SECURITY NEXUS
A free, open access, international, peer-reviewed, online publication for the Daniel K. Inouye Asia-Pacific Center for Security Studies faculty and alumni.
apcss.org/nexus

ASEAN AND CYBER

By Elina Noor, Assoc. Prof., DKI APCSS

On the same day that Kim Jong Un stepped over the demarcation line at Panmunjom to shake the hand of a smiling Moon Jae-in, the 32nd ASEAN Summit released three forward-looking outcome documents focused on the future of Southeast Asia: the ASEAN Leaders' Vision for a Resilient and Innovative ASEAN; Concept Note for an ASEAN Smart Cities Network; and the ASEAN Leaders' Statement on Cybersecurity Cooperation. These were understandably overshadowed by the historic inter-Korean summit but the success and efficacy of ASEAN meetings and statements have also largely come to be judged by the acrobatic verbiage of the grouping's communication on the South China Sea. This is unfortunate.

The three documents outline ASEAN's determination to embrace the digital world and to bank on inter-connectedness despite the economic, social, political, and cultural differences within and among all 10 member states. They extend the regional aspiration of community-building to the digital infrastructural platform and will presumably complement existing initiatives like the Masterplan on ASEAN Connectivity, which has itself been reviewed and renewed for the next milestone of 2025.

With projections of Southeast Asia becoming the fastest growing internet region from 260 million netizens to nearly half a billion users by 2020, ASEAN recognizes that the precepts of prosperity, peace, and stability underlying relations among member-states and dialogue partners will increasingly lie as much in the cyber as in the kinetic domain. In this regard, of the three documents, the ASEAN Leaders' Statement on Cybersecurity Cooperation ("Leaders' Statement") is arguably the most telling.

The Statement points to member states' maturing awareness of cybersecurity as a multi-stakeholder, "cross-cutting issue" requiring international policy and capacity building frameworks. Crucially, the Statement underlines the promotion of voluntary and non-binding cyber norms as well as a resilient rules-based cyberspace reaffirmed by the applicability of international law, particularly the United Nations Charter, in order to maintain peace and stability and to promote an "open, secure, stable, accessible and peaceful" information and communications technology (ICT) environment. The nod to this strategic angle of cybersecurity articulated in the language of economic growth is a far cry from the early days of the mid-1990s when ASEAN, not yet a membership of 10 countries then, met to "discuss appropriate responses to the Internet." Over the decades, the grouping's attention to cyberspace has oscillated from plugging its ten members into the global networked economy to form an "e-ASEAN" to capacity-building, cyber crime and terrorist use of the Internet.

To be sure, these all remain priorities for ASEAN, especially the prospect of economic growth through digital means along with its attendant challenges. The preamble of the Leaders' Statement posits from the beginning that a peaceful, secure and resilient regional cyberspace should serve as an "enabler of economic progress, enhanced regional connectivity and betterment of living standards for all." It goes on to mention the potential of the cyber domain for "significant regional economic and technological development" and as "a significant source of employment." Thus, the primary lens through which ASEAN views cyberspace is economic since development and prosperity are precepts for peace, security, and stability in the region.

Within the last five years, however, spurred in part by the UN Group of Governmental Experts (UN GGE) process and calls from within Track Two, official rhetoric among ASEAN leaders has evolved from truisms about the importance of cybersecurity to tentative but promising steps towards establishing a code of conduct of sorts in cyberspace that will be applicable to states, first and foremost, but also include the indispensable role of industry and other non-state actors. The Leaders' Statement builds upon earlier, similar statements delivered within and beyond the ASEAN context, and demonstrates a maturing realization among ASEAN leaders that the region needs to play a more active role in the evolving debate on norms of behavior in cyberspace.

The leadership of Singapore in ASEAN has been an important catalyst in furthering the regional discussion. In 2016, it committed money to talk, launching a SGD10 million ASEAN Cyber Capacity Programme and hosting the first ASEAN ministerial meeting on cybersecurity. Multiple shades of the Chairman's Statement of the 2nd ASEAN Ministerial Conference on Cybersecurity in Singapore in 2017 color the preamble of this year's Leaders' Statement.

Unsurprisingly, there is also caution built into the Leaders' Statement. Although ministers are tasked to identify a "concrete list of voluntary, practical norms of State behavior in cyberspace," reference is made to the non-binding nature of those norms. This conveniently accords with ASEAN's tempered, incremental approach to matters of peace and security. The document also holds that state sovereignty applies to state conduct of "ICT-related activities" and reinforces state "jurisdiction over ICT infrastructure within their territory." These are completely defensible according to international legal principles and were reflected in the 2015 UN GGE report. At the same time, they echo very real concerns – past and contemporary – about the risk of interference or intervention in a state's internal affairs.

Finally, the Leaders' Statement is also notable for what it does not say as much as what it does say. While the document explicitly underscores state sovereignty in cyberspace, it does not address the role of the private sector which arguably equates to, if not eclipses, that of the state in some respects in the cyber domain. No doubt, the primacy of the state is to be expected in a leaders' statement but the traditional roles of the public and private sectors are uneasily – and sometimes inversely – placed in cyberspace, and must be addressed.

The Leaders' Statement also affirms international law and "the eventual development of a rules-based cyberspace" yet leaves open ended how international law might specifically apply, what kinds of rules might eventually govern cyberspace, and who might influence the shaping of those rules.

The first question stymied the 2017 UN GGE and, consequently, resulted in a near-existential and still unfolding crisis for the future of the norms debate. The second and third questions are also being hotly contended. There is now a Cold War-like cleavage in discussions on a rules-based cyberspace, where sheer political power and influence are couched in the language of international law. This is not new, of course, simply that it is being played out in a different and nebulous domain. As the world's major powers battle for a technological edge, if not for outright superiority, the existing rules-based order in cyberspace and other kinetic domains may well be upended and rewritten.

ASEAN's entry into this debate is timely and encouraging. It must remain engaged with the major powers – its dialogue partners – currently contesting cyberspace and carve out a role for itself while remaining relevant in an increasingly muscular geopolitical landscape. In other words, it must be prepared to do what it has always done only much, much faster.

Ms. Elina Noor ***is an associate professor at the Daniel K. Inouye Asia-Pacific Center for Security studies. The views expressed in this article are those of the author and do not reflect the official policy or position of APCSS, the U.S. Department of Defense, or the U.S. government.***

-END-

The views expressed in these articles are those of the author and do not reflect the official policy or position of DKI APCSS, the U.S. Indo-Pacific Command, the U.S. Department of Defense, or the U.S. government.

May 2018