More Bilateral U.S.-ROK Cooperation Needed in Cyber Policy

blog.keia.org/2020/05/bilateral-u-s-rok-cooperation-needed-cyber-policy/

May 12, 2020

The Peninsula
Covering the economic and foreign policies that impact the Korean peninsula

KEI | KOREA ECONOMIC INSTITUTE
한미경제연구소

By Terrence Matsuo

One of the newest areas in national security is cyber policy. Policymakers in the United States and South Korea have outlined its importance and identified areas of concern such as North Korea's cyber activities. But there remain important questions for the alliance to answer.

Both American and Korean strategy documents highlight the importance of cybersecurity to national defense. In the national security strategy released by the Trump administration in 2017, the U.S. government notes that "cyberspace offers states and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders." The administration adds that "cyberattacks have become a key feature of modern conflict," in order for states to project influence and defend their interests.

Similarly, the most recent South Korean Ministry of National Defense white paper notes that "cyberattacks constitute another serious type of transnational threat." It lists the WannaCry and NotPetya attacks of 2017, and attack on a Turkish cryptocurrency exchange in 2018 as examples of these kinds of incidents. "Many countries around the world are accelerating efforts to develop a strategy for responding to cyber-threats," it observes.

Although the U.S. and South Korea share similar views of the threat posed by cyberattacks, there are certain ambiguities that must be addressed. In particular is the question of a North Korean cyberattack on either side, and what would be the appropriate response. "North Korea is a cyber superpower," says Lt. Gen. Chun In-Bum, a retired member of the South Korean military. "North Korea's ability and intent to harm and cripple the United States and South Korea should not be taken lightly."

But although these policy documents identify the threat from North Korea, other documents need to be updated or clarified. Entering into force in 1953, it is not surprising that the mutual defense treaty that outlines the U.S.-ROK alliance offers little perspective on cybersecurity. Article III of the treaty says that an "armed attack" on territory under either American or Korean jurisdiction "would be dangerous to its own peace and safety," and that both "would act to meet the common danger in accordance with its constitutional processes."

Experts have varying views on what kind of response was appropriate for a cyberattack from North Korea. Lt. Gen. Chun said that a response would be conditioned by the damage it inflicted. "If it is just a lot of money, I don't see the Defense Treaty being invoked," he said in an email. But he also said: "If a cyberattack causes loss of life that's a different matter, especially if it is a lot of people." Col.

David Maxwell is a retired member of the U.S. military now working as an analyst at the Foundation for Defense of Democracies. During a livestreamed event held by KEI, he observed that "if you take down [the] infrastructure of Seoul, or New York City, or Washington, DC, you are going to create tremendous problems for the citizens in those countries."

Other experts are pessimistic that the alliance would have a unified position, much less reaction. Joshua Stanton is an analyst of issues on the Korean Peninsula. In an email, he said that in the event of a North Korean cyberattack, "the government in Seoul would be paralyzed by doubt and hesitation, the alliance would be paralyzed by mutual distrust, and Washington would be paralyzed by Trump's isolationist impulses, his broader antipathy toward South Korea, and his election-year interest in claiming a diplomatic success through his summits with Kim."

Mr. Stanton warns: "In all likelihood…Kim probably calculates that there would be no response all. The implications for deterrence are obvious."

Thus it is critical that American and Korean officials determine how the alliance will handle threats in the cyber domain. The foreign ministries of the U.S. and South Korea have held a series of meetings focused specifically on cyber policy issues. The first round of talks were held in 2012, between Song Bong-heon, Ambassador for International Security Affairs, and Christopher Painter, Coordinator for Cyber Issues. Citing South Korean officials, Yonhap reported at the time that the two officials discussed "ways to strengthen bilateral cooperation for protecting critical government infrastructure and enhancing online security."

The talks have been held biannually since, with the most recent being in 2018. According to a readout from the State Department, Robert Strayer, Deputy Assistant Secretary for Cyber and International Communications and Information Policy met with Ambassador Moon Duk-ho, a successor to Ambassador Song. Both officials led delegations that included representatives from other ministries and agencies related to security and diplomacy from their respective governments. In addition to defending government infrastructure from cyberattacks, they also discussed capacity building, information sharing, and military-to-military cyber cooperation, in addition to other topics.

Unlike their diplomatic counterparts, there have been no meetings focused solely on issues in the cyber domain. But public statements do indicate there is an awareness on the need for greater cooperation in this area. The 51st US-ROK Security Consultative Meeting was held in November of last year and included American Secretary of Defense Mark Esper and South Korean Minister of National Defense Jeong Kyeong Doo. In a joint statement released after the meeting, both sides "committed to maintain close communication and coordination in the cyber domain, including sharing trends of cyber threats as well as corresponding policy changes in their respective nations and discussing common issues of interest."

In some instances the U.S. has clarified its obligations under alliance treaties with regards to a cyberattack. Bruce Klingner, an analyst for the Heritage Foundation, points to the U.S.-Japan Security Consultative Meeting of 2019 as being one example. Secretary of State Pompeo and Acting Secretary of Defense Shanahan met with Minister for Foreign Affairs Kono, and Minister of Defense

Iwaya in Washington. A joint statement released after the meeting said: "The Ministers affirmed that international law applies in cyberspace and that a cyberattack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty."

It is not clear if or when American and Korean officials will meet to discuss these issues. The negotiations over burdensharing, and the coronavirus pandemic have weighed heavily on both bilateral relations and international meetings in general. However, experts are optimistic that talks are likely to be held despite these pressures. Mr. Klingner said that the U.S.-ROK Security Consultative Meeting is usually held in the fall, and Col. Maxwell said that a meeting could be held virtually, as many other international summits are held this year.

As cybersecurity remains an unexplored topic for policymakers in both the U.S. and South Korea, further discussions between both governments is imperative. According to Jenny Town, the Deputy Director of 38 North, the public record clearly demonstrates that Pyongyang is looking to use cyber operations to further its national interest, whether it's electronic robbery or for intelligence gathering. "North Korea's cyber capabilities have really improved in recent years, and their confidence seems to be growing as well," she said.

Terrence Matsuo is a writer and analyst of American foreign policy in the Indo-Pacific region and a Contributing Author for The Peninsula. The views expressed here are the author's alone.

Image from Markus Spiske's photostream on flickr Creative Commons.

Received by NSD/FARA Registration Unit 05/12/2020 3:56:30 PM