Key Findings
United States-Singapore Cyber & Tech Security Virtual Series
Session #1: Cybersecurity Threats and Cooperation in the Indo-Pacific

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

On November 17, 2020, with the support from the US Embassy Singapore, the Pacific Forum hosted the first public session, joined by over 70 individuals, of a series of virtual discussions entitled "United States-Singapore Cyber&Tech Security Virtual Series."

Benjamin Ang, Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), and Cristin Goodwin, Assistant General Counsel at Microsoft, discussed cyber threats in the Indo-Pacific region, the challenges and opportunities encountered by governments and the private sector to fortify their cyber defenses, and the role played by the US and Singapore in enhancing regional cybersecurity.

Key findings from this meeting are described below.

Cyber Threats in the Indo-Pacific

Cybercriminals are the most common threat susceptible devices, data, or networks. However, state-sponsored cyberattacks are particularly worrisome due to the sophistication of their tactics, techniques, and procedures (TTP). Nation-states' TTPs provide cybercriminals, politically motivated activists (hacktivists), and opportunistic insiders with the know-how and resources to develop the similar capabilities. Most state-sponsored cyberattacks originate from Russia, China, Iran, and North Korea.

Nation-states are particularly good at exploiting existing vulnerabilities. Most of the time, when a computer is compromised, a patch is already available but not installed. It is therefore critical to raise awareness among end users about the importance of cyber hygiene (frequent patching, multi-factor authentication, etc.).

Addressing ransomware attacks to critical infrastructure will become a global priority. In addition, the proliferation of Internet of Things (IOT) devices will create new vulnerabilities, increasing points of access for malicious actors and exposing people to new threats. Malicious actors will increasingly use Artificial Intelligence (AI) technology to exploit vulnerabilities, allowing non-state actors to build sophisticated capabilities that would traditionally solely be held by nation-states. The proliferation of these cyber offensive capabilities could affect the cyber balance of power, blurring the lines between state and non-state actors.

Nation-states have the resources to do reconnaissance on their victims and select the attack method that best suits their goal or intended outcome. These methods include password spraying, social engineering, phishing, identity spoofing, malware, and denial of service. Advanced Persistent Threats (APTs) – prolonged and targeted cyberattacks that are usually employed by nation-states or large groups – are typically aimed at organizations in sectors that deal with high-value information, such as national defense and intellectual property.

Common operational aims include espionage, reconnaissance, information operations, and disruption and destruction of network systems. In the Asia Pacific, strategic goals include interfering with elections, supporting protest movements, and promoting individual politicians and businesspeople.

Cybersecurity Measures: Challenges and Opportunities

Organizational culture is critical in the context of insider threats, determining how often patches are installed, whether employees report security incidents, and management's response.

Companies that are victims of cyberattacks are often reluctant to publicly report or share details of incidents, making it difficult to develop mitigation measures. They fear sharing details could harm their reputation and consumer perception. It is therefore critical to build a culture in which companies feel comfortable sharing incident-related information.

It is challenging to verify the identity of an actor in cyberspace, making attack attribution very difficult. Nonetheless, cyber actors are often small groups of people whose operational patterns can be recognized. The most reliable attributions are made by governments because they have the legal authority to intrude into malicious actors' networks.

Trust is key for effective public-private collaboration, especially when it comes to information-sharing. Trust could be enhanced by wider adoption of vulnerability equities processes (VEP) and by extending transparency across the whole cybersecurity ecosystem, including information about malicious actors' TTPs.

Regional actors have adopted different countermeasures to mitigate the impact of information operations, such as restricting foreign funding of political parties, educating the population on critical thinking, enacting relevant legislation, establishing fact checkers, and promoting self-policing by social media platforms. Yet these countermeasures come with their own challenges. For instance, restrictions on foreign funding and the enactment of ad-hoc legislation can have the unintended consequence of suppressing criticism. There are also concerns over the independence of fact-checkers, the standards tech platforms would adopt for self-policing, and the difficulties in educating mobile-only populations on critical thinking.

Singapore's role in enhancing Regional Cybersecurity

Singapore has signed bilateral Memorandums of Understanding (MOUs) with Canada, France, India, the Netherlands, the US, and others to enhance cybersecurity cooperation.

Singapore has allocated US$21.9 million over a five-year period to fund the ASEAN-Singapore Cybersecurity Centre of Excellence for capacity building in the Association of Southeast Asian Nations. From 2016 to 2019, ASEAN has made important progress in the development of regional cybersecurity norms of behavior and has agreed to move forward on a formal cybersecurity coordination mechanism. In October 2020, Singapore announced it will collaborate with the United Nations to draw up a checklist of steps to implement cyber norms supported by ASEAN's experience and knowledge. Moving forward, there are many opportunities to strengthen confidence-building measures and enhance capacity building in ASEAN.

The US and Singapore have a shared commitment to a rule-based world order in cyberspace through their collaboration at the United Nations. As mentioned previously, the two countries have also signed a bilateral MOU for cybersecurity cooperation. Nonetheless, there has been no US Ambassador to Singapore and no top-level US participation at an ASEAN Summit since 2017. Besides addressing these diplomatic matters, cooperation between the US and Singapore could be strengthened on various fronts. These include enhancing information-sharing between the two countries and capacity-building cooperation, in particular on national Computer Emergency Response Teams (CERTs) and small-medium enterprises' cyber hygiene. The US and Singapore could also collaborate on finding innovative solutions to address specific threats, such as ransomware attacks.

This document was prepared by Eugenio Benincasa and Mark Manantan. 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 presentations.