202.464.1982 1800 K Street NW

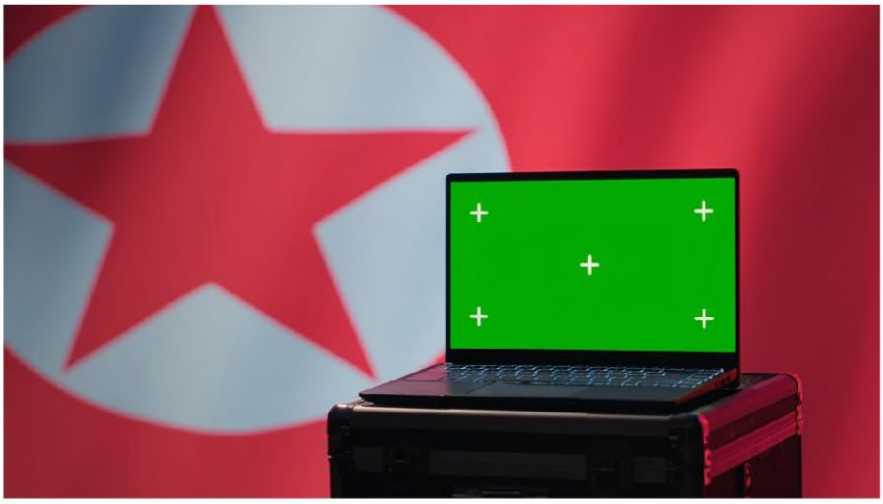
THE PENINSULA

[Policy Brief] US-ROK Cyber Cooperation: Promises and Challenges Ahead

Published December 16, 2024

Author: Jenny Jun, So Jeong Kim

Category: US-Korea alliance



This policy brief offers a concise summary and set of recommendations from a longer paper, featured in the Fall/Winter issue of KEI's flagship journal Korea Policy. The full paper can be found here and the entire Korea Policy issue here.

Executive Summary

In the past decade, the US and South Korea faced a relatively narrow set of challenges in cyberspace, notably North Korea's cybercrime facilitating sanctions evasion. In the next decade, however, the two countries will face a more diversified set of challenges with growing North Korean ties with Russia, its involvement in the war in Ukraine, and intensifying US-China competition. The US and South Korea must develop a joint playbook for responding to scenarios of disruptive cyber operations targeting South Korean public and private sectors and prepare for an even more difficult environment for curbing North Korea's cybercrime as Russia provides a way out.

Background

Over the past two years, the alliance between the United States and South Korea, or the Republic of Korea (ROK), has made a dramatic shift toward fostering greater cooperation on cyber issues. Beginning with cyber cooperation prominently featured in the 2022 US-ROK Leaders' Joint Statement, the two countries have since frequently convened for bilateral dialogues in multiple issue areas and increased diplomatic coordination in multinational and international fora. Several diplomatic and working-level working groups

Received by NSD/FARA Registration Unit 12/16/2024 11:12:54 AM

on the North Korean cyber threat have been formed, and joint advisories and sanctions have been issued. The two countries also engaged in military-to-military cyber dialogues and held a joint cybersecurity drill in early 2024. The United States and South Korea also expanded the conversation to a US-South Korea-Japan trilateral setting, launching a trilateral working group and conducting a multi-domain joint military exercise that included cyber.

At the same time, the midterm report card is less clear on whether this newfound energy on bilateral cooperation has translated into effective curbing of problems such as North Korea's cryptocurrency theft and money laundering. North Korea continues to steal and launder large amounts of cryptocurrency despite bilateral and international efforts to increase friction on its illicit money flows. Increasing Russia-North Korea ties have put a strain on the sanctions regime, including Russia's veto of the mandate extension of the UN Panel of Experts. New efforts such as the Multilateral Sanctions Monitoring Team (MSMT) are commendable, though buy-in from only the like-minded countries are not going to be enough to effectively curb North Korea's criminal enterprise.

More importantly, the two countries need to get on the same page at the strategic and operational level with regards to how to respond to cyber operations with varying degrees of intensity. This is going to be especially important over the next few years as North Korean participation in the war in Ukraine also possibly extends to cyberspace, including attacks on South Korean public and private sectors. Chinese cyber operations such as Volt Typhoon may continue to target overseas US bases, including those in South Korea and Japan in the future. Here, mitigating the risk of accidents and managing escalation is going to be key. While South Korea has made significant updates to its National Cybersecurity Strategy by introducing a new concept of "offensive cyber defense" that allegedly nods to the US cyber strategy of Defend Forward, clarifications to the strategic concept are needed and proper operationalization of the concept will develop over time with many iterations of responding to threats. If the two countries are to cooperate on active defense measures in cyberspace, extensive discussion must be had over mission scope, information sharing, access, authority, and public-private cooperation. As the geopolitical stakes in the Korean peninsula increase, it's time to go after these higher hanging fruits in US-ROK cyber cooperation.

Policy Recommendations & Implementation

– Since it has been recently affirmed that the US-South Korea Mutual Defense Treaty extends to cyberspace, the US and South Korea should come to a clear consensus at the strategic level on whether and what range of cyber attacks need to be deterred versus mitigated preemptively through active defense, and to what extent active defense will be carried out in gray and red space. This is important for mitigating chances of accidents and managing escalation.

– The US and South Korea should develop a joint playbook at the operational level for responding to varying scenarios of intrusion campaigns and disruptive cyber attacks, and determine what range of attacks merit joint responses versus independent action.

– Sanctions may become easier to evade as North Korea increases ties with Russia. To more effectively curb North Korea's cryptocurrency-based cybercrime, focus should be on direct measures to freeze or seize stolen virtual assets and strengthening industry cooperation.

Received by NSD/FARA Registration Unit 12/16/2024 11:12:54 AM

Conclusion

Over the past two years, the US and South Korea have significantly deepened and broadened cooperation on cyber issues and have expanded cooperation further to trilateral and multilateral settings. The two countries established several regular high-level and working-level dialogues, have issued joint sanctions and threat advisories, and deepened mil-to-mil cooperation. At the same time, many initiatives focused on the more immediate threat of North Korean cyber crime where there is clearer consensus on what needs to be done. However, 2024 has been a watershed in terms of shifting geopolitical dynamics in the Korean peninsula. Cyber threats will become more diversified, and the bilateral relationship will be tested at the seams without a clear joint strategic concept and operational plan.

Dr. Jenny Jun is an Assistant Professor at the Sam Nunn School of International Affairs, Georgia Institute of Technology and Dr. So Jeong Kim is Director of Emerging Security Studies and Senior Research Fellow of the Institute for National Security Strategy (INSS). The views expressed here are the authors' alone.

Photo from Shutterstock.

Return to the Peninsula

Tweet Share Share Email

Received by NSD/FARA Registration Unit 12/16/2024 11:12:54 AM