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

RSIS COMMENTARY

www.rsis.edu.sg No. 174 – 22 October 2018

Next Steps for Cyber Norms in ASEAN

By Benjamin Ang

Synopsis

ASEAN has appointed Singapore to propose a mechanism to enhance ASEAN cyber coordination, and has also agreed in principle to certain voluntary norms of behaviour in cyberspace. This choice of norms gives clarity to the region's direction, especially while international discussions have stalled.

Commentary

THE RECENT announcement at the Singapore International Cyber Week 2018 (SICW 2018) that the Republic would propose a mechanism to enhance ASEAN cyber coordination highlights the group's willingness to chart a way forward on rules for state behaviour in cyberspace. Read together with ASEAN's renewed commitment to cyber norms, it also shows a new direction the region is taking.

The announcement was made by the ASEAN Ministerial Conference on Cybersecurity (AMCC), which agreed that Singapore would propose a mechanism to enhance ASEAN cyber coordination. This mechanism is intended to discuss cyber diplomacy, policy and operational issues.

Norms for State Behaviour in Cyberspace

This mechanism should involve cooperation between the private and public sectors and academia of the ASEAN Member States. AMCC also agreed to subscribe in-principle to the eleven voluntary, non-binding norms recommended in the lengthily-named 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security or UNGGE (hereafter referred to as "the eleven UNGGE 2015 norms").

In this context, norms are shared expectations, rules and guidelines outlining appropriate behaviour of states in cyberspace.

The eleven UNGGE 2015 norms include those against knowingly allowing one's territory to be used for internationally wrongful acts using ICTs; against conducting or knowingly supporting ICT activity contrary to international law that damages critical infrastructure; responding to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts; taking reasonable steps to ensure the integrity of the supply chain; and responsible reporting of ICT vulnerabilities.

These norms are essential for international stability. However, the UNGGE process stalled in 2017 without coming to consensus on how to implement the norms.

In the ensuing vacuum, a range of other actors including UNIDIR, The Hague Process, the G7, the Organisation of American States (OAS), and Global Commission on Stability in Cyberspace (GCSC), have continued to pursue initiatives to identify common norms for responsible state behaviour and operational measures to reduce risks of military escalation in cyberspace.

ASEAN and Regional Cybersecurity Norms

Regional organisations regard development of these norms as too important to wait for finality from the UNGGE, especially since history shows that the majority of cyber conflicts and misunderstandings occur between neighbours.

ASEAN Member States have also recognised the value of developing a set of practical cybersecurity norms of behaviour in ASEAN (AMCC 2016), and have supported development of basic, operational and voluntary norms, referring to the eleven UNGGE 2015 norms.

AMCC's present decision that Singapore should devise a framework for cooperation in ASEAN, and the reiteration of the eleven UNGGE 2015 norms, instead of any other set of norms being proposed around the world, indicates that the region has made its clear choice upon which to develop policies and operations for cyberspace, in the midst of numerous other options, some of which are compatible with their values, and of some which are not.

Focusing on the eleven UNGGE 2015 norms sets a clear objective for the region to work towards. ASEAN already faces other challenges including differences in levels of cyber maturity, policy priorities, levels of development and resources, without having to grapple with reaching agreement on an ever-increasing set of cyber norms.

Singapore's Role

The clarity of choice of norms is especially important as there have been rumblings that the UNGGE process will be reconvened. Participants at the GCSC meeting during SICW 2018 discussed the strong possibility of a reconvened UNGGE developing

cyber norms in 2019, as well as the possibility that the UNGGE would consider norms proposed by Russia.

This is surprising because one fundamental difficulty has been the lack of agreement over what constitutes cyberspace with respect to state interests. Countries like the United States and Japan (and Singapore) define this domain as the technology (hardware, software) that allows free access to cyberspace, while countries like China and Russia define it as the content and interactions (speech, expression) between the users of cyberspace.

This difference is believed to have led to the failure of the UNGGE process in 2017. Since this fundamental disagreement has not been resolved, observers are justifiably sceptical that the UNGGE process will be able to resume, and even if it resumes, that it will be able to reach consensus any time soon.

Therefore, Singapore and ASEAN should not wait for UNGGE to be reconvened, much less wait for a fresh consensus to be reached. A future UNGGE will take time to reach consensus on norms, and if there are additional norms to be agreed, those can be considered further down the road. In the meantime, the eleven UNGGE 2015 norms are a clear framework for AMCC to work upon.

Since AMCC has given Singapore this role, there should be no delay. The region now has the opportunity to shape cyber norms in ways that correspond to ASEAN member states' needs and contexts, and can take the proactive role instead of waiting for larger states to dictate the rules of the road.

Benjamin Ang is a Senior Fellow is the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.