PACIFIC FORUM

Key Findings
United States-Singapore Cyber & Tech Security Virtual Series
Session #2: Indo-Pacific Perspectives on the Application of International Law and Norms in Cyberspace

December 17, 2020 (US) | December 18, 2020 (Singapore)

On December 17, 2020, with the support from the US Embassy Singapore, the Pacific Forum hosted "Indo-Pacific Perspectives on the Application of International Law and Norms in Cyberspace," with over 60 participants from governments, private sector, academia, and non-governmental organizations. This was the second public session in the United States-Singapore Cyber&Tech Security Virtual Series.

Debra Decker, Senior Advisor at the Stimson Center; Elina Noor, Director of the Political-Security Affairs and Deputy Director, Asia Society Policy Institute; and Eugene Tan, Associate Research Fellow at the S. Rajaratnam School of International Studies, examined ongoing debates over the development of norms and the application of international law in cyberspace, current capacity-building and confidence-building initiatives in ASEAN, and the roles played by the US and Singapore in norm-building and technical capacity assistance in Southeast Asia.

Key findings from this meeting are described below.

The Application of International Law and Norms in Cyberspace

Globally, the development of cyber norms, laws, and treaties has been challenging given the lack of strong leadership at the multilateral level and differing priorities and actions of individual states. There is a pressing need to unpack issues underpinning cybersecurity from the points of view of individuals, businesses or organizations, and states. From here, each stakeholder can identify its options to manage risks, for example, by mitigating intentional threats for states via attribution, prosecution, and sanctions; reducing vulnerability to harms such as by requiring Codes of Conduct and standards of compliance among Information and Communications Technologies (ICT) companies; and increasing resilience against cyberattacks.

Currently, there are overlapping efforts at the United Nations. Two notable processes include the UN Group of Government Experts (GGE), initiated by the US and comprising 25 nation states from various regions. The UN GGE has pioneered the international conversation on cybersecurity, particularly on norms and confidence-building measures. The second is the Russian-led UN Open Ended Working Group (OEWG), which embraces a multi-stakeholder approach with members from all states as well as the private sector, academia, and civil society organizations. The healthy mix of participants within the UN OEWG aids diversity and transparency. Singapore chaired some of the intersessional panels at the UN OEWG.

There is potential to build cyber norms based on the early efforts of the UN GGE as well as existing agreements such as the Budapest Convention on Cybercrime, which addresses Internet and computer-related crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations; and the Tallinn Manual 2.0, which examines the application of existing international law to cyber operations.

About forty states have proposed that a Programme of Action be developed similar to the one that was developed to help states address illicit trade in small arms. This proposal aims to integrate the dual-track discussions of the UN GGE and OEWG into a single, inclusive, and long-term UN forum, focusing on the implementation of responsible use of ICT among states in the context of international security, among other things.

Southeast Asia has only generally affirmed the application of international law in cyberspace. The region's actors share a concern that international law can be leveraged by powerful state actors to pursue their own ends at the expense of others. International law has often been used to justify military or kinetic action. Wary of such precedents, various Southeast Asian countries have expressed concerns about related developments in the cyber domain. These countries emphasize the values of active and equal participation, multilateralism, consensus-building, dispute settlement, and peaceful use of ICT.

There is also concern that Southeast Asia is at the heart of a geo-technological contest in which international law is being used as a weapon. This concern is evident in how the region views the UN GGE and UN OEWG. Southeast Asia considers the harmony and coordination of the two processes to be important, but the underlying tendency of both processes to contradict one another must be resolved. The region hopes that the parallel processes should complement one another to succeed and deliver meaningful outcomes. Fortunately, there has been coordination and overlap between both processes, a result of deliberate effort by the chairs of the GGE and OEWG. Nevertheless, there are indications that tensions underlying the two tracks remain unresolved. In November 2020, the UN First Committee was faced with a vote of two competing draft resolutions related to the future of the OEWG and the GGE. Malaysia suggested that a better solution would be a single proposal that could garner endorsements from all the UN Member States.

With two competing proposals from the UN processes, Southeast Asia has three main apprehensions about the future of the processes. First involves the nexus between law, politics and power. Although the tendency is to consider international law "neutral," extralegal considerations such as political relations, historical context, and national interest are embedded in legal processes.

The second apprehension is related to the attribution problem, i.e., the challenge in accurately identifying and "naming and shaming" perpetrators of cyber-attacks due to technical, legal, and political difficulties. Attribution is ultimately a political call that relies on the law as a supporting character. There remain numerous outstanding legal considerations related to evidentiary burden, methods of proof surrounding cyberattacks, types of legal tests to assess state responsibility, and what recourse victim states have in the event of an attack.

Southeast Asia's third apprehension is that although the application of international law to cyberspace is a very important one, the main priority for Southeast Asia is on the ground. The region has a granular agenda of leveraging cyberspace for development, or what may be called "developmental digitalization." There is a mismatch in priorities, which translates into a lag in political or policy attention as well as insufficiently allocated resources to more strategic considerations of cyberspace. Thus, it is important for Southeast Asian countries to critically reflect on their priorities and interests rather than make the mistake of importing models just to get up to speed with the application of international law in cyberspace.

External Partners on Cybersecurity

ASEAN has participated in interregional cooperation mechanisms, such as the Organization of American States, which serve as a critical venue for ASEAN to learn from other developing economies about capacity-building and confidence-building measures. The development priorities among developing states should be integrated into confidence-building mechanisms to address vulnerabilities.

Aside from the US, ASEAN has reached out to external partners such as the EU, Japan, and Australia to augment its urgent need for more technical and policy assistance. Some ASEAN member states such as

Myanmar do not have adequate technical personnel, and some countries in the region continue to lag when it comes to Internet access. The region is therefore in dire need of more infrastructure and capacity-building to manage cyberspace risks.

US-ASEAN and US-Singapore Cooperation: Challenges and Opportunities

The current state of US-ASEAN and US-Singapore Cyber cooperation is currently shaped by three factors: the increasing competition for influence among great powers in the region; the lack of US diplomatic efforts; and the differing needs among ASEAN member states for capacity-building and confidence-building measures.

Although the US has initiated technical and policy initiatives, concrete progress has been slow. The US-ASEAN Cyber Dialogue is a broad discussion and presents no specific plan of action. Following the ASEAN Regional Forum (ARF) Seminar on Operationalizing Cyber Confidence Building Measures in 2015, meaningful discussions have stalled.

Capacity-building initiatives such as the ASEAN-Japan Cybersecurity Cooperation Hub based in Bangkok and the ASEAN-Singapore Cybersecurity Center of Excellence are continuing to improve policy and technical know-how among ASEAN member states. The US can partner with these Centers to better understand threats and reach a common understanding of emerging cyber issues.

Strengthening confidence-building measures in ASEAN is vital in building trust and confidence in cyberspace. The US can lead coordination at the state-to-state level and with industry. Confidence can be built by improving individual members' capacity, thus enabling ASEAN to operationalize norms of responsible state behavior, deal with cyber incidents, cooperate with other state cyber agencies, provide timely cyber threat information, and perhaps develop cyber attribution capabilities. Effective capacity-building and confidence-building measures in ASEAN require continuous engagement to keep abreast with the latest developments in the cyber threat landscape. The fundamental aim is for ASEAN member states to build a cybersecurity ecosystem where each member state has the ability to participate in threat information-sharing and threat response so they can tackle common cyberspace problems and challenges.

The creation of a Cyber Points-of-Contact Directory was broached at the ARF in 2014. Australia proposed a similar mechanism to the ARF that is currently awaiting approval from the wider community. Establishing a directory will enable states to consult each other and minimize miscalculation in times of strategic tension. Overall, confidence-building and capacity-building measures in ASEAN require partnership and cooperation. The US can play a role by beefing up its current technical and policy guidance. In doing so, it must pay attention to the needs of ASEAN member states and premise cooperation on mutually beneficial goals.

The majority of ASEAN member states have limited cyber capabilities, which leaves them incapable of achieving deterrence. Although member states can pursue diplomatic means as a form of "countermeasure," investments in both technical and human capacity should remain top priorities. In the grand scheme of issues relating to international law, cybersecurity, and the potential bifurcation of norms and values based on the imminent balkanization of the Internet, ASEAN should regroup and consolidate its own position.

This document was prepared by Mark Manantan and Eugenio Benincasa. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Director of Nonproliferation, Technology, and Fellowships at Pacific Forum. These preliminary findings provide a general summary of the discussion. This is not a consensus document. The views expressed are those of the speakers and do not necessarily reflect the views of all participants. The speakers have approved this summation of their presentation.