Key Findings
United States-Singapore Cyber & Tech Security Virtual Series
Session #4: US-Singapore Perspectives on
Enhancing Critical National Infrastructure Cybersecurity
February 4, 2021 (US) | February 5, 2021 (Singapore)

On February 4, 2021, with the support from the US Embassy Singapore, the Pacific Forum hosted "US-Singapore Perspectives on Enhancing Critical National Infrastructure Cybersecurity," with 35 participants from government, private sector, academia, and other non-governmental organizations. This was the second of two closed-door sessions in the United States-Singapore Cyber&Tech Security Virtual Series.

Ms. Boyden Rohner, Associate Director for Vulnerability Management, U.S. Cybersecurity and Infrastructure Security Agency; Mr. Lim Thian Chin, Director of the Critical Information Infrastructure Division, Cyber Security Agency of Singapore; and Professor Lam Kwok Yan, Director, Nanyang Technopreneurship Center and Professor, School of Computer Science and Engineering, Nanyang Technological University, examined the different mechanisms that the US and Singapore have established to enhance the security of critical national infrastructure (CNI) by improving cyber incident response capabilities and information sharing.

Key findings from this meeting are described below.

U.S. Cybersecurity and Infrastructure Security Agency (CISA)

CISA was established in 2018 as a standalone U.S. federal agency, an operational component under the oversight of the Department of Homeland Security (DHS). It is considered the nation's “risk advisor” in leading country-wide cyber resiliency efforts. Among CISA’s most important goals is the implementation of the DHS National Infrastructure Protection Plan (NIPP) 2013, which governs how government and private sector participants in the critical infrastructure community work together to manage risks and achieve cybersecurity and resilience outcomes.

Public-private partnerships (PPPs) are essential for effective cyber resilience since no single entity can claim all the information, knowledge, and capabilities needed to contain threats on a large scale. CISA has identified 16 critical infrastructure sectors, including energy, communications, emergency services, etc., whose assets, systems, and networks are considered vital to the basic functioning of American society. In 2019, CISA’s strategic approach to critical infrastructure has evolved to include National Critical Functions (NCFs) for the government and private sector that are considered essential for the U.S. economy, the health of its citizens, and its national security. NCFs transcend specific infrastructure assets or organizations and focus instead on how entities could come together to provide essential services.

CISA lies at the intersection of the intelligence community, private sector, local governments, and international partners, allowing it to bridge different communities and facilitate information-sharing through relevant mechanisms. With regard to the services it renders to critical infrastructure owners and

operators of the federal government, CISA plays a key role in raising awareness of imminent threats. Its ultimate goal is to reduce the attack surface by increasing defenders' resilience through the promotion of better security practices--such as zero trust architectures and security by design--and improved incident response capabilities. Since the outbreak of the Covid-19 pandemic, CISA has helped identify those who qualify as essential workers within national critical functions to determine who should continue to work in-person and who should work remotely.

Singapore's Cyber Security Agency (CSA)

The Cyber Security Agency of Singapore (CSA) provides oversight in protecting Singapore's critical national infrastructure. It is a government agency of Singapore nominally under the Prime Minister's Office, managed by the Ministry of Communications and Information (MCI). CSA is headed by the Cybersecurity Commissioner. CSA has identified 11 critical infrastructure sectors, which are headed by sectoral regulators who work to strengthen cybersecurity resilience.

To enhance national cybersecurity preparedness, the Singapore's Cybersecurity Act (2018) has led to the implementation of a regulatory framework setting common standards across the 11 critical infrastructure sectors. Significant effort is also being made toward the establishment of strong PPPs. In addition, CSA is working toward the harmonization of policies and auditing practices to facilitate cooperation and enhance overall resilience. To this end, each critical infrastructure sector is tasked with formulating a detailed plan that articulates its approach to defending critical functions, such as specific threat alert levels. To achieve effective response, coordination between relevant stakeholders is fostered during peacetime. CSA has established comprehensive cooperation mechanisms, such as joint training and exercises to facilitate information-sharing between different entities and to encourage teamwork between the public and private sector. These joint exercises include both national-level and sectoral crisis simulations. At the global level, Singapore has also conducted an international cyber exercise with Israel focused on the energy sector in 2018.

Despite no major cyber incident over the past year, the outbreak of the Covid-19 pandemic has led to new considerations regarding Singapore's approach to cybersecurity. First, the pandemic has increased people's reliance on digital infrastructure, leading to a reconfiguration of what services are considered essential. Cyberspace has now become the epicenter of economic and social life and new policies must be developed accordingly. Second, high connectivity has led to increased interdependence between organizations and supply chains, increasing the attack surface. This new environment creates risks of dangerous data breaches, as demonstrated by the recent SolarWinds attack. Securing the supply chain remains an arduous task as vulnerabilities are inherent in complex software or hardware designs. To address these and other threats, it is important to shift the current approach from a compliance-based to a threat-based mindset, tailored to particular cybersecurity enterprises. Such an outlook will raise awareness of evolving threats, allowing organizations to prepare accordingly rather than simply abiding by government regulations.

Artificial Intelligence (AI) for Threat Analysis

Security mechanisms for critical infrastructure systems span a broad range of technologies. Research and development (R&D) efforts focus on enhancing entity authentication, physical security, access control, encryption, and monitoring to enhance the safety of critical systems and collect valuable information on attackers and common attack patterns. Cross-border cyber intelligence information-sharing between different organizations plays a key role in this process.

In particular, valuable information is useful to develop AI analytical tools that can analyze cyber threat intelligence autonomously, reducing the workload of cybersecurity professionals. While collecting relevant information is essential, analyzing too much information can prove to be impossible. By leveraging AI-powered platforms trained to identify threat patterns and specific characteristics of malwares, analysts can optimize their workload to identify which information they should prioritize. This is highly important to attain preparedness as well as for the timely development of informed response measures.

Nanyang Technology University in Singapore is currently conducting R&D to enhance the effectiveness of cybersecurity operations. In collaboration with Singapore's CSA and industry leaders, such as FireEye, ongoing R&D seeks to optimize the collection of traffic data, attacker profiling, and information-sharing between relevant organizations. To this end, key AI-enabled tools include document analytics and auto-summarization for reading a large amount of cyber threat intelligence reports, summarizing the content, and tagging to support future analysis and research. Summarized reports also contain autonomously-generated graphs and relational models, including the main features of incoming threats. It was noted that these AI-enabled tools are only complementary and do not replace human analysts, whose experience and judgement are still essential.

Building trust

Building trust is essential for the effective functioning of PPPs. To this end, perseverance is key to overcome the cultural differences found across different organizations, such as technical language and procedures. Empathy can make an important difference in this regard, allowing for the understanding and analysis of shared problems as seen from another party's perspective.

To enhance trust, Singapore's CSA has adopted a system that allows regulators to rotate across different sectors--including both public and private entities--allowing them to experience different contexts. CSA also seeks to set up an environment that is conducive to information-sharing across different entities, underscoring the importance of living up to reciprocal expectations by handling other parties' relevant information responsibly and ethically. Finally, cooperation between the private and public sector should not be limited to compliance or cyber incident response. It is particularly important to enhance cooperation in peace time to solve common daily problems. Both the US and Singapore should further prioritize the inclusion of the private sector in their respective national cybersecurity and resiliency policies given the private sector's major ownership and control of critical assets.

The issue of trust is also relevant vis-a-vis the data that is received or analyzed through AI-enabled tools. Data has to be carefully reviewed and prepared for algorithm training to produce accurate results. To enhance trust with respect to supply chains, it is essential to enhance capabilities such as detection technology to limit intrusions in key parts of critical systems and adopt stringent measures and procedures to defend against threats coming from trusted sources.

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.*