Strengthening ROK-United States Science & Tech Partnership on Critical Technologies Dialogue

Session 3: US-South Korea Cybersecurity Cooperation in the era of 5G / 6G

Key Findings

October 27, 2022 (US) | October 28, 2022 (Asia)

On October 27, 2022, with support from the Consulate General of the Republic of Korea in Honolulu, and in partnership with the George Mason University Korea's Center for Security Policy Studies, the Pacific Forum hosted the third session of *Strengthening ROK-United States Science & Tech Partnership on Critical Technologies*, "US-South Korea Cybersecurity Cooperation in the era of 5G / 6G." Over 20 participants (excluding speakers and staff) from the government, private sector, academia, and other non-governmental organizations participated in this webinar.

Dr. Lami Kim, Assistant Professor at the US Army War College and adjunct fellow at the Pacific Forum; Dr. So Jeong Kim, Senior Research Fellow at the Institute for National Security; and Dr. John Park, Director of the Korea Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs, assessed the opportunities, challenges and the prospects of US-South Korean cybersecurity cooperation in the era of 5G and the race to develop 6G.

The Key Findings from this webinar are below.

Through its distributed network, fifth generation mobile technology or 5G has the power to enable faster, lower latency connections that support an interconnected ecosystem of the internet of things and artificial intelligence-enabled technologies. In the military and security domain, 5G could facilitate the integration of autonomous weapons at the tactical and operational levels. Although sixth generation mobile technology (6G) is still in its early stages, it is expected to be fifty times faster than 5G with imperceptible latency, thus permitting the establishment of smart cities.

Given the revolutionary promises of 5G—and its successor 6G—intense adoption is already unfolding. Due to geopolitical and security considerations, advanced economies have favored Samsung, Erickson, and Nokia to build their 5G infrastructure over Chinese Information and Communications Technology (ICT) giants like Huawei and ZTE. This is because the strong ties between Huawei or ZTE and the Chinese Communist Party could be leveraged by the People's Republic of China to conduct espionage through built-in "backdoors." Furthermore, Huawei and ZTE are subject to China's National Intelligence Law of 2017 that compels them to comply with the government's requests for sensitive information.

Despite such perceived security risks and vulnerabilities, Chinese ICT companies have captured many emerging economies. Huawei's competitive suite of offerings from affordable pricing to infrastructure investments to capacity-building makes it an attractive choice, especially in Africa and Southeast Asia.

Apart from meeting the skyrocketing demands of ICT investments in the Global South, Huawei has been a prominent figure in the international technical standards-setting arena. Through its

proactive participation, Huawei is playing an active role in shaping the rules of the road that govern the physical and digital dimensions of the internet.

The growing influence of Chinese ICT companies could undermine the US and South Korea's competitive footing in the Fourth Industrial Revolution. But a more concerning trend is the overall impact of 5G on cybersecurity.

Besides state-sponsored advanced persistent threat actors, policymakers must also contend with the expansion of attack surfaces, the increasing availability and accessibility of cyber weapons sold in the dark web, and the growing community of cyber mercenaries or hackers for hire. The confluence of geopolitical tensions and the low barriers for non-state actors to acquire cyber capabilities could further sink the cyber domain into instability.

The United States and South Korea can maximize their complementary and comparative advantages to foster a more stable and secure cyber domain in the 5G. Both countries are proponents of the Open Radio Access Network, or Open RAN, which would provide a standardized, nonproprietary, and interoperable platform for 5G networks.

Notwithstanding the dominant market position of Huawei, South Korean ICT giants like Samsung are becoming a viable alternative to current 5G suppliers. In addition to meeting the accelerating demands of 5G equipment, Samsung also advocates for Open RAN.

As non-state actors further acquire substantial autonomy and agency in the cyber domain, the US and South Korea must reinforce existing partnerships with the private sector. Both parties must work together to ease existing frictions and effectively target state-sponsored and non-state cyber criminals.

While the private sector prioritizes user experience for their consumers to improve profit margins (removing frictions), governments are more inclined toward regulatory processes (increasing frictions). North Korean cyber criminals have exploited these gaps between policy and practice, evading sanctions and utilizing cryptocurrency payments.

In meeting the evolving cybersecurity challenges, the US and South Korea are encouraged to set up a track-1.5 or track 2-dialogue that complements their existing high-level cyber dialogue. Such a platform can nurture a permissive environment to tackle specific and sensitive issues in the bilateral relationship, especially important given China's growing presence in South Korea’s domestic ICT landscape. Finally, the US and South Korea should further boost their investment in ICT research and development to seize the first-mover advantage in the 6G era.

This document was prepared by Jake Steiner and Mark Manantan. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Vice President of 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.*