Evaluating ASEAN Defence and Security Initiatives with Dialogue Partners – Cybersecurity

By Brunei Darussalam

Introduction

Substantive cybersecurity discussions began to take root in ASEAN roughly 17 years ago, with the ASEAN Regional Forum (ARF) focusing on cyberterrorism, while the ASEAN Telecommunications and IT Ministers (TELMIN) discussing ICT-related initiatives in contributing towards the ASEAN Economic Community (AEC). Thus as a security challenge, cybersecurity is cross-sectoral in nature and cooperation among ASEAN Member States and with Dialogue Partners can involve sectors other than the ASEAN Political Security Community (APSC) pillar.

Overtime, regional cooperation in cybersecurity deepened and expanded to include more areas of cooperation as well as more partners. While this trend is encouraging, there is a risk of duplication of work given that the areas of cooperation in different sectors now overlap. There is also a need to ensure that future cooperation is pursued in a holistic manner, as it contributes towards readiness and preparedness in responding to a cyber-related emergency.

ASEAN Telecommunications and IT Ministers (TELMIN)

The TELMIN is a platform where all ICT-related discussions in ASEAN take place. It was formed in 2001 under the AEC, to harness the potentials of ICTs and help achieve goals outlined in the AEC. In the ASEAN ICT Masterplan 2015, the cyber security dimension falls under the fourth Strategic Thrust called Infrastructure Development. In the ASEAN ICT Masterplan 2020 (AIM2020) however, it assumes a standalone category as the eighth Strategic Thrust.

Looking at the priority areas of the two masterplans, the 2015 Masterplan lays emphasis on the Computer Emergency Response Teams (CERTs) as well as efforts towards enhancing partnerships for data security. In the AIM2020, the region seeks to develop regional guidelines, principles and approaches, in addition to continuing efforts to enhance the CERTs and data security.

These two observations show efforts towards deepening cooperation among ASEAN Member States as well as with Dialogue Partners. These efforts could stem from a realisation that the region needs to pay more attention to cybersecurity. They could also indicate a growing

confidence among the TELMIN ministers following successful partnerships undertaken under the 2015 Masterplan.

ASEAN-Japan Cooperation

The TELMIN began formal engagements with Dialogue Partners in 2006 with China. Cooperation was expanded to other Dialogue Partners and external parties in subsequent years, including South Korea, Japan, India, the European Union (EU) and the International Telecommunication Union (ITU). There was a heavy emphasis on capacity-building in these cooperation, ranging from training to infrastructure development and policy development. When it comes to cybersecurity, it appears that Japan has more developed cooperation with the TELMIN.

Substantive engagement in cybersecurity between ASEAN and Japan began in 2009 with the convening of the ASEAN-Japan Information Security Policy Meeting[1]. Apart from annual dialogues, there were practical cooperation aiming to enhance capacities. Capacity-building remains an important feature in ASEAN-Japan cybersecurity cooperation up to today, where initiatives such as the Enhancing Information Security for ASEAN: Focusing on ISMS and ICS (Information Control System) Security training program[2] and the ASEAN Cyber Capacity Programme (ACCP)[3] were conducted.

The latest ASEAN-Japan Information Security Policy Meeting that took place in October 2016 took note of the following progress[4]:

> 1. Established an information sharing system where officials would be able to share information and swiftly respond to incidents in the event of an attack.[5]
>
> 2. Acknowledged new guidelines concerning protection of critical information infrastructures in Japan and ASEAN. Workshops may be held in 2017 to introduce and discuss the implementation of the new guidelines.
>
> 3. Discussed the possibility of long term training programs, in addition to short-term training courses that Japan has been providing for ASEAN Member States.

Here, it is clear that ASEAN-Japan cooperation has developed to include important aspects of cybersecurity such as information-sharing and developing shared guidelines. They constitute the targets outlined in the AIM2020, in particular, the development of guidelines to protect critical information infrastructures.

Information-sharing platforms between Japan and ASEAN include the Japan-ASEAN Security Partnership (JASPER)[6], which provides visuals of traffic flow and activities, including the neutralisation of threats. Additionally, the Internet Traffic Monitoring Data Sharing (TSUBAME) project[7] provides CERTs threat analyses to facilitate response.

Cybersecurity engagements between ASEAN and Japan also take place outside of the TELMIN framework, such as in the ARF and the ASEAN-Plus Japan Ministerial Meeting on Transnational Crime (AMMTC).

Cooperation in cyber norms

In addition to capacity-building and information-sharing, the region is moving towards new areas of cooperation: cyber norms and international law in the cyber space. These topics have been discussed in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[8] (UN GGE), a working group in the United Nations that focuses on cybersecurity. In 2013, the UN GGE made two important recommendations: firstly, there is a need to promote understanding on cyber norms as a means to reduce risks in the cyber space; and secondly, it affirmed the applicability of international law in the cyber space[9].

ASEAN Member States have been participating in discussions concerning cyber norms and applicability of international law in the cyber space. Indonesia was part of the 2014-2015 session of the UN GGE, while Malaysia took part in the subsequent 2016-2017 session. Also, during the ASEAN Ministerial Conference on Cybersecurity in October 2016, Singapore called for ASEAN to begin dialogue on cyber norms.

Risk of Duplication of Work

It is evident that there is a positive momentum in cybersecurity cooperation in the region. Cooperation thrives with the presence of a handful of bilateral and multilateral platforms. Renowned organisations are positioning their cybersecurity bases in the region such as the INTERPOL, Palo Alto Networks, Boeing and Microsoft. ASEAN Member States have undertaken their own initiatives to contribute to the momentum, such as the Philippines' proposal for an ADMM-Plus EWG on Cybersecurity, the Singapore International Cyber Week (SICW) and Thailand's call for an ASEAN Cyber Unit.

However, amidst the thriving cybersecurity cooperative landscape, there is a risk of duplication of work as areas of cooperation overlap. For instance, both the Japan-ASEAN Cybercrime Dialogue and the ACCP focuses on cybercrime -- do these initiatives make conscious effort to leverage on each other's progress in cybersecurity engagements? The same can be said of the

CERT platform and the ADMM-Plus EWG on Cybersecurity, where both focus on effective response to a cybersecurity-related emergency. In the ARF's Work Plan on Security of and in the Use of Information and Communications Technologies[10], it stated its aim to establish a contacts database –- how is this different from the database that the CERTs has?

Thus, there is a need to clarify the roles of each mechanism in the regional cybersecurity landscape. ASEAN has undertaken such effort before. The 23rd ASEAN Summit in 2013 called for the formation of a joint task force to accelerate well-coordinated and concerted efforts[11] in HADR, which was later known as the Joint Task Force to Promote Synergy with other Relevant ASEAN Bodies on Humanitarian Assistance and Disaster Relief. In 2015, the ASEAN Military Preparedness on Humanitarian Assistance and Disaster Relief Seminar produced a diagram identifying how each HADR mechanism links with each other, thus clarifying their roles during a cyber incident. Therefore, TELMIN's endorsement of the ASEAN Cyber Security Cooperation Strategy in 2016 is a positive move in this respect.

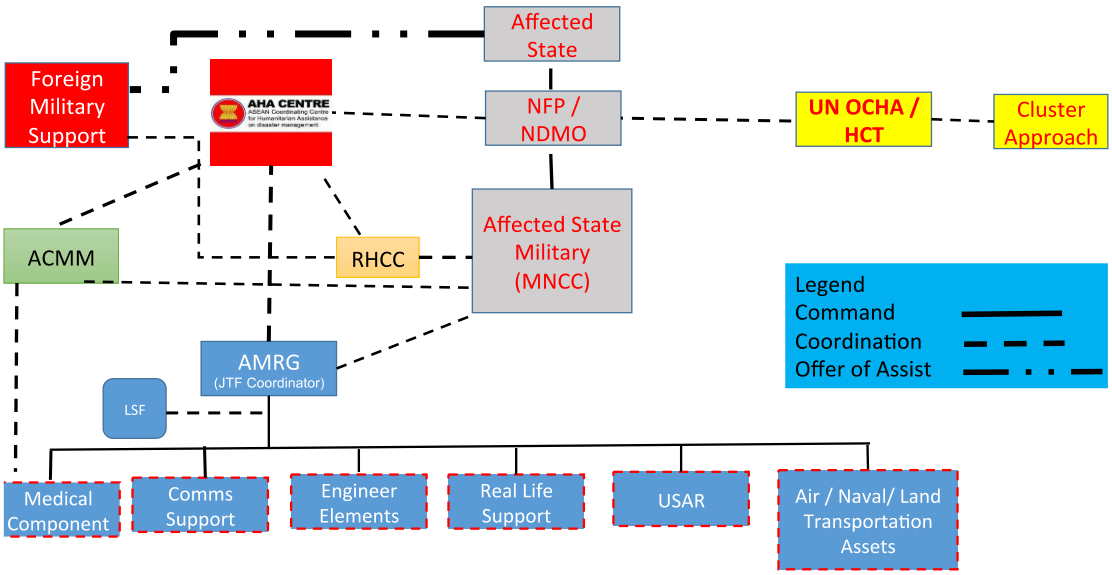

Figure 1 shows a diagram produced during the ASEAN Military Preparedness on Humanitarian Assistance and Disaster Relief Seminar in August 2015, aiming to clarify the linkages of regional HADR mechanisms during a cyber incident.

Conclusion

Unlike HADR, cybersecurity mechanisms have not been tested yet against a real cyber incident that warrants a regional response. Thus, it is difficult to gauge the level of preparedness and readiness of the cybersecurity architecture. Scenario-based exercises such as the ASEAN CERT Incident Drill (ACID), ASEAN-Japan Cyber Exercise and the cyber-attack defense training

conducted by the NEC are positive developments, but it is important to pursue a more holistic approach to threat mitigation and neutralisation. As in HADR, this approach often involves the participation of multiple agencies and the public.

[1] "Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation." *ASEAN*. September 13, 2013. http://www.asean.org/wp-content/uploads/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf, 1.

[2] "METI to Hold Training Programs to Support Enhancement of Information Security in the ASEAN Region." *Ministry of Economy, Trade and Industry*. February 2015. http://www.meti.go.jp/english/press/2015/0216_02.html.

[3] Zafar Anjum. "ASEAN Countries Deepen Joint Efforts against Global Cyber Threats." *Computerweekly.com*. October 20, 2016. http://www.computerweekly.com/news/450401315/Asean-countries-deepen-joint-efforts-against-global-cyber-threats.

[4] "The Ninth ASEAN-Japan Information Security Policy Meeting Held." *Ministry of Economy, Trade and Industry*. October 2016. http://www.meti.go.jp/english/press/2016/1024_03.html.

[5] "The Ninth ASEAN-Japan Information Security Policy Meeting Held." *Ministry of Economy, Trade and Industry*. October 2016. http://www.meti.go.jp/english/press/2016/1024_03.html.

[6] Evans Rodgers. "Japan's NICT Develops Futuristic 'Daedalus' Cyber Attack Alert System." *The Verge*. June 19, 2012. https://www.theverge.com/2012/6/19/3096820/japan-nict-clwit-daedalus-monitor.

[7] "APCERT Annual; Report 2016," *APCERT*. Accessed July 15, 2017, https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2016.pdf, 92.

[8] The UNGGE is a UN-mandated working group in the field of information security whose main outcome is a report. Its recommendations, while not legally binding, carry significant influence globally. They are also often referred to in important Internet documents. "UNGGE." *Digital Watch*. July 31, 2017. https://dig.watch/processes/ungge.

[9] "Sixty-Eight Session, Item 94 of the Provisional Agenda: Developments in the Field of Information and Telecommunications in the Context of International Security." *Ministry of Foreign Affairs, Japan*. June 24, 2013. http://www.mofa.go.jp/files/000016407.pdf.

[10] "ASEAN Regional Forum Work Plan on Security of and in the Use of Information Communications Technologies (ICTs)." ASEAN Regional Forum. May 7, 2015. 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%20Communications%20Technologies.pdf.

[11] "ASEAN Declaration on Enhancing Cooperation in Disaster Management." asean.org. October 9, 2013. http://www.asean.org/wp-content/uploads/images/pdf/Final_Draft_ASEAN_Declaration_on_Disaster_Management_-_23rd_ASEAN_Summit.pdf, 3.