DCAF Geneva Centre for Security Sector Governance

Cybersecurity Governance in Southeast Asia

Thematic SSG Brief

Kevin Socquet-Clerc, Samantha Khoo Su-Yen, Fitriani, Miguel Alberto Gomez and Nguyen Viet Lam

ASIA-PACIFIC SECURITY SECTOR GOVERNANCE NETWORK

Published in Switzerland by DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix, Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva

First published in November 2023.

Cite as: Kevin Socquet-Clerc, Samantha Khoo Su-Yen, Fitriani, Miguel Alberto Gomez and Nguyen Viet Lam. Cybersecurity Governance in Southeast Asia. Thematic SSG Brief. Geneva: DCAF - Geneva Centre for Security Sector Governance, 2023.
Series editor: Albrecht Schnabel
ISBN: 978-92-9222-719-7
Cover picture: World Technology and Business by ProPhotoStock, Creative Commons Attribution 3.0 License.

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

Disclaimer

The opinions expressed in this publication are those of the authors alone and do not necessarily reflect the position of the institutions referred to or represented within this publication.

Acknowledgements

To develop this Security Sector Governance (SSG) Thematic Brief we greatly benefited from the insightful comments, inputs and contextualisation from DCAF Asia-Pacific Unit (APU) SSG Associates and national partners in Southeast Asia who proposed the topic of this brief, participated in the preparation of the workshop, and provided regular feedback and inputs. As with all activities by DCAF APU, their contributions are essential to producing quality work. We therefore thank Abel Amaral, Altaf Deviyati, Somsri Hananuntasuk, Marinet Kham, Jennifer Santiago Oreta, Asyura Salleh, Riyani Sidek, Beni Sukadis, Kim Sun, Laddawan “Job” Tantivitayapitak, Amara Thiha and Julius Cesar Trajano. Their insights shared in this volume, and their patience in responding to our requests for revision and updates during the preparation of this research, were invaluable.

We thank Sabeena Bali for copyediting and proofreading and Floris de Klerk Wolters for the layout.

Executive Summary

Cybersecurity is a major emerging security threat that affects every country in the world and that requires governments to adapt constantly due to its ever-evolving nature. In Southeast Asia (SEA), it is a critical concern as the region rapidly integrates digital technologies into its socioeconomic fabric and strives to capitalise on opportunities for its socioeconomic development. However, with these opportunities come challenges and risks. People in the region have vastly varying levels of digital literacy, primarily due to economic disparities and uneven integration into educational curricula. There are also great differences between each national government's capacity to address cybersecurity. Additionally, differing interpretations of cybersecurity and diverse national priorities render the development of a regionwide, unified response virtually impossible.

At the national level, current cybersecurity policies and regulations are at largely different stages of development, with marked disparities in their effectiveness and focuses. Some countries demonstrate significant progress in advancing their cybersecurity strategies, while others grapple with inadequacies, often due to resource constraints and differing reference points set by both international and national agencies.

To address cybersecurity threats in SEA, a multi-pronged approach which engages both state and non-state security sector actors is imperative. Encouraging responsible vulnerability disclosures and fostering policy dialogue platforms are vital steps toward bolstering cybersecurity. This collaborative approach should materialise through a sequence of short-, medium- and long-term measures dedicated to refining cybersecurity governance.

Further, it is essential that, when developing regional and national cybersecurity strategies, good governance principles are strictly upheld to avoid any negative impacts on basic human rights such as freedom of speech. Encroachments on individual rights through virtual platforms can be intentionally employed by governments as a new tool to subdue opposition but can also simply be the result of inadequate policies.

In conclusion, mitigating cybersecurity threats in SEA demands coordinated actions on both regional and national levels. Specific recommendations can be made to all security sector actors, underpinning their crucial role in developing and upholding efficient, transparent cybersecurity strategies that respect human rights, paving the path for a secure and resilient digital future.

List of Acronyms

ADMM-Plus EWG	ASEAN Defence Ministers Meeting and Expert Working Group
APU	Asia-Pacific Unit
ASEAN	Association of Southeast Asian Nations
BIN	Badan Intelijen Negara (Indonesia's primary intelligence service)
CERT	Computer Emergency Response Teams
DDoS	Distributed denial-of-service
EWG	Expert working group
IMPACT	International Multilateral Partnership Against Cyber Threats
ITU	International Telecommunication Union
NCS	National cybersecurity strategy
NFT	Non-fungible token
NGO	Non-governmental organization
SEA	Southeast Asia
SSG	Security sector governance
TELMIN	ASEAN Telecommunications and Information Technology Ministers Meeting

Table of Contents

Introduction

The emergence of cyberspace has opened numerous possibilities for economic, technological and social development, but it has also introduced new risks. Cybersecurity threats are dynamically and rapidly evolving and pose many challenges, as they endanger the safety, prosperity and resilience of states and individuals. In response, states are tasked with implementing robust policies, strategies and actions to protect both national and human security from these emerging cybersecurity threats.

What is Cybersecurity?

The International Telecommunication Union defines cybersecurity as a "comprehensive set of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies aimed at safeguarding the cyber environment and protecting the assets of organisations and users".[1] Cybersecurity comprises network security, information security, application security, cloud security, incident response, risk management, identity and access management, and security operations and monitoring.[2]

As societies become more digitally connected, the potential risks and vulnerabilities associated with cyber threats have increased exponentially. Cyber threats refer to any circumstance or event with the potential to adversely impact information systems. They encompass a wide range of malicious activities and can be carried out by cybercriminals, state-sponsored actors or non-state groups.

A breach in cybersecurity can result in the theft of classified data, intellectual property or personal information, which can in turn have severe implications for economic stability and public trust. Cyber threats can also cause significant harm to national security if they lead to the loss or compromise of sensitive information, disruption of critical infrastructure, or threats to public safety. For example, cybercriminals can use ransomware to target businesses and critical services like hospitals, schools and municipalities. Other threats such as identity theft and financial fraud can also adversely affect the daily lives of individuals.

Cybersecurity Threats and Good Security Sector Governance

As described above, digitalisation brings not only opportunities, but also significant threats affecting both traditional and human security as well as posing grave dangers to critical state infrastructures.

---

1 Telecommunication Standardization Sector of ITU (2008) "SERIES X: Data Networks, Open System Communications and Security. Overview of Cybersecurity".

2 Tyler Chancey (2021) "What Are the Different Branches in Cyber Security?", Scarlett Cybersecurity, 15 February, https://www.scarlettcybersecurity.com/what-are-the-different-branches-in-cyber-security .

Southeast Asia (SEA) is significantly exposed to cyber threats. The interconnectedness of countries in the region means that cyber threats can easily transcend borders and affect multiple countries simultaneously. Inadequate cybersecurity measures and security failures can undermine regional stability, impede economic growth and development, and pose threats to national sovereignty. The interdependencies between critical infrastructure systems such as telecommunications, transportation and finance make the region vulnerable to cyberattack. To address these dangers, regional cooperation is crucial. By working together, countries can enhance their collective resilience against cyber threats, promote information sharing and develop regional frameworks. These can mitigate risks and safeguard regional stability and security. While ensuring the security of the state is of paramount importance, it is also important to strike a balance between implementing security measures and upholding fundamental human rights, such as freedom of speech.

Good governance principles play a crucial role in finding this balance and developing control measures mindful of preserving individuals' rights and privacy. Moreover, digitalisation can be leveraged positively to defend human rights. For example, platforms like social media can facilitate the documentation of excessive force by security providers and support advocacy movements. Access to information and educational resources can also enhance awareness and democratic participation across different societal groups and, in doing so, contribute to a more inclusive society.

However, applying good governance principles to cybersecurity can be difficult due to the diffused and boundless nature of cyberspace. For example, identifying and holding individuals or entities accountable for cybercrimes is extremely challenging, which makes it difficult to efficiently implement the rule of law. International cooperation often becomes necessary to ensure that justice is served. Moreover, a comprehensive and collaborative approach that involves all relevant stakeholders within a country is crucial to effectively address cybersecurity issues and navigate the complexities associated with the international nature of cyber threats.

1. Digitalisation and Cybersecurity Threats in Southeast Asia

Southeast Asia (SEA) is a dynamic and rapidly growing region. Its growth is significantly supported by digitalisation; the region has a burgeoning digital economy, which is projected to reach a worth of US $300 billion by 2025.[3] Countries like Singapore, Malaysia, Indonesia, and Thailand are investing heavily in digital infrastructure. However, SEA's rapid technological advancement also presents the region with significant challenges to security.

Cyber threats endanger various sectors and organisations, at both national and regional levels. For example, in 2019, the Philippines experienced a major data breach that affected over 900,000 passport holders. The breach exposed sensitive personal information and highlighted significant vulnerabilities in the country's cybersecurity infrastructure. In another case, Indonesia faced cyber-attacks on its government websites, with hackers defacing the websites and disrupting services. These attacks raised concerns about the protection of critical government systems and data. Malaysia has also experienced serious cybersecurity incidents. For example, a data breach in 2017, in which millions of personal records were leaked, affected various government agencies such as the Malaysian Communications and Multimedia Commission, Royal Malaysia Police and Permodalan Nasional Berhad as well as private organisations such as Digi and Jobstreet.com.[4]

Cyberwarfare, which involves countries targeting each other's cyber defence capabilities, adds an additional layer of complexity to SEA's cybersecurity challenges. The region has witnessed a surge in military spending and efforts towards the modernisation of armed forces. This reflects the growing emphasis on military modernisation in the political agendas of several SEA countries. Concurrently, territorial disputes, particularly those in the South China Sea, have generated renewed geopolitical tensions. Notably, these disputes have become a driver of cyber espionage and hacktivism in the region, which adds to the challenges of cybersecurity. This cyber dimension of traditional geopolitical conflict has the potential of escalating hostilities, particularly when patriotic hackers operate independently with minimal government control. SEA has also experienced instances of state-sponsored cyber espionage and use of cyber technologies to influence campaigns.

Additionally, SEA has witnessed several significant cybersecurity incidents that have impacted national security. In 2016, a hacking group called 1937CN based in China targeted Vietnam's airports and hijacked flight information screens and sound systems to broadcast anti-Vietnamese and anti-Philippine propaganda. Another hacking group, APT32 (also known as Ocean Lotus), has been involved in cyber espionage and has

3 Singapore Economic Development Board (2021) "These Mega-Trends Are Re-Imagining Business and Growth in Southeast Asia", 8 February, https://www.edb.gov.sg/en/business-insights/insights/these-megatrends-are-reimagining-business-and-growth-in-southeast-asia.html.

4 John Leyden (2017) "Virtually Everyone in Malaysia Pwned in Telco, Govt Data Hack Spree", *The Register*, 1 November, https://www.theregister.com/2017/11/01/malaysia_telco_government_hack/#:~:text=Wed%201%20Nov%202017%20%2F%2F%2020%3A02%20UTC%20The.

targeted ministries and government agencies in Cambodia and the Philippines. Moreover, ransomware attacks have emerged as a major cybersecurity threat in SEA, targeting small and medium businesses in particular. Indonesia, which has experienced over 1.3 million ransomware-related attacks according to a 2021 Interpol publication, stands out as the most affected country among ASEAN member states.[5] According to the same source, Vietnam, Thailand, the Philippines and Malaysia have also experienced a significant number of such attacks. These incidents cause severe disruptions to critical operations and often incur substantial financial losses.

In addition to traditional cybercrimes, cutting-edge attackers like the Lazarus Group and its sub-group, BlueNoroff, could launch even more significant waves of attacks on cryptocurrency businesses in the future. The Lazarus Group and BlueNoroff are widely believed to be state-sponsored hacking groups linked to North Korea and receiving the support and direction of the North Korean government.[6] SEA countries are at the forefront of non-fungible tokens (NFT) ownership: 32% of people living in the Philippines own NFTs, 26.2% in Thailand, 23.9% in Malaysia, 17.4% in Vietnam and 6.8% in Singapore.[7] Yet the increasing popularity of NFTs in the region also makes it an attractive target for cyber-attacks, as cybercriminals seek to exploit vulnerabilities in this digital asset space.

In summary, although more attention is being paid to cybersecurity in SEA, the region faces several challenges in efficiently addressing cybersecurity threats while at the same time adhering to good governance principles. The lack of a unified regional definition of cybersecurity and varying perceptions of the field among ASEAN countries hinder seamless cooperation on cybersecurity. Moreover, geopolitical rivalries and territorial disputes have increased the intensity of cyber espionage and hacktivism. By developing robust cybersecurity policies and fostering collaboration among its member states, SEA can enhance its resilience against cyber threats and safeguard its economic growth and national security.

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

6 U.S. Department of the Treasury (2019) “Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups”, 9 December, https://home.treasury.gov/news/press-releases/sm774.

7 Bob Reyes (2022) “Southeast Asia’s Cyber Threat Landscape in 2022 by Kaspersky”, *Manila Bulletin*, 14 January, https://mb.com.ph/2022/01/14/southeast-asias-cyber-threat-landscape-in-2022-by-kaspersky/.

2. Overview of Cybersecurity Governance in Southeast Asia

To address the severe, varied and rapidly evolving security threats described in the previous chapter, governments need to develop robust and all-encompassing strategies, including dedicated national cybersecurity strategies (NCSs).

National Cybersecurity Governance Systems

The effectiveness of NCSs is contingent on four fundamental factors:

- Conceptualisation and understanding of the domain of cybersecurity, which influences the development and implementation of policies.
- Perceptions of threat actors, whether state-sponsored, criminal or hacktivist groups.
- Latent and realised capabilities of state and non-state actors to carry out cyber operations.
- Institutional prerogatives and policy frameworks of individual states, which impacts the nature and scope of cybersecurity measures.

Additionally, a fundamental concern is achieving regional and global interoperability of cybersecurity strategies, as cyber threats transcend national borders and require international cooperation and coordination.

NCSs offer governments a cohesive and comprehensive approach, outlining their vision, objectives, institutional responsibilities and priorities in line with national security and economic objectives. They provide a roadmap for safeguarding critical infrastructure, enhancing security and allocating resources effectively. Drawing on the experiences of different countries, these strategies come in diverse formats and levels of detail, and are tailored to specific national objectives, priorities, needs and levels of cyber-readiness.

The priorities of these NCSs can also differ significantly. Some countries focus on critical infrastructure risks, while others prioritise safeguarding intellectual property, building trust in the online environment or raising public cybersecurity awareness, or a combination of these. The development process of an NCS translates a government's vision into a cohesive and actionable policy, outlining the necessary steps, programmes, initiatives and resource allocation to achieve its goals. Metrics are identified to track outcomes within specified budgets and timelines. As of February 2019, 106 countries have already issued cyber or information security policies, which indicates an ongoing global trend towards the development of NCSs, including among ASEAN member states.[8]

8 Mika Kerttunen and Eneken Tikk (2019) “National Cyber Security Strategies: Commitmet to Development”, Cyber Policy Institute, https://blog.apnic.net/wp-content/uploads/2019/04/CPI-NCSS-A-Commitment-to-Development-Feb-2019-1.pdf.

Cybersecurity Governance in Southeast Asia

In SEA, three major contextual factors significantly influence the landscape of cyberspace and the evolution of cyber threats. Firstly, the region's growing and increasingly digitalised economies have led to a surge in technological advancements, which has created both opportunities and risks in the digital realm. Secondly, the modernisation of armed forces and increased military spending in ASEAN countries have raised concerns about cyberwarfare and espionage. Lastly, territorial disputes in the region have fuelled geopolitical tensions which often manifest via cyber espionage and hacktivism.

ASEAN has been actively focusing on advancing regional connectivity, with a particular emphasis on digital integration. Key priorities include the development of the digital economy, data protection and the establishment of a secure cyberspace. Initially, ASEAN's cybersecurity policy centred on bolstering national economic growth supported by cybersecurity capabilities, which continues to be a significant regional priority. To collectively address cybersecurity challenges, ASEAN has adopted a regional approach that is exemplified by the ASEAN Defence Ministers Meeting and Expert Working Group (ADMM-Plus EWG) on Cyber Security. This platform facilitates the exchange of expertise and operational cooperation on cybersecurity, which reflects the growing inclusion of defence and military considerations in cyberspace. Moreover, the ADMM-Plus EWG on Cyber Security serves as a venue for dialogue between ASEAN member states and Eight Plus countries,[9] which fosters the advancement of cyber norms beneficial to the region.

Having recognised the significance of cybersecurity at the regional level, ASEAN has prioritised the issue since the early 2000s, as illustrated by the Singapore Declaration at the 3rd ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) in 2003. TEMLIN underscored the importance of promoting information system integrity, security and interconnectivity within ASEAN. To navigate decision making and promote flexibility, the region employs the ASEAN Way and the ASEAN Minus X mechanism, enabling willing member states to table initiatives, while allowing others to join when ready. By leveraging this unique mechanism, ASEAN could potentially steer member states toward comprehensive cybersecurity strategies, which would ensure collective security and resilience in the ever-evolving cyberspace. However, in the 2000s the region was still lacking in what is considered to be responsible behaviour in the cyberspace and only in 2018 the region adopted, in principle, the UN norms of responsible state behaviour in cyberspace,[10] albeit they are non-binding and therefore implementation is non-enforceable.

While ASEAN does have mechanisms in place, their efficacy varies in large part because countries have diverse perceptions of the threat posed by cybersecurity, which has led to varied approaches in addressing cybercrime on the international, regional and national

9 The term "Eight Plus Countries" collectively refers to eight Dialogue Partners: Australia, China, India, Japan, New Zealand, Republic of Korea, Russia and the United States. These partners engage in dialogues and collaborations with ASEAN member countries to enhance regional cooperation, address common challenges and promote socioeconomic development, including cybersecurity governance initiatives.

10 Elina Noor (2018) “ASEAN Takes a Bold Cybersecurity Step”, *The Diplomat*, https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/.

fronts. This deficit in governing norms and rules of state behaviour in cyberspace presents potential risks to the political and economic stability of the ASEAN region, particularly considering the high-profile cyber incidents it has faced. Cyber-attacks have become a contentious issue among security actors in the region due to the inherent vulnerability of cyberspace.

While progress is not uniform at the national level across the entire region and not all countries have reached the same level of cybersecurity systems, several ASEAN member states have demonstrated significant efforts in supporting the development of cyber norms. For instance, Indonesia has made notable strides in cybersecurity legislation with the enactment of the Personal Data Protection Law in 2022. Similarly, Malaysia has passed legislation including the Personal Data Protection Act in 2010, while the Philippines implemented the Cybercrime Prevention Act and Data Privacy Act in 2012 which are both aimed at protecting privacy and promoting data security. Singapore has established the Cyber Security Agency of Singapore as its central coordinating body. The amendments to the Computer Misuse and Cybersecurity Act in 2017 and the enactment of the Cybersecurity Act in 2018 demonstrate Singapore's strong commitment to addressing cyber threats effectively and adapting to the ever-changing landscape of cybercrime.

3. Challenges to Cybersecurity Governance

Cybersecurity governance provides accountability frameworks and decision-making hierarchies, and so forms a robust framework for countering the multifaceted challenges posed by the fluid nature of cyber threats. However, to achieve effective cybersecurity governance, several intricate challenges should be overcome. Cyber threats necessitate constant adaptation of governance frameworks to match the evolving context of threats as well as technological advancement. Another challenge is that cyber threats often transcend borders and boundaries, requiring collaborative approaches that extend beyond individual entities and implicate national and international cooperation. Yet achieving seamless coordination among diverse stakeholders can be difficult due to varying interests, regulations and levels of cyber maturity.

A key imperative in cybersecurity cooperation lies in building trust and confidence among stakeholders. The landscape should prioritise collaborative efforts that foster responsible behaviour. This approach stands in contrast to leveraging cyberspace for strategic power plays, emphasising instead the establishment of norms and agreements that uphold digital integrity. In this context, effective cybersecurity governance must navigate these competing priorities, ensuring robust protection without compromising individual freedoms.

Achieving cybersecurity frameworks that abide by good security sector governance (SSG) requires a multi-faceted approach. This includes comprehensive training to raise awareness, leadership commitment to prioritise cybersecurity, integration of cybersecurity policies, fostering a collaborative environment, and continuous monitoring and improvement. By embedding good governance principles at all levels of a cybersecurity response, a proactive and resilient stance against cyber threats can be achieved within the framework of good SSG. These measures collectively establish a culture where cybersecurity is a shared responsibility and a core part of security actors' operational mindsets.

In SEA, variations in political will and in cyber maturity across countries create fundamental and structural disparities, thus leading to divergent priorities and impeding the attainment of a consensus. Moreover, strict adherence to the principle of non-interference in domestic affairs further complicates the attainment of a common position, as member states prioritise preserving their national sovereignty. While facing these challenges, some countries, such as Singapore, have made significant commitments by allocating substantial resources under their NCS to promote the development of cybersecurity norms in the region. To overcome these hurdles, foster a cohesive cybersecurity approach and collectively mitigate cyber threats, inclusive efforts are crucial. By adopting a comprehensive and unified approach to cybersecurity, ASEAN can effectively respond to cyber risks, ensuring the stability of the region's political, economic and social landscape. To achieve this goal, continuous dialogue, knowledge sharing and capacity building initiatives are essential to cultivate mutual understanding and cooperation among member states. Only through concerted and collaborative endeavours can SEA standardise its cybersecurity policy and bolster its resilience against dynamic new cyber threats.

Regional and National Efforts on Cybersecurity Governance

ASEAN has established various intergovernmental bodies and working groups to address regional cybersecurity challenges. An example is the ASEAN Ministerial Conference on Cybersecurity, which provides a platform for member states to discuss and coordinate cybersecurity efforts at the regional level. ASEAN also runs cybersecurity cooperation programs that encourage member states to share best practices, knowledge and resources. For instance, the ASEAN-Japan Cybersecurity Capacity Building Centre promotes capacity building and training in cybersecurity across the region. At the regional level, Computer Emergency Response Teams (CERTs) assume a central role in orchestrating responses to cybersecurity incidents and exchanging intelligence about threats. A good illustration of this coordination is the ASEAN CERT Incident Drill, which convenes CERTs from member states to simulate and enhance their coordinated response to incidents.[11]

On a national level, each ASEAN country typically has its own governmental agency or ministry dedicated to cybersecurity. These organisations formulate cybersecurity policies, coordinate responses to cyber threats and collaborate with international counterparts. For instance, Singapore has the Cyber Security Agency of Singapore, which oversees and coordinates cybersecurity efforts across the country.

Many ASEAN countries have also introduced new cybersecurity laws. These laws cover a wide range of areas, from data protection to cybercrime prevention. For instance, Indonesia's aforementioned 2022 Personal Data Protection Law regulates the collection and use of personal data. Several ASEAN nations have established CERTs to strengthen their cybersecurity readiness. These teams collaborate closely with both governmental and private entities to ensure efficient handling of incidents and mitigation of threats. An example of this is the ThaiCERT in Thailand, which is responsible for coordinating cyber incident responses within the country.

Non-governmental organisations (NGOs) and civil society groups also play a role in advocating for cybersecurity awareness, education and policy development. These organisations often collaborate with governments to bridge gaps in cybersecurity knowledge and practices. An example is the Thai Netizen Network, which advocates for digital rights and online freedom.

Challenges to Cybersecurity Governance in Southeast Asia

The initial approach to cybersecurity within ASEAN revolved around enhancing national capabilities to secure the digital environment. This strategy remains a central priority in the ongoing development of cybersecurity policies across the region. However, the frequent and substantial volume of cyber incidents in Southeast Asia underlines the persisting challenges to achieving strong cybersecurity.[12] These include:

11 AusCERT (2020) "AusCERT at the 2020 ASEAN CERT Incident Drill", 9 October, https://auscert.org.au/blogs/2020-10-09-auscert-2020-asean-cert-incident-drill/#:~:text=An%20annual%20drill%20hosted%20by%20Singapore%20since%202006%2C.

12 Michael Raska and Benjamin Ang (2018) "Cybersecurity in Southeast Asia", Asia Centre, https://asiacentre.eu/wp-content/uploads/2021/11/NotePresentation-AngRaska-Cybersecurity_180518.pdf.

- **Lack of strategic mindset and policy preparedness**: at both the national and regional levels, there is a lack of strategic thinking, policy readiness and robust institutional regulations to support efficient oversight.

- **The absence of a unified framework**: the absence of a cohesive framework has led to a dispersal of responsibilities. Different entities such as the national police (for cybercrime), interior ministry (for critical infrastructure), telecommunication ministry (for breaches) and the military (for cyber conflicts) each handle different aspects, which leads to a fragmentation of efforts. ASEAN continuously tries to improve its cooperation and collaboration by issuing regional frameworks, such as the ASEAN Framework on Personal Data Protection (2016), ASEAN Framework on International Mobile Roaming (2017), ASEAN Framework on Digital Data Governance (2018), ASEAN Data Management Framework (2021) and Framework for Promoting the Growth of Digital Startups in ASEAN (2023).[13] Additionally, the regional organisation developed an ASEAN Digital Masterplan 2025 and ASEAN Cybersecurity Cooperation Strategy for the period of 2021-2025. However, national implementation of those frameworks is dependent on individual countries' capacities and priorities.

- **Lack of digital literacy**: a lack of digital literacy, exacerbated by differing perceptions of cybersecurity issues, can result in an unequal understanding and management of digital technologies and thereby hinder collaborative efforts to address cybersecurity concerns regionally.

- **Different approaches to cybersecurity governance**: diverse priorities and varying perspectives often result in distinct approaches to the governance of cybersecurity. For example, Malaysia and Indonesia are actively working on enhancing their military capabilities and developing new doctrines to address cyber threats,[14] while Brunei and Singapore are focusing on fortifying their cyber defensive capacities.[15] These approaches reflect how many diverse strategies are present within the region.

- **The transnational nature of cybersecurity governance**: the need to address cybersecurity threats through existing international and regional jurisdictions introduces many complexities, including variations in internet standards across different countries and challenges in imposing penalties.

- **Limited threat intelligence sharing**: the lack of trust and transparency among SEA countries hampers the sharing of threat intelligence. This impedes effective collaboration on collectively tackling cyber threats.

---

13 ASEAN Secretariat (2023) "ASEAN Digital Sector: Key Documents", https://asean.org/our-communities/economic-community/asean-digital-sector/key-documents/.

14 International Institute for Strategic Studies (2021) "Cyber Capabilities and National Power: A Net Assessment", 28 June, https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power.

15 Rasidah Hj Abu Bakar (2021) "HM: New RBAF Cyber Defence Unit to Protect against Online Threats", *The Scoop*, https://thescoop.co/2021/04/02/hm-new-rbaf-cyber-defence-unit-to-protect-against-online-threats/; Mike Yeo (2022) "Singapore Unveils New Cyber-Focused Military Service", https://www.defensenews.com/global/asia-pacific/2022/11/02/singapore-unveils-new-cyber-focused-military-service/.

- **Fragmented approach in the business sector**: many regional businesses lack a comprehensive approach to cybersecurity, and often view cyber risk as an IT concern, rather than a broader business issue. This fragmented approach can leave problems and vulnerabilities unaddressed.

Cyber-attacks often affect multiple countries between whom a consensus on cybersecurity governance is yet to be established.

Beyond technical vulnerabilities, SEA countries also grapple with various other cybersecurity challenges. Among these, five prominent categories of cybersecurity issues stand out: espionage, foreign interference during political unrest, election-related concerns, the proliferation of misinformation, disinformation and malinformation, and instances of government authoritarianism. These challenges can also manifest themselves in complex combinations.

With regards to espionage, significant examples include those of intelligence agencies and sector targeting. In 2021, the Badan Intelijen Negara (BIN), Indonesia's primary intelligence service, along with nine other agencies, fell victim to a data breach.[16] This incident, revealed by the threat research division of Recorded Future's Insikt Group, appears to be linked to China's substantial investments in Indonesia. While the findings were contested by BIN's spokesperson, the breach underscored concerns about cyber espionage in the context of foreign investments and geopolitical interests. Singapore also experienced a significant data breach in 2018.[17] The breach affected the SingHealth database and compromised 1.5 million health records. It was carried out by Whitefly, a group which was targeting sectors like healthcare, media, telecommunications and engineering between 2017 and 2019. As a consequence, Singapore's privacy watchdog imposed fines on Integrated Health Information Systems, the SingHealth vendor, as well as SingHealth itself, emphasising the need to improve cybersecurity and enhance cybersecurity governance.

The increasing reliance of electoral processes on technology has made them more susceptible to cyber-attacks. Electoral processes increasingly rely on digital voter rolls, biometric registration and electronic voting machines. Both state and non-state actors can exploit these technologies' vulnerabilities through tactics like distributed denial-of-service (DDoS) attacks and malware. Electoral systems are high-value targets and prone to technical vulnerabilities, which mainly involve compromising system confidentiality, undermining data integrity and disrupting availability. Strengthening the use of technology while enhancing its security can lead to more efficient and accurate elections. In a specific instance, during the 2018 Cambodian elections, extensive interest from a threat actor known as TEMP.Periscope was uncovered.[18] This actor compromised numerous Cambodian entities linked to the elections, including government organisations and

16 Dio Suhendra (2021) "State Intelligence Hacked in Alleged Breach of Government Networks", *The Jakarta Post*, https://www.thejakartapost.com/news/2021/09/14/10-state-bodies-allegedly-hacked-in-latest-indonesian-cyber-breach.html.

17 Irene Tham, Rachel Au-Yong, Tin May Linn and Rodolfo Pazos (2018) "SingHealth Cyber Attack: How It Unfolded", *The Straits Times*, 20 July, https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

18 Scott Henderson (2022) "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally", Mandiant Threat Research, https://www.mandiant.com/resources/blog/chinese-espionage-group-targets-cambodia-ahead-of-elections.

individuals such as the National Election Commission, the Ministry of the Interior and human rights advocates that were critical of the ruling party. While the threat actor's focus initially centred on maritime affairs, their involvement in compromising elections indicates a willingness to target the political systems of strategically significant countries.

Another problem is misinformation.[19] The 2019 Indonesian presidential election, which witnessed a significant proliferation of misinformation, provides an illustrative example. President Joko Widodo's re-election bid against ex-military general Prabowo Subianto saw a significant portion of campaigning conducted online and on social media platforms.[20] Election watchdogs reported a surge in fake news during this period, sparking worries about the adverse effects of misinformation on social media users. Despite denials from both camps, investigations revealed the existence of "buzzer teams," groups responsible for generating content to sway voters.

Beyond these challenges, there also exist serious threats to human security. The exploitation of digital tools by authoritarian regimes to spread disinformation, engage in corporate espionage, conduct civilian surveillance and interfere with elections is well documented in SEA. Such abuse of technology also leads to a controlled information flow, which stifles diverse ideas and curbs civil liberties. In 2022, it was revealed that the Thai government employed surveillance software, including the Israeli-made Pegasus spyware, to track individuals thought to pose a risk to national security or to be involved in drug cases.[21] This surveillance affected activists, academics, lawyers and NGO workers, among others, during a period of pro-democracy protests. Many victims had previously faced detention, arrest or imprisonment due to their political activities or criticism of the government; some were even subjected to lèse-majesté prosecutions.[22]

In conclusion, the inherent nature of cyberspace has led to an increased exposure to cyber risks and vulnerabilities, evident through the diverse cyber threats encountered by ASEAN member countries. Addressing these risks demands the implementation of appropriate measures that guide relevant actors in adhering to cybersecurity governance standards.

---

19 Whereas both “misinformation” and “disinformation” are false information, “misinformation” is false information whether spread with or without the intent to mislead, whereas “disinformation” is distinguished by a specific intent to mislead.

20 Fitriani and Habib Abiyan (2023) “Social Media and the Fight For Political Influence in Southeast Asia”, *The Diplomat*, https://thediplomat.com/2023/08/social-media-and-the-fight-for-political-influence-in-southeast-asia/.

21 Panu Wongcha-um and Panarat Thepgumpanat (2022) “Thai Minister Backtracks on Spyware Admission as Government Denies Pegasus Use”, *Reuters*, https://www.reuters.com/world/asia-pacific/thai-minister-backtracks-spyware-admission-government-denies-pegasus-use-2022-07-22/.

22 “Lèse-majesté” refers to the act of showing disrespect or committing an offense against a sovereign, especially a monarch or head of state. It typically involves speech, writings or actions that criticise, insult or threaten the dignity or authority of a reigning monarch or the state.

4. The Way Forward: Recommendations to Strengthen Cybersecurity Governance

General Recommendations

SEA Asian countries are confronted with a number of significant cybersecurity challenges. To address these challenges and achieve good cybersecurity governance, various steps should be undertaken at both the national and regional levels.

First, greater awareness about the significance of cybersecurity should be raised and cultivated among the ASEAN member states. Crucially, more attention should not only be drawn to the many technical issues related to cybersecurity, but also to questions related to politics, diplomacy and law, which are equally important to address. Such a broadening of scope will require an increase in exchanges at both the governmental and non-governmental levels and a stronger involvement of legal experts and senior policymakers.

Secondly, SEA countries should draft NCSs or, where they have already done so, further refine them and use them as starting points to put policy into practice. As national governments are the prime arbiter of security not only in the physical, but also the virtual, domain it is important to define their role in cyberspace and lay down clear protocols. The development and refinement of NCSs is a crucial step towards achieving this goal. Once they have been adopted, NCSs can then serve as a starting point for states to put their policies into practice.

Thirdly, the formulation of policies and adoption of strategies on cybersecurity should be supplemented by regular cybersecurity trainings, tabletop exercises and other preparatory activities. For example, regional cooperation on cybersecurity could be expanded to also include tabletop exercises and simulations in cyber space. This would help to significantly improve joint responses to cyber incidents, as well as to promote transparency and build confidence and trust between countries.

Fourthly, a multipronged approach to cybersecurity should be adopted that also involves the private sector, civil society and academia. The inclusion of the private sector is particularly vital, as private actors such as big tech companies hold significant technical expertise and capabilities. Private actors can also take the lead in promoting strategic cybersecurity where governments are unable or unwilling to do so. The organisation of Track 2 meetings can be a particularly useful tool in this regard, as they offer a number of distinct advantages. They facilitate the exchange of expertise between a diverse number of stakeholders. They also allow stakeholders to openly discuss often sensitive issues in their personal capacities, and thereby candidly share their views and opinions. Another advantage is that Track 2 meetings enable participants to formulate policy recommendations that are aware of, but unbound by, the political constraints that often limit discussions at the governmental level.

Fifthly, confidence and capability-building measures on cybersecurity should be undertaken to assist the socioeconomic development in the region. Crucially, confidence

and capability-building measures can assist SEA countries that are currently less cyber mature to enhance their digital infrastructures and in doing so, also advance their socioeconomic development. In addition, such confidence and capability-building measures can also contribute to developing region-wide cyber norms.

Finally, there exists an urgent need to foster greater regional cooperation and improve coordination between countries, institutions and regional organisations on issues related to cybersecurity. As discussed, many cybersecurity challenges are transnational in nature. Stronger cooperation between individual countries is therefore crucial to address these challenges. Regional cybersecurity architecture can also be significantly strengthened by negotiating both regional and bilateral agreements on a variety of topics, including information sharing, technical assistance, technical training and nontechnical expertise. Such agreements can provide frameworks to jointly address shared challenges, as well as facilitate the development of digital infrastructure and so support the region's socioeconomic development. A promising platform for negotiating such agreements is already provided by ASEAN. Additional assistance could also be provided by third parties such as the European Union and the alliance between the International Telecommunication Union (ITU) and the International Multilateral Partnership Against Cyber Threats (IMPACT).

Specific Recommendations

Regional and International Levels

Reform securitised discourse and language: It is imperative for ASEAN to delineate and advocate for a unified comprehension of the role of cybersecurity in mitigating cyber threats. This measure is essential for establishing a coherent foundation for collaborative efforts and strategic planning, ensuring that member states operate with a shared perspective based on good governance principles.

Undertake capacity building: Regular cybersecurity training, tabletop exercises and other preparatory activities should be conducted to improve joint responses to cyber incidents, promote transparency, and build confidence and trust.

Create new informal and formal spaces for cooperation: This involves creating designated points of contact for facilitating collaboration among SEA countries and potentially beyond the region. This cooperative framework can be supported by functional interactions between relevant agencies.

Promote the establishment of legally binding bilateral and multilateral agreements: ASEAN's existing frameworks are non-binding, but enhancing their impact requires legally binding agreements between countries. These agreements can lead to substantial improvements and may even serve as models for broader multilateral endeavours. Furthermore, negotiations for regional or bilateral agreements encompassing areas such as information exchange, technical support, technical training and expertise beyond the technical realm should be encouraged.

National Governments

Develop comprehensive national cybersecurity strategies: These strategies should encompass a range of aspects, from policy frameworks to technical implementation, and be reviewed regularly to ensure that they remain aligned with evolving cyber threats.

Conduct a capacity mapping: Mapping existing institutions that have, or could have, the capacity to deal with cybersecurity threats is crucial. Once these institutions have been clearly identified, clear mandates and chains of commands can be established. Clear demarcation of mandates coupled with interagency cooperation can resolve the issue of applicable jurisdiction and allow for an improved synchronisation at regional and national levels.

Build confidence and capacity: Providing training programs, workshops and initiatives aimed at both technical and non-technical stakeholders can empower individuals and organisations to effectively respond to cyber threats.

Enhance awareness and understanding: Beyond technical aspects, awareness efforts should highlight the political, diplomatic and legal implications of cybersecurity.

Empower local security actors: Local state security actors are often more aware of the reality on the ground than central governments are. They can therefore take faster and more tailored action, if provided with the necessary means. These means would include a clear and efficient legal framework with provisions for dedicated oversight mechanisms to avoid abuse of power, as well as adequate training in cybersecurity. Finally, the necessary budget should be allocated to local state security actors to enable them to fulfil their new responsibilities.

Promote collaboration: A coordinated effort among governments, private sector and civil societies helps to ensure cyber threats are being addressed in an inclusive manner that considers the needs and rights of everyone. Resources for non-state security actors should be bolstered, as their efficiency can often be negatively affected by a lack of resources, which can potentially result in the abandonment or unrealised potential of important initiatives.

Promote security risk assessments: Creating awareness about the significance of risk assessments helps security institutions understand their cyber risk landscape and take proactive measures to enhance security. These assessments also assist them in prioritising resources and investments to address the most critical security gaps.

Establish a security incident response plan: A comprehensive security incident response plan ensures a well-coordinated and swift reaction in the event of a cybersecurity incident. It outlines predefined steps, roles and responsibilities to mitigate damage, minimise downtime and restore normalcy.

Monitor and adapt to the ongoing security environment: This involves staying updated on threat intelligence, patching vulnerabilities and fine-tuning security protocols to ensure that existing measures remain effective in safeguarding systems and data.

Civil Society

Civil Society plays a key role in filling some of the gaps left by governmental structures, as well as in acting as accountability mechanisms. It is thus important that governments involve and support non-state security actors, while being careful not to hamper their flexibility and freedom of action and speech.

Share information: Non-state security actors can help raise public awareness about cyber threats and necessary cybersecurity policies, as well as ensure that public concerns about restrictive laws are made known to the policymakers.

Promote digital rights: Non-state oversight actors, for example the media and civil society organisations, could support vulnerability disclosure efforts, thus encouraging responsible reporting of vulnerabilities from governments and state security actors. They can also establish policy dialogue platforms to facilitate open discussions between public and government representatives, thus fostering collaborative efforts to shape comprehensive and effective cybersecurity policies and strategies.

Monitor and hold accountable: Non-state oversight actors should act as an oversight mechanism and monitor the implementation of cybersecurity policies, laws and initiatives to ensure that they align with the interests of the public. If they fall short of doing so, non-state oversight actors should advocate for necessary changes. They should also ensure that cybersecurity initiatives and policies consider the diverse perspectives and needs of all parts of society to foster inclusivity and equitable protection. In order to assume this responsibility, national governments will need to develop the necessary protective legal framework.

5. Conclusion

Cybersecurity has begun to make inroads into legal frameworks in Southeast Asia. Yet the formulation of comprehensive national cybersecurity policies remains at a nascent stage due to disparities in capacities and the absence of a unified regional understanding of cybersecurity. The intricate overlap of national, regional and international jurisdictions complicates the application of the rule of law, an essential element of good governance. Progress can be noticed in the establishment of bilateral and multilateral agreements among ASEAN countries, although the current frameworks remain limited in scope and non-binding in nature.

In addressing cybersecurity, a diverse array of security sector actors – whether state or non-state, and whether security providers or oversight actors – need to closely collaborate, supported by the necessary legal frameworks.

This thematic brief highlights numerous challenges that warrant tailored actions from various security sector actors. A concerted push for standardised procedures within the cybersecurity domain and the formulation of an official regional definition for cybersecurity could significantly improve the collective capacity of ASEAN countries to address cyber threats more effectively and equitably distribute responsibilities among stakeholders.

ASEAN's commitment to encouraging cybersecurity collaboration is evident. However, achieving comprehensive reform is no small feat. It requires overcoming the significant challenge of fostering collaboration across security sector actors and governments. Despite the universal acknowledgment of the necessity to reshape cybersecurity paradigms, the consensus on the prioritisation of cybersecurity reform remains fragile because of diverse national priorities and varying capacities across the region. Additionally, it is essential to ensure that any initiative to reinforce cybersecurity applies good governance principles and respects basic human rights to mitigate possible negative effects on the public. In view of this, it is essential to determine how cybersecurity reforms align with the broader policy objectives of national governments and regional entities. Support for such efforts can be strengthened by illustrating how they bolster resilience against cyber threats, enhance digital resilience and foster regional stability. As ASEAN navigates this complex cybersecurity terrain, it is crucial to recognise that cybersecurity governance is not just a national concern, but rather a shared regional challenge that requires unified, strategic and collective action to ensure the digital security and prosperity of all member states.

ASIA-PACIFIC

SECURITY SECTOR
GOVERNANCE NETWORK

DCAF Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E
P.O. Box 1360
CH-1211 Geneva 1

+41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

@DCAF_Geneva