RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 197 – 27 November 2018

Cyber Cooperation for ASEAN: Smoother Ride on Track II?

By Eugene EG Tan

Synopsis

The recently-concluded ASEAN Summit in Singapore called for the promotion of secure and resilient information and communications technologies (ICT) infrastructure. It noted that this can contribute to regional security and stability. The Sydney Recommendations on Practical Futures for Cyber Confidence Building Measures in ASEAN, launched in September 2018, provides a roadmap on how this can be achieved.

Commentary

ASEAN HAS long been an advocate of cyber confidence building measures (CBMs) for cyberspace; in 2014, and ASEAN was seen as a world leader in Cyber CBMs. But ASEAN and its dialogue partners, like the ASEAN Regional Forum (ARF), have not moved past the diplomatic quagmire that has bogged down the development of CBMs. For example, a list of points of contact was mooted by ARF members as early as 2012 but has yet to see fruition due to objections from some members.

Despite these obstacles, ASEAN still recognises the importance of cooperation and developing CBMs and norms in cyberspace. Singapore and Thailand, as the outgoing and incoming chairs of ASEAN, pledged to continue the discussion on cybersecurity at the ASEAN summit in November 2018 to promote an open, secure, stable, accessible and peaceful ICT environment. This is seen as critical to connectivity and economic development.

Challenges in Cyber Confidence Building Measures (CBMs)

Just two months earlier, at Singapore International Cyber Week 2018, Singapore was tasked by the ASEAN Ministerial Conference on Cybersecurity (AMCC) to develop a framework for cooperation in cyberspace; confidence building measures among the various ASEAN member states will be needed for any cooperation to be successful.

There are many challenges that need to be overcome in building this ASEAN-wide cooperation mechanism. Some ASEAN Member States have insufficient capacity to participate in cyber CBMs. For example, Myanmar's national Computer Emergency Response (MMCERT), has only five employees serving the cybersecurity needs of the whole country.

In other ASEAN states, there is insufficient communication between the technology industry, government, academia, civil society, and the public. Companies are reluctant to report incidents because they fear loss of business, or because reporting is too onerous; while governments are reluctant to share information, which may be classified. This in turn hinders the free sharing of information between countries.

Sydney Recommendations for ASEAN CBMs

Track II dialogues – or discussions involving academia, industry, and civil society – can smoothen this process of building confidence and encouraging discussions for cyberspace. The writer was invited by the Australian Strategic Policy Institute (ASPI) to participate in a project that was part of the ASEAN-Australia Special Summit in March 2018 and supported by the Australia-ASEAN Council.

The project was to suggest practical confidence building measures in cyberspace in the ASEAN region that can be readily implemented. This process brought together leading experts in international affairs and/or cyber affairs from think-tanks, research institutes and universities from across the ASEAN region.

The product of those discussions is *The Sydney Recommendations on Practical Futures for Cyber Confidence Building in the ASEAN Region*, which was launched in September 2018 at the Singapore International Cyber Week.

CBMs that were raised range from the coordination of planned and ongoing unclassified cyber activities, to professionalisation of cyber capacity building efforts among ASEAN member states, and the expansion of ASEAN Computer Emergency Response Team Incident Drills (ACID). CBMs are generally undertaken to avert hostilities, minimise escalation of hostilities, and build trust among states, which is sometimes in short supply in cyberspace.

Role of Track II in ASEAN Cyber Discussions

The Sydney Recommendations illustrate how Track II can contribute towards cyber cooperation in ASEAN. To maximise this contribution, ASEAN Track II needs to uplift its capabilities to better support Track I discussions.

Under such circumstances, informal discussions by think-tanks and other non-state actors such as businesses and industry groups on Track II should play an important role in helping move the discussion on regional cyber cooperation forward. These discussions at Track II level should provide a non-threatening environment to discuss and informally advise the various governments on the development of policies, how to carry out or recommend capacity building activities, and to understand the constraints that each state face.

The formulation of the framework on ASEAN cyber cooperation needs to be a regional initiative that represents the ASEAN region. Singapore has in the past facilitated Track II discussions among academia, civil society groups, and industry groups from within and outside the region. Examples are the Global Commission on the Stability for Cyberspace (GCSC) and the Global Forum for Cyber Expertise (GFCE) to bring diverse views on how capacity can be built in cyberspace.

Paucity of Cyber Policy Discussions

Even so, the Track II discussions surrounding the Sydney Recommendations show that ASEAN member states tend to prioritise the building of technological capabilities such as infrastructural protection, threat detection and digital forensics; and place less priority on cyber policies and strategies. The paucity of cyber policy discussions at Track II level reflects this trend, and there is currently a capacity deficit in cyber policy research at Track II in ASEAN.

However, entities with more expertise, such as think tanks which are already working in this field, can contribute to building capacity in cyber policy at Track II for the region. If this is successful, Track II can support governments in creating the vibrant and stable cyber ecosystem laid out by ASEAN leaders.

Eugene EG Tan is Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.