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

RSIS COMMENTARY

www.rsis.edu.sg No. 106 – 28 May 2019

Cyber Security: Will There Be One ASEAN Voice?

By Shashi Jayakumar

SYNOPSIS

How far has ASEAN come in its cyber journey? What is the likelihood that it can begin to speak with one voice on cyber issues and what needs to be done before some coherence in an ASEAN approach to the norms debate can be expected?

COMMENTARY

ASEAN, THE common refrain goes, moves slowly, especially on sensitive issues that touch on sovereignty and security, where the pace of consensus-forming adjusts to fit the comfort level of the most hesitant member state. Nowhere is this more true than when it comes to cyber issues.

Member states approach cyber from various angles: telecommunications, internal security, information technology and law enforcement, to name a few. Consider the ASEAN Ministerial Conference on Cyber Security (AMCC) held in Singapore during International Cyber Week in September 2018: countries were represented by ministers or senior officials from a whole range of portfolios — cyber security (Singapore), communications (Malaysia, Laos, Brunei), digital economy (Thailand), information security (Vietnam) and home affairs (Cambodia).

AMCC: Key ASEAN Platform on Cyber?

Given the myriad lenses through which the issues are viewed, it is easy to underappreciate what ASEAN achieved over the course of 2018 in the cyber realm. The April 2018 leaders' statement on cyber security cooperation tasked relevant bodies to identify a concrete list of non-binding, practical norms of state behaviour.

The ministerial conference followed up in September, reaching an agreement in principle that international law, norms of state behaviour (with specific reference to the voluntary, non-binding norms recommended in the 2015 report of the UN Group of Governmental Experts on developments in information and telecommunications in the context of international security, or UN GGE for short), and practical confidence-building measures are essential for stability in cyberspace.

Some of these gains can trace their lineage directly to the roadmap of the 2017 ASEAN cyber security cooperation strategy, which had at its heart a focus on norms, cooperation and capacity-building.

The discussion platforms of choice also now seem to have resolved themselves. It is now clear that the AMCC will be the key ASEAN platform for discussing cyber matters. Other platforms — such as the ASEAN Regional Forum Inter-sessional Meeting on Security of and in the Use of ICT, and the ASEAN Defence Ministers' Meeting-Plus Experts' Working Group Meeting on Cyber Security — will be the critical forums for engaging external partners.

CERT: Computer Emergency Response Teams

A key facet of cyber cooperation, and one in which tangible progress is being made, is in upskilling, levelling up and knowledge transfer. There is an acute need for this given the differing levels of resourcing among members states. Myanmar's CERT, for example, had just five people in 2017. (A CERT is a national computer emergency response or readiness team.)

While CERT–CERT cooperation will remain to some degree behind the scenes, in the coming years we should expect to hear more on the progress of the ASEAN CERT maturity framework, which provides a common blueprint to assess the maturity of national CERTs. Other key mechanisms include the S$10 million ASEAN Cyber Capacity Programme (launched by Singapore in 2016), which aims to boost cyber security know-how across the region.

Under the programme's aegis, the Singapore–ASEAN Cyber Security Centre of Excellence will be launched in 2019. The centre will in turn presumably find ways to harmonise its efforts with the Bangkok-based ASEAN–Japan Cyber Security Capacity Building Centre, launched in September 2018.

Pressing Questions on Digital Futures

But beyond the high politics of cyber dialogue and the nuts and bolts of technical cooperation, there are pressing questions in terms of how ASEAN members view their digital futures. Many countries struggling with cyber attacks, fake news or disinformation campaigns may be remaking their regulatory regimes through the prism of cyber as a threat vector.

Vietnam's cyber security law, which took effect on 1 January 2019, is aimed ostensibly at preventing cyber attacks. It bans Internet users from spreading 'anti-state' information, and has been criticised by some observers as totalitarian. Thailand's

cyber security bill, which passed in February, has general clauses pertaining to the authorities' right to seize data and equipment.

The trifecta — viewing cyber from the perspectives of opportunity, data protection, and information control — is a source of continual tension. Nations need to be able to hold these tensions and to assess and act in a balanced way. If the balance is lost, countries might simply remake themselves in a more authoritarian way in order to protect themselves.

These tensions will inevitably affect states' positions when it comes to the debate on international cyber norms. ASEAN leaders have given a nod to the importance of the UN GGE norms, but there is a competing vision: an open-ended working group, sponsored by Russia, is also working within the UN to develop cyber norms.

Russian attempts to secure buy-in have been canny, referencing inclusiveness, and participation in norms-shaping. The working group may in the end be more attractive to many nations than the UN GGE simply because it seems to give more of a nod to countries' concerns about information security and fake news.

In Search of One ASEAN Voice

There are no easy answers, and discussions over coming months on, and in, the concurrent UN processes will say much. It should be observed here that Track 2 mechanisms for cyber, which seem to have taken something of a backseat in ASEAN, do have a role. Informal dialogues can allow member states to share challenges and ideas openly, and help to build shared understandings.

An example is the Council for Security Cooperation in the Asia Pacific, or CSCAP. Think tanks working on these issues can take the lessons from such meetings to inform and guide their stakeholders. And the field should not be limited to ASEAN nations. Think tanks further afield with well-thought-out cyber engagement strategies can, when they have knowledge of ASEAN states' concerns and sensitivities, play a useful role in the norms-shaping debate at the Track 2 level.

Member states now clearly want to have an ASEAN voice in the international cyber norms conversation. But how coherent or unified that voice will be likely is dependent on three things: an appreciation of internal cyber threats without being consumed by them; a nuanced awareness of the agendas and power plays within the international cyber norms debate; and a clear-headed drive to look to the best ideas in the field, whether they come from within or outside of ASEAN.

Shashi Jayakumar is Head, Centre of Excellence for National Security (CENS) and Executive Coordinator, Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.
This commentary first appeared in The Strategist, the online publication of The Australian Strategic Policy Institute (ASPI), on 22 May 2019.