RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No. 017 – 15 November 2021

No. 017/2021 dated 15 November 2021

The Potential and Way Forward for Greater Regional Cybersecurity Cooperation

Eugene E. G. Tan and Shawn Ho

What can Singapore do to prevent cyber threats from running rings around regional cyber capabilities?
Photo by FLY:D on Unsplash.

SYNOPSIS

What role can Singapore, as chair of the new United Nations Open-Ended Working Group (OEWG), and Track 2 platforms play to help develop rules, norms and principles of responsible state behaviour in cyberspace?

COMMENTARY

There were two consistent messages that Singapore gave at the Singapore International Cyber Week (SICW) and the Singapore Defence Technology Summit (SDTS) in October 2021: first, in pushing for the implementation of norms and international law to ensure responsible state behaviour in cyberspace; and second, the need for cooperation for this to happen.

This urgent need to develop rules, norms and principles of responsible state behaviour in a collaborative manner resulted in the establishment of a second round of the Open-ended Working Group on security of and in the use of information and communications technologies from 2021 to 2025, even before the first OEWG had ended. A robust set of norms, rules and international laws is required to ensure a rules-based order is present in cyberspace as is the case in the physical realm.

Broad-based support for a rules-based order in cybersecurity is also reflected by the recent OEWG and United Nations Group of Governmental Experts (UNGGE) reports that were approved by consensus in March and August 2021 respectively. The latest UNGGE report also highlighted threats against critical infrastructure as the major concern area in Information and Communications Technology (ICT) that states should focus more on.

Of course, no state can implement and enforce norms and international law on their own. This means that states require greater international cooperation and collaboration for better management of cyberspace, and to tackle the threats posed by cyberattacks. In the case of Singapore for instance, it has made some progress on those fronts through its signing of memoranda of understanding on cyber cooperation with the United States, Estonia and Finland respectively in the past few months.

With the election of Singapore's Permanent Representative to the UN as chair of the new OEWG in June 2021, it is important and timely to assess the role that Singapore and Track 2 platforms can play to help develop rules, norms and principles of responsible state behaviour in cyberspace.

Collaborative Efforts in the Region and Beyond

As OEWG chair, Singapore can make a stronger push to promote cyber diplomacy among states at the international level through existing institutions, like the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and the ASEAN Ministerial Conference on Cybersecurity (AMCC). Singapore can initiate more cooperation among states both in the region (by working more closely with the ASEAN member states) and beyond by steering the agenda for building responsible behaviour in cyberspace, through the implementation of norms and international law, capacity building and confidence building measures, by leveraging on these institutions.

Conducting capacity building will help deepen understanding on the obligations and responsibilities of states in ensuring cybersecurity both domestically and internationally, and in doing so, build confidence that states in the region can be relied

upon in a cyber incident. Garnering regional cooperation on cybersecurity should not be difficult as there is already substantial interest among ASEAN member states to cooperate on cyber issues. ASEAN ministers have already stated at the 1st ASEAN Digital Ministers' Meeting in January 2021 that "enhancing cybersecurity cooperation is key to the security of our future economy and digitalisation initiatives especially in view of the recent rise of global cybersecurity and supply chain attacks and threats".

Building Greater Intra-governmental Cooperation

There is also a need for ASEAN member states to build greater intra-government cooperation in order to achieve a whole-of-government (and consequently a whole-of-ASEAN) approach to cybersecurity. Currently, the development of cybersecurity capacity in the region appears to be done through a sectoral approach rather than an aggregation of whole-of-government approaches from ASEAN member states.

This is especially true with military use of cyber capabilities. The creation by the ASEAN Defence Ministers' Meeting (ADMM) of two new institutions dealing with cyber issues, namely the ASEAN Cyber Defence Network (ACDN) and the ADMM Cybersecurity and Information Centre of Excellence (COE), is a good example in showing how the cooperation effort can potentially be fragmented into sectors. These institutions primarily focus on the role of the military in defending against cybersecurity threats, and how militaries can cooperate with one another when such situations arise.

What is unclear however is how these new institutions will interface with civilian agencies as well as with other ASEAN and international processes. While the COE has signalled that it will cooperate and coordinate with the ASCCE, there is a concern that cyber cooperation among ASEAN member states might become too narrowly defined in terms of the military-security complex.

To avoid this scenario, militaries should be encouraged to work with their civilian agencies in dealing with cyber threats, and they should be more forthcoming in terms of how norms and international law will govern their cyber operations.

The Role That Track 2 Can Play

Singapore can also foster greater contributions from non-governmental organisations (NGOs). The final reports of the UNGGE and OEWG recognised the need for greater NGO participation in the discussions on the governance of cyberspace. NGOs in ASEAN should be encouraged to join the discussion.

To this end, existing Track 2 dialogue mechanisms in the region such as the Network of ASEAN Defence and Security Institutions (NADI) and the Council for Security Cooperation in the Asia Pacific (CSCAP) can play a bigger role in providing policy recommendations and advice to Track 1. This will help address the paucity of voices from the region.

NADI and CSCAP can be tapped as platforms for non-governmental experts to share and highlight different views that may be overlooked at the Track 1 level. These Track 2 platforms can also help provide a neutral space to discuss the concerns of states that do not wish to take sides in the governance of cyberspace. This will add value to

the intergovernmental processes and fulfil the mandate to solicit views from all states regarding cybersecurity issues.

There should also be greater impetus for Track 2 to be more involved in academic discussions on international law and norms. For instance, CSCAP has completed a study group on international law and cyberspace although there is still much to discuss in terms of how international law applies to cyberspace. Getting involved with the *Tallinn Manual on the International Law Applicable to Cyber Operations* is a good place to start. Work on a third edition of the *Tallinn Manual* reflecting state practice on cyber operations and positions on international law has begun, and it is expected to take about five years to complete.

Conclusion

In conclusion, states need platforms, the trust and the confidence to discuss these important cyber issues with one another, and it is in Singapore's interest as chair of the OEWG to facilitate this process. Cyberattacks are inevitable and there are always lessons that can be learnt from each episode, such as how to enhance cyber resilience and create better systems to manage these incidents. This will further enable states to have the confidence to adopt and reap the benefits of digitalisation despite the risks of cyberattacks such as through ransomware and supply chain attack.

Ultimately, it is only through greater and regularised international cooperation efforts that progress can be made towards the establishment of international norms, rules and laws in governing cyberspace. Singapore should endeavour to work towards this cyber future that will be beneficial to all users of cyberspace.

Eugene E. G. TAN is an Associate Research Fellow at the Centre of Excellence for National Security (CENS) at RSIS. Shawn HO is an Associate Research Fellow at the Regional Security Architecture Programme at the Institute of Defence and Strategic Studies (IDSS), RSIS.