ASEAN CYBERSECURITY COOPERATION STRATEGY

(2021 – 2025)

Contents

CYBERSECURITY IN ASEAN

1. Cybersecurity is a key enabler of the economic progress and betterment of living standards in the digital economy. This has become even more evident during the Covid-19 pandemic where we have been forced to adopt rapid digitalisation, and the migration of government, business, and social activities online. As a result, malicious cyber actors can exploit a larger attack surface. Moreover, cyber-attacks are evolving to increasingly have real-world, physical impact. Therefore, having a robust regional cybersecurity strategy is essential for ASEAN Member States (AMS) to ensure the continued security and stability of our cyberspace.

2. Regional organisations like ASEAN offer a platform for member states to share and offer regional perspectives, exchange information on emerging and existing threats, implement Confidence Building Measures (CBMs), and build capacity. Our regional initiatives are important to facilitate AMS in responding to future crises in a timely manner, and also build readiness for a safer cyberspace as a region. This will ensure that our cyberspace can continue to be a trusted enabler that will allow the delivery of essential services to the public, and a key enabler of the digital economy to aid in the post-pandemic recovery efforts.

(I) RECAP OF FIRST ASEAN STRATEGY PAPER (2017-2020)

3. The ASEAN Cybersecurity Cooperation Strategy (2017-2020) was written to provide a roadmap for regional cooperation to achieve the objective of a safe and secure ASEAN cyberspace. This would help to strengthen Information and Communications Technology (ICT) security in ASEAN, in line with the strategic thrust on Information Security and Assurance in the ASEAN ICT Masterplan 2020 (AIM2020).

4. The 1st Strategy approved by Telecommunications and Information Technology Ministers Meeting (TELMIN) had focused on **strengthening CERT-CERT cooperation and capacity building,** and **coordinating regional cybersecurity cooperation initiatives** as a means of raising regional cyber capabilities against ever evolving and increasingly sophisticated cyber threats, and avoiding the duplication of resources.

5. The strategy recommended the adoption of the:

a) **ASEAN CERT Maturity Framework**, to enhance ASEAN's approach to levelling up its incident response capabilities in a coordinated and targeted manner. AMS were provided with a self-assessment toolkit to measure the maturity level of their CERT based on a list of questions and checklist.

b) **Establishment of future ASEAN Regional Computer Emergency Response Team (CERT)** to synergise the individual strengths and areas of expertise of the ASEAN national CERTs to bolster the overall effectiveness of regional incident response capabilities.

c) **Telecommunications and Information Technology Senior Officials Meeting and Ministers Meeting (TELSOM/TELMIN), now renamed to ASEAN Digital Senior Officials Meeting and Ministers Meeting (ADGSOM/ADGMIN), to take a leading role** in coordinating these activities listed above.

d) **Targeted Capacity Building Initiatives** to ensure that ASEAN's resources were judiciously channelled into initiatives that are targeted and necessary, to ensure efficiency and effectiveness.

6. This was further strengthened by the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation which highlighted the need to build closer cooperation and coordination among AMS on cybersecurity policy development and capacity building initiatives.

(II) KEY ASEAN ACHIEVEMENTS IN SUPPORT OF CYBER COOPERATION

7. Since the first ASEAN Cybersecurity Cooperation Strategy (2017 – 2020) as recapped earlier, ASEAN has made progress in regional cyber cooperation over the years.

2.1 Policy Coordination

8. For better **coordination** across ASEAN sectoral bodies overseeing cybersecurity, AMS Leaders agreed on the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation to set the direction for cyber discussions.

9. Additionally, the ASEAN Digital Masterplan (ADM) 2025 was developed in 2021 to suggest actions AMS governments and regulators can take to best achieve the vision of ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies and ecosystem.

10. To recognise the importance of the digital sector, ASEAN renamed the TELSOM/TELMIN to ADGSOM/ADGMIN in 2019. This illustrated the role of ICT as a digital transformation variable for other sectors, as well as to transform the region into a digitally enabled economy and society.

11. As cybersecurity is a cross-cutting issue, the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) comprising representatives from relevant ASEAN sectoral bodies overseeing cybersecurity issues was set up in 2020 to strengthen cross-sectoral coordination on cybersecurity, while preserving the exclusive work domains of the sectoral bodies. It stemmed from an initial proposal for better cybersecurity policy coordination in ASEAN, as set out in the 2018 ASEAN Leaders' Statement, issued during Singapore's ASEAN Chairmanship. The inaugural meeting of the ASEAN Cyber-CC was held on 5 November 2020, chaired by Laos (then-ADGSOM Chair). The Terms of Reference for the committee was confirmed, and proposals for the workplan was discussed.

12. Further to the efforts to secure ASEAN's cyberspace, the informal ASEAN Ministerial Conference on Cybersecurity (AMCC) also gathered ASEAN Ministers of Telecommunications and/or Cybersecurity in 2018 to subscribe in-principle to all 11 voluntary, non-binding norms of responsible State behaviour in cyberspace contained in the 2015 UN Group of Governmental Experts report, making ASEAN the first region to do so. Malaysia and Singapore co-chair the working committee for the Development of a Long-term Implementation Roadmap for Norms of Responsible State Behaviour in Cyberspace to chart the implementation roadmap at a comfortable pace to all AMS. In 2020, participants also agreed on the urgent need to protect national and cross-border Critical Information Infrastructure (CII).

2.2 Incident Response

13. To strengthen ASEAN's cybersecurity **incident response** so as to secure the growing ASEAN digital economy in the face of increasingly sophisticated transboundary cyberattacks, ASEAN agreed on the establishment of an ASEAN CERT to facilitate the timely exchange of threat and attack-related information among AMS National CERTs. ASEAN CERT would also foster CERT-related capacity building and coordination, but in a manner that does not take over or impinge on the operational role, mandate and functions of each AMS' National CERT. A Feasibility Study for the ASEAN CERT was conducted by MITRE, a research and development non-profit organisation, in 2019, and the report would serve as a guide in the establishment of the ASEAN CERT. As gathered from the feasibility study, AMS agreed at the 10th ANSAC Meeting that the ASEAN CERT should have the following functions:

- Facilitate coordination and information sharing between AMS National-level CERTs
- Develop and maintain an ASEAN POC network of cybersecurity experts and organisations
- Host ASEAN cybersecurity conferences, trainings and drills for AMS national CERTs
- Facilitate and conduct regional cybersecurity exercises
- Partner with other international and regional organisations in support of ASEAN cybersecurity interests and objectives
- Develop partnerships with industry and academia
- Support AMS National CERT capacity building and best practices
- Conduct and support cybersecurity awareness campaigns

14. To support the upcoming ASEAN CERT's work, the ASEAN Digital Ministers welcomed Singapore's proposal at the 1st ASEAN Digital Ministers' Meeting in January 2021 for the establishment of an ASEAN CERT Information Exchange Mechanism. This will facilitate incident response and exchanges amongst all AMS CERTs, and coordinate CERT capacity-building programmes in the region.

2.3 Capacity Building

15. For more targeted **capacity building** initiatives, ASEAN completed the ASEAN CERT Maturity Framework study in 2020 that assessed AMS' cybersecurity posture, and training and development actions needed to meet AMS's cyber capacity needs. This allowed a systematic identification of gap areas where appropriate training or capacity building efforts could be directed towards.

16. AMS have organised various capacity building activities under the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), and ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) to facilitate communication, information sharing, as well as the exchange of know-how and best practices. Despite the travel restrictions imposed by the COVID-19 pandemic, these activities continued to be held online since 2020.

17. Further to these efforts, under the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF ISM on ICTs Security), 7 Confidence Building Measures (CBMs) were adopted over the 3 ISMs and 7 Open Ended Study Group (OESG) meetings from intersessional years 2018 to 2021:

- Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations [Co-lead country: Philippines and Japan]

- Awareness-Raising and Information Sharing on Emergency Responses to Security Incidents in the Use of ICTs [Co-lead countries: Cambodia, Singapore, and China]

- Workshop on Principles of Building Security in The Use of ICTs in the National Context [Co-lead countries: Singapore and Canada]

- Establishment of ARF Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs) [Co-lead Countries: Malaysia and Australia]

- Protection on ICT-Enabled Critical Infrastructures [Co-lead Countries: Singapore and EU]

- Workshop on Countering the Use of ICTs for Criminal Purposes [Co-lead Countries: Viet Nam, China, Russia]

- ARF Terminology in the field of Security of and in the use of Information and Communication Technologies [Co-lead countries: Cambodia and Russia]

(III) CHANGES IN CYBERSECURITY LANDSCAPE

3.1 Accelerated Digitalisation

18. During these few years, while we have strengthened our cybersecurity cooperation in several areas as elaborated in the previous section, ASEAN as a region has also experienced **accelerated digitalisation which has helped to grow the region's digital economy, but have also led to new and novel challenges.**

19. Prior to the outbreak of COVID-19, AMS were undergoing rapid digital transformation and the digital economy was taking shape in ASEAN. For example, Small and Medium Enterprises (SMEs) in the region leveraged on technology to disrupt industries such as the brick-and-mortar retailers which led to a proliferation of e-commerce platforms. ASEAN is also one of the fastest growing internet markets in the world with 125,000 new users coming online every day. As a result, the ASEAN digital economy is projected to grow significantly with an estimated US$1 trillion to be added to the regional GDP over the next decade[1]. Moreover, ASEAN's potential has not gone unnoticed and many multinational companies have been trying to penetrate the ASEAN market as evidenced by major technology companies' increased footprint in the region.

20. ASEAN also has plans to leverage technology for the development of their cities to improve the lives of their citizens. At the 32nd ASEAN Summit in 2018, the ASEAN Leaders established the ASEAN Smart Cities Network (ASCN). The ASCN is a collaborative platform where cities from the 10 AMS work towards the common goal of smart and sustainable urban development. It currently comprises 26 pilot Smart City Action Plans.

21. Moreover, the COVID-19 pandemic further accelerated this trajectory as governments, businesses, and individuals have turned to digital solutions to enable the continuation of work, economic activities, and social interactions. A 2020 report[2] showed that the pandemic has sped up the

[1] Data taken from World Economic Forum's project on "Digital ASEAN".
[2] e-Conomy SEA 2020 Report jointly compiled by Google, Temasek and Bain and Company.

region's uptake of digital platforms and technologies, with 40 million people in several AMS[3] coming online for the first time in 2020. This brings the total number of internet users in the region to 400 million, up from 250 million in 2015. The size of the region's economy in 2020 also exceeded US$ 100 billion for the first time.

22. **In an era where everything is "digital by default", platforms which we never thought of as critical infrastructure have become vital to how we live, work, and play in the midst of the pandemic and beyond**. Consequently, this "new normal" has not only changed habits and engendered a shift towards a more digitalised way of life, but this has also increased the attack surface area for cyberattacks. However, this does not mean that we shy away from digitalisation, as movement to the digital space powers our Digital Economies and Smart Nations ambitions. Cybersecurity needs to be viewed as an enabler of digitalisation, such that while we accrue the benefits of digitalisation and the enhanced connectivity, at the same time we address the cybersecurity risks faced.

3.2 Sophistication of Cyberattacks and its Implications

23. Accelerated digitalisation has been possible due to technological advancements. However, new technology has grown increasingly complex, and new digital innovations are outpacing our abilities to keep it secure. Our systems and networks are more interconnected today, with supply chains of computer products and services being complex and varied. In this context, a sophisticated exploit such as the recent high-profile cyberattacks have indiscriminately impacted many unsuspecting victims beyond the prime targets and potentially create consequences that disrupt regional and international stability. That is why the cybersecurity community is particularly concerned about such exploits and its downstream implications, in particular, on the CIIs that we rely on for essential services, as well as government and private sector networks including 5G and Internet of Thing (IoT) devices, all of which are key for the economic viability of ASEAN's digital economy. These trends are proof of what we already know – that cyber threats will continue to evolve and grow in sophistication.

3.3 Complex Interrelation of Cyber and Digital Issues

24. Lastly, traditional cyber and digital risks issues are no longer as straightforward as they used to be as these domains have evolved to be more cross-cutting and complex. International and domestic conversations on the correlation between cyber and digital issues like data security, misinformation and disinformation, influence operations and fake news, to name a few, are gradually gaining more traction in cybersecurity discussions. ASEAN has recognised the need for a holistic approach towards addressing these cross-cutting issues and has established relevant platforms to this end, such as the ASEAN Cyber-CC. This was a good step forward in the right direction.

25. However, State governments do not have a monopoly on the solutions to cyber and digital challenges. Leading technology companies' clout and influence over operations and development of critical and emerging technologies have grown significantly, and industries have also helped build up cyber capacities and provide training in technical solutions. Governments will need to work with the industry on better cybersecurity, for example, on securing products and services, given that the private sector manufactures these products. Civil society and academia have also been increasingly

[3] The report focused on six Southeast Asia economies: Indonesia, Malaysia, Singapore, Thailand, the Philippines and Vietnam

vocal and active and have contributed innovative solutions that can help make cyberspace safer. The cyber and digital environment is fast changing, and it is even more crucial for government and non-government stakeholders to work together to address the cyber threats that have arisen as result of new technology. It is only with the collective, concerted, and deliberate efforts of all stakeholders can we address the prevailing cyber threat landscape adequately, and in turn create a cyberspace that is able to support ASEAN's digital ambitions.

(IV) OBJECTIVE OF 2021-2025 STRATEGY

26. In view of the changes in the cyber and digital domain, the overarching objective of developing a new ASEAN Cybersecurity Cooperation Strategy is to update ASEAN's approach, while continuing to build on existing achievements. This update will guide the creation of a safer and more secure cyberspace in the ASEAN region. A secure, interoperable, and resilient cyberspace in the ASEAN region undergirds and enables ASEAN's digital ambitions. These digital ambitions are reflected in numerous initiatives such as the ASCN, the ASEAN Declaration on Industrial Transformation to Industry 4.0, and the ADM 2025[4]. These ambitions can be curtailed by the greater attack surface resulting from increased digital interconnectedness, complexity of increasingly interrelated cyber and digital issues, and increasingly sophisticated cyberattacks.

27. To support ASEAN's digital economy and ambitions, the 2021 – 2025 Strategy seeks to support the establishment of a rules-based multilateral order for cyberspace, one that is open, secure, stable, accessible, interoperable and peaceful; built through the application of voluntary, non-binding norms of responsible State behaviour, confidence building measures, and coordinated capacity-building by enhanced cooperation within ASEAN and with our ASEAN Dialogue Partners.

28. The 2021 – 2025 Strategy builds on the foundation laid by the first Strategy in incident response, CERT and capacity building cooperation, and considers the rapid cybersecurity landscape changes for the purpose of creating a safe and secure cyberspace in the ASEAN region. It contains five dimensions of work: **(1) Advancing Cyber Readiness Cooperation; (2) Strengthening Regional Cyber Policy Coordination; (3) Enhancing Trust in Cyberspace; (4) Regional Capacity Building; and (5) International Cooperation.**

[4] The ASEAN Cybersecurity Cooperation Strategy dimensions will directly support some of the ADM 2025 Desired Outcomes (DO) and Enabling Actions (EA), as well as other relevant digital efforts in ASEAN. A mapping of ADM 2025 DOs and EAs relevant to the Cybersecurity Dimensions are appended in Annex A: Cybersecurity in Support of ASEAN's Digital Ambitions.

(V) CYBERSECURITY IN SUPPORT OF ASEAN'S DIGITAL AMBITIONS

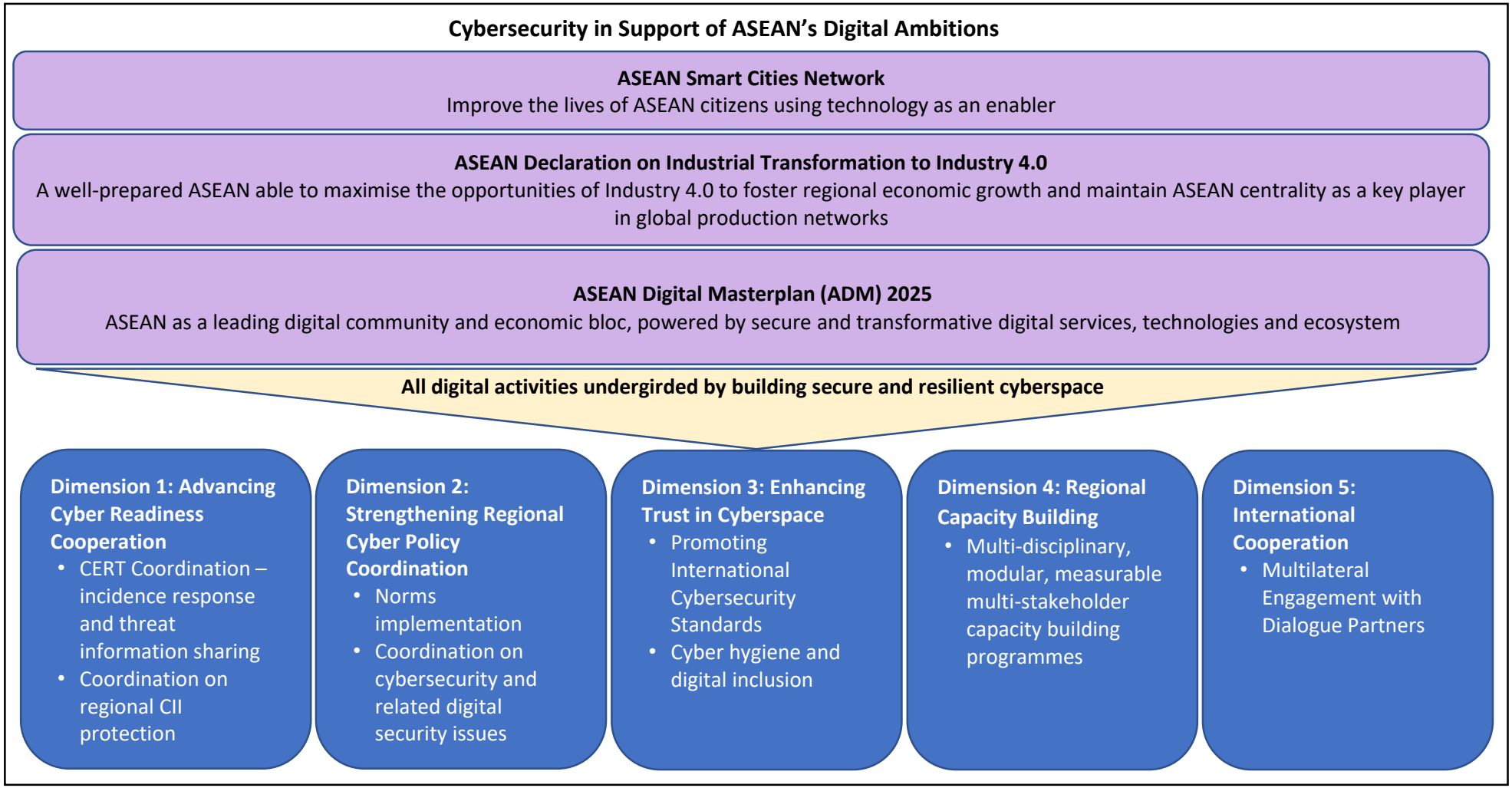

Figure 1: Cybersecurity in Support of ASEAN's Digital Ambitions

DIMENSION 1: ADVANCING CYBER READINESS COOPERATION

29. ASEAN continues to face many types of cyber threats such as Distributed Denial of Service (DDoS) attacks and disruption to CII services, which will increase in sophistication. Referencing recent supply chain attacks, this is a serious issue because once a trusted software is compromised, it can potentially subvert the entire cybersecurity posture from within. These attacks exploit a vulnerability that can impact the entire digital ecosystem through the supply chain, given the interconnectivity of the digital domain. Unintended collateral damage could easily occur and indiscriminately impact other unsuspecting users beyond the prime target or targets.

30. By establishing greater cooperation such as through the sharing threat information quickly, ASEAN can respond to incidences in a timely manner and mitigate the impact or potential spread of an attack.

31. This dimension focuses on bringing together national CERTs in all AMS to share information resources and best practices to facilitate collective responses and build future readiness against such attacks. As ASEAN moves towards digitalisation, it is important that AMS continue to build on the existing regional CERT-CERT cooperation to stay united and build the group's resilience. This will no doubt help ASEAN build a safer, more secure and trusted regional cyberspace, that can be a key enabler of economic progress and opportunity for the region.

CERT Cooperation

32. To strengthen incident response effectiveness through regional CERT-to-CERT coordination and incident readiness through CERT-to-CERT threat information sharing, given the increased sophistication and fast evolving threats and coordinate CERT capacity-building programmes in the region, ASEAN will embark on the following initiatives:

ASEAN Initiatives	Lead ASEAN Sectoral Body
• ASEAN Regional CERT Establishment • ASEAN CERT Information Exchange Mechanism Establishment • ASEAN cybersecurity threat landscape annual report	• ANSAC[5] • ASEAN Cyber CC

CII Protection

33. To improve coordination efforts for the protection of CIIs, including those cross-border CIIs that provide essential services to more than one State and serve as the backbone for regional communications and trades, ASEAN will embark on the following initiative:

ASEAN Initiatives	Lead ASEAN Sectoral Body
• Development of ASEAN Critical Information Infrastructure Protection (CIIP) Coordination Framework, built upon the ASEAN CIIP Framework (2020)	• ANSAC

34. Further details on initiatives listed in the tables above can be found in Annex B. Individual AMS initiatives supporting this dimension of work of can also be found listed in Annex C.

[5] ASEAN Network Security Action Council, a cybersecurity working group under ADGSOM.

DIMENSION 2: STRENGTHENING REGIONAL CYBER POLICY COORDINATION

35. In order to achieve the vision set out by ASEAN leaders in the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation of a "*peaceful, secure, and resilient cyberspace that serves as an enabler of economic progress, enhanced regional connectivity and betterment of living standards for all*"[6], ASEAN leaders reaffirmed the need to build closer cooperation and coordination among AMS on cybersecurity policy. While ASEAN has made significant progress on this front, the inherently cross-border and cross-cutting nature of the cyber and digital domain, coupled with the rapidly evolving cyber threat landscape underscores the need to further strengthen regional cyber policy coordination.

36. ASEAN can build on its strong foundation where established platforms such as the ASEAN Cyber-CC, ARF ISM on ICTs Security, and AMCC can be used to further enhance coordination, not just between AMS, but also with Dialogue Partners and the wider ecosystem, where appropriate.

37. As the first regional organisation to subscribe in-principle to the 11 voluntary, non-binding norms as set out in the 2015 UNGGE report, ASEAN has embarked on a process of developing a plan of action to implement these norms. ASEAN also endeavours to add value to international conversations on cybersecurity in support of a multilateral rules-based order in cyberspace. In this regard, ASEAN is pleased to note the adoption of the consensus report of two UN cybersecurity processes, namely the inaugural UN Open Ended Working Group (OEWG) and the 6th iteration of the UNGGE. These reports have increased the understanding and awareness of AMS and the wider international community on key cybersecurity issues and will act as useful guides in ASEAN's work on norms implementation.

<u>Coordination on Cybersecurity and Related Digital Security Issues</u>

38. In order to strengthen cross-sectoral coordination on cybersecurity and related digital security issues in view of the increasingly blurred boundaries, ASEAN will be embarking on the following initiatives:

ASEAN Initiatives	**Lead ASEAN Sectoral Body**
• ASEAN Leaders' Statement on Advancing Digital Transformation • Regional Internet Governance Forum (IGF) on cross-jurisdictional approach to online content regulation	• ADGMIN • ATRC[7]; in coordination with SOMRI[8] Working Group on Information, Media and Training (WG-IMT)[9]

<u>Norms Implementation</u>

39. To enhance ASEAN's ability to implement the voluntary, non-binding norms in the 2015 UNGGE report – which ASEAN subscribed in-principle to – in a more concerted and deliberate manner, ASEAN will be embarking on the following initiative:

[6] Language from OP1 of the 2018 ASEAN Leaders' Statement on Cybersecurity Cooperation.
[7] ASEAN Telecommunications Regulators Council, a senior officials sectoral body under ADGMIN.
[8] Senior Officials Meeting Responsible for Information.

ASEAN Initiatives	Lead ASEAN Sectoral Body
• Development of Matrix for ASEAN Regional Plan of Action (RAP) on the Implementation of Norms of Responsible States Behaviour in Cyberspace	• ASEAN Cyber-CC • ARF ISM on ICTs Security

40. Further details on initiatives listed in the tables above can be found in Annex B. Individual AMS initiatives supporting this dimension of work of can also be found listed in Annex C.

DIMENSION 3: ENHANCING TRUST IN CYBERSPACE

41. With digitalisation comes the proliferation of the use of new technologies such as 5G and the IoT. This is a natural result of ASEAN's digital ambitions to build Smart Cities and transform industries for Industry 4.0.

42. Cybersecurity underpins the trust of ASEAN's increasingly digital dependent way of life. It is well known that there are financial costs to attacks on digital systems. In IBM Security's 2020 Cost of a Data Breach Report[10], the average cost of a data breach in ASEAN in 2020 was estimated to be USD 2.7 million. More importantly, fostering trust in the use of technology is key to ASEAN's digital ambitions. Businesses need to know they can operate in a secure environment. Citizens need to know that public services supporting their continued safety, health and welfare remain accessible. The increase of highly sophisticated cyberattacks, have also underscored increased need for trust between nations to behave responsibly in cyberspace.

43. Everyone has a role to play in the cybersecurity of our shared digital space. While governments take a role at the national level to roll out initiatives to protect our digital infrastructure, enterprises, organisations and individuals must strengthen their cybersecurity posture by regularly practicing good cyber hygiene. 80% of cyberattacks are not highly sophisticated and can be prevented if individuals and businesses adopt cyber hygiene measures such as strong passwords and regular software updates.

44. This dimension focuses on building trust through the adoption of international cybersecurity standards to secure the increased use of emerging technology. It also addresses the need for cyber hygiene and digital inclusion as enterprises, organisations and individuals all play a role in securing our shared digital space.

<u>Promoting International Cybersecurity Standards</u>

45. To secure emerging technology such as 5G and IoT through adoption of international best practices and standards, ASEAN will be embarking on the following initiatives:

ASEAN Initiatives	Lead ASEAN Sectoral Body
• Development of regional cybersecurity standards for IoT	• ANSAC • ADGSOM and ATRC

[10] IBM Security Cost of a Data Breach Report 2020 dashboard, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

• Development of regional cyber security policy, procedure and guideline for 5G and IoT implementation; • Development of regional cyber security policy, procedure and guideline for SMART City implementation • Capacity building activities on digital infrastructure product and software security testing and certification	• ASCN, in coordination with ANSAC • ANSAC

Cyber Hygiene and Digital Inclusion

46. To secure our shared digital space, ASEAN will be embarking on the following initiatives:

ASEAN Initiatives	**Lead ASEAN Sectoral Body**
• Development of Cybersecurity Awareness Programme for AMS; • Development of digital literacy training modules or programmes.	• ANSAC • SOMRI Working Group on Information, Media and Training (WG-IMT)

47. Further details on initiatives listed in the tables above can be found in Annex B. Individual AMS initiatives supporting this dimension of work of can also be found listed in Annex C.

DIMENSION 4: REGIONAL CAPACITY BUILDING

48. Cybersecurity capacity building serves an effective tool, not only to strengthen collective cybersecurity posture, but also to enable countries to contribute meaningfully to international discussions, which is a key step towards achieving security and resilience in cyberspace. As such, it is important for ASEAN to continue such efforts and learn from each other's experiences through coordinated capacity-building to improve ASEAN's cyber resilience.

49. Given the increasingly cross cutting nature of cybersecurity, there is a need for continued training not only on technical and operational matters, but also on cybersecurity policy, legislation, and strategy. Training should also be politically neutral with participation of multiple stakeholders.

50. This dimension focuses on reviewing investments in cyber capacity-building to ensure that ASEAN is moving toward the end goal of building an engaged ASEAN for a more secure and resilient ASEAN cyberspace. This will also help ASEAN better allocate its resources and engage its Dialogue Partners.

Multi-disciplinary, Modular, Multi-stakeholder and Measurable Programmes

51. In line with the 2019-2021 UN Group of Governmental Expert (UNGGE) consensus report, capacity building should be voluntary, politically neutral, mutually beneficial and reciprocal in nature. It should also be conducted in a manner that is multi-disciplinary, multi-stakeholder, modular and measurable. To build regional capacity, ASEAN will be embarking on the following initiatives:

ASEAN Initiatives	Lead ASEAN Sectoral Body
• ASEAN-Japan Cybersecurity Capacity Building Centre's (AJCCBC) programmes • ASEAN-Singapore Cybersecurity Centre of Excellence's (ASCCE) programmes	• ADGSOM + Japan • n/a
• ADMM Cybersecurity and Information Centre of Excellence (ACICE)	• ADMM

52. Further details on initiatives listed in the table above can be found in Annex B. Individual AMS initiatives supporting this dimension of work of can also be found listed in Annex C.

DIMENSION 5: INTERNATIONAL COOPERATION

53. It is very important for ASEAN and its Dialogue Partners (DPs) to tackle an issue like cybersecurity together. ASEAN serves as a hub for services spanning the banking and finance sector, telecommunications, as well as the aviation and maritime sectors. The recent supply chain attacks are a reminder of the increasing sophistication of cyber threats and how they could potentially impact the entire digital ecosystem and the CII that underpin these essential services.

54. This dimension focuses on exploring ways that ASEAN can work with our international partners in a way that is mutually beneficial and effective. This could include initiatives that pursue stronger engagement opportunities with DPs to work on the identified gaps in the region's cybersecurity developments where needed, ensuring that ASEAN+1 workstreams meet ASEAN's needs and priorities, and improving ASEAN's standing on international platforms.

<u>Multilateral Engagement with Dialogue Partners</u>

55. To enhance ASEAN's existing engagement with ASEAN DPs, leverage ASEAN DPs cybersecurity operational, technical, and policy expertise through multi-stakeholder training for AMS, the following initiatives are proposed:

ASEAN Initiatives	Lead ASEAN Sectoral Body
• Engagement with DPs and other countries in the region for Confidence Building Measures, including through ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF ISM on ICTs Security). • Establish a schedule and coordination/follow-up mechanism for ASEAN Cybersecurity Dialogues with related DPs to discuss specific topics, while at the same time ensuring inclusivity and avoid duplication. • CERT to CERT dialogues and joint exercises with Dialogue Partners.	• ARF ISM on ICTs Security, in coordination with ASEAN Cyber-CC • ARF ISM on ICTs Security, in coordination with ASEAN Cyber-CC • ANSAC

56. Further details on initiatives listed in the table above can be found in Annex B. Individual AMS initiatives supporting this dimension of work of can also be found listed in Annex C.

(VI) **CONCLUSION**

57. The ASEAN Cybersecurity Cooperation Strategy (2021 – 2025) builds on the past 2017-2020 Strategy to identify initiatives in **(1) Advancing Cyber Readiness Cooperation; (2) Strengthening Regional Cyber Policy Coordination; (3) Enhancing Trust in Cyberspace; (4) Regional Capacity Building; and (5) International Cooperation** for an updated roadmap to build a safe and secure cyberspace in the ASEAN region. This paper is submitted to ADGMIN for adoption, as ASEAN continues to move forward as a region to achieve its digital ambitions.

ANNEX

Annex A: Cybersecurity in Support of ASEAN's Digital Ambitions

The ASEAN Cybersecurity Cooperation Strategy dimensions will directly support some of the ADM 2025 Desired Outcomes (DO) and Enabling Actions (EA), as well as other relevant digital efforts in ASEAN. A mapping of ADM 2025 DOs and EAs relevant to the Cybersecurity Dimensions are appended:

ASEAN Cybersecurity Cooperation Strategy Dimensions	**ADM 2025 Desired Outcomes (DO)**	**ADM 2025 Enabling Action (EA)**	**Other relevant ASEAN digital efforts: ASEAN Smart Cities Framework and ASEAN Declaration on Industry 4.0**
Dimension 1: Advancing Cyber Readiness Cooperation • CERT Coordination; • Coordinate regional CII protection.	**DO 3**. The delivery of trusted digital services and the prevention of consumer harm.	**EA 3.1**. Enable trust through greater and broader use of online security technologies. **EA 3.2**. Build trust through enhanced security for finance, healthcare, education and government. **EA 3.4**. Improve coordination and cooperation for regional computer incident response teams.	Cybersecurity to support and undergird ASEAN's investment in: • Smart infrastructure to improve the security, efficiency, and access to key services such as healthcare. • Smart solutions to improve the civic and social lives of citizens.
	DO 5. Increase in the quality and use of e-government services.	**EA 5.4**. Help developing AMS improve the quality of their e-government e-services.	
Dimension 2: Strengthening Regional Cyber Policy Coordination	**DO 5**. Increase in the quality and use of e-government services.	**EA 5.2**. Help make key government departments more productive through their internal use of ICT and e-services.	Cybersecurity to support and undergird ASEAN's efforts to:

ASEAN Cybersecurity Cooperation Strategy Dimensions	ADM 2025 Desired Outcomes (DO)	ADM 2025 Enabling Action (EA)	Other relevant ASEAN digital efforts: ASEAN Smart Cities Framework and ASEAN Declaration on Industry 4.0
• Norms implementation; • Coordination on cybersecurity and related digital security issues.	**DO 6.** Digital services to connect business and to facilitate cross-border trade	**EA 6.1.** Facilitate compliance and secure the benefits of telecommunications services and electronic commerce in line with relevant ASEAN trade agreements.	• Grow competitiveness of ASEAN's digital economy through the adoption of technologies involving industry 4.0 such as IOT and 5G to generate business opportunities. • Provide comprehensive range of support to accelerate ASEAN transformation to Industry 4.0 with special focus on Start-ups, MSMEs, e-government and Smart Cities.
Dimension 3: Enhancing Trust in Cyberspace • Promoting International Cybersecurity Standards; • Cyber hygiene and digital inclusion.	**DO 2.** Increase in the quality and coverage of fixed and mobile broadband Infrastructure.	**EA 2.7.** Adopt regional policy to deliver best practice guidance on AI governance and ethics, IoT spectrum and technology.	Cybersecurity to support and undergird ASEAN's efforts to: • Improve equality in access to goods and services and social infrastructure such as education using Smart technology, to improve citizens' quality of life. • Promote and facilitate conformance and certification of digital standards.
	DO 8. A digitally inclusive society in ASEAN	**EA 8.1.** Ensure citizens and businesses have the skills and motivation to use digital services. **EA 8.2.** Reduce accessibility barriers to getting online.	

ASEAN Cybersecurity Cooperation Strategy Dimensions	ADM 2025 Desired Outcomes (DO)	ADM 2025 Enabling Action (EA)	Other relevant ASEAN digital efforts: ASEAN Smart Cities Framework and ASEAN Declaration on Industry 4.0
Dimension 4: Regional Capacity Building • Multi-disciplinary, modular, multi-stakeholder programmes	**DO 3.** The delivery of trusted digital services and the prevention of consumer harm.	**EA 3.1.** Enable trust through greater and broader use of online security technologies. **EA 3.2.** Build trust through enhanced security for finance, healthcare, education and government.	Cybersecurity to support and undergird ASEAN's efforts to: • Multi-stakeholder approach to resource and support development of smart cities in ASEAN. • Intensify engagement and interaction among AMS to explore possibilities for government, academia and industry to provide a range of support.
	DO 5. Increase in the quality and use of e-government services.	**EA 5.4.** Help developing AMS improve the quality of their e-government e-services.	
Dimension 5: International Cooperation • Multilateral Engagement with Dialogue Partners	**DO 6.** Digital services to connect business and to facilitate cross-border trade.	**EA 6.1.** Facilitate compliance and secure the benefits of telecommunications services and electronic commerce in line with relevant ASEAN trade agreements.	Cybersecurity to support and undergird ASEAN's efforts to: • Form partnerships with external partners and other city networks to resource and support development of smart cities in ASEAN.

Annex B: Details of ASEAN Initiatives Supporting the 5 Dimensions of Work

DIMENSION 1: ADVANCING CYBER READINESS COOPERATION

CERT Co-operation

<table>
<tr><th colspan="3">ASEAN Regional Computer Emergency Response Team (CERT) Establishment</th></tr>
<tr><th>Initiative Description</th><th>Lead ASEAN Sectorial Body</th><th>Status Update</th></tr>
<tr><td>Facilitate the timely exchange of threat and attack-related information among AMS National CERTs and foster CERT-related capacity building and coordination – but without in any way taking over or impinging on the operational role, mandate and functions of each AMS National CERT.
AMS agreed at the 19th ANSAC meeting that the functions of the ASEAN CERT, taking reference to MITRE's Feasibility Study, would be as follows:

<table>
<tr><td>1) Facilitate coordination and information sharing between AMS National-level CERTs</td><td>5) Partner with other international and regional organisations in support of ASEAN cybersecurity interests and objectives</td></tr>
<tr><td>2) Develop and maintain an ASEAN POC network of cybersecurity experts and organisations</td><td>6) Develop partnerships with industry and academia</td></tr>
<tr><td>3) Host ASEAN cybersecurity conferences/meetings, trainings and drills for AMS national CERTs</td><td>7) Support AMS National CERT capacity building and best practices</td></tr>
<tr><td>4) Facilitate and conduct regional cybersecurity exercises</td><td>8) Conduct and support cybersecurity awareness campaigns in coordination with other ASEAN Sectoral Bodies related to cybersecurity and the ASEAN Cyber-CC</td></tr>
</table>
</td><td>ANSAC</td><td>Singapore is consolidating the input from AMS</td></tr>
</table>

<table>
<tr><th colspan="3">ASEAN CERT Information Exchange Mechanism</th></tr>
<tr><th>Initiative Description</th><th>Lead ASEAN Sectorial Body</th><th>Status Update</th></tr>
<tr><td>Facilitate incident response and exchanges amongst all AMS CERTs, and coordinate CERT capacity-building programmes in the region</td><td>ANSAC</td><td>Singapore is consolidating the input from</td></tr>
</table>

through the ASCCE. The mechanism will form a core part of the work of the ASEAN CERT.		AMS (as part of the ASEAN CERT Implementation Paper)

ASEAN cybersecurity threat landscape annual report		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Annual document which may include, but not limited to malicious or anomaly traffic activities that occur in AMS, cyber security incident and the lesson learned (mitigation strategy, TTP, etc), hot issues related to cyber security (policy or regulation, etc).	ASEAN Cyber CC	Initiative

CII Protection

Critical Information Infrastructure Protection Framework		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
ASEAN Critical Information Infrastructure Protection Framework identified CIIs that have strategic imperatives and provided strategic recommendations and coordinated approaches to create more resilient cybersecurity across ASEAN's critical information infrastructure through six pillars: (1) policy coordination, (2) identifying CIIs, (3) protecting CIIs, (3) information sharing, (5) incident response, and (6) capacity building.	ANSAC AMCC	The project was completed by Thailand in 2019.

DIMENSION 2: STRENGTHENING REGIONAL CYBER POLICY COORDINATION

Coordination on cybersecurity and related digital security issues

ASEAN Digital Leaders' Statement		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
To advance the important agenda of digital transformation in ASEAN, Brunei is proposing for an ASEAN Leaders' Statement on Digital Transformation. The aim of this Statement is to encourage AMS to acknowledge the imperative of digital transformation for post-COVID-19 economic recovery and to seize the opportunities presented by digital technologies.	ADGMIN	The proposal is currently being drafted.

Regional Internet Governance Forum (IGF) on cross-jurisdictional approach to online content regulation		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Development of a cross-jurisdictional coordination mechanism for inappropriate online content handling.	ATRC, in coordination with SOMRI WG-IMT	A concept note is to be

		jointly developed.

Norms implementation

Development of Matrix for ASEAN's Plan of Action on the implementation of norms of Responsible States Behaviour in Cyberspace		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Having subscribed in-principle to the UNGGE norms in 2018, the ASEAN Ministerial Conference on Cybersecurity in 2019 agreed to start a workstream on the development of a long-term Implementation Roadmap for Norms of Responsible State Behaviour in Cyberspace ("Matrix") under the ambit of ASEAN Cyber-CC. Malaysia and Singapore have agreed to be co-proponents of this effort and have convened a workshop to develop the Matrix together with AMS Updates on the Matrix will be reported to the next ASEAN-Cyber CC and AMCC in 2021 and be submitted to ADGSOM for endorsement, ADGMIN for adoption and ASEAN Leaders for notation.	• ASEAN Cyber-CC • ARF ISM on ICTs Security	The draft Matrix of the ASEAN Regional Action Plan (RAP) on the Implementation of Norms of Responsible State Behaviour in Cyberspace has been presented and adopted during the 2nd ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber CC) on 30 November 2021. The implementation of the norms will focus on the low-hanging fruit initiatives first, i.e. capacity building initiatives. The matrix will become a living document and can be updated from time to time.

DIMENSION 3: ENHANCING TRUST IN CYBERSPACE

Promoting International Cybersecurity Standards

Development of regional cybersecurity standards for IoT		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
The operating landscape in the region is fast evolving and AMS' are increasingly interconnected. In this regard, cyberspace should be interoperable and ASEAN would benefit from promoting common security standards and frameworks, as well as the sharing of best practices. For example, the Internet of Things (IoT) landscape is fast-evolving and pose distinctive threats and risks. Given that the proliferation of smart devices gives rise to a potentially huge attack surface, common standards could be promoted to collectively raise the security levels of consumer IoT devices.	ADGMIN	

Development of regional cyber security policy, procedure and guideline for 5G and IoT implementation;		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**

Development of regional cyber security policy, procedure and guideline for SMART City implementation		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**

Capacity building activities on digital infrastructure product and software security testing and certification		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
To conduct a series of symposium involving the private sector on security testing and certification of digital infrastructure products and software.	ANSAC, in coordination with ACCSQ	A concept note is to be jointly developed.

Cyber Hygiene and Digital Inclusion

Development of Cybersecurity Awareness Programme for AMS		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**

	ADGMIN	

Development of digital literacy training modules or programmes		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Digital literacy programmes are part of SOMRI WG-IMT's current strategic action plan	SOMRI WG-IMT	Ongoing

DIMENSION 4: REGIONAL CAPACITY BUILDING

Multi-disciplinary, Modular, Multi-stakeholder and Measurable Programmes

AJCCBC's programmes		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) was established in Bangkok, Thailand in 2018 and funded by the Japan-ASEAN Integration Fund (JAIF 2.0). Since its inception AJCCBC has trained over 500 participants and is expected to accomplish its target 700 trained cybersecurity professionals and exhaust its funding by Dec 2022. Currently AJCCBC is developing a new proposal "Project for Enhancing ASEAN-Japan Cybersecurity Building Programme for Cybersecurity and Trusted Digital Services", with the objective to build upon the current expertise and experience and continues to provide capacity building services to ASEAN Member States in 2023-2026.	ANSAC	Being proposed for Japan's continuing support On-going regional capacity building programme

ASCCE's programmes		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Singapore launched the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in October 2019 to move capacity building efforts forward in a coordinated manner. The ASCCE training facility is currently operational and will open officially in 2021. In response to the global travel restrictions due to Covid-19, ASCCE started delivering online capacity building programmes in 2020. The ASCCE has since trained over 270 AMS officials in 2020, and over 600 since its inception. The ASCCE undertakes a modular, multi-disciplinary, multi-stakeholder and metrics-based approach to deliver its programmes, which covers both policy, strategy as well as technical aspects of cybersecurity. To maintain the relevance and quality of programming, the ASCCE engages top international cybersecurity experts and trainers, in collaboration with other AMS, ASEAN Dialogue Partners and UNODA as well as industry and academia, to design and deliver cybersecurity capacity building programmes for senior ASEAN policy and technical officials.	ADGMIN	

ACICE's programmes		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
The ADMM Cybersecurity and Information Centre of Excellence (ACICE) was proposed by Singapore and approved by the 15th ADMM in Jun 2021, to enhance regional cooperation among ASEAN defence establishments in the cybersecurity and information domains. Given our increasing reliance on digital and information technologies, the defence sectoral is well-positioned to contribute to efforts to tackle these common security challenges. The key objectives of the ACICE are to: (a) function as a node for confidence-building measures, information-sharing and capacity building among regional militaries; (b) enhance regional cooperation and information sharing, focusing on cyber security, disinformation and misinformation threats including through the dissemination of regular and timely reports; and (c) work with international experts to improve collective resilience against common security threats. The ACICE will host the defence sectoral's first Malware Information Sharing Platform, for regional militaries to share unclassified malware information. The ACICE will also work with the ASCCE to offer training courses to defence sectoral personnel where relevant.	ADMM	Singapore has begun to operationalise the ACICE, with a view to formally launch the ACICE in 2022.

DIMENSION 5: INTERNATIONAL COOPERATION

Multilateral Engagement with Dialogue Partners

Engagement with DPs and Other Countries in the Region for Confidence Building Measures, including through ARF ISM on ICTs Security		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Proposed Confidence Building Measures in the form of workshops, seminars, table-top exercises, and the updating of the ARF Point of Contacts (POC) Directory on Security of and in the Use of ICTs	ARF	Initiative

Establish a Schedule and Coordination/Follow-Up Mechanism for ASEAN Cybersecurity Dialogues with Related DPs to Discuss Specific Topics, while at the Same Time Ensuring Inclusivity and Avoiding Duplication		
Initiative Description	**Lead ASEAN Sectorial Body**	**Status Update**
Proposed policy strategy for engaging in Dialogues with ASEAN Dialogue Partners	ASEAN Cyber-CC	Initiative agreed on at ASEAN Cyber-CC

Annex C: Details of AMS Initiatives Supporting the 5 Dimensions of Work

[In this Annex, AMS may choose to profile national initiatives that support each of the 5 Dimensions and their subsections. AMS may add initiatives by filling in a table for each initiative.]

DIMENSION 1: ADVANCING CYBER READINESS COOPERATION

[Insert initiative name]	
Initiative Description	**AMS**

DIMENSION 2: STRENGTHENING REGIONAL CYBER POLICY COORDINATION

[Insert initiative name]	
Initiative Description	**AMS**

DIMENSION 3: ENHANCING TRUST IN CYBERSPACE

[Insert initiative name]	
Initiative Description	**AMS**

DIMENSION 4: REGIONAL CAPACITY BUILDING

[Insert initiative name]	
Initiative Description	**AMS**

DIMENSION 5: INTERNATIONAL COOPERATION

[Insert initiative name]	
Initiative Description	**AMS**