US-South Korea Cyber Cooperation: Towards the Higher-Hanging Fruits

By Dr. Jenny Jun and Dr. So Jeong Kim

Introduction

The range of cyber threats facing the United States and South Korea, or the Republic of Korea (ROK), over the next decade will not be the same as that of the past decade. In the past, the United States and South Korea jointly faced a relatively narrow set of challenges in cyberspace, mainly limited to North Korea's cybercrime and its funding of the country's nuclear and missile program. However, the geopolitical situation surrounding the Korean Peninsula is rapidly changing, and these changes will trickle down to the cyber domain as well. North Korea is increasing military ties with Russia and has entered the war in Ukraine. US-China strategic competition is intensifying, which has resulted in Chinese cyber intrusions to overseas US military bases in the Indo-Pacific. A second Donald Trump administration will also intensify trade tensions with China, increase volatility in US alliances in the region, and result in potential changes to the United States' North Korea policy.

Under these circumstances, cyber threats will also diversify. In the future, the two countries will have to worry about more than North Korea's cybercrime. For instance, there may be more disruptive or destructive cyberattacks beyond crime or espionage targeting South Korean public and private sectors, especially to coerce or influence South Korea's Ukraine policy. Pro-Russian hacktivists have already launched a distributed denial-of-service (DDoS) campaign against South Korean government agency websites.[1] We may see Chinese cyber intrusions similar to Volt Typhoon in 2023 and 2024, where the suspected goal was to maintain access and persistence on systems connected to US military bases to create effects in the event of a crisis in the Indo-Pacific. The Korean Peninsula is again caught in competition among superpowers, and this is no exception for the cyber domain. The stakes are getting higher, and there is going to be less room for error in order to minimize accidents and manage escalation.

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 the Director of Emerging Security Studies and Senior Research Fellow of the Institute for National Security Strategy (INSS).

Therefore, now is the time to reach for the higher-hanging fruits in US-South Korea cyber cooperation. Over the past two years, the two countries have made a dramatic shift toward fostering greater cooperation on cyber issues and have made some significant progress in regularizing workshops and expanding cooperation to trilateral and multilateral settings. Much of the content of such meetings concerned jointly combatting North Korea's cybercrime, which is appropriate given that it is the modal threat and there is little disagreement as to a need to respond. Going forward, now that the basic structure of the dialogues has been established, it is time to touch on the more difficult questions.

Much of these more difficult conversations come down to coming to a consensus at the strategic level as to whether and what range of cyber threats jointly concerning the two countries need to be deterred versus mitigated through active defense measures and how responsibilities and authorities will be divided up for such operations, if any. South Korea's new national cybersecurity strategy that introduces the concept of "offensive cyber defense" needs to be further refined, and policymakers need to have more discussions on how such a strategy will work in tandem with the US cyber strategy of Defend Forward and Hunt Forward missions.[2] Jointly thinking through these questions in advance will help clarify responsibilities and improve readiness ahead of future cyber incidents on the Korean peninsula.

In this paper, we provide an overview of the range of cyber threats facing the United States and South Korea and analyze the progress made so far in the past two years of cyber cooperation between the two countries. We then highlight the remaining challenges and suggest topics for further discussion by policymakers in both countries.

The Evolving Cyber Threat Landscape

North Korea

Currently, the modal cyber threat jointly facing the United States and South Korea is undeniably coming from North Korea. North Korea's cyber operations have become more brazen, sophisticated, and diversified throughout the past decade. Most importantly, North Korea has significantly expanded its cybercrime enterprise to fund its nuclear and missile program, creating a gaping loophole in the international sanctions regime. North Korea has engaged in fraudulent SWIFT transactions targeting banks, fraudulent ATM cashouts, and ransomware, as well as cryptocurrency heists against exchanges and gaming platforms.[3] North Korean IT workers have also sought jobs at foreign companies under false identities, generating revenue for the regime while also laying the grounds for further exploitation.[4]

Among these, the most important category of illicit revenue from North Korea's cybercrime activities is the theft of virtual assets, including cryptocurrencies. Virtual assets are highly attractive targets for North Korea due to the large sums of money that can be stolen at once and the relatively low-security protections on targets compared to traditional financial institutions. Although exact estimates are difficult, the UN Panel of Experts on North Korea reported that they are investigating 97 suspected cases between 2017 and 2024, valued at USD 3.6 billion.[5] Industry analysis also assesses that North Korea was responsible for almost a third of all cryptocurrency heists in 2023.[6] A single heist can range in the hundreds of millions of dollars worth of virtual assets, such as the 2022 hack of Axie Infinity's Ronin Bridge in which North Korean hackers stole about USD 620 million worth of Ethereum.[7] Comparing this amount to North Korea's legitimate sources of foreign cash provides a sense of how much the regime relies on illicit money flows. In 2022, North Korea's total exports were a meager USD 160 million, where 96.7 percent were exported to China, and minerals accounted for 41.3 percent of total exports.[8] The revenue from such heists is thus a lifeline for the cash-strapped regime.

North Korea having such a lucrative outside option further dilutes the power of sanctions as a policy lever in slowing down North Korea's weapons program and pressuring the regime to change its calculus. About half of North Korea's missile program is funded by cybercrime, according to a 2023 assessment by US Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger.[9] Furthermore, effective sanctions enforcement is likely to be undermined even more with the dismantling of the UN Panel of Experts that has served as the primary monitoring body for UN sanctions vis-a-vis North Korea in early 2024. This is why the North Korean cybercrime issue is no longer a technical issue dealt with at the working level but integral to the US and South Korea's overall North Korea policy.

In addition to cybercrime, North Korea also conducts extensive industrial espionage to obtain sensitive information on areas such as nuclear facilities, unmanned weapons systems, satellite technologies, and radar systems, often targeting foreign critical infrastructure in the process.[10] North Korean hackers have also targeted researchers and experts focusing on the Korean Peninsula, directly obtaining strategic analysis and compromising their accounts to further exploit other researchers in the network.[11] These activities are likely to continue, and responding to North Korea's cybercrime and espionage will remain a major pillar of US-South Korea cyber cooperation, as they have been for the past two years.

Future Threats

Beyond these threats, however, lie other categories of cyber threats that the United States and South Korea should have a clear playbook for. South Korea also faces cyberattacks intended to have disruptive and/or destructive effects beyond financial crime or espionage. The actors are also more diverse than just North Korea; South Korea has been targeted by state and non-state actors from Russia and China. While these may occur with less frequency, they may have a higher impact and entail different geopolitical risks beyond the narrowly defined North Korean threat. With escalating tensions in Northeast Asia amid increasing Russia-North Korea ties and US-China competition, these types of threats may also occur more frequently in the future.

First, South Korea may see more disruptive and/or destructive cyberattacks going forward. These may be a response to protest certain South Korean policies, or they may be accompanied by a coercive threat. For example, after South Korea announced that it may review its previous policy against directly supplying arms to Ukraine in response to North Korean troops joining the war in Ukraine, pro-Russian hackers have launched DDoS attacks against South Korean government agency websites.[12] While DDoS attacks themselves have had a minimal disruptive impact, this incident shows that South Korea's cyber threat landscape will diversify because of the war. Though less frequent in recent years, South Korea has experienced major cyberattacks, such as the disruption of the 2018 Pyeongchang Winter Olympics opening ceremony by Russian state actors.[13] It has also faced coercive threats such as the attack on Korea Hydro and Nuclear Power (KHNP) in 2014, where the hackers demanded that South Korea shut down three of its civilian nuclear reactors by Christmas and released stolen blueprints and employee information as part of the threat.[14] These less frequent, but high impact threat scenarios require more coherent thought leadership at the strategic level and a clear playbook at the operational level.

Second, South Korea's growing role as an arms exporter and its increasing role in the global supply chain for critical goods may increase cyber threats to the private sector, affecting US security interests as well. For example, Hanwha Ocean won a contract earlier this year to perform maintenance, repair, and overhaul (MRO) for the US Navy, as the United States increasingly seeks to reduce downtime of its ships through utilizing international shipyards.[15] Because South Korea's shipbuilding industry is already frequently targeted by cyber actors, increasing cooperation between the US military and South Korean shipbuilding companies poses new supply chain risks.[16] South Korea is also becoming a major arms exporter to Western Europe and the Middle East, making such South Korean companies a prime target for cyber espionage and

supply chain compromise by adversaries of the weapons importers, not just North Korea. These are also a different category of threats than disruptive and/or destructive cyberattacks and thus require a separate discussion for appropriately defending against such threats.

Third, as a major treaty ally of the United States in the Indo-Pacific, South Korea is not immune from campaigns such as Volt Typhoon as the strategic competition between the United States and China intensifies. Volt Typhoon was a Chinese campaign that sought access and persistence on US critical infrastructure, including communications, energy, transportation, and wastewater systems, and it was believed to cause disruptive effects in the event of a crisis or a conflict.[17] Targets of this campaign included infrastructure serving US military bases in Guam.[18] Such efforts to retain the capacity to cause friction on US military forces stationed in the Indo-Pacific may also extend to the Korean Peninsula. These intrusions may not directly target US forces but target South Korean civilian infrastructure that serves such bases, and detection of such intrusions may also, in part, depend on the private sector. Such scenarios highlight a need for close coordination on cyber issues between the US and South Korea and with the private sector.

The State of US-South Korea Cyber Cooperation

Despite the growing significance and impact of the North Korean cyber threat over the past decade, US-South Korean cooperation on the issue has been mostly sporadic until 2022. On many occasions, the United States independently responded to North Korea's cybercrime and espionage activities through its own security and law enforcement agencies and in cooperation with the private sector. The South Korean government's response to the North Korean cyber threat has oscillated between administrations, depending on their broader policy on inter-Korean relations and perception of the North Korean threat. For instance, South Korea's 2019 National Cybersecurity Strategy did not mention North Korea as the country's main threat. During the Moon Jae-in administration, existing US-ROK dialogues, such as the bilateral cyber cooperation working group, stopped convening, and mentions of cyber cooperation in high-level joint statements were limited to the context of ASEAN and domestic abuse, without mentioning the North Korean cyber threat.[19] In many ways, the United States and South Korea did not see eye to eye on the level of threat posed by North Korea's cyber operations, much less an articulation of a shared vision for how the two countries would manage security issues in the cyber domain.

In 2022, the conservative Yoon Suk-yeol administration came into power in South Korea, shifting the government's North Korea policy to a more hawkish posture compared to the previous Moon administration. This extended to the cyber domain as well. The word "cyber" appeared 10 times in the 2022 joint statement between President Yoon and US President Joe Biden, with an explicit statement on responding to North Korean cyber threats and a full paragraph that enumerated specific areas of cooperation. The statement specified "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."[20] This signaled a willingness to significantly deepen and broaden bilateral cooperation on cyber issues. Not only were issues related to the North Korean cyber threat listed with specificity, but they also hinted that South Korea was willing to look beyond just the North Korean issue to seek strategic cyber cooperation with the broader regional and international security context in mind.

Over the next two years, the United States and South Korea had a dizzying number of diplomatic and working-level engagements on cyber issues. Many of the dialogues have become frequent and regularized, providing a stable platform at the working level. The newly created US-ROK working group on the North Korean cyber threat met seven times. Other similar bilateral fora were convened, including the US-ROK Cyber Policy Consultations, the US-ROK Cybersecurity Senior Steering Group, and the US-ROK Joint Symposium on countering DPRK Cyber Threats to Cryptocurrency Exchanges. The United States and South Korea also issued several joint sanctions and threat advisories on the North Korean cyber threat, signaling that the two countries are aligned on the issue. In 2023, Presidents Biden and Yoon signed the Strategic Cybersecurity Cooperation Framework following their summit, expanding on many of the items discussed in the previous year.[21] 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 broadened their cyber cooperation to multilateral and international fora. One of the most notable developments was the expansion of the conversation to a US-South Korea-Japan trilateral setting. After a trilateral summit at Camp David in August 2023, the three countries launched a US-ROK-Japan Trilateral Diplomatic Working Group on North Korea's Cyber Activities in December of that year. In addition, the three countries conducted FREEDOM EDGE, a multi-domain joint military exercise

that included cyber. In 2022, South Korea also became the first Asian country to formally join the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) as a contributing participant.[22] A list of publicly reported meetings and joint actions between 2022 and 2024 is in Appendix A.

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. It is also difficult to delineate the extent to which progress is still largely a function of preexisting independent intelligence activity and law enforcement actions by the US government and the extent to which cooperation with South Korean counterparts has yielded additional gains. On the military front, mil-to-mil dialogues and joint exercises are welcome developments. At the same time, South Korea's new cyber strategy leaves room for further conceptual clarification and thinking through how it will work in tandem with US cyber operations to send the right signals and manage miscalculation risks. Cooperation on related topics such as misinformation and artificial intelligence is beginning to occur, though their progress remains to be seen. These are all promising areas for further discussion as the initial excitement of the first few years hopefully matures into a more routine working relationship.

Progress in Countering North Korea's Cyber Crime

Because of this issue's connection to North Korea's nuclear and missile threat, the US government has taken North Korea's cybercrime enterprise seriously. Over the past few years, the United States has been ramping up efforts to use a variety of means at their disposal to impose friction. The main approach has been to intervene in the intermediary steps between the moment funds are stolen and the point where they end up in North Korean-controlled accounts, mainly done through existing authorities in the Department of Treasury, Department of Justice, and FBI. This includes various indictments of hackers and money-laundering intermediaries, some of which have led to arrests and sentences.[23] They were also able to directly seize parts of the stolen funds in cooperation with the private sector and foreign governments—for example, USD 30 million out of about USD 600 million stolen in the Axie Infinity heist were recovered.[24] They have also sanctioned crypto mixers that facilitate money laundering, such as Tornado Cash and Sinbad.io.[25] The founders of Tornado Cash have also been indicted for money laundering and sanctions violations.[26] Many of these efforts have been conducted independently by the US government outside of the context of US-South Korea cyber cooperation.

South Korea has demonstrated solidarity with the United States by following suit with independent and joint sanctions as well as threat advisories on multiple occasions.[27] In 2023, the South Korean government issued its first-ever sanctions related to North Korea's cyber threat, designating seven entities and four individuals.[28] Although some of these entities and individuals had already been sanctioned by the US government, new names were also added. In turn, they have been subsequently sanctioned by the United States.[29] This is an instance of the value-add from closer working-level cooperation between the United States and South Korea.

On the illicit IT workers issue, the United States and South Korea have issued separate and joint advisories to raise awareness of the methods used by these individuals in an effort to disrupt their activities. US law enforcement officials have also arrested intermediaries that facilitate such operations, such as a Nashville resident who operated "laptop farms" for North Korean IT workers.[30] Although general awareness of this issue has increased over the past few years, North Korean workers continue to successfully secure jobs by creating new identities that leverage AI deepfakes or exploiting third parties to obtain contracts.[31]

These are certainly promising signs of progress. At the same time, there is room for further cooperation as the relationship matures. Even after both countries' earnest efforts, North Korea continues to steal and launder large sums of money and shows no signs of slowing down. There are important limits to how much sanctions and threat advisories can effectively curb the illicit money flow. North Korean hackers find alternative mixers and laundering schemes with relative ease, and effectively enforcing sanctions remains difficult as some entities, such as the Russia-based Garantex exchange, continue to operate despite being sanctioned and allow transactions from North Korean heists.[32] Slightly more effective are interventions that indict and arrest money-laundering intermediaries and those that directly seize parts of the stolen funds. Such measures, however, require close law enforcement cooperation with not just South Korea and Japan but with a variety of international partners due to the global nature of North Korea's illicit networks. Similarly, greater regulation of virtual assets generally requires extensive discussion and buy-in at the international level. These efforts to build a broad global consensus on virtual asset regulation, however, will be further delayed as a crypto-friendly second Trump administration moves to deregulate the industry in the United States.

While the United States and South Korea have closely coordinated on the IT workers issue, they also face some challenges ahead as this becomes a cat-and-mouse game. There is a growing trend of North Korean IT personnel

relocating to Southeast Asian countries as they face difficulties in securing work. This complicates direct sanctions against them. In such cases, additional measures may be required, such as restricting access to IT infrastructure, limiting their activities, or expelling them through cooperation with the respective countries. There is also a concern of displacement, specifically that North Korean IT personnel who fail to meet their assigned revenue quotas may become further involved in more explicitly malicious activities, such as being hackers-for-hire in greater numbers. This could lead to their operations becoming more malicious and covert, which makes complete eradication a challenging task.[33] Strengthening relationships and enhancing cooperation with countries where North Korean IT personnel operate freely is necessary to address this issue. Like the virtual assets issue, combatting this issue requires buy-in from key third-party states, and thus, issue-based diplomatic coordination is key.

This means that the United States and South Korea should increase diplomatic coordination to convince third parties to cooperate on this issue. This is a difficult task as further efforts are needed to build a consensus on the importance of virtual asset theft as a national security issue. In particular, states such as Russia are actively trying to downplay the threat by characterizing this issue as a mere crime that does not merit discussion in international organizations. While the UN Open-ended Working Group (OEWG) listed virtual asset theft as a major threat for the first time in its third Annual Progress Report (APR), Russia and other states have argued that ransomware and virtual asset theft are merely cybercrimes and should not be dealt with by the OEWG. If virtual asset theft is treated solely as a crime, it could undermine current actions taken from a national security perspective, including sanctions and countermeasures. This year, Russia also vetoed extending the mandate of the UN Panel of Experts, the key body that monitored UN member states' enforcement of the international sanctions regime against North Korea.[34] Although the United States launched an alternative 11-state multilateral monitoring body called the Multilateral Sanctions Monitoring Team (MSMT), details are currently sparse, and there is uncertainty on whether this body will have the authority and capacity to monitor sanctions pertaining to UN Security Council resolutions.

Considering the closer relationship between North Korea and Russia through the signing of the Treaty on Comprehensive Strategic Partnership, the United States and South Korea can expect an actively contested arena for agenda setting and norms development on combating cybercrime. At the same time, it also means that the United States should work with close allies such as South

Korea and Japan to shape the debate and increase buy-in from third-party states. North Korea targets globally and has stolen hundreds of millions of dollars from victims around the world, so treating the issue similarly to ransomware may help increase buy-in from states that are otherwise geopolitically disinterested in North Korea. Raising the profile of the issue, such as the debate held at the UN Security Council in June 2024, is a start.[35]

Maturing South Korea's Cyber Strategy

Another important aspect of US-South Korea cyber cooperation is in the military domain, forming a coherent strategy and accompanying operational capacity to effectively manage threats in the cyber domain. In this regard, South Korea made significant changes to its own national cyber strategy that show a desire to align more closely with the US cyber strategy of Defend Forward. In 2024, South Korea published its National Cybersecurity Strategy and the National Cybersecurity Basic Plan, an implementation roadmap for the strategy.[36] These two documents represent a major departure from the 2019 National Cybersecurity Strategy, which focused more on defensive measures at home.[37]

Most notably, one of the key aspects of the strategy is a new posture called "offensive cyber defense (공세적 사이버 방어)."[38] Although a clear articulation of the fine-print strategic logic behind the phrase remains murky, and it is still unclear how it will be operationalized and implemented by individual agencies, the spirit of this posture is likely the South Korean government's desire to align its cybersecurity strategy with the US cyber strategy of Persistent Engagement and Defend Forward.[39] Other pillars of South Korea's strategy stress greater diplomatic engagement with the international community on cyber issues, critical infrastructure resilience at home, and securing competitiveness around critical and emerging technologies. The strategy and the accompanying basic plan also make important updates to the bureaucratic chain of command, delegate tasks to individual agencies, and advocate for updating legal and regulatory frameworks.

However, South Korea's current articulation of the strategy, especially the key phrase of "offensive cyber defense," needs further refinement in its strategic logic. This is a prerequisite that should precede further discussions regarding the capabilities needed to achieve such ends, which agencies will have authority and autonomy in operational decision-making, and how these capabilities will create synergistic effects with existing US cyber operational concepts.

The phrase "offensive cyber defense" is the first pillar and appears 11 times in South Korea's new national cybersecurity strategy. The importance of the phrase has been further echoed by President Yoon in key government-organized conferences such as the Cyber Summit Korea 2024, during which he stated that "attack is the best defense."[40] On the surface, this looks like a pivot toward Defend Forward because it starts from the same realization that passive defense at home is not enough to stop cyberattacks or intrusions from occurring. Upon a closer look, however, South Korea's conceptualization is quite different from that of the US strategy.

Where the two states diverge is in their thinking on the best approach for achieving deterrence in cyberspace. South Korea's strategy indicates a focus on acquiring offensive capabilities as a response to cyberattacks to achieve deterrence by punishment through attribution and subsequent retaliation. This is seen in language such as "The Republic of Korea must shift the paradigm to offensive responses to threats, including those from North Korea."[41] This focus on deterrence by punishment becomes clearer further down the document, where it states that South Korea will acquire capabilities to "identify perpetrators of cyber attacks," "enhance response capabilities…by advancing systems for identifying attack origins," "identify the entities behind cyber attacks…and impose corresponding accountability," and "develop deterrence strategies against national security threats in cyberspace."[42] However, the same section also "task[s] intelligence agencies and the military with…preparing for anticipated attacks to preemptively and offensively respond to threats"—language that is quite different from deterrence by punishment.[43] Similarly, the Basic Plan also focuses on attribution and identifying "attack origins."[44] The Yoon administration's strategic thinking reflecting a reliance on deterrence by punishment is also not unique to cyberspace and is echoed in other domains as well.[45]

In cyberspace, the United States moved away from this kind of thinking in 2018. The motivation for the pivot was the realization that deterrence by punishment in cyberspace is hard to achieve, especially against routine attacks and intrusions that occur at the threshold below armed conflict.[46] Instead, the US approach turned to Persistent Engagement—the idea that in a domain characterized by constant contact, actors constantly maneuver to compete for limited advantages. The strategy born from that conceptualization of the domain was Defend Forward, which aims to "disrupt or halt malicious cyber activity at its source" in order to "stop threats before they reach our targets."[47] The desired end state is not necessarily malicious cyber actors being deterred as a result of Defend Forward operations but competition at a manageable level.

Knocking the knife out of the attacker's hand before an attack versus acquiring a knife oneself to slash back, such that the attacker does not think about attacking again, are very different strategic concepts and, accordingly, require very different operational capabilities. For example, acquiring capabilities for attribution and the identification of an attack's origin are more important for the latter. South Korea's first mission should be to clarify the meaning of "offensive cyber defense" and whether they really want to achieve cyber deterrence and examine whether there is a disconnect between the means and the end. If they instead meant to emphasize active defense, South Korea's second mission should be to clarify what kind of active defense they plan to adopt. Not all active defense is equal—some states, such as the United Kingdom, prefer to conduct active defense mostly in blue space, while the United States conducts operations in gray and red space in third-party and adversary-controlled systems.[48] This will determine the necessary authorities and capabilities. South Korea should also discuss the degree to which agencies will have autonomy in planning and executing such offensive cyber operations and how oversight will work. It will also inform how South Korea's operations will work alongside US initiatives, such as Hunt Forward missions.

Furthermore, South Korea should think about the signaling effects of its posture beyond the North Korean threat. South Korea is targeted not just by North Korea but also by other states such as China and Russia. This is where language around offensive cyber operations should be calibrated closely so as to minimize misperception and miscalculation. This is especially relevant as US-South Korea cyber cooperation expands to include Japan, multi-domain joint military exercises are held with the broader Indo-Pacific geopolitical context in mind, and South Korea joins organizations such as NATO CCD COE. How to engage Chinese and Russian cyber activity targeting South Korea is a sensitive discussion that requires close coordination with US counterparts. Sharing a similar strategic vision is important, but that does not always mean that South Korea must acquire the same capabilities as the United States to carry out its independent operations. Just like how European allies rarely conduct offensive cyber operations on their own but still work with the United States to dismantle servers and expose adversary toolkits, it is important to assess how South Korea's capabilities can complement and augment existing US capabilities and missions.

The Harder Questions of US-South Korea Cyber Cooperation

The deepening and broadening of cyber cooperation and proactive engagement over the past two years is commendable. The United States and South Korea are coordinating on a variety of fronts, including the North Korean cyber threat,

military-to-military dialogues and exercises, and US-South Korea-Japan trilateral dialogues. Conversations are happening at both the working level and the diplomatic level, embedded in multilateral and international fora. Efforts are also being made to update national strategies to better align with one another. At the same time, real challenges remain as the initial flurry of establishing workshop series and consultative meetings transition to mature working relationships. Soon, there will also be a need to assess the practical impact of such discussions and initiatives.

Of course, the most immediate challenge for both countries is to effectively curb North Korea's revenue generation through cyber means. In some ways, a full report card on the impact of bilateral cooperation on this issue is premature, as initiatives are just starting to kick off. In the short term, there are instances where cooperation has concrete synergy, such as identifying entities and individuals to be sanctioned. In some cases, such as the issue of illicit IT workers, issuing joint threat advisories helps raise public awareness about the problem in both countries. At the same time, there are limits to how much sanctions designations and joint advisories can directly stop the flow of money to the North Korean regime. Interventions, such as directly seizing stolen virtual assets and increasing regulatory oversight on virtual asset transactions, are promising, though they require partnerships with key third-party states. In a crypto-friendly second Trump administration, it remains to be seen whether virtual asset theft will be seen as a threat to the industry to be cracked down on or overlooked in the push to deregulate the industry.

Locking in the initial enthusiasm into long-term, regularized cooperation also remains uncertain. Historically, enthusiasm for cooperation on cyber issues has waxed and waned in South Korea depending on the administration in power and their perception of the North Korean threat, the US-ROK alliance, and close cooperation with Japan. Navigating South Korea's bureaucracy and streamlining efforts is also another challenge. There is also a risk of duplicating efforts, with cooperation on the same topic taking place through both working-level partnerships and diplomatic channels. Strengthening policy expertise within South Korea's Ministry of Foreign Affairs and enhancing the professional capacity of relevant departments is also necessary. The ROK National Security Office's support capabilities should be bolstered to provide more realistic oversight and coordination. On the US side, a second Trump administration is likely to result in severe budget cuts to key federal agencies, increase uncertainty in the alliance, and undermine multilateralism. Keeping up the momentum of the past two years will be challenging on both sides.

Finally, there are harder questions that need to be asked beyond the narrowly defined issue of North Korean cybercrime. The core of the bilateral relationship is the US-ROK military alliance, and increasing geopolitical tensions surrounding the Korean Peninsula also raise stakes in the cyber domain as well. Increasing Russia-North Korea ties and South Korea's growing role as an arms exporter and an integral part of the global supply chain entangle South Korea in affairs beyond Northeast Asia to a greater extent, increasing the possibility that South Korea's public and private sector will become more frequent targets of disruptive cyberattacks, espionage, and supply chain compromise, by state and non-state cyber actors other than North Korea. Certain South Korean civilian critical infrastructure may be targeted as a way to maintain persistence in the event of a crisis in the Indo-Pacific. While they may not be the current modal threat, they will have greater impact and risk miscalculation and escalation when they do occur.

The US-ROK alliance needs a joint vision and strategic clarity on cyberspace and needs a playbook for responding to varying scenarios of intrusion campaigns and disruptive cyberattacks. First, to perform any joint actions responding to a cyber incident, the two countries need to come to a consensus as to whether the goal of performing such an action is to achieve deterrence of further similar incidents or denial and for which types of cyber incidents. To be fair, the US cyber strategy has also not completely resolved similar tensions between active defense and deterrence.[49] This tension, however, is much more pronounced in South Korea's current cyber strategy under the concept of "offensive cyber defense." Coming to such a shared vision is especially important given the recent confirmation by Secretary Blinken that the scope of the US-ROK Mutual Defense Treaty extends to space and cyber domains.[50] Perhaps there is a small range of destructive cyberattacks on critical infrastructure that rise to the level of armed attack, but the vast majority of cyber intrusions and attacks do not rise to this level of intensity. How the two countries will coordinate response, if at all, to this latter category of cyber threats is the more important and thorny question.

Whether South Korea decides to deal with cyber threats that fall below the level of armed attack through active defense or deterrence by punishment will have important implications for what practical capabilities and authorities are needed to implement such a goal. If South Korea wants to move towards active defense, this means that the main agency tasked with such operations will need augmented intelligence capabilities to "detect threats before they reach the target," which may be in gray and red space. This generally goes beyond what is

currently listed in the South Korean strategy of "identifying attack origins," which makes more sense for retaliatory measures. This increases the mission scope of that agency. This then brings up questions of nuances in oversight and operational autonomy as to what extent that agency can perform cyber operations beyond intelligence gathering in gray and red space without prior authorization from the National Security Council, where expediency is key in active defense. Also related to this question is the extent to which acquiring independent operational capabilities makes sense in relation to an already global reach of US Defend Forward and Hunt Forward missions. The United States, on the other hand, needs to think about managing possible miscalculations and escalation on the Korean Peninsula arising from such exchanges.

Major breakthroughs in US-South Korea cyber cooperation come at a time of intensifying geopolitical competition in the Indo-Pacific region. Over the past two years, the focus has been on the most immediate threat from North Korea. In some ways, however, responding to North Korea's cybercrime is not necessarily a strategic challenge but a question of implementing an existing playbook with a menu of options. On the other hand, thinking about how cyber cooperation works in the military domain in the alliance context is uncharted territory and requires careful strategic thinking, coordination on joint operations and areas of delegation, and long-term concerted development of corresponding operational capabilities. In many ways, the conversation has only just begun.

Appendix A: List of Publicly Reported Instances of US-South Korea Cyber Cooperation, 2022-2024[51]

Date	Title	Meeting Type
5/21/2022	United States-Republic of Korea Leaders' Joint Statement	Joint Statement
8/10/2022	Outcome of the First ROK-U.S. Working Group Meeting on the DPRK Cyber Threat	NK Working Group Meeting
11/16/2022	Second U.S.-ROK Working Group Meeting on the DPRK Cyber Threat	NK Working Group Meeting
11/17/2022	U.S.-ROK Joint Symposium on Countering DPRK Cyber Threats to Cryptocurrency Exchanges	Cyber Consultation
12/16/2022	The Sixth ROK-U.S. Cyber Consultation	Cyber Consultation
2/9/2023	#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities	Joint Advisory
3/9/2023	The Third U.S.-ROK Working Group Meeting on the DPRK Cyber Threat	NK Working Group Meeting
4/20/2023	Strategic Cybersecurity Cooperation Framework Between the Republic of Korea and the United States	Joint Statement
4/26/2023	Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea	Joint Statement
5/23/2023	Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities	Joint Sanction
6/1/2023	U.S., ROK Agencies Alert: DPRK Cyber Actors Impersonating Targets to Collect Intelligence	Joint Advisory
6/23/2023	First ROK-U.S. Cybersecurity Senior Steering Group	Cyber Consultation
7/26/2023	Fourth U.S.-ROK Working Group Meeting on the DPRK Cyber Threat	NK Working Group Meeting

8/11/2023	The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States	Joint Statement
8/31/2023	Treasury Targets Individuals and Entity Supporting the Democratic People's Republic of Korea's Weapons of Mass Destruction Program	Joint Sanction
10/18/2023	Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers	Joint Advisory
11/1/2023	Second ROK-U.K. Cybersecurity Senior Steering Group	Cyber Consultation
11/7/2023	Fifth United States-Republic of Korea Working Group Meeting on Democratic People's Republic of Korea Cyber Threats	NK Working Group Meeting
11/9/2023	CISA Signs Memorandum of Understanding with the Republic of Korea to Share Cyber Threat Information and Cybersecurity Best Practices	Joint Advisory
11/30/2023	Treasury Targets DPRK's International Agents and Illicit Cyber Intrusion Group	Joint Sanction
12/7/2023	Inaugural United States-Japan-ROK Trilateral Diplomatic Working Group Meeting on DPRK Cyber Activities	US-ROK-Japan Meeting on Cyber
12/9/2023	U.S.-ROK Next Generation Critical and Emerging Technologies (CET) Dialogue	Joint Statement
1/24/2024	Seventh U.S.-ROK Cyber Policy Consultations	Cyber Consultation
1/26/2024	S. Korea, U.S. Hold 1st Joint Cyber Security Drill	Joint Cyber Military Exercise
3/27/2024	Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program	Joint Sanction
3/28/2024	Sixth United States-Republic of Korea Working Group Meeting on Democratic People's Republic of Korea Cyber Threats	NK Working Group Meeting

3/29/2024	Second United States-Japan-Republic of Korea Trilateral Diplomatic Working Group Meeting on Democratic People's Republic of Korea Cyber Activities	US-ROK-Japan Meeting on Cyber
5/12/2024	Third ROK-U.S. Cybersecurity Senior Steering Group Held	Cyber Consultation
6/28/2024	First Execution of Multi-Domain Japan-ROK-U.S. Exercise FREEDOM EDGE	Joint Cyber Military Exercise
7/25/2024	FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity	Joint Advisory
7/25/2024	North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs	Joint Advisory
8/27/2024	Joint U.S.-ROK Symposium on Protecting the Virtual Asset Industry from DPRK Exploitation and Disrupting DPRK Revenue Generation	Cyber Consultation
9/5/2024	Seventh United States-Republic of Korea Working Group to Counter Cyber Threats Posed by the Democratic People's Republic of Korea	NK Working Group Meeting

Endnotes

[1] Joon Ha Park and Shreyas Reddy, "Seoul's defense ministry hit by DDoS cyberattack, possibly by North Korea," NK News, November 6, 2024, https://www.nknews.org/2024/11/seouls-defense-ministry-hit-by-ddos-cyberattack-possibly-by-north-korea/.

[2] Office of the President, "Office of National Security, Establishment of the Yoon Suk-yeol Administration's 'National Cybersecurity Strategy' [국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립]," February 1, 2024, https://www.president.go.kr/newsroom/press/gdXzwtKB; US Department of Defense, "2018 Department of Defense Cyber Strategy," September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[3] US Cybersecurity and Infrastructure Security Agency, "North Korea State-Sponsored Cyber Threat: Advisories," https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/north-korea/publications.

[4] Codi Starks et al., "Staying a Step Ahead: Mitigating the DPRK IT Worker Threat," Google Cloud Blog, September 23, 2024, https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat.

[5] Michelle Nichols, "Exclusive: North Korea Laundered $147.5 Mln in Stolen Crypto in March, Say UN Experts," Reuters, May 14, 2024, https://www.reuters.com/technology/cybersecurity/north-korea-laundered-1475-mln-stolen-crypto-march-say-un-experts-2024-05-14/.

[6] "North Korean Hackers Stole $600 Million in Crypto in 2023," TRM Labs, January 5, 2024, https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023#:~:text=The%20Democratic%20People%27s%20Republic%20of,not%20linked%20to%20North%20Korea.

[7] Aaron Schaffer, "North Korean Hackers Linked to $620 Million Axie Infinity Crypto Heist," *The Washington Post*, October 28, 2024, https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/.

[8] Jenny Jun, "Testimony before the House Foreign Affairs Subcommittee on Indo-Pacific: Illicit IT: Bankrolling Kim Jong Un," Center for Security and Emerging Technology (CSET), Georgetown University, July 27, 2023, https://cset.georgetown.edu/wp-content/uploads/Jenny-Jun-Testimony-before-the-House-Foreign-Affairs-Subcommittee-on-Indo-Pacific.pdf.

[9] Sean Lyngaas, "Half of North Korean Missile Program Funded by Cyberattacks and Crypto Theft, White House Says," CNN, May 10, 2023, https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html.

[10] Jonathan Greig, "North Korean Hacking Group Targeted Weapons Blueprints, Nuclear Facilities in Cyber Campaigns," The Record, July 25, 2024, https://therecord.media/north-korea-andariel-apt45-weapons-systems-nuclear-facilities.

[11] Michelle Ye Hee Lee and Tim Starks, "North Korean Hackers Play the 'Long Con' by Targeting Experts," *The Washington Post*, March 28, 2023, https://www.washingtonpost.com/world/2023/03/28/north-korea-hackers-phishing-attack/.

[12] Shreyas Reddy, "Pro-Russia Hackers Attack ROK over Response to North Korean Troop Dispatch," NK News, November 7, 2024, https://www.nknews.org/2024/11/pro-russia-hackers-attack-rok-over-response-to-north-korean-troop-dispatch/.

[13] Andy Greenberg, "Inside Olympic Destroyer, the Most Deceptive Hack in History," Wired, October 17, 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

[14] Seungmin (Helen) Lee, "Revisiting the 2014 Korea Hydro and Nuclear Power Hack: Lessons Learned for South Korean Cybersecurity," 38North, March 22, 2024, https://www.38north.org/2024/03/revisiting-the-2014-korea-hydro-and-nuclear-power-hack-lessons-learned-for-south-korean-cybersecurity/.

[15] Lee Jeong-gu and Kim Seo-young, "Hanwha Ocean Secures S. Korea's 1st U.S. Navy MRO Contract," *Chosun Ilbo*, August 30, 2024, https://www.chosun.com/english/industry-en/2024/08/30/LNZCXD44F5F2NDNEWQPZC6JI6Q/.

[16] Nam Hyun-woo, "National Intelligence Service: 'North Korea Is Concentrating on Hacking the National Shipbuilding Industry [국정원 '北, 국내 조선업계 집중 해킹 정황']," ZDNet Korea, October 5, 2023, https://zdnet.co.kr/view/?no=20231005163027.

[17] Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[18] Hannah Ritchie, "Microsoft: Chinese Hackers Hit Key US Bases on Guam," BBC, May 25, 2023, https://www.bbc.com/news/world-asia-65705198.

[19] The White House, "U.S.-ROK Leaders' Joint Statement," May 21, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/u-s-rok-leaders-joint-statement/.

[20] The White House, "United States-Republic of Korea Leaders' Joint Statement," May 21, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/21/united-states-republic-of-korea-leaders-joint-statement/.

[21] Office of the President, "Strategic Cybersecurity Cooperation Framework Between the Republic of Korea and the United States of America," April 20, 2023, https://www.president.go.kr/download/644956452f9e3.

[22] Charlie Campbell, "South Korea's Intelligence Agency Has Joined NATO's Cyber Defense Unit. China Isn't Happy," *TIME*, May 5, 2022, https://time.com/6173812/south-korea-cyber-nato-china/.

[23] US Department of Justice, "Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams," November 7, 2022, https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions.

[24] "U.S. Seizes $30 Mln in Crypto from North Korea-Linked Hackers," Reuters, September 8, 2022, https://www.reuters.com/technology/us-seizes-30-mln-crypto-north-korea-linked-hackers-2022-09-08/.

[25] US Department of the Treasury, "Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency," November 29, 2023, https://home.treasury.gov/news/press-releases/jy1933.

[26] US Department of Justice, "Tornado Cash Founders Charged with Money Laundering and Sanctions Violations," August 23, 2024, https://www.justice.gov/opa/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations.

[27] US Department of the Treasury, "Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program," March 27, 2024, https://home.treasury.gov/news/press-releases/jy2215.

[28] Park Hyun-ju, "South Korea Hit by Infamous Lazarus andPark Jin Hyok Hack…North Korea's First Independent Sanctions [韓, 악명 높은 라자루스·박진혁 때렸다…北사이버 첫 독자제재]," *Joongang Ilbo*, February 10, 2023, https://www.joongang.co.kr/article/25139694.

[29] US Department of the Treasury, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," May 23, 2023, https://home.treasury.gov/news/press-releases/jy1498.

[30] US Department of Justice, "Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator," August 8, 2024, https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and.

[31] Stu Sjouwerman, "How a North Korean Fake IT Worker Tried to Infiltrate Us," KnowBe4, July 23, 2024, https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us.

[32] Tom Robinson, "North Korea-Linked Atomic Wallet Heist Tops $100 Million," Elliptic, June 13, 2023, https://www.elliptic.co/blog/analysis/north-korea-linked-atomic-wallet-heist-tops-100-million.

[33] Kim Sojeong, "Cybersecurity Implications of the North Korea-Russia Treaty [러북 신조약의 사이버안보 함의 및 시사점]," Institute for National Security Strategy, July 22, 2024.

[34] Victor Cha and Ellen Kim, "Russia's Veto: Dismembering the UN Sanctions Regime on North Korea," Center for Strategic and International Studies, March 29, 2024, https://www.csis.org/analysis/russias-veto-dismembering-un-sanctions-regime-north-korea.

[35] Alexander Martin, "UN Security Council to Debate Cybersecurity Threats, despite Russian Veto," The Record, June 20, 2024, https://therecord.media/un-security-council-cybersecurity-threats-debate.

[36] Office of the President, "Office of National Security, Establishment of the Yoon Suk-yeol Administration's 'National Cybersecurity Strategy' [국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립]"; National Cyber Security Center, "Government Announces National Cybersecurity Basic Plan [정부 합동 '국가 사이버안보 기본계획' 발표]," September 2, 2024, https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=147016&menuNo=010000&subMenuNo=010300&thirdMenuNo=#LINK.

[37] Korea Internet and Security Agency, "First Publication of the South Korean Government's National Cybersecurity Strategy [대한민국 정부 최초 '국가사이버안보전략' 발간]," April 3, 2019, https://www.kisa.or.kr/401/form?postSeq=2372&lang_type=KO&page=.

[38] Office of the President, "Office of National Security, Establishment of the Yoon Suk-yeol Administration's 'National Cybersecurity Strategy' [국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립]."

[39] US Department of Defense, "2018 Department of Defense Cyber Strategy," September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[40] Jaeyoon Woo and Seonghoon Kim, "President Yoon Suk Yeol Emphasized the Importance of Active Defense in Cybersecurity, Saying 'Attack Is the Best Defense,'" *Maeil Business Newspaper*, September 11, 2024, https://www.mk.co.kr/en/politics/11115594.

[41] Office of the President, "Office of National Security, Establishment of the Yoon Suk-yeol Administration's 'National Cybersecurity Strategy' [국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립]."

[42] Office of the President, "Office of National Security, Establishment of the Yoon Suk-yeol Administration's 'National Cybersecurity Strategy' [국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립]."

[43] Office of the President, "Office of National Security, Establishment of the Yoon Suk-yeol Administration's 'National Cybersecurity Strategy' [국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립]."

[44] Office of the President, "National Cybersecurity Basic Plan Executive Summary," September 1, 2024, https://eng.president.go.kr/briefing/TE0xsLB6.

[45] Clint Work, "Navigating South Korea's Plan for Preemption," War on the Rocks, June 9, 2023, https://warontherocks.com/2023/06/south-koreas-plan-for-preemption/.

[46] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (January 1, 2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003.

[47] US Department of Defense, "2018 Department of Defense Cyber Strategy," September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[48] Government of the United Kingdom, "National Cyber Strategy 2022," December 15, 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

[49] Jenny Jun, "Preparing the next phase of US cyber strategy," Atlantic Council, March 30, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/preparing-the-next-phase-of-us-cyber-strategy/.

[50] US Department of State, "Secretary Antony J. Blinken Secretary of Defense Lloyd J. Austin III, Republic of Korea Minister of Foreign Affairs Cho Tae-yul, and Republic of Korea Minister of Defense Kim Yong-hyun at a Joint Press Availability," October 31, 2024, https://www.state.gov/secretary-antony-j-blinken-secretary-of-defense-lloyd-j-austin-iii-republic-of-korea-minister-of-foreign-affairs-cho-tae-yul-and-republic-of-korea-minister-of-defense-kim-yong-hyun-at-a-joint-pre/.

[51] This list has been compiled until September 5, 2024, at the time of writing this draft.