SHHBIDSS Paper
NADI Workshop on Counter-Terrorism, Counter-Radicalisation and Cybersecurity
25-29 June 2018, Singapore

Mapping Cybersecurity Cooperation Mechanisms

Overview

As the world grows more dependent on cyberspace and continues to pave its way into the fourth industrial revolution, cybersecurity continues to gain more traction and relevance in the minds of countries' decision makers especially as the growing dependence comes with great benefits and risks. The region also witnessed the proliferation of regional cooperation in cybersecurity with an aim to reduce its associated risks on national security and manage its challenges effectively together regionally.

Realities of Cyberspace

Cyberspace is a unique domain where on one hand, its borderless nature allows information to be created, stored and transmitted seamlessly regardless of one's geographical location; and on the other hand, attracts malicious activities including cyberterrorism, cyber fraud and identity theft due to its anonymity.

Cyberspace as a medium and target where as a medium, non-state actors such as terrorists and its affiliated groups exploits the current platform to recruit followers, spread propaganda and finance their activities. As a target, attacks in cyberspace disrupt functions of critical national infrastructures by disabling technology-reliant industries and services such as banking, health, water and electrical supplies. The same goes for the military where cyberspace has been widely regarded as the fifth domain of warfare.

Mapping cybersecurity cooperation frameworks

Given the ability of cyberattacks to inflict considerable damages due to its unique and pervasive nature, there are several cooperation mechanisms within ASEAN that looks at cybersecurity including the ASEAN Ministerial Meeting on Transnational Crimes (AMMTC), ASEAN Telecommunications and IT Ministers (TELMIN), ASEAN Ministers Responsible for Information (AMRI) and ASEAN Regional Forum (ARF). These cooperation mechanisms continues to multiply in the region where from 2016 to 2017, during which at least three mechanisms were established namely (i) ADMM-Plus EWG on Cybersecurity, (ii) ARF-ISM on Security of and in the Use of Information and Communication Technologies and (iii) ASEAN Ministerial Conference on Cybersecurity. The following matrix are few selected cooperation seen within the region.

ASEAN			
MECHANISMS		PRIORITY AREAS	INITIATIVES / CBMs / PROJECTS
1	ADMM-Plus EWG on Cybersecurity	• Defence and Military Practical Cooperation	• Shared Information on National Cyber Security Strategies. • Established POC for ADMM-Plus countries. • Military Exercises – TTX and FTX. • Cyber Glossary of Terms.
2	ARF-ISM on Security and the Use of Information and Communication Technologies (ARF-ISM on ICTs Security)	• Awareness Building and Exchange of Best Practices • CERT-CERT Cooperation Frameworks • Combating Criminal and Terrorist Use of ICTs	• Establishment of ARF POC. • Info-sharing on National Laws, Policies, Best Practices and Strategies. • ARF Workshop on National Cybersecurity Strategy Building.
3	ASEAN Ministerial	• Promoting Cyber Norms	• ASEAN Cyber Capacity Program,

	Conference on Cybersecurity	among AMS • Cyber Capacity Building	amounting to 10 million for the period of 5 years beginning 2016. • Encourage ASEAN to begin its own dialogue on cyber norms.
4	ASEAN Ministers Responsible for Information (AMRI)	• Countering Fake News • Communicating the right information	• Shared experiences in countering fake news including legislation to regulate and manage online space and fake accounts. • Implementing programs to enhance media literacy, especially among the youths.
TRACK 1.5 and 2			
5	Australian Strategic Policy Institute (ASPI)	• Raise awareness on cyber-related issues for broader strategic policy • Facilitating cross sectoral conversations on cyber issues.	• Publication of an annual report on Cyber Maturity in the Asia-Pacific region
		• Strengthening existing CBMs on Cybersecurity	• Draft of Sydney Document
6	Council for Security Cooperation in the Asia Pacific Working Group (CSCAP WG)	• Focused on cyber threat scenarios in Asia Pacific • To proposed cybersecurity strategy for ARF's consideration	• Cybersecurity Study Group • Preparation of a draft CSCAP Memorandum on Cyber

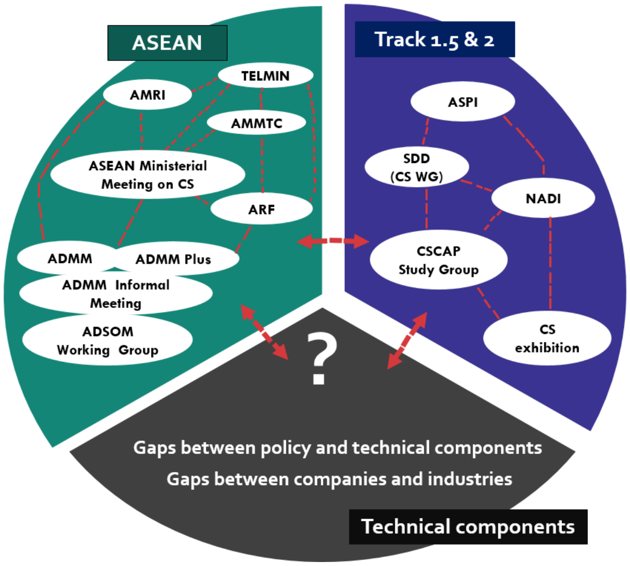
Observations. Despite all these initiatives, there remains to be apparent gaps between various cooperation mechanisms within and across different tracks.

a) **Lack of cross-cutting discussion in cybersecurity.** Among the various cybersecurity cooperation mechanisms, the ASEAN Ministerial Conference on Cybersecurity is the only Track I mechanism that discusses on cross-cutting cybersecurity issues. Last September, Ministers, among others, reaffirmed the need for ASEAN to take a holistic and more coordinated approach to regional cybersecurity cooperation and capacity building. Others such as AMMTC, TELMIN and ARF looks into different aspects of cybersecurity and cybercrime. However, the ministerial mechanism does not have strong linkages with other Track 1 platforms.

b) **Lack of cross-sectoral collaboration between cybersecurity cooperation mechanisms as seen in Figure 1.** In the last five years, the focus on cybersecurity issues have significantly increased at the national, regional and international level. For example, since 2014, South Korea has hosted the annual Cyber WG meeting at the sidelines of the Seoul Defence Dialogue and in 2016, cybersecurity has been added to the areas of ADMM-Plus practical cooperation. This year, in January, the ARF-ISM on ICTs Security has its first open ended Study Group (SG) on CBM co-chaired by Japan, Malaysia and Singapore in Tokyo; and Australia organised a Roundtable on Practical Futures for Cyber Confidence Building in the ASEAN region back in March.

However, these initiatives remains fragmented due to the lack of cross-sectoral collaboration between the mechanisms. Consequently, these lack of synergy makes (1) plans and discussions on cybersecurity often not translated into executable actions on a policy and operational level; (2) the risk of overlapping and duplication of efforts higher rather than complementing each other towards building up national and regional cybersecurity capacities as seen between the ADMM and ARF; and (3) disconnect between the policy and technical components of cybersecurity.

Figure 1 – Cybersecurity Cooperation across different



Managing Cybersecurity in Brunei Darussalam

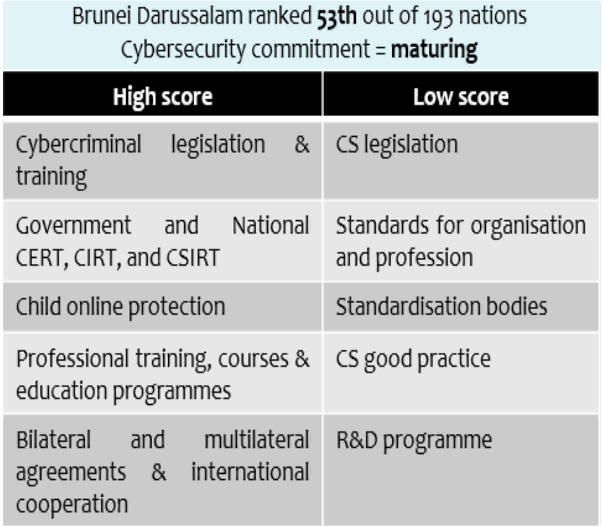
Brunei Darussalam has one of the highest internet penetration among the ASEAN member states at 95 percent. In the last fifteen years, Brunei has continuously develop strategies to manage its increasing dependence on the cyberspace and gaps in addressing its IT and cyber challenges. Among some of its national initiatives can be seen below:

- Establishment of the National Security Committee with a host of local security agencies to manage and address cybersecurity threats.
- E-government Strategic Plan 2009 – 2014 with an aim to develop an integrated e-services and deliver better public services and assist the public to better adapt to the advancement of ICT.
- The Digital Government Strategy 2015-2020 driven by the Wawasan 2035 aiming to support the goals envisioned. (Goals: highly skilled and well-education citizens, high quality of life, and a dynamic and sustainable economy)
- Establishment of numerous agencies responsible for the different areas related to IT and CS including:
    - The Authority for Info-communications Technology Industry (AiTi) established in 2003 is a statutory body where one of the area it is responsible for is the country's ICT industry development.
    - IT Protective Security Services Sdn Bhd (ITPSS) established in 2003 looks into information security solutions, providing various specialised information security and physical security services including penetration testing, digital forensics, secure event management and IT security training.
    - Brunei National Computer Emergency Response Team (BruCERT) formed in 2004 is the nation's first trusted referral agency dealing with online threats and computer security incidents in the country. It is a platform for ITPSS to test its Incident Response and serves as a monitoring mechanism that addresses any computer-related and internet-related incidents through issuing early warning, early response and post-mortem of such incidents.

Currently, Brunei is focused on strengthening existing cooperation and ensure an integrated whole-of-nation approach in dealing with cyber threats. These includes (1) promoting cyber awareness especially among the society, (2) drafting of the National Cyber Security Framework to identify laws and measures needed to protect the public and roles of agencies in both the public and private sector, and (3) strengthening its cyber early warning system.

In recognising the global efforts in addressing cybersecurity and its challenges, a report published in July 2017 by the UN International Telecommunications Union (ITU) ranked Brunei's cybersecurity efforts at 53th out of 193 nations in the Global Cybersecurity Index 2017 and is perceived to be in the maturing stage in terms of its commitment as seen in Figure 2. The figure also highlights areas Brunei did well and gaps that needed more work to achieve near-perfect approach to cybersecurity. This is further supported by the findings in another report by ASPI on Cyber Maturity in the Asia Pacific 2017 which highlighted the country's effort in dealing with cybersecurity and at the same time highlighted its slow progress where gaps remains overlooked.

Figure 2 – Global CS Index 2017



Brunei Darussalam ranked **53th** out of 193 nations
Cybersecurity commitment = **maturing**

High score	Low score
Cybercriminal legislation & training	CS legislation
Government and National CERT, CIRT, and CSIRT	Standards for organisation and profession
Child online protection	Standardisation bodies
Professional training, courses & education programmes	CS good practice
Bilateral and multilateral agreements & international cooperation	R&D programme

Recommendations

The borderless nature of cyberspace and the increasing risks makes threats and challenges more complex in nature and in ensuring cooperation mechanisms are able to tackle threats more effectively, there is a need for ASEAN to:

1. Firstly, engage multi-stakeholders in cybersecurity dialogues and practical initiatives, on a national, regional and international level to ensure initiatives across the various sectors are complementing each other, while avoiding duplication. There is also a need to bridge the gap between the policy and technical components in the cybersecurity ecosystem as current approaches to cybersecurity challenges are done separately in policy and technical platforms.

2. Secondly, in view of the different priorities and inconsistent focus on cybersecurity depending on ASEAN Chairman, there is a need to devise a comprehensive regional plan to ensure continuity of cybersecurity cooperation is maintained and momentum is not lost after the end of championing chairmanships.

3. Thirdly, to stock take existing cybersecurity cooperation and future plans across the various sectors and tracks. This will allow everyone to synergise its respective cybersecurity initiatives and produced more concrete outcomes needed to strengthen national and regional cybersecurity capabilities and resilience against cyber challenges. Here, Track II can support Track I by raising awareness on all the work that has been done across the various sectors through international cooperation and discussion. Track II can achieve this by:
   - ➢ Mapping out laws and regulations, policies, doctrines in the ASEAN region track,
   - ➢ Tracking and reporting ongoing unclassified cyber activities such as exercises, workshops, conferences, and
   - ➢ Providing support to the ASEAN Secretariat in their cybersecurity agenda throughout succeeding chairmanships.