ASEAN CYBERSECURITY COOPERATION STRATEGY

2026-2030

one vision
one identity
one community

ASEAN Cybersecurity Cooperation Strategy 2026-2030

The Association of Southeast Asian Nations (ASEAN) was established on 8 August 1967. The Member States of the Association are Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste, and Viet Nam.
The ASEAN Secretariat is based in Jakarta, Indonesia.

Author:
ASEAN Network Security Action Council

For inquiries, contact:
The ASEAN Secretariat
Community Relations Division (CRD)
70A Jalan Sisingamangaraja Jakarta 12110
Indonesia
Phone: (+62 21) 724-3372, 726-2991
Fax: (+62 21) 739-8234, 724-3504
E-mail: public@asean.org

ASEAN Cybersecurity Cooperation Strategy 2026–2030
Jakarta, ASEAN Secretariat, April 2026

338.92
1.ASEAN - Economic – Cybersecurity
2.Data Protection - Digital Economy

ASEAN Cybersecurity Cooperation Strategy 2026–2030

The ASEAN Secretariat
2026

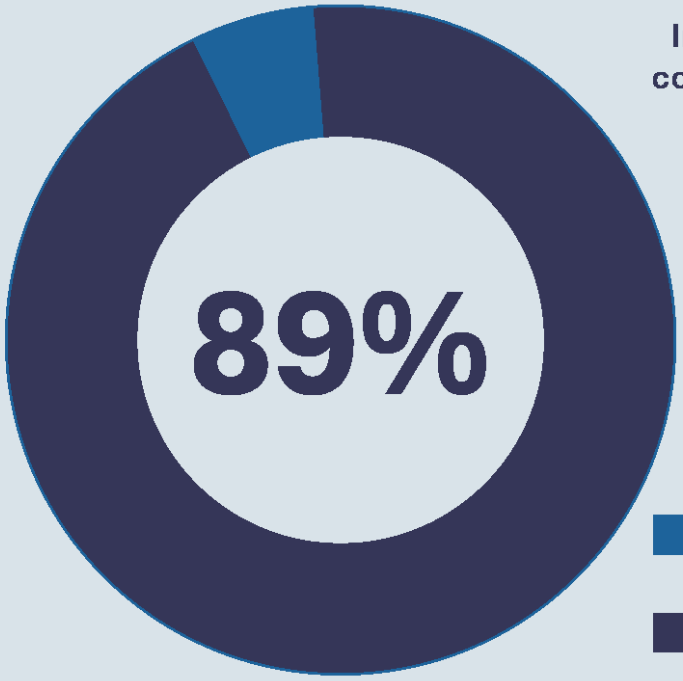
Contents

Glossary of abbreviations

ACCS	ASEAN Cybersecurity Cooperation Strategy
ACCSQ	ASEAN Consultative Committee for Standards and Quality
ACICE	ADMM Cybersecurity and Information Centre of Excellence
ACID	ASEAN CERT Incident Drill
ADGMIN	ASEAN Digital Ministers Meeting
ADGSOM	ASEAN Digital Senior Officials Meeting
ADGSOM-ATRC	ASEAN Digital Senior Officials Meeting-ASEAN Telecommunications Regulators Council
ADM	ASEAN Digital Masterplan
AJCCBC	ASEAN-Japan Cybersecurity Capacity Building Centre
AMCC	ASEAN Ministerial Conference on Cybersecurity
ANSAC	ASEAN Network Security Action Council
ARF	ASEAN Regional Forum
ASCCE	ASEAN-Singapore Cybersecurity Centre of Excellence
ASEAN Cyber-CC	ASEAN Cybersecurity Coordinating Committee
ATRC	ASEAN Telecommunications Regulators Council
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Team
DEFA	Digital Economy Framework Agreement
DTSC-WG	Digital Trade Standards and Conformance Working Group
DP	Dialogue Partners
SOMRI WG-IMT	SOMRI Working Group on Information, Media and Training

ASEAN Cybersecurity Cooperation Strategy 2021-2025 snapshot

Initiatives' completion status



*As of June 2025

Establishment of ASEAN Regional CERT

2022
Endorsement of the ASEAN Regional CERT implementation paper

2023
Endorsement of the operational Framework of ASEAN Regional CERT

2024
Endorsement of the financial framework and launch of physical facility of ASEAN Regional CERT

2025
Launch of the ASEAN Regional CERT's Information Sharing Mechanism

Advancing Rules, Norms, Standards for Secured Cyberspace

2021
Endorsement of ASEAN Regional Plan of Action (RAP) Matrix on the Implementation of Norms of Responsible States Behaviour in Cyberspace.

2022
Endorsement of ASEAN Cybersecurity Assessment Model

2024
Completion of the ASEAN Norms Implementation Checklist

2025
Inventory of Critical Information Infrastructure (CII) Identification Frameworks in ASEAN

Cybersecurity graduates

4774 graduates*

AJCCBC ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE

ASCCE ASEAN-SINGAPORE CYBERSECURITY CENTRE OF EXCELLENCE

*graduates from AJCCBC and ASCCE

Multilateral cybersecurity engagements with dialogue partners

- ASEAN-China Cyber Policy Dialogue
- ASEAN-Russia Dialogue on ICT Security-related issues
- ASEAN-US Cyber Policy Dialogue
- ASEAN-India Cyber Dialogue
- ASEAN-Australia Cyber Policy Dialogue
- ASEAN-Japan Cybersecurity Policy Meeting & ASEAN - Japan Cybersecurity Working Group Meeting

1. Cybersecurity in ASEAN

1.1. A decade of cooperation

1. The first ASEAN Cybersecurity Cooperation Strategy was elevated from the ASEAN Cyber Capacity Programme (ACCP) introduced in 2016. Developed by ASEAN's Network Security Action Council (ANSAC)[1], the pioneering ACCS called for the creation of a safe and secure cyberspace in ASEAN by strengthening cybersecurity cooperation in cybersecurity incident response, Computer Emergency Response Team (CERT) policy and coordination, and cybersecurity capacity building. This was succeeded by the second ACCS iteration that updated ASEAN's approach amidst the region's rising digital ambitions implemented between 2021 to 2025.

1.2. Institutional developments

1. ASEAN has pursued significant institutional developments to address safety and security in the use of cyber. Figure 1 illustrates ASEAN's sectoral bodies tasked with cybersecurity such as the bodies and working groups dedicated to cybersecurity.

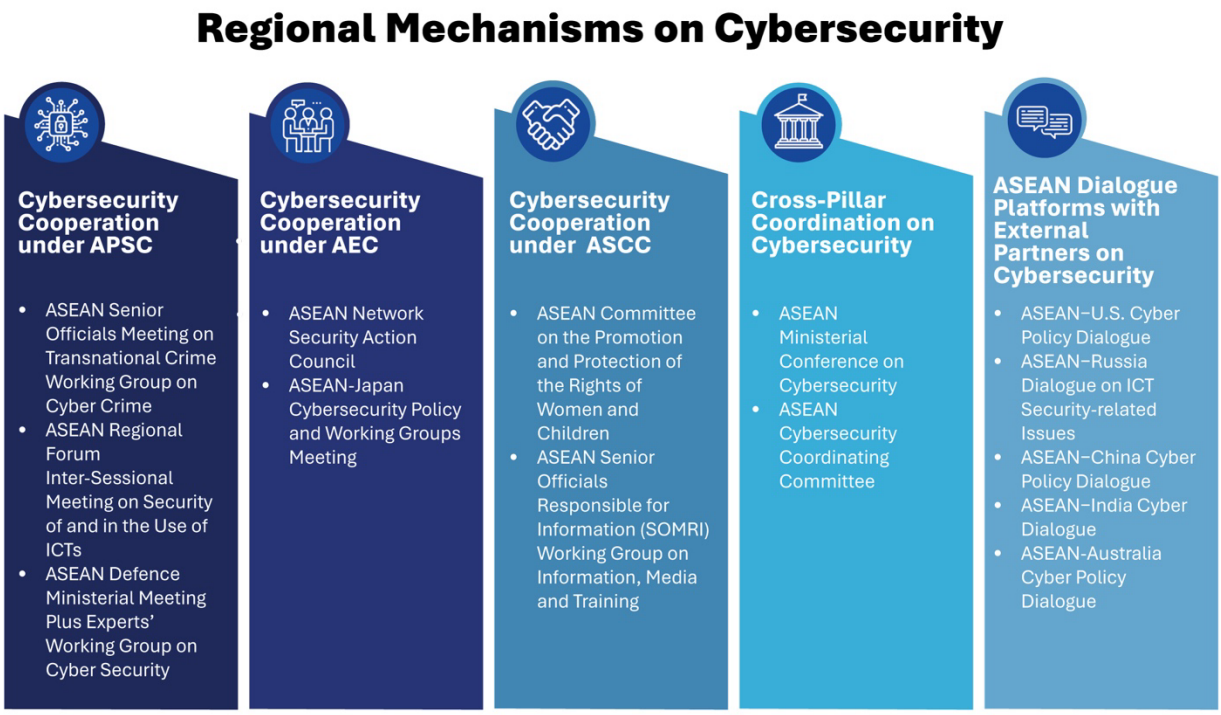
2. ANSAC under the ASEAN Digital Ministers Meeting (ADGMIN), plans, coordinates and facilitates ASEAN cooperation activities in the development of ASEAN cybersecurity capacity, including with ASEAN Dialogue Partners. ANSAC's purview in the cybersecurity domain is focused on (i) promoting and coordinating the implementation of all cybersecurity-related initiatives under ASEAN Digital Masterplan, (ii) coordinating cybersecurity capacity building in ASEAN, (iii) taking the lead in coordinating with ASEAN Dialogue Partners and international organisations on cybersecurity policy cooperation, including information sharing and cyber hygiene initiatives, and (iv) exploring the potential for cybersecurity cooperation with other ASEAN sectoral bodies. ASEAN's cross-sectoral cybersecurity coordination is supported by ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) which consists of ASEAN Senior Officials Meeting on Transnational Crime Working Group on Cyber Crime (SOMTC WG on CC) and ASEAN Senior Officials Responsible for Information Working Group on Information, Media and Training (SOMRI WG-IMT). ASEAN Cyber-CC reports to ADGMIN.

3. Institutional developments for cybersecurity include the successful development and operationalisation of ASEAN Regional Computer Emergency Response Team (CERT). With the physical facility launched at the 9th ASEAN Ministerial Conference on Cybersecurity (AMCC) in October 2024, the ASEAN Regional CERT would serve as a focal point for regional capacity building, information management and crisis communication.

[1] Reference from ASEAN's Major Sectoral Bodies/Committee website

4. Meanwhile, the region has also developed a number of regional frameworks to navigate emerging technologies and evolving architecture. These are inclusive of ASEAN Guide on Artificial Intelligence (AI) Governance and Ethics, ASEAN Framework on Digital Data Governance and the Enhanced ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables. Furthermore, ASEAN has achieved substantial conclusion of Digital Economy Framework Agreement (DEFA) negotiation in October 2025 and remains on track to finalise the agreement by 2026, reflecting the region's collective aspiration to build an open, inclusive, secure, and interconnected digital economy.

Figure 1 on regional mechanisms on cybersecurity



1.3. National policy development to protect critical information infrastructure and digital security

1. Regional regulatory trends are accompanied by maturity in legislation for the protection of cyber and digital systems among AMS. Since 2017, a majority of AMS have developed laws to protect Critical Information Infrastructure (CII) and data protection illustrated in Table 1.

Table 1: National policy developments in AMS

Country	Protection of CII	Data Protection
Brunei Darussalam	Cybersecurity Act Chapter 272 (Passed in 2024)	Personal Data Protection Order 2025 (Passed in 2025)
Cambodia	Draft on cybersecurity law (Draft announced in 2022)	Draft law on personal data protection (Released in 2023)
Indonesia	Presidential Regulation Number 82 of 2022 on Protection for Vital Information Infrastructure (Issued in 2022)	Personal Data Protection Law, Law No. 2 of 2022 (Passed in 2022)
Lao PDR	Draft Cybersecurity Law (Presented on 2025, June)	Law on Electronic Data Protection (No. 25/NA) (Passed in 2017)
Malaysia	Cyber Security (Act) 2024 – Act 854 (Enforced in 2024)	Personal Data Protection (Amendment) Act 2024 (Amended in 2024)
Philippines	Critical Information Infrastructure Protection Act of 2022 (Pending approval in congress)	Republic Act 10173, Data Privacy Act of 2012 (Passed in 2012)
Singapore	Cybersecurity (Amendment) Act 2024 (Amended in 2024)	Personal Data Protection (Appeal) (Amendment) Regulations 2024 (Amended in 2024)
Thailand	Section 49 of the Cybersecurity Act 2019 (Passed in 2019)	Personal Data Protection Act, B. E. 2562 (2019) (Passed in 2019)
Viet Nam	Law on Cybersecurity 2018 (Passed in 2018) National Cybersecurity Strategy 2025	Personal Data Protection Law (Passed in 2025) Decree No. 13/2023/ND-CP on Personal Data Protection (Passed in 2023)

1.4. International summits and impact on regional cybersecurity

1. ASEAN's regional and international engagements have structured the region's approach to responsible state behaviour in incident response and crisis. Platforms such as ASEAN Regional Forum (ARF) have served as vehicles for capacity-building and confidence-building measures. Programmes cover principles of building security in The Use of ICTs in the national context, protection of ICT-enabled critical infrastructures, establishing ARF Points of Contact Directory on Security of and in the Use of ICTs, in addition to developing an ARF Terminology in the field of security of and in the use of ICT.

2. Meanwhile, the United Nations (UN) remain a vital arena of international diplomatic conversations on cyber and digital governance. The Open-Ended Working Group on the security of and in the use of ICTs 2021–2025 (OEWG 2021–2025) had engaged stakeholders in a systematic and substantive manner with the Final Report acknowledging the importance of capacity building and the need to continue addressing the diverse landscape of ICT threats. The formation of a permanent UN Global Mechanism, replacing the OEWG 2021–2025, indicates global commitment

for sustained dialogue on ICT security and the framework of responsible state behaviour. ASEAN's observation of developments at the UN also underpins efforts to strengthen trust and regional cybersecurity foundations. These efforts include the ASEAN Regional Action Plan (RAP) on the implementation of the Norms of Responsible State Behaviour in Cyberspace, developed in support of UNGA Resolution 70/237. The RAP matrix was adopted in November 2021. Subsequently, a norms implementation checklist was completed by ASEAN in September 2024 to offer practical cybersecurity practices that operationalise the 11 norms of responsible state behaviour.

2. Key achievements of ACCS 2021–2025

1. The ACCS 2021–2025 was endorsed at the 2nd ASEAN Digital Ministers Meeting (ADGMIN) in January 2022. Constructed in the midst of the pandemic, ACCS 2021–2025 acknowledged the complex interrelation of cyber and digital issues inclusive of those covering misinformation and disinformation. Additionally, with rising digitalisation and dependence on digital platforms and services during the pandemic years, the ACCS 2021–2025 grappled with increasing sophistication of cyberattacks on critical infrastructure and supply chain.

2. The strategy consisted of 5 dimensions in line with the ASEAN Economic Blueprint and the ASEAN Digital Masterplan (ADM) 2025, 8 focus areas and 19 initiatives. As of June 2025, the implementation of all key initiatives have already commenced, with a total of 17 initiatives completed and 2 partially completed.

3. The two initiatives that remain partially completed are the development of ASEAN CII Protection Coordination Framework and the development of regional security policy, procedure and guidelines for SMART city implementation. Under the development of ASEAN CII Protection Coordination Framework, work is ongoing to complete a project on the Inventory of CII Identification Frameworks in ASEAN, expected to conclude by 2025 with the Philippines as the proponent. Meanwhile, the initiative on the development of regional cyber security policy, procedure and guidelines for smart city implementation was recommended to be reviewed for further recommendation as part of the ASEAN Cybersecurity Cooperation Strategy 2026–2030, with capacity building activities on this topic already implemented in 2024.

Figure 2: Achievement of ACCS 2021–2025 dimensions, focus areas and initiatives (as of June 2025)

Indicator	Achievement
Dimension 1: Advancing cyber readiness cooperation	
Focus area 1: CERT cooperation	
Initiative 1: ASEAN Regional CERT establishment	✓
Initiative 2: ASEAN CERT information exchange mechanism establishment	✓
Initiative 3: ASEAN cybersecurity threat landscape annual report	✓
Focus area 2: Critical Information Infrastructures (CII) protection	
Initiative 4: Development of ASEAN CII Protection Coordination Framework	Partially completed
Dimension 2: Strengthening regional cyber policy coordination	
Focus area 3: Coordination on cybersecurity and related digital security issues	
Initiative 5: The ASEAN Leaders' Statement on Advancing Digital Transformation	✓
Initiative 6: Regional Internet Governance Forum (IGF) on cross-jurisdictional approach to online content regulation	✓
Focus area 4: Norms implementation	
Initiative 7: Development of Matrix for ASEAN Regional Plan of Action (RAP) on the Implementation of Norms of Responsible States Behaviour in Cyberspace	✓
Dimension 3: Enhancing trust in cyberspace	
Focus area 5: Promoting international cybersecurity standards	
Initiative 8: Development of regional cybersecurity standards for IoT	✓
Initiative 9: Development of regional cyber security policy, procedure and guidelines for 5G and IoT implementation	✓
Initiative 10: Development of regional cyber security policy, procedure and guidelines for smart city implementation	Partially completed
Initiative 11: Capacity building activities on digital infrastructure product and software security testing and certification	✓
Focus area 6: Cyber hygiene and digital inclusion	
Initiative 12: The development of cybersecurity awareness programme for AMS	✓
Initiative 13: Development of digital literacy training modules or programmes	✓
Dimension 4: Regional capacity building	
Focus area 7: Multi-disciplinary, modular, multi-stakeholder and measurable programmes	
Initiative 14: ASEAN-Japan Cybersecurity Capacity Building Centre's Programmes	✓
Initiative 15: ASEAN-Singapore Cybersecurity Centre of Excellence's (ASCCE) programmes	✓
Initiative 16: ADMM Cybersecurity and Information Centre of Excellence	✓
Dimension 5: International cooperation	
Focus area 8: Multilateral engagement with the dialogue partners	
Initiative 17: Engage with DPs and other countries in the region for confidence-building measures (CBM), including through ARF intersessional	✓

meeting on security of and in the Use of Information and Communication Technologies (ARF ISM on ICTs Security)	
Initiative 18: Establish coordination/follow-up mechanism for ASEAN Cybersecurity Dialogues with related DPs to discuss, to ensure inclusivity and avoid duplication	
Initiative 19: Conduct CERT to CERT dialogues and joint exercises with Dialogue Partners	

4. The ACCS 2021–2025 fully establishes the ASEAN Regional CERT and the CERT's information sharing mechanism. The ASEAN Regional CERT synergises strengths and expertise of AMS national CERTs to enhance effectiveness of regional incident response capabilities. Playing a role for information exchanges and capacity building, the ASEAN Regional CERT prepares the region for effective CERT–to–CERT threat information sharing, crisis coordination and CERT capacity-building program.

5. The ASEAN's Leaders Statement on Advancing Digital Transformation in ASEAN on 26 October 2021 also served as a declaration of commitment for ASEAN's post-pandemic economic recovery which would be dependent on digital transformations.[2] The statement emphasised cooperation and capacity building in cybersecurity especially in the development of a secure, resilient, interoperable and rules-based cyber space. Efforts should encourage policy coherence across the sectors while strengthening ASEAN centrality in the region's cybersecurity architecture and enhancing alignment of regional cybersecurity policy.

6. Furthermore, ASEAN has made progress on the ASEAN Norms Implementation Checklist and Regional Action Plan (RAP) matrix on norms implementation. The RAP matrix adopted in November 2021 and the checklist completed in September 2024 identified specific capacity-building activities and practical initiatives that would assist ASEAN Member States in implementing the voluntary-non-binding norms of responsible state behaviour in cyberspace in alignment with national priorities and needs.

7. The ACCS 2021–2025 also saw the establishment of a Guideline for IoT and 5G cybersecurity implementation. IoT implementation standards was discussed in the ASEAN-Japan Cybersecurity Standards workshop in December 2024. The IoT cybersecurity standards were discussed further in a webinar on security labelling for IoT organised by AJCCBC, Japan's MIC and METI in December 2024. Meanwhile, the 'Cybersecurity Standards and Conformance to Support Digital Trade in ASEAN' whitepaper was published in 2023. The whitepaper details standards to facilitate digital trade between ASEAN and global markets such as the US. Additionally, in the midst of rising interest in 5G, the region published Guidelines for 5G Ecosystem Development in ASEAN endorsed in January 2022.

[2] ASEAN Leaders' Statement on Advancing Digital Transformation in ASEAN.

8. Efforts by regional institutions such as AJCCBC and ASCCE cultivated talent for cybersecurity. AJCCBC in Thailand continues to be supported by Japan and has trained 2,741 officials as of July 2025. ASCCE has trained 2,033 senior government officials in 69 cyber capacity building programmes as of 2025. The ASEAN Cyber Shield Project supported by ROK also conducted online education programmes and scholarship exchanges for youth and students to enhance cyber resilience in ASEAN. Additionally, annual ASEAN Cyber Shield Hacking competition and the Cyber SEA Games were held to enhance talent development.

9. The years 2021–2025 also convened multi-stakeholder efforts to address disinformation and misinformation infodemic. The Regional Internet Governance Forum held the ASEAN Forum on Tackling Disinformation and ASEAN Workshop on Best Practices of Digital Transformation in Media. Additionally, the Vision Statement by AMRI-ASEAN 2035, Da Nang Declaration and Guideline on Management of Government Information in Combating Fake News and Disinformation in the Media sought to future-proof ASEAN's approaches to manage the information environment, inclusive of transformations by AI.

10. Between 2021 to 2025, ASEAN expanded its cyber policy dialogues with Dialogue Partners to a total of five, with India and Australia joining existing dialogue partners; United States, China and Russia. To strengthen transparency, ASEAN had constructed a term of reference that anchors dialogues in exchanges rather than advocacy of specific stances. ASEAN Cyber-CC play pivotal roles in facilitating Cyber Policy Dialogues and consolidating capacity building efforts. Under ACCS 2021–2025, ASEAN also held the first ASEAN-ITU CyberDrill conducted via video conference in 2022.

3. ASEAN and the cybersecurity landscape

3.1. ASEAN's digital transformation

1. ASEAN's digital economy is rapidly expanding, underpinned by its status as the fastest-growing internet market in the world. Projections estimate the digital economy could contribute up to USD 1 trillion to regional GDP and potentially double to USD 2 trillion with the successful implementation of the DEFA.[3] Meanwhile, ASEAN's internet is accessed by 72% of the population[4], with an estimation of 125,000 new users coming onto the

[3] Data from World Economic's Forum project on "Digital ASEAN"
[4] Data from ASEAN Statistical Yearbook 2023, ASEAN Secretariat, 2023

Internet every day.[5] Google-Temasek estimates ASEAN's gross merchandise value (GMV) at USD 263 billion, with revenues reaching USD 89 billion in 2024.[6] The 2024 UN E-Government Survey[7] ranks Asia as the fastest-growing region for digitalisation in the public sector, and ASEAN leaders[8] have reaffirmed their commitment to the ASEAN Digital Master Plan 2025 to position ASEAN as a leading digital community. As digitalisation in the region grows, this also adds complexity to the cybersecurity landscape.

2. Shared infrastructure and emerging technologies impact traditional cybersecurity practices. Undersea cables and orbital communication networks have been instrumental to developing connectivity architectures. Meanwhile, the ASEAN Power Grid that is necessary to fuel data centres also enables cross-border electricity trade while incorporating digital transformation in the energy sector. Emerging technologies such as AI, IT/OT integration and cloud technologies are catalysts for the digital infrastructure, making core challenges such as securing supply chains and protecting critical infrastructure, a dynamic environment. However, growing trends of malicious ICT activity deliberately exploiting the vulnerability of technologies like industrial control systems (ICS), operational technology (OT), 5G networks, the Internet of Things (IoT), data centers, and cloud computing services are of grave concern. These could have widespread consequences as digital transformations occur in commercial and critical sectors.

3.2. Cybersecurity landscape

1. In an increasingly volatile geopolitical climate, cyber threats have intensified and evolved significantly, affecting the cybersecurity landscape. The increasing likelihood of ICTs being used in conflicts between states is a mounting concern. This use of ICTs in conflicts have already occurred in different regions and impacts both military forces and civilians. A disturbing trend is the continuous increase in malicious use of ICTs by state and non-state actors, including criminal and terrorist groups. Some non-state actors now possess ICT capabilities that were previously only available to states. Meanwhile, ICT activities targeting CI and CII could disrupt essential services across borders. These malicious ICT activities can undermine trust and confidence between states, and disrupt political, electoral, and public institutions. While new technologies like AI and Quantum Computing offer development opportunities, these emerging technologies may also create new vulnerabilities that threat actors can exploit. The risk, in addition to a growing market for ICT intrusion capabilities disseminated by states and non-state actors calls the need for meaningful action.

---

[5] Data from World Economic's Forum project on "Digital ASEAN"
[6] Data from e-Conomy SEA 2024 Report, by Google, Temasek, and Bain & Company.
[7] Data from United Nations E-Government Survey, 2024
[8] Leaders' Statement on the Development of the ASEAN Digital Economy Framework Agreement (DEFA). ASEAN Indonesia 2023

3. The aggregation of data from the use of new and emerging technologies, including IoT, AI, cloud computing, and quantum computing highlights the increasing importance of data protection and security. Data is fundamental to realise digital ambitions such as AI and its protection amid digital transformation is essential.

3.3. Operational Technology (OT) security

1. Further integration between IT and OT environments will complicate the attack surface, particularly when systems and technologies are not regularly updated to address emerging gaps and vulnerabilities. A Kaspersky and VDC Research report found that a majority (63.6%) of industrial organisations surveyed are undergoing rapid digitalisation. However, approximately 46.6% of research respondents expressed inadequate security measures within their existing infrastructure while 41.7% emphasised complexities of IT/OT integration.[9] As convergence accelerates, maintaining robust OT security will require not only technical upgrades but also a workforce equipped with the necessary skills and awareness to recognise and respond to evolving threats effectively.

3.4. Artificial intelligence

1. AI could transform systems and cybersecurity practices. While continuing to encourage innovation, it is also necessary that AI is adopted in a safe, secure and responsible manner. On one hand, AI can identify and address threats more quickly, accurately and efficiently. On the other hand, AI can also be misused to develop sophisticated cyber and social engineering attacks. In a survey by Cloudflare covering Asia Pacific, half of the respondents anticipate that AI will be leveraged to crack passwords or encryption codes, whereas 47% believe it will enhance phishing and social engineering attacks.[10] An increase in reliance and dependence on AI for cybersecurity could introduce vulnerabilities while jailbroken Generative AI tools could result in data breaches, misinformation and productivity challenges. The risk is further exacerbated by the shortages of AI security talent to build and maintain resilient defenses against emerging threats.

3.5. Cloud technologies

1. With investments in data centres in the region surpassing USD 30 billion[11] and e-government policies encouraging further utilisation of cloud, insecure cloud architecture could induce data breaches, exploit insecure APIs or expose systems to DDOS attacks. Globally, the Thales 2025 Cloud Security Study reported 55% of respondents believe that cloud environments are

[9] From Securing OT with Purpose-built Solutions report, 2025, by VDC Research and Kaspersky
[10] From Cloudflare's Navigating the New Security Landscape: Asia Pacific Cybersecurity Readiness Survey 2024 report
[11] Estimations from AWS and Microsoft announcements.

harder to secure, with organisations relying on five or more tools to monitor, classify or manage encryption keys across different platforms.[12] As cloud becomes fundamental in computing and telecommunications infrastructure, there is a need to examine secure practices. Alignment in regional practices, common standards, as well as capacity building in cloud security could support uptake by organisations. Confidential computing which encrypts data in use in addition to at rest or in transit has to be considered especially when it is estimated that 9% of regional cloud storage resources contain sensitive data.[13]

3.6. Data breaches and unauthorised system intrusions

1. Data breaches in ASEAN are causing significant financial losses and eroding trust. According to IBM, economic losses from data breaches in ASEAN had reached USD 3.67 million in 2025, an increase from USD 3.23 million in 2024.[14] Data will be the enabler of future technologies. Yet, the underlying risks of data breaches and unauthorised system intrusions remain insufficiently mitigated. Be it caused by human errors, lapses in cybersecurity processes or gaps in outdated software, these open pathways to vulnerabilities that impact trust between consumers and states or raises levels of crime.

3.7. Quantum computing and cryptography

1. The National Institute of Standards and Technology (NIST)'s Report on Post-Quantum Cryptography estimates that initial breaches from quantum computing might come as soon as 2030.[15] Quantum computing has the capability to weaken or break public key cryptography. This would compromise secure communications and encryption across industries and governments. Thus, present sensitive and critical data may be at risk of being stolen to be decrypted at a later date ("store now, decrypt later"). This bears heavy risks as many governments or enterprises are unaware of the sensitive and critical data stored, processed or transiting through their systems. Furthermore, where some nations can invest in quantum-safe solutions such as Quantum Key Distribution (QKD); others may not have the capacity. This makes for an uneven playing field, leaving less prepared countries and organisations at higher risk.

2. Cryptography is fundamental component for cybersecurity. However, concerns over leaked cryptographic keys and exploitation in third party vendors require monitoring. The Heartbleed bug in OpenSSL discovered in 2014 for instance, exploited a typical function in computer protocols amid gaps in encryption. Additionally, reliance on external cryptography

[12] From Thales' Global Cloud Security 2025 report
[13] Tenable's 2025 Cloud Security Risk report
[14] From IBM's Cost of a Data Breach Report 2025: The AI Oversight Gap
[15] National Institute of Standards and Technology Report on Post-Quantum Cryptography, April 2016.

standards can create security and sovereignty challenges especially in niche sectors with unique data protection requirements. As quantum computing capabilities advance, there will be a critical need to develop talent for cryptography and implement quantum-resistant cryptographic solutions to ensure that sensitive data remains secure against emerging threats and technology.

3.8. Fraud and online scams

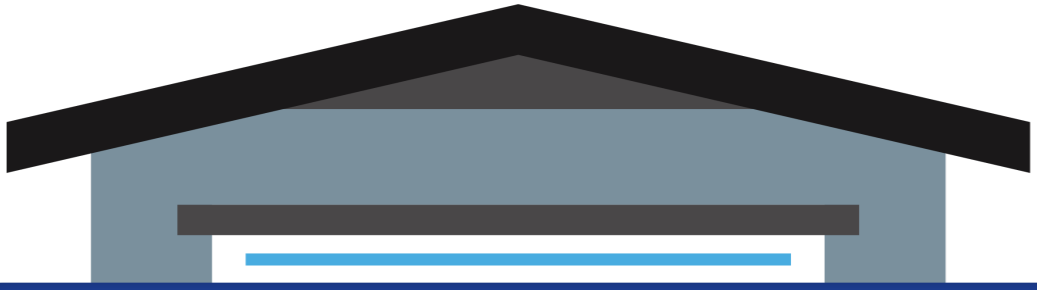
1. Fraud and online scams are major issues in the region. Losses related to online scams are significant, with Singapore reporting victims lost more than SGD 385 million in the first half of 2024[16], and the Thai people losing 79.5 billion baht from online fraud between 2022 and 2024.[17] In serious cases, online scams intertwine with human trafficking, with Laos estimating 150,000 victims annually.[18]

3.9. Ransomware

1. Ransomware is a growing threat in the ASEAN region, driven by exploited vulnerabilities, compromised credentials, phishing, and brute force attacks. States have raised alarms as the hiring of ransomware-as-a-service becomes more accessible[19]. Concerns extend to the CIs, CIIs and state institutions with rising impacts on essential services. In Viet Nam, cyberattacks in 2023 caused an estimated USD 716 million in losses[20], while Malaysia faced over 1,500 attacks in 2024[21], including a USD 10 million ransomware demand on Malaysia Airports Holdings Berhad (MAHB)[22]. In Indonesia, the national government temporary data centre was compromised by a ransomware attack, all of which underscores the urgent need for stronger regional cyber resilience.

[16] Singapore police's mid-year scam and cyber-crime statistics, August 2024.
[17] Thailand's National Cyber Security Agency (NCSA), 2025
[18] RFA Lao. 25 May 2024. Lao official: Gov't can't afford to address rise in human trafficking. RFA.
[19] UNGA's Open-ended working group on security of and in the use of information and communications technologies 2021-2025, *Eleventh substantive session*, New York, 7-11 July 2025
[20] Bkav Technology Group's Cyber Security Assessment program, 2023
[21] Malaysia's Prime Minister's department, November 2024
[22] Malaysia's Prime Minister's keynote address, 218th Police Day, March 2025

4. ASEAN Cybersecurity Cooperation Strategy 2026–2030



ASEAN Community Vision 2045

- To realise a resilient, innovative, dynamic, and people-centred ASEAN by 2045 and envisions ASEAN as the epicentre of growth in the Indo-Pacific.
- To promote responsible digital growth through comprehensive regulations and enforcement that facilitates secure and seamless cross-border data flows, ensures data protection for business purposes, and strengthens online safety and cybersecurity.

ASEAN Digital Masterplan 2030

- ASEAN as an integrated, secure, trusted, innovative, and inclusive digital community where citizens and businesses can access opportunities, build capabilities and thrive in the global digital economy.

Objective of ASEAN Cybersecurity Cooperation Strategy 2026-2030

1. To realise cyberspace that is trusted, secure, safe, interoperable and is an enabler of the digital economy.
2. To enhance cybersecurity which is envisioned to be resilient, adaptive to emerging technologies and is capable of responding to cyber crisis and incidences effectively.
3. To move towards a consolidated ASEAN in cybersecurity efforts, capable of projecting a unified voice to international fora.

Dimension 1	Dimension 2	Dimension 3	Dimension 4	Dimension 5
Strengthening cyber readiness	Advancing regional cyber policy coordination	Embedding trust in the ecosystem	Bolstering capacity building for the future	Synergising cooperation

Dimension 1: Strengthening cyber readiness

1. The ASEAN Community Vision 2045 stated the commitment to the development of ASEAN as "a leading and connected Digital and Technological Community with open and interoperable, secure and trusted

digital ecosystem".[23] Simultaneously, the 5th ASEAN Digital Ministers' Meeting and Related Meetings Joint Media Statement emphasised the "importance of delivering trusted digital services", which is further supported by "robust efforts to enhance cybersecurity and the prevention of consumer harm".[24]

2. ASEAN has made significant strides in cyber readiness. On policy, ASEAN Member States have introduced, or are in the final stages of drafting policies to protect critical infrastructure and data. In operational readiness, ASEAN has prepared institutions to strengthen incident response. The ASEAN Regional CERT was operationally launched in 2024 with the task of streamlining information sharing and improving regional incident response. Technical readiness has also moved forward with the completion of Cybersecurity Standards and Conformance to Support Digital Trade in ASEAN and the IoT standards by USASEAN and ASEAN-Japan, respectively. Legal readiness has also advanced with laws for cybersecurity and ICT misuse introduced or updated to meet current challenges. Furthermore, the region's cybersecurity readiness in cybersecurity diplomacy has strengthened, supported by the expansion of cyber policy dialogues with ASEAN Dialogue Partners.

3. However, ASEAN's digital environment is not stagnant. With digital maturity comes a larger canvas for vulnerabilities and attacks to occur. Emerging and transformative technologies such as AI could enhance cybersecurity but could also raise the volume of attacks. Agentic AI could strengthen cybersecurity approaches, especially if it could adapt to large volumes of attacks. Quantum infrastructure could enhance computing and strengthen encryption. Yet, transition of infrastructure to quantum safe could take decades and current vulnerabilities are in existing data sets, which are vulnerable to data harvesting that could be decrypted later.

4. Meanwhile, supply chain, unprotected IoT and cloud computing remain ongoing concerns, especially where there is over-reliance on ICT service providers, which may affect resiliency of systems. The SolarWinds attack highlighted how vulnerabilities can be exploited through third parties. Addressing such risks may require broader oversight that examines the relationship between an operator and the vendor, where obligations cover ICT vulnerability reporting and penetration testing. Addressing the challenge would necessitate coordinated joint responses.

5. Additionally, interconnected and shared infrastructure underscores the need for shared readiness, robust incident management and effective

[23] From the ASEAN Community Vision 2045 statement, paragraph 24, 26 May 2025.
[24] The 5th ASEAN Digital Ministers' Meeting and Related Meetings Bangkok, Thailand, 16 - 17 January 2025.

information sharing mechanisms. Recent conflicts have shown that critical infrastructure is often a primary target of attacks.

6. ASEAN would have to strengthen the region's information sharing mechanisms which could support real-time information sharing especially in moments of crisis. Improved coordination to address crisis are necessary, especially in areas such as incident coordination, and rendering technical assistance and sharing of information where relevant. These are fundamental readiness to address cyberattacks targeting multiple countries simultaneously.

7. ASEAN would also have to consider developing cybersecurity baselines for critical sectors, especially where benchmarking processes, technological standards and incident response could strengthen cybersecurity.

8. To improve cyber readiness, ASEAN would have to collaborate with private sector to improve threat information sharing and cultivate best practices. Further information sharing is needed to identify, assess and mitigate threats from emerging technologies such as artificial intelligence, quantum computing and IoT. Regional bodies primed for engagement, such as the ASEAN Regional CERT, could play a vital role in information sharing, crisis management and incident response.

Goals	Details	Potential Initiatives
1.1 Advancing critical infrastructure protection and improving crisis response	• Effective policies can enhance efficiency in regional response to cyber incidents. However, differences in definitions, communication protocols, and procedures can hinder readiness. Clear frameworks and protocols are essential, for personnel to know how to manage requests for assistance and make decisions in real time. This could be inclusive of pre-establishing communication channels, including diplomatic ties between states and partnerships with technology companies prior to a crisis and incident. • While ASEAN has advanced in protecting critical infrastructure, sustained progress requires	• Develop an ASEAN Best Practice for Governance Framework for Incident Response. • Conduct an ASEAN Feasibility Study on Regional Crisis Response. • ASEAN study on what constitutes harmful ICT practices. • Develop a strategic guideline for identification of critical sectors. • Conduct simulation/tabletop exercises, cyber exercises and joint drills. • Build a regional cybersecurity information repository to ease access

	shared responsibility, cooperation and clear codes of conduct. • There may be a need to practice information sharing and joint incident handling to enhance regional resilience particularly during cross-border cyber threats.	to information on ICT threats and incidents.
1.2 Raising cybersecurity baselines practices to protect critical infrastructure	• Cybersecurity baseline could become the foundational guideline for organisations to maintain the minimum protection standard for security controls. • A baseline can set basic expectations for process, information management, network security standards or sector-specific cooperation, especially for the protection of critical infrastructure which can vary in practice across sectors. • Pursuing recommended baselines could benchmark good practices to elevate cybersecurity levels. • The development of baselines can be based on ASEAN's existing research and could cover common processes among AMS to protect CII such as risk assessment.	• Feasibility study for ASEAN's cybersecurity baseline. • Continued development of the cybersecurity threat landscape report.
1.3 Positioning ASEAN Regional CERT as a regional hub for crisis and information exchange	• ASEAN Regional CERT have consolidated and developed mechanisms which enhances its role as a coordinator during crisis and for information exchange. • To deepen its role in information sharing, ASEAN Regional CERT would have to develop effective mechanisms that link with various networks for the latest	• Establish touchpoints for threat information sharing with key business associations/private sector partners. • Capacity building programmes by ASEAN with business associations/private sector and other governments on incident

	threats and technology vulnerabilities. This could include engagements with Dialogue Partners, international organisations, business associations/private sector or other regional CERTs. • Furthermore, the regional hub could enhance incident management through capacity building activities with various stakeholders.	response and emerging technologies. • To enhance ASEAN Regional CERT's collaboration opportunities through inter-regional CERT/CSIRT exchanges.

Dimension 2: Advancing regional policy coordination

1. The ASEAN Community Vision 2045 envisions ASEAN as "a rules-based Community", "committed to the letter and spirit of the Charter of the United Nations (UN), the ASEAN Charter, the Treaty of Amity and Cooperation in Southeast Asia (TAC) and other instruments".[25] The Community Vision also stated the necessity for the promotion of "peace, security and stability in the region, as well as to the peaceful resolution of disputes, including full respect for legal and diplomatic processes, without resorting to the threat or use of force".[26]

2. The harmonisation of policies is necessary to increase the region's ability to cope with digital security amid digitalisation and the emergence of technologies such as AI, quantum and IoT. Additionally, policies that facilitate information sharing, enable joint investigations, digital evidence handling and prosecution of criminals across borders strengthen the region's capability for incident response.

3. The ASEAN's norms implementation checklist aims to raise cybersecurity in the region in terms of process, practices and policy clarity for the purpose of building a secure, safe and interoperable cyberspace while strengthening the region's profile as responsible states amid cyber incidences. The region upholds sovereignty as articulated in the UN charter, such as sovereign equality of all states and the principles of non-intervention, the prohibition of the threat or use of force, respect for the territorial integrity and political independence of other states and the peaceful settlement of disputes.

[25] From paragraph 1 of the ASEAN Community Vision 2045: Resilient, Innovative, Dynamic and People-Centred ASEAN

[26] From paragraph 12 and 17 of the ASEAN Community Vision 2045: Resilient, Innovative, Dynamic and People-Centred ASEAN

4. Meanwhile, the ASEAN Community Vision 2045 also has the ambition of projecting the "ASEAN position on regional and global issues".[27] Policy statements on responsible state behaviour would communicate the region's commitment to peace, stability and rule of law.

5. ASEAN's activities would also consider the UN OEWG 2021–2025 Final Consensus Report and the recently established "Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible state behaviour in the use of ICTs" to determine the modality and subject areas where ASEAN could engage UN and international fora effectively.

Goals	Details	Potential Initiatives
2.1 Strengthening regional and national policy development for a stable and transparent cyber environment	• ASEAN's norms implementation checklist features key voluntary and non-voluntary recommendations across policy, operational, technical, legal, and diplomacy for responsible state behaviour. • Implementing the norms would require development of rules, guidelines and frameworks, which would provide clarity on what the region would do and could do during cyber incidences. • This could include developing national interpretations and statements on ICT incidences, interpretations of international law and misuse of ICT. • Additionally, regional policy harmonisation for protocols and procedures for digital evidences, information sharing, or joint investigations could improve regional incident response mechanisms.	• Periodic reviews that monitor the performance of the norms implementation checklist can be shared with ANSAC or the UN to illustrate the norm's practical application especially for national and regional experiences on the implementation of norms.
2.2	• As threats utilise interlinked infrastructure, greater	• Consider establishing incident reporting

[27] From paragraph 13 of the ASEAN Community Vision 2045: Resilient, Innovative, Dynamic and People-Centred ASEAN

Entrenching responsible state behaviour mechanisms in state-to-state responses	considerations and improvements to build trust between states is needed. Greater clarity and mechanisms for transparency such as clarity on responses, peaceful settlement of disputes and constructing mechanisms to respond to calls for assistance, would strengthen responsible state behaviour projections.	template and communication channels with other states to allow them to reach out for assistance or to notify on the misuse of ICT systems at the operational level.
2.3 Projecting ASEAN as a region upholding the norms of responsible state behaviour	• In a shifting landscape, declarations of commitment to the UN 11 voluntary, non-binding norms of responsible state behaviour in cyberspace would project ASEAN's intention to be responsible states in the digital era, especially statements to protect CERTs and critical infrastructure.	• Consider an ASEAN statement with business associations/private sector, organisations and academia to not damage critical infrastructure. • Consider an ASEAN statement on CERTs as neutral emergency services and should not be attacked.
2.4 Crisis/conflict policy for the protection of National CERT	• As per norm 13 (k), states should not conduct or knowingly support activity to harm the information systems of CERTs. • Policies need to be developed to maintain the neutrality and functionality of CERTs in times of peace or conflict.	• Issue a list of CERTs/CSIRTs on the territory.

Dimension 3: Embedding trust in the ecosystem

1. ASEAN Community Vision 2045 seeks to develop ASEAN as a hub and centre of excellence, able to leverage on advances in sciences, technology and innovation.[28] The 9th ASEAN Ministerial Conference on Cybersecurity affirmed the importance of cybersecurity as a key enabler for the region to reap the benefits of digitalisation and promote the safe interaction within the digital economy.[29] At the heart of efforts are the ASEAN peoples, where

[28] From the ASEAN Community Vision 2045, paragraph 23
[29] From Chairman's Statement of the 8th ASEAN Ministerial Conference on Cybersecurity, 18 October 2023, paragraph 2

it would require inclusive participation of stakeholders to build the ASEAN Community envisioned.[30]

2. There are challenges to addressing misuse of ICT which are cyber-enabled, especially where investigations cross jurisdictions, information-sharing affected by technological developments and communication impeded by gaps between stakeholders and operators. Such ICT misuse is inclusive of ransomware and phishing in addition to acts that destabilises trust in digital spaces such as unauthorised access to systems, malicious code and unauthorised alteration of data.

3. Proactive threat and information sharing between the private and public sector could strengthen cybersecurity, especially against a landscape of rapidly developing technologies and common threat perceptions. Efforts which could facilitate improved sharing mechanisms between the private and public sector, especially for vulnerability disclosures, could enhance trust while closing response gaps. Additionally, engagements between relevant ASEAN sectoral bodies and stakeholders could scale efforts to address cybersecurity challenges.

3. Meanwhile, as ASEAN focuses on technology development and innovation for the next economic chapter, shifting cybersecurity to the left is important. This includes socialising secure-by-design principles and AI Governance and AI Safety goals to uphold cybersecurity, ensure network security and enhance privacy and data protection. For this, ASEAN could leverage on the Cybersecurity Standards and Conformance to Support Digital Trade in ASEAN and the IoT standards developed by USASEAN and ASEAN-Japan, respectively to enhance safe and secure development of technology.

4. Specifically, IoT such as routers and IP cameras continue to be exploited by APT groups and criminal groups. For instance, the report by Greynoise in May 2025 detailed the vulnerability in Asus routers that attackers could abuse, highlighting the severity of persistent remote access.[31] Criminal groups such as Akira used IP cameras as initial entry into enterprise networks before launching ransomware attacks. These incidences amplify cybersecurity concerns brought by unprotected IoTs heavily impacting both consumers and businesses. In the face of these APTs, AMS could work together to foster cooperation to protect consumer IoT devices against cyber threats, raising the overall cyber hygiene and readiness of the region.

[30] From ASEAN Community Vision 2045, paragraph 3
[31] From Greynoise research, GreyNoise Discovers Stealthy Backdoor Campaign Affecting Thousands of ASUS Routers, 28 May 2025

Goals	Details	Potential Initiatives
3.1 Building trust in the ecosystem against ICT vulnerabilities	• Cyber is operated by various stakeholders who have varying levels of visibility on ICT vulnerabilities. Developing a reporting mechanism with private sector, researchers and penetration testers could improve preparation against threats. The guideline could ensure efficient reporting, coordination, mitigation and patching vulnerabilities with the researchers and penetration testers.	• ASEAN Guideline on Responsible ICT Vulnerability Reporting that includes an SOP of confidentiality for ICT vulnerability disclosure.
3.2 Enhancing whole-of-society approaches to security and safety-by-design	• Awareness on security and safety-by-design standards is needed in the development of technologies, especially where ASEAN has developed standards, the implementation and socialisation of the standards are imperative to raising resilience. • Additionally, regional partnerships could be strengthened with international organisations and the business associations/private sector to enhance the security of and in the use of ICTs. Such approaches could also address security and safety-by-design with new technologies such as AI and quantum.	• Capacity building in the implementation of regional IoT cybersecurity standards in development of digital products and services. • Explore how the region can work together to share best practices and develop national capacities to enhance IoT standards and protect consumer devices • Implementing targeted cybersecurity awareness programmes tailored to urban and rural populations, focusing on digital literacy, cyber hygiene, and protection from online threats.

	• In addition, clarifying mechanisms for private sector to engage with ASEAN could create opportunities for multi-stakeholder contributions to regional cybersecurity goals.	

Dimension 4: Bolstering capacity building for the future

1. The Bangkok Digital Declaration highlights "digital inclusivity without leaving any ASEAN Member States behind", thus emphasising the necessity of closing the skills gap to foster innovation, enhance the region's competitiveness and build the region's capability to adapt to technological needs.[32] The *ASEAN 2045: Our Shared Future ASEAN Economic Community Strategic Plan 2026-2030* states the necessity of enhancing talent development on frontier technologies[33], which is facilitated by capacity building.

2. However, the ASEAN Leaders' Statement on Cybersecurity Cooperation in 2018 reiterated various discussions in ASEAN sectoral bodies and also emphasised the need to synergise relevant undertakings across ASEAN Sectoral Bodies and Pillars to avoid duplication of efforts.[34] Duplication of capacity building could lead to gaps in enhancing cybersecurity capabilities or utilise resources for similar activities. Seeking ways to harness capacity building activities that meet national and regional goals would be useful to strengthen the region's cybersecurity practices.

3. ASEAN's ability to address cybersecurity challenges depends on the development of both talent and technology. A broad spectrum of expertise is essential across various cybersecurity domains, including policy, technical, operational, legal, and diplomacy. Professionals in these fields play a pivotal role in tackling emerging threats by contributing to joint initiatives, simulations, and capacity-building exercises. In particular, deep technical expertise is crucial for the detection, response, and recovery from cyber threats and incidents.

4. To foster deeper expertise, it is necessary to curate specialised cybersecurity education and training programmes that equip the workforce

[32] From Bangkok Digital Declaration, 16-17 January 2025, Secure, Innovative, Inclusive: Shaping ASEAN's Digital Future. Paragraphs 10 and 11
[33] From ASEAN 2045: Our Shared Future ASEAN Economic Community Strategic Plan 2026-2030
[34] From ASEAN Leaders' Statement on Cybersecurity Cooperation, April 27, 2018, paragraph 10

with advanced technical skills and a comprehensive understanding of the implications of emerging technologies such as AI and quantum computing for cybersecurity. Additionally, shared cybersecurity workforce frameworks can facilitate cross-recognition of skills, enhance talent mobility, and elevate workforce quality through professionalisation.

5. Emerging technologies such as AI could strengthen cybersecurity approaches but could also be compromised due to gaps in technology or process. CrowdStrike Falcon's outage in 2024 for instance was the result of high privileges by the AI-powered platform.[35] AI managing content can be jailbroken where perpetrators can bypass the AI's guardrails to perform restricted actions. These challenges reveal gaps to protect cyberspace which requires assessments and cybersecurity processes that adheres to existing principles.

6. ASEAN would have to draw on capacity building efforts to meet regional goals efficiently. The region also has AJCCBC and the ASCCE for capacity building and training. The institutes have provided capacity building programmes on talent, cybersecurity, IoT standards and trusted digital services.

Goals	Details	Potential Initiatives
4.1 **To ensure cyber capacity building is targeted, effective with tangible outcomes**	• Cyber capacity building should be targeted, effective with tangible outcomes • Additionally, cyber capacity building programmes should aim to be consistent and sustainable, with the possibility of strengthening local and regional cybersecurity associations.	• Existing centres could conduct a needs analysis to streamline capacity building efforts by identifying potential gaps in regional capacity building efforts that informs a clearing house mechanism. • Existing centres could also continue capacity building programmes on international law and legal awareness. Such courses could prepare states to implement cyber-related legal frameworks into their own legislations. • Training on handling digital evidence at technical and legal levels such as training

[35] Sean Michael Kerner, 29 October 2024, *CrowdStrike outage explained: What caused it and what's next*

		on writing mutual legal assistance requests. • Conduct capacity building programs on human rights, privacy and safety. • Develop a framework for the professionalisation and cross-recognition of the cybersecurity workforce to meet growing and maturing cybersecurity needs.
4.2 Raise awareness on risk assessment of new technologies	• Emerging technologies such as AI and quantum computing carry monumental risks. AI could introduce novel threats while quantum computing would impact public key cryptography. • Meanwhile cybersecurity practices could change with the complexity of technology. • This raises the imperative to engage various stakeholders on new technologies. • Additionally, exchanges with the private sector could cover emerging technologies such as AI and quantum, especially to enhance awareness on standards and the magnitude of risk with the deployment of the emerging technologies.	• Develop a playbook on common strategies for quantum-safe migration. • Conduct knowledge sharing session on emerging technologies such as AI and quantum computing with private sector.

Dimension 5: Synergising cooperation

1. ASEAN is a region in the midst of flux. Various forms of competition and development have reinforced the ASEAN Community Vision 2045's emphasis for "ASEAN Centrality in external relations" which should be sustained by ASEAN-led mechanisms.[36] The ASEAN Leaders' Statement on Cybersecurity Cooperation in 2018 recognises the value of enhanced dialogue and cooperation on cybersecurity issues with Dialogue Partners and other External Parties[37], especially as conversations highlight best practices and policy exchanges.

2. Therefore, dialogues that could focus on policies for regional cooperation could be helpful to improve mechanisms for collaboration or strengthen efforts for the protection of critical infrastructure. As technology diplomacy impact cybersecurity standards, clarity on engagements, mechanisms and new forms of cooperation could be helpful to innovate regional cooperation.

3. The ASEAN Community Vision 2045 also has goals for institutional strengthening, which are inclusive of enhancing institutional capacity and effectiveness while being future-ready.[38] ASEAN's institutional growth to address cross-sectoral challenges in the cybersphere is reflected in the Bangkok Digital Declaration articulated which includes statements such as strengthening collaboration through the ASEAN Working Group on Anti-Online Scam, coordinating regional approaches in the ASEAN Regional CERT, strengthening trust through the ASEAN Working Group on Artificial Intelligence Governance, promoting free flow of data within the ASEAN Working Group on Digital Data Governance and strengthening information sharing network in the Working Group on Submarine Cables.[39]

4. ASEAN's sectoral approach to cyber can be challenged by misuse of ICT vectors, which can be cross-sectoral. An example is scams which could utilise platforms for phishing or unauthorised access to systems, take advantage of cross-border financial transactions, be enhanced by AI and may even result in trafficking in persons for the completion of its operations. Thus, enhancing intra-ASEAN cooperation for effective solutions would be fundamental to ensure such cybersecurity challenges are addressed.

[36] From ASEAN Community Vision 2045, paragraph 7 and 12
[37] From ASEAN Leaders' Statement on Cybersecurity Cooperation, April 27, 2018, paragraph 15
[38] From ASEAN Community Vision 2045, paragraph 41
[39] From Bangkok Digital Declaration, 16-17 January 2025

Goals	Details	Potential Initiatives
5.1 Increasing communication transparency on international cooperation	• The ASEAN leans on the international community for capacity building, cybersecurity standards, and cooperation on responsible state behaviour. • Innovative cooperation solutions are needed to address challenges from a shifting cybersecurity landscape. Partnerships and cooperation should be accessible to ASEAN and all ASEAN Member States where feasible.	• Exchanges with ASEAN Dialogue Partners and international organisations to learn about their policies on regional cooperation. Such policies could include case studies of ICT misuse and governance of cyber policies which could be addressed during ASEAN Dialogue Partner Cyber Policy conversations and international organisation engagements.
5.2 Enhancing intra-ASEAN cooperation for cybersecurity	• While responsibilities correspond to jurisdiction and borders, threats from cyberspace may not adhere to similar borders. • There may be a need to improve ASEAN and AMS internal coordination to address the cross-sectoral gaps which are exploited.	• Feasibility study on enhancing the ASEAN Cybersecurity Coordination Committee (Cyber-CC) as the main body for ASEAN's cybersecurity coordination/ mechanisms.

5. Annex

Dimension 1: Strengthening cyber readiness

Goals	Details	Potential Initiatives	Alignment with current programmes
1.1 Advancing critical infrastructure protection and improving crisis response through policy, diplomacy, and operational preparedness	• Effective policies can enhance efficiency in regional response to cyber incidents. However, differences in definitions, communication protocols, and procedures can hinder readiness. Clear frameworks and protocols are essential, for personnel to know how to manage requests for assistance and make decisions in real time. This could be inclusive of pre-establishing communication channels, including diplomatic ties between states and partnerships with technology companies prior to a crisis and incident. • While ASEAN has advanced in protecting critical infrastructure, sustained progress requires shared responsibility, cooperation and clear codes of conduct.	• Develop an ASEAN Best Practice for Governance Framework for Incident Response • Conduct an ASEAN Feasibility Study on Regional Crisis Response. • ASEAN study on what constitutes harmful ICT practices. • Develop a strategic guideline for identification of critical sectors. • Conduct simulation/tabletop exercises, cyber exercises and joint drills. • Build a regional cybersecurity information repository to ease access to information on ICT threats and incidents	• ASEAN Workshops on Implementing Best Practices for Submarine Cable Protection and Repairs (Singapore) *(Proposal)*

	• There may be a need to practice information sharing and joint incident handling to enhance regional resilience particularly during cross-border cyber threats.		
1.2 Raising cybersecurity baselines practices to protect critical infrastructure.	• Cybersecurity baseline could become the foundational guideline for organisations to maintain the minimum protection standard for security controls. • A baseline can set basic expectations for process, information management, network security standards or sector-specific cooperation, especially for the protection of critical infrastructure which can vary in practice across sectors. • Pursuing recommended baselines could benchmark good practices to elevate cybersecurity levels. • The development of baselines can be based on ASEAN's existing research and could cover common processes among AMS to protect CII such as risk assessment.	• Feasibility study for ASEAN's cybersecurity baseline. • Continued development of the cybersecurity threat landscape report.	• ASEAN Guidelines on Cloud Adoption for Public Sector (Brunei Darussalam) • Inventory of Critical Information Infrastructure ("CII") Identification Frameworks in ASEAN (The Philippines) • Ensuring Trust: Symposium on Software Security Certification (ANSAC) (Indonesia) *(Proposal)* • Feasibility Study on the Implementation of Open Radio Access Network (Open RAN) in ASEAN (Indonesia) • ASEAN Digital Public Infrastructure for Cross-Border Digital Trade (Phase 1 – Framework Recommendation) (Brunei Darussalam)

			• ASEAN Framework on Cross Border Cloud Computing (Malaysia)
1.3 Positioning ASEAN Regional CERT as a regional hub for crisis and information exchange	• ASEAN Regional CERT have consolidated and developed mechanisms which enhances its role as a coordinator during crisis and for information exchange. • To deepen its role in information sharing, ASEAN Regional CERT would have to develop effective mechanisms that links with various networks for the latest threats and technology vulnerabilities. This could include engagements with private sector, Dialogue Partners, international organisations or other regional CERTs. • Furthermore, the regional hub could enhance incident management through capacity building activities with various stakeholders.	• Establish touchpoints for threat information sharing with key private sector partners. • Capacity building programmes by ASEAN with private sector and other governments on incident response and emerging technologies. • To enhance ASEAN Regional CERT's collaboration opportunities through inter-regional CERT/CSIRT exchanges.	

Dimension 2: Advancing regional policy coordination

Goals	Details	Potential Initiatives	Alignment with current programmes
2.1 Strengthening regional and national policy development for a stable and transparent cyber environment	• ASEAN's norms implementation checklist features key voluntary and non-voluntary recommendations across policy, operational, technical, legal and diplomacy for responsible state behaviour. • Implementing the norms would require development of rules, guidelines and frameworks, which would provide clarity on what the region would do and could do during cyber incidences. • This could include developing national interpretations and statements on ICT incidences, interpretations of international law and misuse of ICT. • Additionally, regional policy harmonisation for protocols and procedures for digital evidences, information sharing, or joint investigations could improve regional incident response mechanisms.	• Periodic reviews that monitor the performance of the norms implementation checklist can be shared with ANSAC or the UN to illustrate the norm's practical application especially for national and regional experiences on the implementation of norms.	• ASEAN Digital Trade Infrastructure (Phase 2 – Implementation Strategy & Roadmap for Use Case) (Brunei Darussalam), and (ii) Study on the Digital Public Goods (DPG) and Digital Public Infrastructure (DPI) in ASEAN (Lao PDR) – (merged project proposals) • ASEAN Workshops on Implementing Best Practices for Submarine Cable Protection and Repairs (Singapore) *(Proposal)* • ASEAN Framework on Cross Border Cloud Computing (Malaysia)

2.2 Entrenching responsible state behaviour mechanisms in state-to-state responses	• As threats utilise interlinked infrastructure, greater considerations and improvements to build trust between states is needed. Greater clarity and mechanisms for transparency such as clarity on responses, peaceful settlement of disputes and constructing mechanisms to respond to calls for assistance, would strengthen responsible state behaviour projections.	• Consider establishing incident reporting template and communication channels with other states to allow them to reach out for assistance or to notify on the misuse of ICT systems at the operational level.	• ASEAN Workshops on Implementing Best Practices for Submarine Cable Protection and Repairs (Singapore) *(Proposal)*
2.3 Projecting ASEAN as a region upholding the norms of responsible state behaviour	• In a shifting landscape, declarations of commitment to the UN 11 voluntary, non-binding norms of responsible state behaviour in cyberspace would project ASEAN's intention to be responsible states in the digital era, especially statements to protect CERTs and critical infrastructure.	• Consider an ASEAN statement with private sector, organisations and academia to not damage critical infrastructure. • Consider an ASEAN statement on CERTs as neutral emergency services and should not be attacked.	
2.4 Crisis/conflict policy for the	• As per norm 13 (k), states should not conduct or knowingly support activity to	• Issue a list of CERTs/CSIRTs on the territory.	

protection of National CERT	harm the information systems of CERTs. • Policies need to be developed to maintain the neutrality and functionality of CERTs in times of peace or conflict.		

Dimension 3: Embedding trust in the ecosystem

Goals	Details	Potential Initiatives	Alignment with current programmes
3.1 Building trust in the ecosystem against ICT vulnerabilities	• Cyber is operated by various stakeholders who have varying levels of visibility on ICT vulnerabilities. Developing a reporting mechanism with the private sector, researchers and penetration testers could improve preparation against threats. The guideline could ensure efficient reporting, coordination, mitigation and patching vulnerabilities with the researchers and penetration testers.	• ASEAN Guideline on Responsible ICT Vulnerability Reporting that includes an SOP of confidentiality for ICT vulnerability disclosure.	• Code Craft: Unleash Your Digital Potential - ASEAN Coding Bootcamp for Workforce in the future (The Philippines)
3.2 Enhancing whole-of-society	• Awareness on security and safety-by-design standards is needed in the development of	• Capacity building in the implementation of regional IoT cybersecurity standards in	• Feasibility Studies on Digital Certificate Adoption for

approaches to security and safety-by-design	technologies, especially where ASEAN has developed standards, the implementation and socialisation of the standards are imperative to raising resilience. • Additionally, regional partnerships could be strengthened with international organisations and the private sector to enhance the security of and in the use of ICTs. Such approaches could also address security and safety-by-design with new technologies such as AI and quantum. • In addition, clarifying mechanisms for private sector to engage with ASEAN could create opportunities for multi-stakeholder contributions to regional cybersecurity goals.	development of digital products and services. • Explore how the region can work together to share best practices and develop national capacities to enhance IoT standards and protect consumer devices • Implementing targeted cybersecurity awareness programmes tailored to urban and rural populations, focusing on digital literacy, cyber hygiene and protection from online threats.	trusted Digital Services in ASEAN (Lao PDR) • Advancing ASEAN Connectivity: Harnessing Satellite Technology and Innovative Regulations to Bridge the Digital Divide (Lao PDR) • The Development of Guidelines for Digital Platform Regulation in ASEAN (Lao PDR & Thailand) • The study on Telecommunications Infrastructure Safeguard and Future Risks for Scam Prevention in ASEAN (Thailand) *(Proposal)* • The Declaration on the Establishment of an ASEAN AI Safety Network (ASEAN AI SAFE) (Malaysia) • Harnessing AI and New Technologies for Smart Cities and Digital Government (Viet Nam) • ASEAN GeoAI Fusion: Bootcamp and Hackathon for Geospatial Innovation (Malaysia) *(Proposal)*

			• Feasibility Study on the Implementation of Open Radio Access Network (Open RAN) in ASEAN (Indonesia) • Capacity and capability development of ASEAN's 5G skilled workforce (Malaysia) • ASEAN AI Skilling Framework (Brunei Darussalam) (proposal) • Report on Privacy Enhancing Technologies (PETs) in ASEAN (Singapore)

Dimension 4: Bolstering capacity building for the future

Goals	Details	Potential Initiatives	Alignment with current programmes
4.1 **To ensure cyber capacity building is targeted, effective with tangible outcomes**	• Cyber capacity building should be targeted, effective with tangible outcomes • Additionally, cyber capacity building programmes should aim to be consistent and sustainable, with the possibility of strengthening local and regional cybersecurity associations.	• Existing centres could conduct a needs analysis to streamline capacity building efforts by identifying potential gaps in regional capacity building efforts that informs a clearing house mechanism. • Existing centres could also continue capacity building programmes on international	

		law and legal awareness. Such courses could prepare states to implement cyber-related legal frameworks into their own legislations. • Training on handling digital evidence at technical and legal levels such as training on writing mutual legal assistance requests. • Conduct capacity building programs on human rights, privacy and safety. • Develop a framework for the professionalisation and cross-recognition of the cybersecurity workforce to meet growing and maturing cybersecurity needs.	
4.2 Raise awareness on risk assessment of new technologies	• Emerging technologies such as AI and quantum computing carry monumental risks. AI could introduce novel threats while quantum computing would impact public key cryptography. • Meanwhile cybersecurity practices could change with the complexity of technology.	• Develop a playbook on common strategies for quantum-safe migration. • Conduct knowledge sharing session on emerging technologies such as AI and quantum computing with private sector.	• Advancing ASEAN Connectivity: Harnessing Satellite Technology and Innovative Regulations to Bridge the Digital Divide (Lao PDR) • ASEAN Digital Public Infrastructure for Cross-Border Digital Trade (Phase 1 – Framework

	• This raises the imperative to engage various stakeholders on new technologies. • Additionally, exchanges with the private sector could cover emerging technologies such as AI and quantum, especially to enhance awareness on standards and the magnitude of risk with the deployment of the emerging technologies.		Recommendation) (Brunei Darussalam) • ASEAN Framework on Cross Border Cloud Computing (Malaysia) • The Declaration on the Establishment of an ASEAN AI Safety Network (ASEAN AI SAFE) (Malaysia) • Harnessing AI and New Technologies for Smart Cities and Digital Government (Viet Nam) • Report on Privacy Enhancing Technologies (PETs) in ASEAN (Singapore) • ASEAN 5G Conference 2026 (Viet Nam) (Proposal)

Dimension 5: Synergising cooperation

Goals	Details	Potential Initiatives	Alignment with current programmes
5.1 Increasing communication transparency on international cooperation	• The ASEAN leans on the international community for capacity building, cybersecurity standards and cooperation on responsible state behaviour.	• Exchanges with ASEAN Dialogue Partners and international organisations to learn about their policies on regional cooperation. Such policies could include case studies of ICT	

	• Innovative cooperation solutions are needed to address challenges from a shifting cybersecurity landscape. Partnerships and cooperation should be accessible to ASEAN and all ASEAN Member States where feasible.	misuse and governance of cyber policies which could be addressed during ASEAN Dialogue Partner Cyber Policy conversations and international organisation engagements.	
5.2 Enhancing intra-ASEAN cooperation for cybersecurity	• While responsibilities correspond to jurisdiction and borders, threats from cyberspace may not adhere to similar borders. • There may be a need to improve ASEAN and AMS internal coordination to address the cross-sectoral gaps which are exploited.	• Feasibility study on enhancing the ASEAN Cybersecurity Coordination Committee (Cyber-CC) as the main body for ASEAN's cybersecurity coordination/ mechanisms.	• ASEAN Digital Masterplan 2026-2030 (Vietnam) • ASEAN Digital Outlook (Malaysia) *(proposal)* • Roadmap on ASEAN Cooperation on Online Safety (Brunei Darussalam) *(proposal)* • The Declaration on the Establishment of an ASEAN AI Safety Network (ASEAN AI SAFE) (Malaysia) • The study on Telecommunications Infrastructure Safeguard and Future Risks for Scam Prevention in ASEAN (Thailand) *(Proposal)*

6. References

ASEAN. (n.d.). *Major Sectoral Bodies/Committees*. Asean.org; ASEAN Secretariat. https://asean.org/our-communities/economic-community/asean-digital-sector/major-sectoral-bodies-committees/

ASEAN. (2021). *ASEAN Leaders' Statement on Advancing Digital Transformation in ASEAN*. 38th ASEAN Summit. https://asean.org/wp-content/uploads/2021/10/7.-ASEAN-Leaders-Statement-on-Digital-Transformation.pdf

ASEAN. (2023a). *Leaders' Statement on the Development of the ASEAN Digital Economy Framework Agreement (DEFA)*. ASEAN Indonesia 2023. https://asean.org/wp-content/uploads/2023/09/Leaders-Statement-DIGITAL-ECONOMY-FRAMEWORK-AGREEMENT.pdf

ASEAN. (2023b, October 18). *Chairman's Statement of the 8th ASEAN Ministerial Conference on Cybersecurity*. Singapore. https://asean.org/wp-content/uploads/2023/11/8th-AMCC-Chairmans-Statement.pdf

ASEAN. (2025a). *ASEAN 2045 Our Shared Future*. ASEAN Secretariat. https://asean.org/wp-content/uploads/2025/05/ASEAN-2045-Our-Shared-Future.pdf

ASEAN. (2025b, January). *Bangkok Digital Declaration. Secure, Innovative, Inclusive: Shaping ASEAN's Digital Future*. 5th ASEAN Digital Ministers' Meeting. https://asean.org/wp-content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf

ASEAN. (2025c, January). *The 5th ASEAN Digital Ministers' Meeting and Related Meetings*. 5th ASEAN Digital Ministers' Meeting and Related Meetings. https://asean.org/wp-content/uploads/2025/01/15-ENDORSED-JOINT-MEDIA-STATEMENT-5th-ADGSOM-v2-Cleaned.pdf

ASEAN. (2025d, May 26). *ASEAN Community Vision 2045*. 46th ASEAN Summit. https://asean.org/wp-content/uploads/2025/05/05.-ASEAN-Community-Vision-2045_adopted.pdf

ASEAN . (2018, April). *ASEAN Leaders' Statement on Cybersecurity Cooperation*. 32nd ASEAN Summit. https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf

ASEAN Secretariat. (2023). *ASEAN Statistical Yearbook 2023*. ASEAN Secretariat. https://www.aseanstats.org/wp-content/uploads/2023/12/ASYB-2023-v1.pdf

Bangkok Post. (2025, March 5). *Thailand sees more than 28,000 web threats per day*. Https://Www.bangkokpost.com; Bangkok Post. https://www.bangkokpost.com/business/general/2974171/thailand-sees-more-than-28-000-web-threats-per-day

Bkav Technology Group. (2024). Summary of Cyber Security Assessment 2023. Bkav. https://www.bkav.com/top-new/-/view-content/1891161/summary-of-cybersecurity-in-2023-and-forecast-for-2024

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

Cloud Security Research. (2025). 2025 Thales Cloud Security Study. Thales. http://cpl.thalesgroup.com/cloud-security-research#form-download

Bkav Technology Group . (2024). Cyber Security Assessment for Individual Users. In *Bkav Corporation*. Bkav. https://www.bkav.com/en/top-news/-/view-content/1891161/summary-of-cybersecurity-in-2023-and-forecast-for-2024

Cloudflare. (2024). *Navigating the New Security Landscape: Asia Pacific Cybersecurity Readiness Survey*. Cloudflare. https://assets.ctfassets.net/slt3lc6tev37/n4x2bmAeqPOFCaRzlms9v/6a4fd0772b4ca39e67989c311e3c43ea/Navigating_the_New_Security_Landscape_Asia_Pacific_Cybersecurity_Readiness_Survey.pdf

Google, Temasek, & Bain & Company. (2024). *e-Conomy SEA 2021 report - Google*. Economysea.withgoogle.com. https://economysea.withgoogle.com/report/

Greynoise. (2025). *Greynoise research, of ASUS Routers.* Greynoise. https://www.greynoise.io/blog/stealthy-backdoor-campaign-affecting-asus-routers

Hirdaramani, Y. (2024). *Asia an emerging leader in digital government, says UN report*. Govinsider.asia. https://govinsider.asia/intl-en/article/asia-an-emerging-leader-in-digital-government-says-un-report

IBM. (2025). Cost of a Data Breach Report 2025: The AI Oversight. IBM. https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

Kaspersky. (2025, April 24). *Almost 40% of industrial enterprises identify cybersecurity as a key challenge in digitalizing OT environments*. Kaspersky. https://www.kaspersky.com/about/press-releases/almost-40-of-industrial-enterprises-identify-cybersecurity-as-a-key-challenge-in-digitalizing-ot-

environments?srsltid=AfmBOooE-uHzmnXgde7dGU-a9SYWcqxfQvaIW7iDYjQt2VyZW3Gzgctx

Kerner, S. M. (2024, October 29). *CrowdStrike outage explained: What caused it and what's next*. TechTarget; Informa TechTarget. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next

Mahusin, M., & Prilliadi, H. (2024). Strengthening ASEAN's Cybersecurity: Collaborative Strategies for Enhanced Resilience and Regional Cooperation. [Policy brief]. ERIA. https://www.eria.org/uploads/Strengthening-ASEAN-Cybersecurity.pdf

Research and Markets. (2025, July). Southeast Asia Data Center Landscape Report 2025-2030 | $30+ Bn Market Booms as Malaysia, Indonesia, Thailand, and Vietnam Emerge as Prime Investment Destination. Yahoo Finance. https://finance.yahoo.com/news/southeast-asia-data-center-landscape-131600486.html

Lee, B., Lai, A., & Vethasalam, R. (2024, November 4). *Over 1,500 cyber attacks on Malaysia's ministries in 2023*. The Star. https://www.thestar.com.my/news/nation/2024/11/04/over-1500-cyber-attacks-on-malaysia039s-ministries-in-2023

RFA Lao. (2024, May 24). *Lao official: Gov't can't afford to address rise in human trafficking*. Radio Free Asia; Radio Free Asia. https://www.rfa.org/english/news/laos/trafficking-government-resources-05242024151331.html

Sallehuddin, Q., & Camoens, A. (2025, March 25). [UPDATED] Hackers demand USD10mil ransom in MAHB cyberattack, says PM [WATCH]. NST Online; New Straits Times. https://www.nst.com.my/news/nation/2025/03/1192902/updated-hackers-demand-us10mil-ransom-mahb-cyberattack-says-pm-watch

Singapore Police Force. (2024). Mid-Year Scams and Cybercrime Brief 2024. Singapore Police Force. https://www.police.gov.sg/Media-Hub/Statistics?type=Type&year=Year&month=Month

Sulaiman, S., & Widianto, S. (2024, June 28). Indonesia president orders audit of data centres after cyberattack. Reuters. https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/

Sallehuddin, Q., & Camoens, A. (2025, March 25). *Hackers demand USD10mil ransom in MAHB cyberattack, says PM*. NST Online; New Straits Times. https://www.nst.com.my/news/nation/2025/03/1192902/updated-hackers-demand-us10mil-ransom-mahb-cyberattack-says-pm-watch

Sulaiman, S., & Widianto, S. (2024, June 28). Indonesia president orders audit of data centres after cyberattack. *Reuters*. https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/

Sun, D. (2024, August 22). *Scam victims in S'pore lost $385.6m in first half of 2024 as number of cases hits high of 26,587*. The Straits Times. https://www.straitstimes.com/singapore/scam-victims-in-s-pore-lost-3856m-in-first-half-of-2024-as-number-of-cases-hit-high-of-26587?ref=inline-article

Tenable. (2025). Tenable Cloud Security Risk Report 2025. Tenable. https://www.tenable.com/cyber-exposure/tenable-cloud-security-risk-report-2025

The Star Online. (2024, November 4). Over 1,500 cyberattacks against ministries' infrastructure systems. The Star. https://www.thestar.com.my/news/nation/2024/11/05/over-1500-cyberattacks-against-ministries-infrastructure-systems

United Nations. (2024). E-Government Survey 2024. In *UN E-Government Knowledgebase*. United Nations, Department of Economics and Social Affairs. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

United Nations General Assembly's open-ended working group on security of and in the use of information and communications technologies 2021-2025. (July, 2025). *Draft Final Report, Eleventh Substantive Session*. United Nations General Assembly Eleventh Substantive session, New York.

Vigilant Asia. (2025, February 3). *AI-Powered Cyber Attacks: A Growing Concern for Organisations in Asia Pacific*. Vigilant Asia. https://vigilantasia.com.my/ai-cyber-attacks-organisations-asia-pacific/

World Economic Forum. (n.d.). *Digital ASEAN*. World Economic Forum. https://www.weforum.org/projects/digital-asean/