PACIFIC FORUM

Key Findings
Adapting to COVID-19: Indonesia, the United States, and the Indo-Pacific
Session #2: Assessing Cybersecurity Trends and Threats in the US and Indonesia
March 29, 2021 (US) | March 30, 2021 (Jakarta)

On March 29, 2021, with support from the US Embassy in Jakarta and in cooperation with the Centre for Strategic and International Studies (CSIS) Indonesia, Pacific Forum hosted a webinar entitled "Assessing Cybersecurity Trends and Threats in the US and Indonesia," with 124 participants from government, private sector, academia, and other non-governmental organizations. This was the second session of the virtual forum series "Adapting to COVID-19: Indonesia, the United States, and the Indo-Pacific."

COVID-19 and cyber (in)security

Over the course of the pandemic, the techniques, tactics and procedures used by cyber criminals have evolved. Cyber criminals have recalibrated their approaches by leveraging cloud services and exploiting the uncertainty brought by the global pandemic. Microsoft's Digital Crimes Unit (DCU) has identified the uptick of cyber crime activities during the pandemic classified under six categories: (1) business email compromise, (2) fraud, (3) malware, (4) ransomware, (5) child exploitation, (6) tech support fraud, and (7) business operation integrity.

Well-resourced cyber criminal syndicates launched malware attacks through armies of infected computers to profit from the socio-economic uncertainty caused by the pandemic. Relatedly, ransomware, a low-cost and high-profit yielding criminal activity, shifted from targeting institutions to specific individuals. Meanwhile, business email compromise has been steadily on the rise, where nefarious actors use phishing attacks to trick victims, steal important information, and redirect money into criminal bank accounts. Similarly, cyber criminals also use tech support scams amid looming financial anxieties to prey on less tech-savvy customers.

Through the DCU, Microsoft has launched various international investigations led by its team of lawyers and data analysts in collaboration with law enforcement agencies such as Interpol, Europol, and the US Federal Bureau of Investigation. For instance, DCU requested the US government to issue restraining orders to repossess domains used by cyber criminals for phishing or technology-related scam campaigns. Meanwhile, to combat online child exploitation, Microsoft has provided its scanning services to help government law enforcement agencies remove online photos of child abuse. DCU has also been notifying government authorities regarding repeat offenders who are using Microsoft-related applications such as Skype.

Regional outlook on cybercrime and cyberattacks

ASEAN's digitalization is driven by both economic and development priorities. Micro, Small and Medium Enterprises (MSMEs) are considered the linchpin of most ASEAN economies and contributed 41% of the region's overall GDP from 2010-2019. In the case of Indonesia, MSMEs comprise 97% of its economy and contribute approximately 60% to its overall GDP.

As MSMEs increasingly use the Internet, they become more exposed to cyber crime. In 2020, phishing campaigns targeting MSMEs had increased by 56% compared to the previous year. According to Kaspersky, Indonesia was the primary target of phishing attacks in Southeast Asia, accounting for the highest number of incidents at approximately 750,000. Conversely, Indonesia also suffered an enormous spike in ransomware with 1.3 million reported cases in 2020, representing almost half of the detected incidents in all of Southeast Asia.

Indonesia is also susceptible to the potential disruptions of major cyber operations that could endanger its critical national infrastructure. As financial institutions continue to be primary targets of larger cyberattacks, key stakeholders from the public and the private sector are faced with the daunting challenge of how to establish trust, coordination, and familiarity with one another through initiatives like information-sharing to forge a more resilient response.

As a region that is both geographically strategic and geo-technologically significant, the boundaries between cyber criminal activities and state-sponsored cyber operations are becoming increasingly blurred. Geopolitical clashes bleeding into cyberspace present new risks and vulnerabilities, especially with the region's lagging technical and human capacity in cybersecurity.

US-Indonesia: Avenues for cooperation in cyberspace

The impact of cyberattacks encompasses physical and economical damage, psychological trauma, and security posture weakness.

To mitigate such negative effects, six areas should be prioritized: organizational readiness, situational awareness/intelligence, cyber defense, detection, mitigation and containment, and recovery. Given that MSMEs are the central engine of Indonesia's economy, the government must undertake steps to raise awareness and strengthen their cyber defenses. Through the US-Indonesia strategic partnership, avenues for capacity building that emphasize MSMEs must be explored.

There is no one-size-fits-all solution against cyber crime, so the US and Indonesia must continue to strengthen public-private partnerships and raise education and awareness through academia and civil society organizations to disrupt cyber criminals. Government agencies can use economic incentives to promote cooperation between larger enterprises and MSMEs, where the former can help the latter in the provision of cybersecurity. Such an arrangement can help bolster the overall cyber resiliency of the business community.

As the likelihood of hybrid warfare -- which includes the use of cyber capabilities and kinetic means -- continues to increase, there is an urgent need to discuss possible and acceptable countermeasures within the remit of international law. As members of the UN Group of Governmental Experts (GGE) on advancing responsible state behavior in cyberspace in the context of international security, the US and Indonesia are well-entrenched in the application of cyber norms and international law in cyberspace. They can provide support toward regional and practical efforts to initiate a Track-2 dialogue in Southeast Asia which eventually can be elevated to Track 1 to address the enormous challenges in cyberspace faced by the entire region.

This document was prepared by Mark Manantan and Daniel Mitchum. 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.*