Issue Brief,
The Summaries

Vol.51, No.24, 2022

The 2022 ROK-U.S. Summit and Cybersecurity: Strategic Challenges to Strengthen Deterrence

So Jeong Kim (Senior Research Fellow, INSS)

INSS
INSTITUTE FOR NATIONAL SECURITY STRATEGY
국가안보전략연구원

The 2022 ROK-U.S. Summit and Cybersecurity: Strategic Challenges to Strengthen Deterrence

So Jeong Kim (Senior Research Fellow, INSS)

Abstract

At the 2022 ROK-U.S. Summit, the two presidents reaffirmed their commitment to strengthen the ROK-U.S. alliance and enhance cooperation on specific and in-depth topics. The two countries pledged in the Joint Statement to "significantly expand cooperation to confront a range of cyber threats from the DPRK, including but not limited to, state-sponsored cyber-attacks," and to "deepen and broaden cooperation on critical and emerging technologies, and cybersecurity." Highlighting the "shared belief in the extraordinary benefits afforded by an open, free, global, interoperable, reliable, and secure Internet," the two leaders committed to "continue to deepen ROK-U.S. cooperation on regional and international cyber policy, including cooperation on deterring cyber adversaries, cybersecurity of critical infrastructure, combating cybercrime and associated money laundering, securing cryptocurrency and blockchain applications, capacity

building, cyber exercises, information sharing, military-to-military cyber cooperation, and other international security issues in cyberspace."

To strengthen ROK-U.S. cooperation on cybersecurity, the South Korean government should: secure in advance the collection and sharing of technical information for joint response; expand participation in joint cyber exercises; develop a common criteria to evaluate the impact of cyber attacks; establish a decision support system to safeguard national interests during cyber crises; and promote normative order and value-oriented diplomacy in the cyber realm. The government should further assess whether the specific cooperation items sufficiently reflect its priorities and national interests. Cooperation between the two countries should not be limited to technical developments, but also include norms-setting processes. Competition between great powers in cyberspace is ever-growing, and high dependency upon U.S. big tech and infrastructure providers is inevitable. Under such circumstances, South Korea should pursue technological independence and strategic autonomy, and solidify its position as an international and regional strategic key point by actively engaging in joint efforts to develop critical technologies and form international norms.

At the 2022 ROK-U.S. Summit, the two presidents agreed to enhance cooperation on specific and in-depth topics, envisioning a clear path for future bilateral cooperation between the two countries. In comparison to the 2021 ROK-U.S. Summit, a particularly noticeable distinction can be found regarding the agenda of cybersecurity and technology cooperation.

In the Joint Statement of the 2021 ROK-U.S. Summit, the two countries pledged to deepen cooperation in domains such as "cyber and space, to ensure an effective joint response against emerging threats," and to "expand regional coordination on law enforcement, cybersecurity, public health and promoting a green recovery." Issues regarding the creation of the ROK-U.S. Supply Chain Task Force, confirming ROK-U.S. partnership on global agendas including cybersecurity, and establishing a cyber-working group have been mainly addressed in the ROK-U.S. Partnership Fact Sheet.

The 2022 Summit Leaders' Joint Statement specifically addresses cooperation in cybersecurity and technology in detail. The Statement explicitly notes joint responses against North Korean cyber threats, stating that both countries "will significantly expand cooperation to confront a range of cyber threats from the DPRK, including but

not limited to, state-sponsored cyber-attacks." It also pledges to "deepen and broaden cooperation on critical and emerging technologies, and cybersecurity" to strengthen a strategic economic and technology partnership. Highlighting the "shared belief in the extraordinary benefits afforded by an open, free, global, interoperable, reliable, and secure Internet," the two leaders committed to "continue to deepen ROK-U.S. cooperation on regional and international cyber policy, including cooperation on deterring cyber adversaries, cybersecurity of critical infrastructure, combating cybercrime and associated money laundering, securing cryptocurrency and blockchain applications, capacity building, cyber exercises, information sharing, military-to-military cyber cooperation, and other international security issues in cyberspace." Remarks not specific to cyber issues, e.g., promoting a rules-based international order, combating digital authoritarianism, and endorsing *the Declaration for the Future of the Internet,* are also likely to be relevant to cybersecurity issues. More general topics regarding enhanced cooperation, exchange of skilled personnel, promotion of investment, and research and development cooperation in the critical and emerging technologies sector would also open the path for indirect collaboration in the field of cybersecurity.

Cyber and ICT aspects also have implications for topics discussed in the defense sector, such as: revision of the

ROK-U.S. Mutual Defense Treaty, initiating Reciprocal Defense Procurement agreement negotiations, building supply-chain resiliency and diversity, nuclear energy cooperation, and strategic materials export control. The addition of cybersecurity issues to the ROK-U.S. Mutual Defense Treaty and wartime operational control (OpCon) transition has long been discussed in South Korea. Current U.S. policies on software security reaffirm the need to consider the software aspects of the issue: the U.S. government has been implementing policies for securing the ICT supply chain, and the National Security Agency, in particular, has been operating a software verification scheme for government procurement. Heightening regulation and export controls over cyber weapons developed by the private sector, which may be deployed for terrorism or financial purposes, is also a current topic of debate in the U.S. Further consideration should be given to connecting ICTs and systems to ensure interoperability in the defense sector for both countries.

The Joint Statement reflects the views of leading think tanks in the U.S. emphasizing technology cooperation between South Korea and the U.S. through reports submitted to the Biden administration. This paper briefly reviews the think tank reports, and also comments on the cyber aspects of the Joint Statement and future challenges.

Suggestions from U.S. think tanks underscoring ROK-U.S. cooperation ('20-'21)

A report from Georgetown University's Center for Security and Emerging Technologies (CSET) suggested for the U.S. to establish "agile alliances" to combat digital authoritarianism.[1] The report outlined a “three-pronged strategy” of defending against cyber threats, networking with like-minded countries, and projecting influence, and also identified partner states for each strategy. Among the suitable partners paired for each plan, the report pointed South Korea as a partner for a critical hardware hub, joint AI R&D, and developing human resources for AI research.

The Joint Statement reflects the proposal by defining leading-edge semiconductors, eco-friendly EV batteries, and artificial intelligence as critical and emerging technologies and detailing concrete technical cooperation with South Korea. President Biden unquestionably demonstrated U.S. priorities regarding the bilateral cooperation through his visit to Samsung and meetings with industry leaders.

The Center for a New American Security (CNAS) made 13 proposals in their report promoting a tech alliance

[1] Andrew Imbrie et al., "Agile Alliances: How the United States and Its Allies Can Deliver a Democratic Way of AI," Center for Security and Emerging Technology (February 2020) https://cset.georgetown.edu/publication/agile-alliances/ (accessed: 2021/9/24)

among ten democratic states, including Korea, the U.S., and the European Union.[2] The report suggests the U.S. form and utilize the alliance to: secure supply chains, safeguard critical technologies, create new investment mechanisms, establish international norms and standards, strengthen cooperation mechanisms with foreign states and organizations, form an informal organization, ensure multi-stakeholder participation to influence alliance decision-making, and codify norms and values for the use of ICTs, etc. Such proposals appear in the Joint Statement in the notions of commitment to creating a consultative body, including the engagement of the National Security Office.

The Atlantic Council's report is tailored to the future visions for the ROK-U.S. alliance. "The future of the U.S.-ROK Alliance" report includes recommendations on the 5G network, supply chain, and cyber defense and deterrence.[3] It suggests South Korea join the alliance of the so-called "D-10",[4] including the U.S., Canada, France,

---

[2] Marijin Rasser et al. 2020. "Common Code: An Alliance Framework for Democratic Technology Policy: A Technology Alliance Project Report." Center for a New American Security (October) https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Common-Code-An-Alliance-Framework-for-Democratic-Technology-Policy-1.pdf?mtime=20201020174236&focal=none (accessed: 2021/8/20).

[3] Robert Dohner et al., "The Future of the US-ROK Alliance," Atlantic Council (February 2021) https://www.atlanticcouncil.org/wp-content/uploads/2021/03/The-Future-of-the-US-ROK-Alliance-Report-FIN.pdf (accessed: 2021/6/7); for further analysis, see Young-in Yoo and So-jeong Kim, "A review of 'the Future of the US-ROK Alliance'," the Korea-US Alliance'", NSR Brief, 2021. 4., pp. 1-6.

[4] D10 refers to the group of democratic states including the G7 (U.S., U.K., France, Germany, Canada, Italy, Japan) and Australia, India, and South Korea.

and Japan, to facilitate a secure 5G standard, rather than flying solo in confronting the Chinese telecoms market. They argue that South Korea and the U.S. should collaborate to diversify the global supply chain to enhance the robustness and resiliency of the existing Indo-Pacific supply chain, and to facilitate global development and deployment of 5G networks. It also suggests the alliance establish a cyber defense and deterrence mechanism modeled after the NATO. These suggestions are embodied in the Joint Statement by, in particular, the notions of deterring adversaries in cyberspace, strengthening critical infrastructure security, enhancing cyber exercises and information sharing, and continued deepening of ROK-U.S. cooperation on international cyber policy. The Joint Statement appropriately reflects such proposals and lays out the path for technological cooperation accordingly. Although it is difficult to predict the outcomes of the economic and technology partnership, it is evident that South Korea is considered an essential partner in the U.S.' plan to innovate alliance relations.

The cooperative measures outlined in the ROK-U.S. Summit Joint Statement signify various issues for the South Korean government in the future, which include the following implications and strategic considerations.

Securing in advance and enhancing shared technical information for joint response

To enable a joint response against North Korean cyber threats under the U.S. strategic concept of "defend forward," technical capacity and intelligence sharing at the operational level are crucial. For the past several years, the U.S. has operated the "defend forward" strategy for cyberspace security which laid the foundations for assisting Ukraine in the Russo-Ukrainian war. The U.S. has further conducted dozens of "hunt forward" operations in collaboration with Ukraine, as well as with other partners, according to Gen. Paul Nakasone, Director of the NSA.[5]

Under the “defend forward” strategy of the U.S., it is crucial to share technical skills and intelligence at the working level for a joint response to North Korea’s cyber threats. For an effective response before and after an incident, information regarding North Korea's systems and networks must be shared and informed thoroughly as prior action. As the U.S. intends to engage actively in preventive activities, and North Korean threats being a primary subject, ROK should take its intelligence capabilities to the next level to support the alliance with

[5] Paul M. Nakasone. The U.S. Senate Select Committee on Intelligence. ’22. 3. 10.; Paul. M. Nakasone. Subcommittee on Intelligence and Special Operations Hearing: “Defense Intelligence Posture to Support the Warfighters and Policy Makers”. ’22. 3. 17.

further substantial and accumulated intelligence regarding North Korea's cyber capabilities (technical, operational, and policy/strategic levels), and build capacity for the joint utilization of such information. Simultaneously, securing technical information on states with higher potential to assist North Korea is also vital to deterring collaborative attempts.

The disclosure dilemma, however, requires careful planning and preparations to set up pre-defined decision-making criteria that determine whether, how, and to whom to disclose information. A preemptive response based on previously obtained information may compromise the intelligence routes, further compromising any strategic advantages.

Expand participation in joint cyber exercises

North Korea's cyber capabilities, as an asymmetric power, have evolved to threaten both the U.S. and ROK. However, unlike the U.S. or EU, South Korea does not enjoy the option of imposing unilateral sanctions for an effective cyber deterrence and thus its strategic response options are limited. South Korea's cyber deterrence posture is likely to become more effective when the foundation

for ROK-U.S. collaborative response is established in accordance with the Joint Statement.

South Korea has recently joined the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) as a contributing partner, and participated as a single team in Locked Shields 2022, the Centre's joint cybersecurity exercise.[6] As a joint exercise to improve the cyber security level within the region, South Korea's participation should be appraised as a step forward in the effort for collective defense in cyberspace.

The next step should include participating in other cybersecurity exercises such as the Cyber Storm, a U.S.-hosted biennial joint cyber exercise. International partners at the 2020 event included Australia, Canada, France, Germany, Hungary, Japan, the Netherlands, New Zealand, Singapore, Sweden, Switzerland, and the United Kingdom. Joint cyber defense, research, training, exercise, and coordinated technological stance with the U.S. would contribute to strengthening South Korea's overall cybersecurity capacity by enhancing joint response capabilities and also play a significant role in deterring cyber threats from North Korea and entities with malicious intentions.

---

[6] In 2014, NATO proposed to Korea's representative to E.U. in Brussels cooperation in NATO-led exercise and critical infrastructure protection, with no outcome.

Develop a common criteria to evaluate the impact of cyber attacks for joint response

South Korea needs to develop a common criteria to evaluate the severity of damages caused by cyber attacks and execute domestic and/or external responses accordingly, applicable to cyber attacks from North Korea. In the event of significant cyber attacks, major countries such as the U.S., UK, and EU respond by publicly naming and shaming foreign governments accused of perpetration or by imposing economic and/or diplomatic sanctions, whereas South Korea has yet to take any such measures.

For a successful joint response against North Korea's cyber threats, the South Korean government, in particular the Office of the Secretary to the President for Cyber Security, should establish a risk assessment methodology, guidelines and procedures, and a response options list to determine the threat severity level and response level, and execute countermeasures accordingly[7]. In addition, follow-up measures such as the development of relevant guidelines or manuals and the revision of relevant departmental governance should be implemented and

[7] Sunha Bae et al., "Cyber-attack Severity Assessment (CASA) and National Response Matrix (NRM) in Korea," 34:2 The Journal of East Asian Affairs 67, February 2022.

incorporated into the new administration's National Cybersecurity Strategy.

Establish a decision support system to safeguard national interests during crises

The Joint Statement commits to launching mechanisms led by respective National Security Councils to coordinate bureaucratic and policy approaches between the two governments. As such, the role of South Korea's Secretary to the President for Cyber Security at the National Security Office is increasingly highlighted. While the traditional sanctions are imposed at the economic, political, and diplomatic front, current ICT developments enable technical sanctions as an option. Infrastructure operating companies and security firms can impact foreign adversaries' infrastructures by, for example, denying operational and security updates to their infrastructures and control systems, eventually causing devastating harm to the adversaries' critical national infrastructures or C4 networks. Such technical measures are only available through proactive intelligence on the adversary's systems and networks, and robust collaboration with private sector experts and businesses.

At the same time, pre-prioritizing essential services at the national level is also imperative to avoid aggravated chaos during cyber incidents. For instance, a cyber attack causing a power outage may trigger interruptions of hospitals' medical prescription management systems, patient information systems, or treatment devices, simultaneously. The South Korean administration shall be tasked with continuous prioritization and execution of recovery and response measures, with appropriate coordination with the U.S. in the process. For such purposes, it is indispensable to establish a multi-dimensional support mechanism for decision-making to impose effective sanctions and responses, that is inclusive of all relevant government agencies, as well as the academia, industry, and research community.

Promote normative order and value-oriented diplomacy in the cyber realm

Pledging to "develop, use, and advance technologies in line with the shared democratic principles and universal values," the two presidents in the Joint Statement constantly underscored joint efforts for a "rules-based international order." Assumably, such efforts include decade-long issues in international cyber policy that were not explicitly mentioned in the Statement: coordination in

participating in the UN Open-Ended Working Group (OEWG) and accession to the Convention on Cybercrime, as well as the endorsement of *the Future of the Internet Initiative*. In response to such agendas, adequate consideration should be given to the strategic values for national security, as well as diplomatic concerns. However, under the current structures of the South Korean Ministries of Defense and Foreign Affairs, national cyber security issues are tasked to divisional units. It would be advisable to restructure both Ministries and expand the divisions to bureaus similar to the Cyber Terror Response Center of the National Police Agency and the National Cyber Security Center of the National Intelligence Service (NIS) to facilitate comprehensive and multi-dimensional assessment of cyber incidents. In addition, the National Police Agency and NIS may also benefit from expanding their relatively small policy and strategic departments to adequately respond to various issues in the future.

Future Challenges

The 2022 ROK-U.S. Summit solidified the partnership between the Republic of Korea and the United States. Regarding cybersecurity, it is particularly promising that the Joint Statement dedicated a separate section to the issue clearly stating both countries' determination to work

together in responding to North Korea's cyber threats and boosting ROK's cyber deterrence, along with specific research cooperation.

To maximize the effectiveness of this momentum, the government should pursue technology cooperation with specificity and continuity. The Yoon administration should further assess whether the specific cooperation items sufficiently reflect its priorities and national interests, and ensure that cooperation between the two countries not be limited to technical developments and be inclusive of the norms-setting process. Competition between great powers in the cyber realm is ever-growing, and high dependency upon U.S. big tech and infrastructure providers is a reality. Under such circumstances, South Korea should actively participate in the joint development of critical technologies and formation of international norms to secure technological independence and strategic autonomy, and solidify its position as an international and regional strategic key point.