BROADENING AND DEEPENING CYBERSECURITY COOPERATION FOR A SECURE AND RESILIENT ASEAN CYBERSPACE

ASEAN Cybersecurity Cooperation Strategy 2017-2020

ASEAN CYBERSECURITY COOPERATION STRATEGY

1. INTRODUCTION

1.1. Need for ASEAN Cybersecurity Cooperation Strategy

ASEAN is a region of immense opportunity. Demographically, ASEAN has a relatively young population, with a median age of 28.3, compared to 37.9 in the US and 42.4 in the European Union.[1] About 40% of ASEAN's 630 million people are connected to the Internet, and this will increase to 50% within the next few years. Those under the age of 35 are among the most active social media users in the world. ASEAN's economy is set to become the fourth largest single market after the EU, US, and China by 2030.[2] ASEAN is a hub for many economic sectors such as banking, ecommerce, transportation (aviation and maritime), and telecommunications.

As ASEAN grows, our digital connectivity has likewise improved. For example, the number of mobile subscriptions per 100 inhabitants rose from 90.43 in 2010 to 121.75 in 2014. The cost of accessing fixed broadband as a percentage of GNI per capita in the region had decreased considerably from 37.16% in 2010 to 6.21% in 2013. However, as the number of Internet users across the region increases, so does the risk of cyber-attacks and their impact on AMS.

1.2 Increased Cyber-attacks on the ASEAN Region

Cyber threats are growing exponentially. Moreover, because cyber attacks do not respect national boundaries, they can be launched from anywhere around the world, which makes attributing the source of attacks a challenging task. They are also becoming technically more advanced, and more difficult to defend. Cyber-attacks can create knock-on and disproportionate effects that reverberate across the entire region and the rest of the world, especially when they hit national Critical Information Infrastructure (CII) sectors such as banking and finance, aviation, maritime, and telecommunications. Such cyber-attacks sometimes carry indirect and psychological ramifications that are widespread and damaging not just to the affected country, but its neighbours as well.

In recent years, the ASEAN region has fallen victim to cyber-attacks. In Indonesia, the number of cyber-attacks increased by 33% from 2014 to 2015 and the Bank of Indonesia saw a 66.7% increase in cybercrimes in 2015. Hackers infiltrated SWIFT, a worldwide interbank communication network handling transactions, and managed to break into several banks' systems around the world, including some banks in ASEAN in October 2016. Singapore's Ministry of Defence also experienced a breach in its Internet system in early-2017, resulting in the leak of personal details of 850 soldiers and staff. As of June 2016, over 2,100 servers in Malaysia belonging to banks, businesses and government agencies were compromised and their access put up for sale to hackers. In Vietnam, there were cyber-attacks on the websites of two airports and Vietnam Airlines in July 2016.

Fortunately, ASEAN has not stood still in response to this risk. Over the years, AMS have cooperated on many occasions to strengthen regional cybersecurity. For the past 11 years, AMS and Dialogue

[1] CIA World Factbook; Eurostat (statistical office of the EU); and the report "Unleashing the Potential of the Internet for ASEAN Economies" by Internet Society, a leading US think tank focusing on Internet-related policies.

[2] https://www.usasean.org/system/files/downloads/Investing-in-ASEAN-2013-14.pdf

Partners have participated in the annual ASEAN CERT Incident Drill (ACID) to test the coordination amongst the incident response teams and their incident handling procedures. In 2012, ASEAN Telecommunications Regulators Council (ATRC), a sectoral body under TELMIN, established the ASEAN Network Security Action Council (ANSAC) to, among others, promote CERT cooperation and sharing of expertise. TELSOM's cooperation with Dialogue Partners such as China and Japan has also helped to bolster regional cybersecurity. Individual AMS have also collaborated with Dialogue Partners on this front.

But there is more that AMS can do to enhance ASEAN cybersecurity incident response capabilities, CERT-CERT exchanges and cybersecurity capacity building to ensure that the ASEAN region will not be vulnerable to cyber threats. This is especially so with the establishment of the ASEAN Economic Community in 2015. The integrated nature of our region's economies wills us to come together to protect the region from the risk of cyber-attacks that might affect not just one, but all of our economies in one way or another.

1.3 ASEAN Leaders Have Endorsed Strong Cybersecurity Cooperation

ASEAN leaders have, on many occasions, proclaimed the importance of cybersecurity in the region and reaffirmed their commitment to working together towards achieving the common goal of a safe and secure cyberspace for ASEAN that is not easily susceptible to the risk of cyber-attacks. In the Chairman's Statement of the **28th and 29th ASEAN Summits** in Vientiane 2016, ASEAN leaders recognised the importance of cybersecurity and "welcomed the convening of the inaugural ASEAN Ministerial Conference on Cybersecurity (AMCC) in Singapore on 11 October 2016 to facilitate greater cybersecurity cooperation among AMS, which will complement existing ASEAN efforts to strengthen cybersecurity in the region."[3] Noting the multi-disciplinary nature of cybersecurity, ASEAN ICT and Cybersecurity Ministers and Senior Officials attending the **inaugural ASEAN Ministerial Conference on Cybersecurity** held during the Singapore International Cyber Week from 10-12 October 2016 emphasised the urgent need for ASEAN to take a holistic and more coordinated approach to regional cybersecurity discussions and cybersecurity capacity building.

At the 15th **ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings (TELMIN)**, ASEAN Ministers reaffirmed "the importance of collective efforts in ensuring a secure ICT ecosystem in ASEAN"[4] and expressed their vision of moving towards a "digitally enabled economy, which is secure, sustainable, and transformative; and one that would enable the achievement of an innovative, inclusive and integrated ASEAN Community."[5]

In the Joint Declaration of the **ASEAN Defence Ministers on Promoting Defence Cooperation For a Dynamic ASEAN Community (ADMM)**, ASEAN Defence Ministers expressed concern over the "frequency, scale and complexity posted by non-traditional threats and reaffirming the need, commitment and collective responsibility of the ADMM to address such threats to promote peace, security and prosperity of the region."[6] Cyber threats are considered a non-traditional threat and

[3] Chairman's Statement of the 28th and 29th ASEAN Summits, Vientiane, 6-7 September 2016, para 34
[4] Joint Media Statement of the 15th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings, 2015
[5] Ibid.
[6] Joint Declaration of the ASEAN Defence Ministers on Promoting Defence Cooperation For a Dynamic ASEAN Community, 2016

hence, there is a need to ensure that AMS are working together to protect themselves and each other from such attacks.

The **ASEAN Ministerial Meeting on Transnational Crime (AMMTC)** has also periodically underlined "the importance of enhancing joint cooperation to address cybercrime as a new challenge in the whole region" as well as the need to enhance cybercrime-related capacity building[7].

ASEAN's focus is in line with actions taken by the International Community. The United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications Report recognised the importance of a safe and secure cyberspace and recommended 'limiting norms' such as "states should not knowingly allow their territory to be used for internationally wrongful acts using ICT"[8] and 'good practices and positive duties' such as "states should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices."[9] The European Union Cybersecurity Strategy 2013 highlights the need to have an open and free cyberspace, and that countries have to undertake the main task to "safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet."[10] The International Telecommunication Union (ITU) National Cybersecurity Guide recommended that "governments use all instruments of national power to reduce cyber risks appropriately."[11]

2. SCOPE OF THE CYBERSECURITY COOPERATION STRATEGY

2.1 Objective of the ASEAN Cybersecurity Cooperation Strategy

The main objective of the ASEAN Cybersecurity Cooperation Strategy is the creation of a safe and secure cyberspace in the ASEAN region. This objective can be advanced by building on and enhancing the work already undertaken by TELMIN to improve ASEAN cybersecurity incident response capabilities, CERT-CERT exchanges and cybersecurity capacity building.

With this objective in view, the 15th ASEAN TELMIN tasked ANSAC with preparing this strategy paper to provide a roadmap for regional cooperation to achieve the objective of a safe and secure ASEAN cyberspace, which will also help to strengthen information security in ASEAN – in line with the strategic thrust on Information Security and Assurance in the ASEAN ICT Masterplan 2020 (AIM2020).

2.2 Three Main Areas of Focus of the ASEAN Cybersecurity Cooperation Strategy

[7] Joint Statements of the First and Second ASEAN Plus Japan Ministerial Meeting on Transnational Crime, 2013 and 2015
[8] 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law
[9] Ibid.
[10] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[11] ITU National Cybersecurity Strategy Guide

This Strategy proposes that, as a first step, TELMIN tasks TELSOM to identify, assess and strengthen cybersecurity cooperation on three main areas: (i) **cybersecurity incident response**; (ii) **Computer Emergency Response Team (CERT) policy and coordination**; and (iii) **cybersecurity capacity building**.

In line with the Strategy's objective to limit proposals to areas within TELMIN's focus and mandate, the proposed strategy will only focus on enhancing cybersecurity cooperation within the civilian cyberspace, and will **not** cover other domains such as cybercrime, cyber defence and cyber diplomacy, since these are presently not within TELMIN's mandate.

2.3 A Holistic Response to Secure ASEAN Cyberspace

Concerted, real-time coordination among multiple agencies across countries is required to counter the increasing sophistication of today's cyber-attacks. To protect against cyber threats effectively and collectively, ASEAN will need to come up with a strategy at the ASEAN level to guide its cybersecurity cooperation efforts, and to bring all AMS to a higher capability level to counter modern cyber challenges.

There is a clear consensus at the ASEAN level on the need for stronger and more coordinated cybersecurity cooperation among AMS. This has been expressed on numerous occasions and in numerous documents. At the inaugural AMCC in October 2016, ASEAN representatives recognised the importance of a safe and secure cyberspace and the need to work together as a regional organisation to decrease the dangers and risks of cyber-attacks. ASEAN representatives believe that it is "very critical for AMS to cooperate"[12] to counter cyber threats issues. In October 2016, the 37th ASEAN Inter-Parliamentary Assembly (AIPA) General Assembly agreed to "[f]urther strengthen cooperation in cybersecurity within ASEAN and between ASEAN and its partners".[13] Ministers at the 15th Meeting of the ASEAN TELMIN in November 2015 also reaffirmed "the importance of collective efforts in ensuring a secure ICT ecosystem in ASEAN".[14] A main objective of the ARF Workplan on Security of and in the Use of ICTs was to "improve cooperation…through improved coordination and coordinated response."[15]

ASEAN should leverage the consensus generated from these statements to devise a strategy with a clear framework for cybersecurity cooperation initiatives as well as more closely coordinate cyber initiatives undertaken in the TELMIN tracks. This framework will help to steer and guide ASEAN's cooperation efforts, and also provide a holistic cover and ensure synergy in these efforts so as to achieve coherent outcomes and clear deliverables.

3. REVIEW OF ASEAN'S PAST CYBERSECURITY COOPERATION INITIATIVES

[12] AMCC 2016; Directions for ASEAN Cybersecurity Strategy and Policy
[13] http://www.aipasecretariat.org/report-37th-general-assembly/
[14] http://www.asean.org/storage/images/2015/November/statement/15%20--%20TELMIN-15-JMS%20-%20darft%2025112015%20CN%20JP%20KR%20IN%20US%20ITU_FINAL.pdf
[15]http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20yCommunications%20Technologies.pdf

AMS have already started an effort to coordinate responses and build capacity together as a regional organisation, and also with ASEAN Dialogue Partners. The existing initiative in ASEAN has started the process of strengthening cooperation and capacity building. It is important to review ASEAN's cooperation framework and come up with a strategy to build capacity to ensure a safe and resilient cyberspace in this region.

A review of ASEAN's cybersecurity cooperation initiatives shows that ASEAN's efforts over the past four years have been focused primarily on three areas – (1) Incident Response; (2) Technical Capacity Building; and (3) Public Awareness-raising. These three areas are important for having strengthened ASEAN's cyber incident response capability and fostered close working relationships among the ASEAN CERTs. Efforts in these areas have been made in close collaboration among AMS and Dialogue Partners, and have allowed ASEAN to achieve a level of cybersecurity preparedness, especially in inter-operability and cooperation when dealing with cyber incidents.

4. A BROAD AND DEEP CYBERSECURITY COOPERATION STRATEGY

4.1 Enhancement to the ASEAN Cybersecurity Cooperation Approach

The chart in Figure 1 shows that ASEAN has devoted strong focus to areas such as Incident Response Capacity Building, and Information-Sharing Processes and Exercises. Efforts in these areas have played a critical role not only in developing cybersecurity capabilities and building trust among AMS, but also in setting a firm foundation for the next phase of regional cybersecurity cooperation. In this regard, the ASEAN CERT Maturity Framework proposed in this paper will build on past ASEAN efforts and help equip AMS with a targeted approach to regional cybersecurity cooperation by **identifying** needed areas of cybersecurity cooperation and **assessing** progress in these areas. This will lead to a more robust and relevant set of capacity building initiatives and better coordination of efforts for ASEAN and its Dialogue Partners.

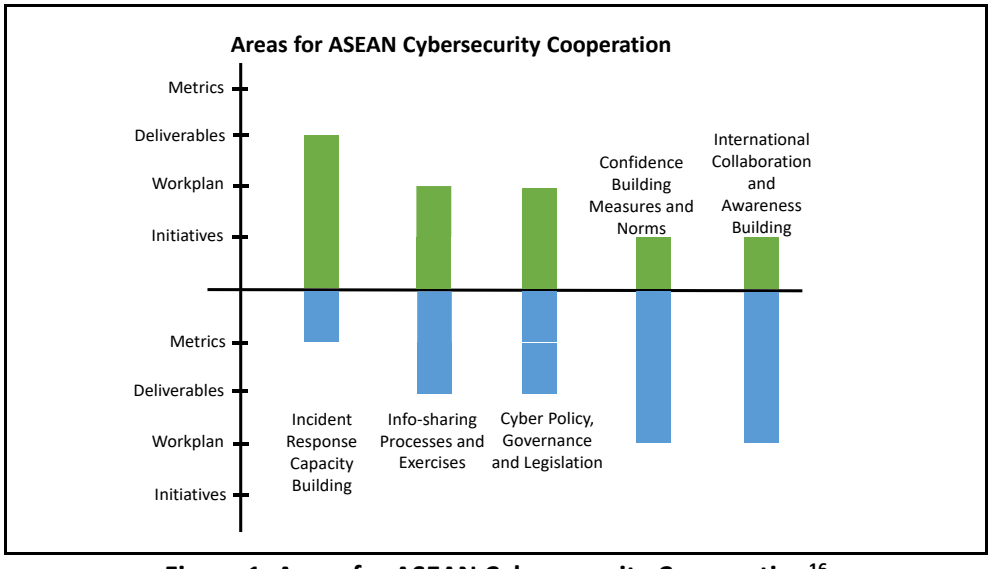

Figure 1: Areas for ASEAN Cybersecurity Cooperation[16]

5. IMPLEMENTING AN ASEAN CERT MATURITY FRAMEWORK

[16] Green bars denote areas that ASEAN has covered, blue bars denote areas that are not yet covered. This chart is derived from a broad and simple survey of initiatives that ASEAN has come up with over the past four years.

5.1 Proposed ASEAN CERT Maturity Framework

The crux of this cooperation strategy is to enhance ASEAN's approach to levelling up its incident response capabilities in a coordinated and targeted manner. The ASEAN CERT Maturity Framework can serve as a common reference to determine the maturity level of the respective AMS' national CERT, and systematically identify gap areas where appropriate training or capacity building effort can be directed towards. A common framework will also enable mutual understanding and facilitate enhanced collaboration among CERT partners in times of need, thereby increasing the collective cybersecurity level of ASEAN CERTs.

Currently, there is no universal standard to define the maturity level of a national CERT. There are, however, established maturity models developed to quantify an organisational CERT's incident response capabilities. The **S**ecurity **I**ncident **M**anagement **M**aturity **M**odel (SIM3) is one such model that is widely used by the European CSIRT community. Over 100 EU CSIRTs currently support the use of SIM3. It is proposed that the ASEAN CERT maturity framework makes use of SIM3 as the basis for its maturity model with appropriate refinements.

To enhance the SIM3 model, two additional components are proposed to be incorporated: (1) a Foundation layer and (2) a Technical Capability Index; so as to provide a more holistic maturity assessment. The "Foundation" layer would cover the existence of supporting factors, such as legal framework and business plan, while the Technical Capability Index measures five specific technical functions, namely a) cyber threat monitoring and analysis, b) incident handling, c) vulnerability handling, d) artifact handling, and e) technical alerts and advisory drafting. These five functions have been chosen as they are deemed to be core technical capabilities for a CERT to function effectively.

The Technical Capability Index uses a provisional scoring system adapted from SIM3. The average scores for the Technical Capability Index components are assessed vis-à-vis a grading system which allows an ASEAN national CERT to measure its technical capability. Refer to **Annex A** for more information on the Technical Capability Index and its scoring.

Based on the above, the proposed framework for ASEAN national CERT maturity measurement (Figure 2) thus comprises six areas: (1) Foundation, (2) Organisation, (3) Human, (4) Tools, (5) Processes, and (6) Technical Capability Index.

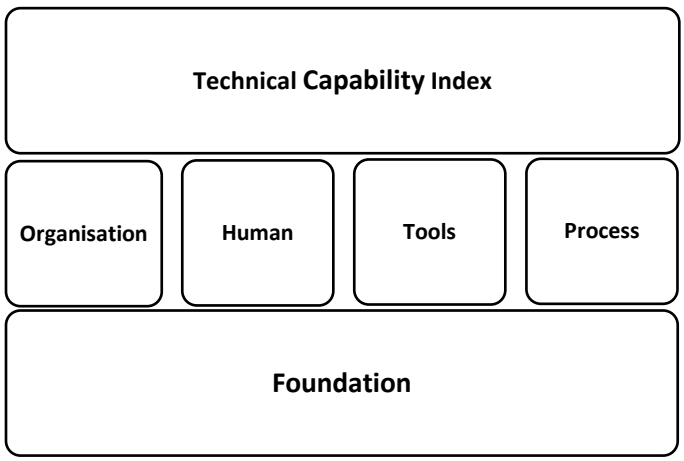

Figure 2: Proposed framework comprising 6 areas of assessment

In line with the adoption of the CERT Maturity framework, the CSIRT Maturity Quick Scan online tool developed by the NCSC-NL (Netherlands) can also be adopted to facilitate CERT maturity assessment.

This is a simple and straightforward self-assessment aid for assessors to measure the maturity level of a CERT based on a list of questions and checklist.[17]

Based on this provisional self-scoring system, it is proposed that ASEAN CERTS strive for a minimum colour grade of "**Green**" in their Technical Capability Index.

Score	Colour Grade	Description
0 – 1.9	Red	Low overall maturity, demands attention on most if not all areas.
2 – 2.9	Amber	Mixed overall maturity, requires closer auditing and attention on lacking areas.
3 – 4	Green	Good overall maturity, deserves closer auditing and attention on focus areas.

Table 1: Technical Competency Index Grading

Following TELMIN's endorsement of the strategy paper, ANSAC will formulate an implementation plan in consultation with AMS. A period of six to nine months will be required for AMS to perform a first-level self-assessment for all ASEAN CERTs. This includes a Workshop. This will be pivotal for identifying areas of need and training opportunities required by each ASEAN CERTs, facilitating mutual understanding and enhancing collaboration, and developing regional cyber readiness and incident response capacity.

5.2 TELMIN and ANSAC to Take a Leading Role

Given the inherent role of ICT in the cyber environment, TELSOM/TELMIN is the appropriate platform to coordinate the implementation of cybersecurity cooperation activities as identified by individual AMS through self-assessment using the above ASEAN CERT Maturity Framework. To ensure a coordinated approach in undertaking these actions, ANSAC will be tasked to take guidance from these inputs in order to assess, identify and implement coordinated cybersecurity cooperation activities with the respective Dialogue Partners.

5.3 Establishment of a Future ASEAN CERT

The establishment of an ASEAN CERT is in line with AIM2020's Initiative 8.2 on strengthening information security preparedness in ASEAN. It will also provide inputs that can contribute to the scenarios and scope of the ACID exercise. Instead of diminishing the respective roles of the national CERTs in ASEAN, an ASEAN CERT will cement the critical roles that national CERTs play in strengthening regional cybersecurity. An ASEAN CERT will give national CERTs in ASEAN a formal mechanism to tighten coordination and enhance collaboration. This will allow them to synergise their individual strengths and areas of expertise to bolster the overall effectiveness of regional incident response capabilities.

[17] The current CSIRT Maturity Quick Scan online tool covers the four SIM3 components as well as the "Foundation" components. The Technical Capability Index is not incorporated and will need to be developed separately to make the assessment more holistic.

5.4 Plugging Into International and Regional Cybersecurity Capacity Building Initiatives

5.4.1 Targeted and Effective Capacity Building Initiatives

ASEAN can further bolster its cybersecurity capacity via frameworks and cooperative programs such as the ASEAN CERT Maturity Framework and ASEAN cybersecurity capacity building cooperation in collaboration with Dialogue Partners and international organisations. These include information-sharing, threat awareness building, exchange of best practices, CERT-CERT cooperation and exercises such as CYDER, and ASEAN-Japan cybersecurity incident response training program, and the Cyber SEA Games, an ASEAN cybersecurity competition for youth. Use of the framework will help to ensure that ASEAN's resources are judiciously channelled into initiatives that are not only targeted and necessary, but, assessed through the framework's metrics, effective in building incident response capacity.

The multi-disciplinary nature of cybersecurity threats requires that capacity building initiatives address not only technical but also policy aspects of capacity gaps. One of the initiatives that AMS can tap into to address these gaps is the ASEAN Cyber Capacity Programme (ACCP), a modular programme that takes a multi-stakeholder approach to develop ASEAN's capacity in areas such as incident response and strategy development. It will include the annual Singapore International Cyber Week, which incorporates the AMCC platform to provide a Track 1.5 (governmental and non-governmental) forum for ministers, including non-ICT ministers, to engage industry and other stakeholders on regional cybersecurity discussions. Another initiative is the CyberGreen project that uses open-source information to measure and create awareness of the cyber health status of a country.[18] Through CyberGreen's development of cyber health metrics, measurements, and mitigation best practices, cyber incident response teams and network operators can better identify and remediate different classes of threats.

5.4.2 Potential Future Areas of Cooperation

Given the cross-cutting nature of cybersecurity threats, there is also a need to take a more holistic ASEAN approach towards other important cybersecurity policy issues. These include the discussion and coordination of ASEAN cybersecurity policy on a single ASEAN platform, the development of a broader ASEAN cybersecurity strategy, the need to expand the scope of cyber exercises which are currently designed to cater for the telecommunications sector, and the discussion of regional cybersecurity norms of behaviour and confidence building measures in partnership with stakeholders from the other ASEAN sectorial bodies like the AMMTC and ADMM. As there is no single ASEAN platform to discuss these issues at present, and some of the issues identified may not fall under TELMIN's mandate, these discussions can for the present be undertaken at other platforms such as the annual AMCC hosted by Singapore.

6. CONCLUSION

ASEAN has the potential to further bolster its status as a significant regional presence on the international cybersecurity landscape. It is a young, dynamic and resourceful bloc with the wherewithal to build a safe and robust cybersecurity landscape through greater coordination in incident response, CERT cooperation, and capacity building.

[18] All AMS can access the CyberGreen portal to gauge their own cyber health status at http://www.cybergreen.net/mitigation/asean/ throughout the three-year period that Singapore is a cornerstone sponsor of the CyberGreen project.

This paper is submitted to TELSOM for endorsement based on TELMIN's instruction at the 16th TELMIN. As ASEAN moves forward as one region, AMS can join hands and work together to build a secure and resilient cyberspace.