023, Vietnam and Singapore agreed to strengthen their cooperation under the scheme of the Comprehensive Strategic Partnership (CSP). Yet, the agreement did not specifically address issues related to cyber issues (Golan, 2025). Cambodia and the Philippines maintain a connection with Singapore on cyber partnership mostly under ASEAN's framework, such as the SICW and ASEAN Regional CERT (W.Media, 2021; Phillippines Embassy, 2024).

Adamson & Homburger (2019) assert that small states have certain benefits when they utilize multilateralism for norms engagement, i.e., reputation, neutrality, and effectiveness. Through its strategic cyber programs at the regional level, Singapore is being recognized as a major player in cybersecurity in the region. People have labelled the city-state as "the digitally advanced nation", "the mature country in cybersecurity", "leader of ASEAN cybersecurity", and "regional leader in cyber resilience" (Tay, 2023, p. 14; Ramadhan, 2022; Poetranto et al., 2021, p. 324; Detros, 2023). Utilizing ASEAN, Singapore might also prevent negative sentiments from other members as it puts forward the initiatives based on collective interests. In terms of effectiveness, the regional body has already basic structure and mechanisms for cooperation; thus, it will be less challenging for Singapore to arrange coordinated joint efforts. Several ASEAN forums and bodies focusing on cyber issues are the ASEAN Digital Ministers' Meeting (ADGMIN), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the ASEAN Regional Forum (ARF), the East Asia Summit (EAS), and the ASEAN Defence Ministers' Meeting (ADMM)-Plus (Sari, 2024, pp. 28-29).

Singapore's ICT Development

According to Adamson and Homburger's arguments (2019), small states will have a bigger influence in cyber norms entrepreneurship when they possess a high level of ICT development. For Singapore, its leading role in ASEAN's cyber issues also aligns with its ICT capabilities. Much literature has shown that Singapore is way ahead in terms of technology compared to its Southeast Asian counterparts. Detros' (2023) report shows that Singapore has the highest score in cyber resilience in the region. Assessment of cyber resilience is based on a framework consisting five domains, namely "identify, protect, detect, respond and recover, and adapt". Being ranked among the top countries in the region signifies Singapore's level of cyber power. The state aims to strengthen its cyber

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

capabilities as it is limited in other aspects, such as territory and population.

The island nation not only performs well regionally but also globally. It is consistently ranked in the top position in surveys and indexes related to ICT. The 2024 Global Security Index (GSI) publication also provides evidence of Singapore's superiority in cybersecurity (International Telecommunication Union, 2024). The country is grouped in the Tier 1 – Role Modelling meaning that Singapore has a very high cybersecurity commitment through its government programs and initiatives. In the United Nations E-Government Survey (2024), Singapore was placed in the 3rd position out of 193 states. The four indicators used are digital infrastructure, technology, regulations, and society's engagement and inclusivity. The Smart City Index 2026, which relies on citizens' living experiences, reveals that Singapore is listed in ninth position globally. The assessment is based on the city's health and safety, mobility, activities, opportunities, and governance sector (Gov Tech, 2025). The IMD World Competitiveness Center's Digital Competitiveness Ranking (WDCR) last year also ranked Singapore among the most digitally savvy nations in the world, based on three indicators: Knowledge, Technology, and Future Readiness. In addition, the government has allocated a substantial amount of funding for ICT development. In 2024, USD 3.3 billion was invested in digital infrastructure and services development (Gov Tech, 2024). According to Adamson and Homburger's (2019) arguments, Singapore's cyber policy initiatives at the regional level are influenced by its strength in the digital sector. The city-state has developed its domestic cyber capability to an advanced position then gradually expanded its focus to the ASEAN scope.

Conclusion

Cybersecurity has been a primary concern for Singapore in cyberspace for a long period of time. It is proven through its commitment to the ASEAN Regional CERT development and

hosting cybersecurity related events, such as ACID and AMCC. Its priority on cybersecurity corresponds to cyber norms constructed by the United Nations and currently being adopted by the Southeast Asian bloc. The ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace clearly demonstrates the significance of CERT in the operationalization of norms. This shows that Singapore's efforts and initiatives within ASEAN contribute to strengthening the cyber norms position in the region. Additionally, the endorsement of ASEAN Checklist document by the member states signifies the considerable progress on regional cyber norms development. Furthermore, based on the three indicators of small states as cyber norm entrepreneurs, Singapore is compatible with all of them. The island nation can therefore be categorized as a Southeast Asian cyber norm entrepreneur. It is actively engaged in regional cybersecurity cooperation through soft approaches, for instance, contributing financially to the regional grouping, forming a coalition, and persuasion. Singapore mainly uses the multilateralism framework within ASEAN as a platform for constructing and developing cyber norms. Domestically, its ICT is also highly developed in comparison to other Southeast Asian nations.

Acknowledgement

The initial part of this research was presented at the 11th International Conference on Southeast Asia (ICONSEA), held at the University of Malaya, Malaysia on December 11-12, 2025. The authors also thank the Faculty of Social and Political Sciences (FISIP), Universitas Andalas, for funding the research under Grant No. 187/UN16.08.WDII/PT.01.03/2025.

References

Adamson, L., & Homburger, Z. (2019). Let them roar: small states as cyber norm entrepreneurs. *European Foreign Affairs Review,* 24(2), 217-234. https://doi.org/10.54648/eerr2019014

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

Ali, A. S., Zaaba, Z. F., Singh, M. M., Anuar, N. B., & Shariff, M. R. B. M. (2025). Advancing cybersecurity in ASEAN: current trends, emerging challenges, and opportunities for enhanced resilience. *International Journal of Information Security*, *24*(5). https://doi.org/10.1007/s10207-025-01111-2

Ang, B. (2022). Small states learn different survival lessons. *The Cyber Defense Review,* 7(1), 93–100. https://doi.org/10.2307/48642041

ASEAN. (n.d.). *Priority areas of cooperation*. Retrieved April 16, 2026, from https://asean.org/our-communities/economic-community/asean-digital-sector/priority-areas-of-cooperation/

ASEAN Tech & Sec. (2025). *Singapore International Cyber Week 2025: partnerships, innovation and regional collaboration strengthen cyber resilience*. Retrieved January 11, 2026, from https://aseantechsec.com/singapore-international-cyber-week-2025-partnerships-innovation-and-regional-collaboration-strengthen-cyber-resilience/

Athaya, M., Hakeem, G., Dyo Febriza, M., & Putra, A. E. (2025). Cyber security governance: peran organisasi internasional dalam pembentukan norma keamanan siber global. *Media Hukum Indonesia (MHI),* *3*(4), 636–643. https://doi.org/10.5281/zenodo.17695151

Bennett, A. (2002). Case study methods: Design, use, and comparative advantages. In D. F. Sprinz & Y. Wolinsky (Eds.), International relations research methods (pp. 27–64). Palgrave Macmillan.

Bernama. (2023). *Malaysia, Singapore sign MoU on data protection, cybersecurity and digital economy*. Retrieved December 21, 2025, from https://www.nst.com.my/news/nation/2023/01/875015/malaysia-singapore-sign-mou-data-protection-cybersecurity-and-digital

Bernama. (2024). *Malaysia to enhance ASEAN cybersecurity with regional CERT leadership*. Retrieved February 17, 2026, from

https://bernama.com/en/news.php?id=2353786#:~:text=The%20ASEAN%20Regional%20CERT%20physical%20facility%2C%20co%2Dlocated%20at%20the%20ASEAN%2DSingapore&text=budget%20of%20US$10.1%20million%20for%2010%20years.

Burnay, M., & Chaisse, J. (2020). Global commons as an emerging arena of contestation of global governance structures and norms. *International Community Law Review*, *22*(5), 533–558. https://doi.org/10.1163/18719732-12341446

Chan, S. (2025). *Malaysia, Singapore strengthen maritime cybersecurity ties amid rising threats*. Retrieved April 16, 2026, from https://www.cyberdsa.com/malaysia-singapore-strengthen-maritime-cybersecurity-ties-amid-rising-threats

Chen, X., & Yang, Y. (2022). Different shades of norms: comparing the approaches of the EU and ASEAN to cyber governance. *International Spectator*, *57*(3), 48–65. https://doi.org/10.1080/03932729.2022.2066841

Cloramidine, F., & Wibisono, A. A. (2024). Global cyber norms subsidiarity (UN GGE and UN OEWG) within ASEAN's body. *Hasanuddin Journal of Strategic and International Studies (HJSIS)*, *2*(2), 21–37. https://doi.org/10.20956/hjsis.v2i2.35313

Cooper, A. F. (1997). *Niche diplomacy: a conceptual overview*. Palgrave Macmillan London. https://doi.org/10.1007/978-1-349-25902-1

CSA. (2025a). *CERTS from ASEAN member states gather in Singapore for the first time to participate in the ASEAN CERT Incident Drill (ACID)*. Retrieved March 23, 2026, 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-/

CSA. (2025b). *Who we are*. Retrieved March 23, 2026, from https://www.csa.gov.sg/about-csa/who-we-are/

CSA. (2021). *The Singapore cybersecurity strategy 2021*. Cyber Security Agency of Singapore

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

Dai, C. 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

Detros, K. (2023). *Towards a resilient cyberspace in Southeast Asia*. The Tech for Good Institute

Erskine, T., & Carr, M. (n.d.). *Beyond "Quasi-Norms": the challenges and potential of engaging with norms in cyberspace*. Retrieved December 23, 2025, from https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckda

Fierke, K. M. (2006). Constructivism. In T. Dunne, M. Kurki, & S. Smith (Eds.), International relations theories: Discipline and diversity (pp. 166–184). Oxford University Press.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479. https://doi.org/10.1017/s0002930000016894

Finnemore, M. (2017, November 30). Cybersecurity and the concept of norms. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2017/11/cybersecurity-and-the-concept-of-norms

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy.* 45 (3), 426-458. https://doi.org/10.3929/ethz-b-000679804

Glen, C. M. (2021). Norm entrepreneurship in global cybersecurity. *Politics and Policy*, *49*(5), 1121–1145. https://doi.org/10.1111/polp.12430

Golan, D. (2025). *Vietnam and Singapore upgrade ties to a comprehensive strategic partnership*. Retrieved March 9, 2026 from https://www.aseanbriefing.com/news/vietnam-and-singapore-upgrade-ties-to-a-comprehensive-strategic-partnership/

Gov Tech. (2024). *FY24: Government to spend more than $3B to modernise ICT infrastructure and develop digital services*. Retrieved February 17, 2026, from https://www.tech.gov.sg/media/fy24-

government-to-spend-more-than-3b-on-infrastructure-and-digital-services/

Gov Tech. (2025). *Our digital government rankings*. Retrieved February 17, 2026, from https://www.tech.gov.sg/about-us/our-achievements/our-digital-government-rankings/

Heinl, C. H. (2014). Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime. *Asia Policy*, *1*(1), 131–159. https://doi.org/10.1353/asp.2014.0026

Hogeveen, B. (2022). The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for member states of ASEAN. Australia: ASPI.

IMD – International Institute for Management Development. (2025). *IMD world digital competitiveness ranking 2025*. IMD World Competitiveness Center

Internal Security Department. (2026.) *Cyberspace – A new threat frontier.* Retrieved June 8, 2026, from https://www.isd.gov.sg/our-functions/cyberspace---a-new-threat-frontier/

International Telecommunication Union. (2024). *Global cybersecurity index 2024 5th Edition*. ITU Publications

International Telecommunication Union. (2025). *Measuring digital development fact and figures 2025*. ITU Publications

Jones, E., Kira, B., & Tavengerwei, R. (2024). Norm entrepreneurship in digital trade: the singapore-led wave of digital trade agreements. *World Trade Review*, *23*(2), 208–241. https://doi.org/10.1017/S1474745624000089

Kewalramani, Manoj. (2024). *China as a rising norm entrepreneur: examining GDI, GSI and GCI*. ISEAS - Yusof Ishak Institute.

Lamont, C. (2015). Research methods in international relations. SAGE Publications.

Lee, B. T. F., Kornphetcharat, K., Sims, J. P., Linh Dieu, D., & Salman Ali, B. (2025). ASEAN cybersecurity cooperation strategy: combating cyber terrorism and hackers through CERT coordination. *International Journal of Law and Public Policy*

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

(IJLAPP), *7*(1), 20–30. https://doi.org/10.36079/lamintang.ijlapp-0701.788

Lee, T. (2024). Special issue: domestic determinants of Southeast Asia's relations with the United States and China. *Southeast Asia*, *46*(1), 77–102. https://doi.org/10.2307/27301255

Lutmar, C. (2025). Perspective Chapter: Small states – a new research agenda. In Social Sciences. IntechOpen. https://doi.org/10.5772/intechopen.1012412

Meyer, P. (2016). Outer space and cyberspace: A tale of two security realms. In A.-M. Osula & H. Rõigas (Eds.), International cyber norms: Legal, policy & industry perspectives. NATO CCD COE Publication.

MFA. (2026). *Small states*. Retrieved January 11, 2026, from https://www.mfa.gov.sg/about-mfa/international-issues/small-states/

Nila, S. M. (2024) ASEAN's Regional Effort on Cybersecurity and Its Effectiveness. *Keio SFC Journal*, 23(1), 26-42.

Open Gov Asia. (2025). *Indonesia-singapore defence partnership embraces cyber frontiers*. Retrieved March 24, 2026, from https://opengovasia.com/indonesia-singapore-defence-partnership-embraces-cyber-frontiers/?c=id

Phillippines Embassy. (2024). *Philippines Participates in 9th Singapore International Cyber Week*. Retrieved March 23, 2026, from https://www.philippine-embassy.org.sg/philippines-participates-in-9th-singapore-international-cyber-week/

Poetranto, I., Lau, J., & Gold, J. (2021). Look south: challenges and opportunities for the 'rules of the road' for cyberspace in ASEAN and the AU. *Journal of Cyber Policy*, *6*(3), 318–339. https://doi.org/10.1080/23738871.2021.2011937

Prasodjo, H., Nursetiani, E., & Rijal, N. K. (2024). Towards cybersecurity in Southeast Asia: Singapore's role as the ASEAN chair in 2018. *In Economic sustainability and social equality in the technological era* (1st ed., pp. 238–246). Routledge.

Ramadhan, I. (2022). ASEAN consensus and forming cybersecurity regulation in Southeast Asia. In Proceedings of the ICONIC-RS Conference. EAI. https://doi.org/10.4108/eai.31-3-2022.2320684

Ramadhan, I., Sumadinata, R. W. S., Djumala, D., & Darmawan, W. B. (2024). Interpreting the Role of State, Non-State, and International Organization to form Cybersecurity Governance in Southeast Asia. *Geopolitics Quarterly*, *20*(2), 255–278. https://doi.org/10.22034/igq.2024.198274

Raska, M. & Ang, B. 2018. Cybersecurity in Southeast Asia. Asia Centre

Statista. (2025). *Internet usage in Southeast Asia - statistics & facts*. Retrieved March 23, 2026, from https://www.statista.com/topics/9093/internet-usage-in-southeast-asia/?srsltid=AfmBOop1gC1IOBVKNHbtGcYWuHIRGKlvI6aszZ2oxcyzRUYtFfL6M4wQ#topicOverview

Sundrijo, D. A. (2021). Regionalizing global human rights norms in Southeast Asia. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-54798-1

Tay, K. L. (2023, June). *ASEAN cyber-security cooperation: Towards a regional emergency response framework*. The International Institute for Strategic Studies (IISS)

Teo, A. G., & Koga, K. (2022). Conceptualizing equidistant diplomacy in international relations: The case of Singapore. *International Relations of the Asia-Pacific*, *22*(3), 375–409. https://doi.org/10.1093/irap/lcab011

Tran, B. (n.d.). *Southeast Asia's Cybersecurity Trajectory Beyond the UN OEWG*. Retrieved www.rsis.edu.sg

Vourlaki, S. (2025). *Hack The Box supports the 20th ASEAN CERT Incident Drill 2025*. Retrieved March 24, 2026, from https://www.hackthebox.com/blog/hackthebox-supports-asean-cert-incident-drill-2025

W. Media. (2021). *Cambodia & Singapore to strengthen cyber security capacity*. Retrieved April 1, 2026, from

Copyright (c) 2026 Rifki Dermawan, Diah Anggraini Austin

https://cybersecurity.w.media/cambodia-singapore-to-strengthen-cyber-security-capacity/

Yau, J. (2022). *The wild, wild web: Explaining variation in ASEAN member-state cyber policy* (Master's thesis, University of British Columbia). https://open.library.ubc.ca/media/stream/pdf/24/1.0417521/3

Yeo, L. H. (2019). Singapore's policy in the Asia-Pacific: ASEAN and open regionalism. *Baltic Journal of European Studies*, *9*(2), 20–39. https://doi.org/10.1515/bjes-2019-0012