Enhancing Strategic Alignment in Cyberspace Within the U.S.-South Korea Alliance

By Sebastian Garcia

The United States and South Korea both began 2026 with announcements that the respective governments would soon release new, comprehensive national cybersecurity strategies. Following a year of rising cyberattacks against both public and private entities and changes in political leadership, the two countries have recognized the need to update their cyberspace policies to better reflect the changing geopolitical security environment and domestic political priorities. With the release of the U.S. national cybersecurity strategy in March 2026, the Donald Trump administration aligned its cyberspace posture with the same "America First" principles that guided the formulation of its 2025 *National Security Strategy* and *2026 National Defense Strategy*. This new strategy's emphasis on enhancing offensive capabilities, deregulating cybersecurity compliance to foster innovation, and ensuring fair cost distributions with allies may give some trepidation to South Korea as it continues to formulate a strategy that seeks to bolster cybersecurity regulations for the private sector and deepen its intelligence-sharing and cyber capacity-building initiatives with the United States.

At the same time, opportunities arise from the seeming alignment between the allies on strategic priorities, such as building talent pipelines and sustaining technological superiority in AI and other emerging technologies. A South Korean national cybersecurity strategy that actively aligns with U.S. priorities can serve as a new anchor for alliance cooperation and stability, reinforcing credible U.S. commitments to South Korea's defense and leveraging both countries' resources to strengthen private investments in cybersecurity and foster cyber policy innovation.

Considering these significant shifts in cyber policy at a time of proliferating cyber threats and heightened geopolitical tensions, the United States and South Korea should more proactively align their cybersecurity strategies to avoid points of friction, bolster the alliance's combined cyber defense posture, and maintain their technological advantage in cyber warfare. This paper begins by outlining the nature of the threat posed to critical infrastructure and private enterprises by North Korea and other critical cyber threats. The following section assesses the strategic shifts in the cybersecurity policies of the Trump and Lee Jae Myung administrations, noting where the allies diverge and where they may find common ground. Based on these shared priorities, the paper makes three recommendations for strengthening U.S.-South Korea strategic alignment. Allied cooperation in building a framework that measures cost and impact to better induce private-sector cybersecurity investment and in developing a talent pipeline for the cyber workforce are two means by which the United States and South Korea can jointly increase cyber resilience and maintain their technical advantage in cyberspace. Meanwhile,

---

Sebastian Garcia is Program Officer at the Korea Economic Institute of America. He received his M.S. in Foreign Service from Georgetown University.

expanding South Korea's multilateral cyber cooperation with other allied nations can demonstrate both its leadership efforts and commitment to sharing the cybersecurity burden. The paper concludes with a brief discussion of the need for vigilance and a high degree of flexibility in allied cybersecurity strategy, given the rapidly evolving cyber-threat landscape.

North Korean Cyber Capabilities and Proliferating Cyber Threats

Rather than being an ancillary issue in the array of security challenges facing the U.S.-South Korea alliance, North Korea's cyber capabilities are increasingly becoming a primary threat to the alliance given their centrality to North Korea's asymmetric warfare strategy and role as revenue generators for the regime's ballistic missile and weapons of mass destruction (WMD) programs. Outmatched in conventional military capabilities and under heavy international sanctions, North Korea has invested in cyber warfare and cybercrime capabilities to pursue its strategic objectives through asymmetric means for decades, opening its first institute dedicated to the training of "cyber warriors" as early as 1984.[1] Year over year, the pace and scope of North Korean cyberattacks continues to increase, with the vectors of attack diversifying from hacking vulnerable software and critical infrastructure to sophisticated fraud schemes where North Koreans gain employment as remote IT workers for foreign firms, generating revenue for the regime (a reliable stream of around USD 250 million to USD 600 million per year) and stealing sensitive corporate information from the inside.[2] These efforts continue to intensify at a time when multilateral commitments to monitor and report on North Korea's illicit cyber activities and other aspects of international sanctions regime compliance have faltered. Most recently, in March 2024, Russia vetoed the extension of the mandate of the UN Panel of Experts, the primary multilateral investigative body at the UN Security Council responsible for monitoring North Korea's violations of international sanctions—including its illicit cyber operations.[3]

In the absence of the UN Panel of Experts, the United States and South Korea have collaborated closely within a new framework of the eleven-member Multilateral Sanctions Monitoring Team (MSMT) to continue tracking and reporting on North Korea's sanctions violations and criminal activities in cyberspace.[4] The MSMT's first report on North Korea's cyber operations, released on October 22, 2025, details the systematic nature of North Korea's sanctions evasion through cybercriminal activities like cryptocurrency theft and laundering. These attacks are conducted by a cyber force described as "a full-spectrum, national program operating at a sophistication approaching the cyber programs of China and Russia."[5] North Korea has invested heavily in training its cyber force to generate revenue for the regime since the early 2010s, in the face of a floundering domestic economy and stringent international sanctions. These cyber capabilities serve as a means of asymmetric warfare, allowing the country to impose high costs on the United States and South Korea using relatively cheap, elusive tools.

Emerging technologies such as cryptocurrencies and other digital assets are particularly vulnerable to exploitation by adaptive North Korean hacker groups. The total value of cryptocurrency that North Korea has stolen in digital heists rose from USD 1.19 billion in 2024—already a 50 percent increase from 2023—to USD 1.65 billion between January and September

2025 alone, including the USD 1.4 billion Bybit crypto exchange hack, the largest cryptocurrency heist in history.[6] Some attacks are devastating enough to force cryptocurrency exchanges to liquidate their assets and cease operations, as the firm WazirX was forced to do after 45 percent of its users' digital assets were stolen.[7] North Korean officials then use laundered cryptocurrency assets, including less volatile stablecoins and fiat currency exchanged for cryptocurrency by foreign facilitators, to procure military equipment and raw materials such as copper, in violation of international sanctions law. The final UN Panel of Experts report in 2024 estimated that around 40 percent of North Korea's ballistic missile and WMD program was funded through illicit cyber-theft operations, emphasizing the importance of decreasing North Korean cryptocurrency and ransomware heists for U.S.-South Korea deterrence and nonproliferation strategy.[8]

In addition to financing the development of kinetic weapons systems, North Korea's use of cyber operations as a tool of intelligence gathering and irregular warfare in and of itself poses significant security threats to the United States and South Korea. Through social engineering and malware, North Korean hackers continue to infiltrate critical infrastructure like information and communications technology (ICT) firms, steal sensitive data from South Korean defense firms to reverse engineer South Korean missile and missile defense capabilities, and leak thousands of files of personal data from public entities, including the South Korean Supreme Court.[9] Likewise, U.S. entities and digital infrastructure are under constant threat, with the latest North Korean cyberattack targeting Axios—a program that connects apps and web services and has over 100 million weekly downloads. In March 2026, North Korean hacker group UNC1069 gained access to an Axios software developer's work account for three hours and uploaded malware capable of infecting Windows, macOS, and Linux devices, sparking a scramble across thousands of U.S. companies in industries ranging from healthcare to finance to identify compromised devices.[10]

The rapid integration of AI-enabled tools into North Korean cyber operations fits squarely with North Korea's strategy of pursuing asymmetric capabilities that can deliver devastating impacts at relatively low cost. Analysis from the Stimson Center's 38 North program details how North Korean hacker groups have used AI to formulate new tactics for advanced persistent threat (APT) operations, including efforts to stealthily gain access to secure networks and go undetected for long periods.[11] The report highlights that AI tools are thus a significant force multiplier for North Korea's cyber operations, requiring concerted allied efforts to research AI cyber-defense applications and devise coordination mechanisms that enable agile, highly adaptable defense and deterrence strategies. Multifaceted and often hard to detect, North Korea's irregular warfare strategy poses challenges to the U.S.-South Korea alliance in strengthening its cyber-defense capabilities and devising a proportional retaliatory posture to attacks that fall short of the conventional international definition of an act of armed aggression.[12]

North Korea is not the only actor advancing its cyber capabilities to threaten critical U.S. and South Korean interests. Other state adversaries have shown the capacity to penetrate the allies' cyber defenses, as recently evidenced by the Iranian hacker group Handala's attack on the U.S.-based medical device manufacturer Stryker.[13] The growing cyber cooperation between North Korea and Russia, evidenced by reports that North Korean and Russian cyber-

espionage groups are sharing malware developed in both countries, creates a unified cyber-threat landscape among U.S. allies in Europe and the Indo-Pacific, especially as Russian APT operations expand beyond Ukraine to target NATO member states as part of the country's hybrid warfare strategy.[14]

Besides state-sponsored cyberattacks, sector-specific cyber-resilience gaps have become a critical vulnerability for South Korea. In the past year, telephone carriers, credit card companies, and the online retail giant Coupang have all suffered significant data breaches at the hands of non-state cybercriminals, prompting authorities to investigate lax sectoral cyber-management practices and structural weaknesses in South Korea's data governance framework.[15] Although North Korea is the looming threat to the U.S.-South Korea alliance, it is these other country-specific vulnerabilities that have informed recent shifts in both countries' strategic thinking.

Evolution in U.S. and South Korean Cybersecurity Strategy

U.S. cybersecurity strategy began as piecemeal cyber-policy reforms, including presidential directives to secure critical infrastructure and legislation mandating security plans for all online federal systems. However, major cybersecurity incidents and non-cyber national security incidents, such as the September 11 attacks, prompted the George W. Bush administration to publish the first comprehensive U.S. *National Strategy to Secure Cyberspace* in 2003.[16] Focused on priority areas such as protecting critical infrastructure and government systems, promoting cyber training and awareness, and increasing cooperation with the private sector and international partners, the fundamental pillars of U.S. cybersecurity strategy outlined in the Bush administration's document remained largely unchanged over the following two decades, regardless of who occupied the White House. In that vein, the *National Cybersecurity Strategy* released by the Joe Biden administration in 2023 maintained continuity with prior cybersecurity strategies and with defense strategies' "defend forward" approach to proactively identifying and neutralizing threat actors, while expanding the scope of core U.S. cybersecurity interests to include allied cyber defense and non-traditional security concerns such as "secur[ing] our clean energy future."[17]

By contrast, President Trump's *Cyber Strategy for America* takes a far narrower view of national security priorities in cyberspace, as evidenced by its far shorter length (the Trump administration's strategy document amounts to five pages, compared to the Biden administration's thirty-eight pages). What the new strategy does not mention is just as notable as what it does, as there is no description of state actors that pose significant cyber threats to U.S. interests in the document, including North Korea. However, the strategy makes clear that the United States maintains a robust offensive posture in cyberspace to identify and shut down threats from cybercriminals and other adversaries. Ancillary priorities in support of this central goal include modernizing and securing networks and critical infrastructure, unleashing private-sector innovation in cybersecurity and emerging technologies, and constructing a robust U.S. cyber workforce through new talent pipelines.[18]

The Lee administration is still finalizing its new national cybersecurity strategy, scheduled for release within the year.[19] Compared to the United States, South Korea was a latecomer in developing a whole-of-government cyber policy, with the Moon Jae-in administration publishing the first *National Cybersecurity Strategy* in 2019.[20] Following a decade of proliferating cyber threats and increased cyberattacks on vulnerable South Korean infrastructure, the 2019 strategy prioritized enhancing defensive cyber-response capabilities and improved cyber-policy guidance through a governance framework headed by the National Security Office.[21] However, this original strategy was reactive in its overall policy stance, catching up with years of neglect in the cyber-policy space, and it did not identify international and state-sponsored hacking as major national security risks, perhaps due to the sensitive nature of ongoing diplomatic engagements with North Korea.

Under the framework of the Yoon Suk Yeol administration's 2024 *National Cybersecurity Strategy*, South Korean policy shifted toward pursuing offensive cyber capabilities to detect and neutralize North Korean threats, emulating the U.S. "defend forward" approach.[22] Such efforts aligned with the Yoon administration's more hawkish posture toward North Korea, and the 2024 strategy for the first time explicitly named North Korea as the greatest cyber threat to South Korea.

Whether the Lee administration's cybersecurity strategy continues this trend or follows the U.S. example of scaling back its naming and shaming of North Korea remains to be seen. However, it is clear that President Lee seeks to expand South Korea's strategic thinking to encompass his ambitious agenda of establishing South Korea as an "AI Powerhouse" in the cyber domain and tightening private-sector regulations.[23] To protect consumer data and assets and ensure greater information-sharing and proactive cyber defense by the private sector, the new South Korean cybersecurity strategy will feature proposals to expand the government's investigative authority, mandate the disclosure of information regarding cyberattacks, and heavily penalize failures to report hacking incidents.[24] It is this final pillar of Lee's cyber agenda that most directly contravenes the U.S. strategic shift toward deregulation and increased public-private partnerships to maintain a technological advantage in cyberspace.

Opportunities and Vulnerabilities

The simultaneous review and reiteration of national cyber-strategy frameworks in the United States and South Korea present several opportunities and potential pitfalls for alliance cooperation. Whether the Lee administration's cybersecurity strategy follows the U.S. example of scaling back its identification of North Korea as a major cyber threat remains to be seen. But given both leaders' preference for a reconciliatory approach to engaging North Korea, it is likely that the allies' new cybersecurity postures will align in placing less focus on directly challenging state adversaries. While this eases tensions within the alliance, both countries deprioritize state-sponsored cyber threats at their own peril, as the deleterious impact of cyber warfare in the cases of the wars in Ukraine and Iran demonstrates.

The scope of U.S. cyber activity also factors into the potential alignment of U.S.-South Korea cybersecurity strategy. For South Korea, North Korea is its primary and most persistent cyber threat. In 2023, 80 percent of cyberattacks against South Korean public networks were attributed to North Korea, totaling 1.3 million attacks a day.[25] The United States, on the other hand, faces a much wider scope and scale of cyber threats. According to cybersecurity firm CloudSEK, the United States was the most targeted country in 2025 due to its vast digital infrastructure.[26] Cyberattacks against the United States stem from a wide array of state and non-state actors, and while North Korea is responsible for a number of state-sponsored cyberattacks disproportionate to its size, it remains outpaced by the activities of other significant U.S. adversaries such as China, Iran, and Russia.[27] In addition to maintaining robust defensive cyber operations against this multifarious cyber-threat landscape, U.S. cyber-warfare personnel have been called upon to conduct offensive cyber operations in support of multi-domain military campaigns that require significant coordination with other warfighting domains, such as the January 2026 intervention in Venezuela where U.S. Cyber Command carried out attacks to shut down electricity in the city of Caracas and disable Venezuela's air defense radars.[28] These constraints on finite U.S. cyber talent and resources, combined with the aforementioned omission of North Korea from the Cyber Strategy for America, mean that South Korea will have to make an active effort to keep U.S. attention on the North Korean cyber threat and justify the use of U.S. cyber capabilities to deter North Korea. South Korea must also approach this issue carefully, given the new U.S. cybersecurity strategy's emphasis on renegotiating alliance burden-sharing and calling on allies to take on a fairer share of the cost and responsibility for their cyber defense.[29]

While the U.S. focus on burden-sharing has raised concerns about vulnerabilities within the U.S.-South Korea alliance, burden-sharing in cyberspace offers opportunities for mutually beneficial strategic alignment that can help alleviate these frictions. South Korea has made significant advancements in diversifying its arms exports as it aims to achieve USD 20 billion worth of defense exports and become the world's fourth-largest defense industrial exporter by 2030.[30] Increasingly, the Lee administration has also pledged significant investments into domestic AI startup firms to develop new AI-based security products to defend against next-generation cyber threats, with the Korea Internet & Security Agency (KISA) recently announcing a KRW 12 billion (USD 8.31 million) package to support eighteen projects for new security products and services.[31] South Korea's initiatives to increase defense exports and develop the latest AI-enabled cyber countermeasures thus create an opportunity to show the United States how it is making major contributions to its own cyber defense, as well as how it can further improve burden-sharing across the U.S. alliance network through high-technology defense exports to other key allies.

Though Washington's strategy places primacy on unleashing cyber innovation through the private sector with government support, scholars doubt whether reliance on public-private partnerships as a cornerstone of cybersecurity strategy actually produces effective policy and security outcomes.[32] Private firms are often more reticent to take on national security responsibilities than policymakers realize, and the government's agenda of providing

cybersecurity for the public good does not always align with the cost-benefit calculus of entities operating under market conditions. The success of public-private partnerships, therefore, depends on the formation of shared interests or the delineation of clear rules, roles, and liabilities between the public and private sectors.[33] South Korea may take the latter rule-setting approach to reorganize its domestic cyber governance, but to reach strategic alignment within the U.S.-South Korea alliance, it must work with the United States to seek alternative methods of creating shared interests between the public and private sectors without enacting stringent regulations that the United States will not countenance.

Recommendations for Enhancing U.S.-South Korea Cybersecurity Cooperation

Quantifying Risk, Cost, and Policy Efficacy

Professor VA Greiman of Boston University notes that cybersecurity policies must balance sharing the government's more advanced intelligence-gathering capacity with the private sector "in a manner that permits enhanced protection while protecting the government's sources and methods."[34] In that vein, the United States and South Korea should collaborate to construct a framework that demonstrates the negative externalities imposed by North Korean and other threat actors' cybercrime on private-sector profits to align the private sector's priorities with those of national security-oriented governments. The U.S. national cybersecurity strategy makes it clear that the Trump administration will not pursue this alignment by imposing mandatory minimum cybersecurity regulations that it views as "burdensome" and a drag on firms' innovative capacity.[35]

Scholars have argued that overreliance on minimum-standard checklists is ineffective, as they quickly become outdated, only incentivize compliance rather than innovation and security, and can price out smaller firms that lack the resources to comply with the standards.[36] While South Korea's initiatives to more clearly define liability for cyber incidents and to enforce greater compliance with incident reporting are understandable, given recent trends in large-firm data breaches, its strategic approach to working with the United States to strengthen public-private cybersecurity cooperation should align with the U.S. preference for a non-regulatory approach.

Harvard University's "Cybersecurity Strategy Scorecard" report recommends that states follow Singapore's Cyber Risk Management (CyRiM) project to facilitate private investment in cybersecurity by quantifying cyber risks and the costs of cyberattacks.[37] CyRiM was the product of a collaboration between Nanyang Technological University, the Monetary Authority of Singapore, and other industry and academic partners to estimate the costs of cyberattacks and subsequently build a pricing tool to calculate cybersecurity insurance premiums.[38] Not only would measurable cyber risk demonstrate whether specific government regulations and cyber defense tools are effective or not, the formulation of a baseline insurance premium calculation backed by U.S. and South Korean expertise would also facilitate explosive growth in the cybersecurity insurance market, which has historically experienced slow growth and equally slow adoption—only around 47 percent of eligible firms globally have a cyber insurance policy in

place.[39] Regularizing the expected scope of coverage and services provided by cyber insurance companies and the average cost of incidents such as ransomware attacks can help close the cyber insurance gap. This model, which uses public, private, and academic resources in both countries to develop risk and cost calculation tools, creates new incentives for firms to adopt cybersecurity best practices. It also allows U.S. and South Korean firms to continue competing and conducting business freely without having to navigate differences in the two countries' regulatory frameworks. Insurance markets also provide protection for small and medium-sized enterprises with limited means to independently manage their cyber defense, enabling them to withstand losses from ransomware payments, server downtime, or reputational costs at relatively affordable premium rates.

The advantage of prioritizing joint research into quantifying risk, costs, and regulatory impact as part of U.S.-South Korea cybersecurity collaboration, besides the wealth of technical and academic expertise latent within each nation, stems from the ease of generalizing the cost examples across the United States and South Korea, given their shared threat actors and geopolitical contexts.[40] The allies are intimately aware of North Korean cyber capabilities and the extent of damage North Korean cyberattacks have wreaked in the recent past; creating a shared calculated risk model that can accurately reflect the impact of a ransomware attack on a hospital in Seoul as easily as one in New York City, for instance, would come relatively easily for the allies. Generalized cost examples can also apply across differences in infrastructure, allowing firms in both countries to participate in the insurance market without having to disclose sensitive data about their current cybersecurity practices and prior cyberattack losses.

Developing the Nontechnical Cyber Workforce

Both the U.S. and South Korean cybersecurity strategies have historically outlined talent-building initiatives to expand the technical cybersecurity workforce. Less emphasized, however, is the need for new generations of cybersecurity policy and cyberlaw talent who understand the rapidly advancing corpus of domestic cybersecurity laws and international policy debates. This gap in legal and policy expertise risks long-term "regulatory gaps, ineffective policies, legal vulnerabilities, inefficient cross-sector collaboration, and missed opportunities in international cyber diplomacy."[41] Ensuring a strong nontechnical cybersecurity workforce will be integral to advancing cyber norms agreed upon by the United States and South Korea. North Korea takes advantage of the gray area in international law over whether cyberattacks meet the threshold for acts of war to act aggressively in the cyber domain. In multilateral forums such as the United Nations, South Korea has worked to advance its position and that of the United States, principally that international law applies to cyberspace, striving to build a consensus for establishing the cyber norms of warfare, self-defense, and humanitarian law.[42] Closing the gap in international cyber norms and laws restricts North Korea's ability to conduct offensive cyber operations, as doing so risks exposure to legally sanctioned retributive attacks with limited diplomatic cover, reasserting deterrence by denial in cyberspace.

U.S. and South Korean initiatives to encourage new technical cybersecurity talent pipelines highlight how both states are prioritizing the expansion of the nontechnical cyber labor pool in their cybersecurity strategies. The Trump administration's strategy outlines the broad strokes of "reconciling and taking advantage of existing avenues within academia, vocational and technical schools, corporations, and venture capital opportunities" and "eliminat[ing] roadblocks that prevent industry, academia, government, and the military from aligning incentives and building a highly skilled cyber workforce" that apply in equal measure to the development of technical and nontechnical cyber experts.[43] Cybersecurity competitions and gaming initiatives, such as those sponsored by private cybersecurity firms and the U.S. National Institute of Standards and Technology (NIST), are effective tools for engaging prospective cyber-policy experts across educational levels. High school, college, and professional programs can bring together interested individuals to participate in interactive, competitive cyberattack scenarios to develop their skills in threat analysis, threat response, and defense policy formulation.[44] By sponsoring these competitions, government agencies and private firms alike can identify talent early on, and participants gain the opportunity to develop hard policy skills through hands-on experience, as well as the softer skills of leadership and translating technical subjects into business and policy terms.

The United States and South Korea can also collaborate to foster educational and public-private partnerships that rapidly upskill workers and share talent across different spheres of the cyber-policy environment. Financial firms seeking to invest in future cybersecurity talent often support career programs in academia, including JPMorgan Chase's support for the University of South Florida's Florida Center for Cybersecurity and Capital One's grants to community colleges establishing cybersecurity programs.[45] U.S. and South Korean firms can facilitate similar transnational educational partnerships and exchanges to mutually develop exceptional nontechnical cybersecurity talent, with the potential for support from the U.S. and South Korean governments, depending on the Trump administration's appetite for resuming international cybersecurity aid. Improved opportunities for rotations between U.S. cyber defense agencies and private-sector legal and compliance departments, or temporary assignments of private cybersecurity experts to cyber defense agencies, could also increase the efficacy of public-private cybersecurity partnerships in both countries. As cybersecurity experts become more familiar with the role of the public and private sectors, they can help mend the trust deficit, enhance the speed of threat intelligence-sharing, and inform the government about the latest private-sector innovations and best practices.[46]

Integrating South Korea into Multilateral Cybersecurity Networks

The Lee administration's multilateral diplomacy prioritizes deepening collaboration in cyber defense and AI-enabled resilience with partners in NATO and the Indo-Pacific. From a December 2025 visit to Seoul by a NATO Parliamentary Assembly delegation to bilateral and trilateral U.S.-South Korea-Japan meetings on the sidelines of the Cyber Champions Summit in Czechia in March 2026, South Korea has engaged numerous partners to expand the scope of its threat assessment and defense technology cooperation efforts, closely collaborating with

private South Korean stakeholders in the defense industry for these meetings.[47] South Korea's cybersecurity strategy should continue to prioritize expanding cyber-defense cooperation with like-minded liberal democracies, especially as its ambitions to become a significant developer of advanced dual-use and AI-enabled weapons systems can expand the country's market share in the European defense industry.[48] Deepening these ties also demonstrates to the United States that South Korea is not a free rider on U.S. security guarantees in cyberspace but a proactive contributor to bolstering its own cyber capabilities and those of other U.S. allies. An exchange of lessons learned between NATO's experience providing cybersecurity assistance to Ukraine amid Russian cyberwarfare attacks and South Korea's cyber defense posture against persistent North Korean cyberattacks would also contribute to both sides' understanding of the latest threat actors and capabilities of common adversaries. Such an exchange is increasingly necessary as North Korea continues to lend military assistance to Russia in its war effort against Ukraine, and the two nations likely share and jointly develop their asymmetric cyber capabilities.[49]

South Korea has already made progress in joining multilateral policy dialogues and military exercises related to cyber defense: South Korea's Cyber Operations Command first participated in the NATO Locked Shields cyber defense exercise in 2021, the multinational U.S.-led Cyber Flag exercise in 2022, and jointly launched the first trilateral U.S.-South Korea-Japan Freedom Edge cyber exercises in 2024.[50] The South Korean ambassador for international cyber affairs and the NATO assistant secretary general for cyber and digital transformation have regularly met for high-level cybersecurity dialogues since 2023.[51] The next step for South Korea is to translate these dialogues and engagement into concrete agreements and defense industrial investment deals to establish new South Korean research and development (R&D) centers in NATO member countries and jointly pursue the development of new AI-driven battle management systems, including counter-cyber capabilities to thwart large-scale cyberattacks and APT infiltrations.[52] Chung Min Lee of the Carnegie Endowment for International Peace points to the success of the co-development of new synthetic aperture radar satellites by European aerospace firm Thales Alenia Space and South Korea's Agency for Defense Development, Korea Aerospace Industries, and Hanwha Systems as an example of the potential for NATO-South Korea defense industrial cooperation.[53] He also points to initiatives such as the Security Action for Europe (SAFE) program as avenues for South Korea to increase its joint R&D and defense exports to European partners. South Korea should also push to integrate into NATO's cybersecurity intelligence-sharing infrastructure and regularize the exchange of South Korea's cyber-threat assessments of North Korea and NATO's analyses of Russian cyber threats.

The United States has stated that "the distribution of cost and responsibility must be fair across the U.S. and allies who share our democratic values."[54] South Korea stepping up to fill critical gaps in European cyber and AI warfare defenses and develop broader cyber-threat intelligence-sharing between U.S. allies will cement its status as a model ally committed to burden-sharing and collective defense. Pursuing stronger NATO and Indo-Pacific cyber-defense ties advances the strategic alignment of the U.S. and South Korean cybersecurity strategies and fulfills President Lee's goal of making South Korea the world's fourth-largest defense exporter by 2030.[55]

Conclusion

The Trump and Lee administrations are simultaneously undertaking considerable changes to their respective cybersecurity strategies. While divergent approaches to shaping public-private cooperation and an increased U.S. demand for fair burden-sharing in cyber defense could emerge as points of contention in allied cybersecurity strategy, this moment also offers an opportunity for renewed strategic alignment in the U.S.-South Korea alliance's cyber-defense posture. A joint initiative to quantify cyber risk and costs can form the basis of a combined cyber insurance market that creates shared interests between the public and private sectors in investing in adequate cybersecurity and innovating new solutions to advanced cyber threats. Transnational partnerships and competitions to foster the next generation of nontechnical cybersecurity talent will ensure that, over the long term, the U.S.-South Korea alliance will continue to hold the advantage in proliferating advantageous cybersecurity norms and harmonizing compliance and information-sharing standards across both countries. South Korea can also address the U.S. desire for greater burden-sharing by deepening its integration with the cyber-defense cooperation frameworks of both NATO and Indo-Pacific partners, providing intelligence and R&D investments in cutting-edge AI-enabled cyber-defense capabilities to defend U.S. allies and grow the South Korean defense industry.

Cybersecurity is a field that requires constant adaptation and agility to remain ahead of the latest threat capabilities; tools and strategies considered industry standards and top-of-the-line can become outdated liabilities within the year. Technological disruptions like the emergence of AI and quantum computing, and new geopolitical developments like the strengthening of North Korea-Russia ties, only shorten these time horizons and add to the uncertainty of whether a given cybersecurity strategy is working. However, the U.S.-South Korea alliance has proven resilient and highly adaptive over more than seven decades of geopolitical upheaval and breakthroughs in military capabilities and technology. So long as the allies maintain institutionalized, regularized coordination on cyber policy and cyber defense and accept that their cybersecurity strategies will need to remain flexible frameworks rather than rigid plans, they can successfully safeguard their cyber domains from North Korean and other cyber adversaries.

Endnotes

[1] Jason Bartlett, "Mapping Major Milestones in the Evolution of North Korea's Cyber Program," The Diplomat, July 18, 2022, https://thediplomat.com/2022/07/mapping-major-milestones-in-the-evolution-of-north-koreas-cyber-program/.

[2] Office of Public Affairs, "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes," U.S. Department of Justice, June 30, 2025, https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote; Amanda Gerut, "North Korean IT workers are stealing remote jobs and raking in billions—and Americans are helping them do it," Fortune, April 25, 2026, https://fortune.com/2026/04/25/north-korean-it-worker-scheme-american-faciliators/.

[3] 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.

[4] Participating MSMT countries at the time of writing include Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, South Korea, the United Kingdom, and the United States. See "About MSMT," Multilateral Sanctions Monitoring Team, accessed June 1, 2026, https://msmt.info/About/MSMT.

[5] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," October 22, 2025, 7, https://msmt.info/Publications/detail/MSMT%20Report/4221.

[6] Taylor Rajic and Julia Brock, "The ByBit Heist and the Future of U.S. Crypto Regulation," Center for Strategic and International Studies, March 18, 2025, https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation.

[7] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions," 26.

[8] UN Panel of Experts, "Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)," March 7, 2024, 60, https://docs.un.org/en/S/2024/215.

[9] Multilateral Sanctions Monitoring Team, "The DPRK's Violation and Evasion of UN Sanctions," 8; Hyung-sik Joo et. al., "S. Korean Supreme Court stolen 1TB data by North Korea: Damage extent uncertain," *Chosun Ilbo*, May 13, 2024, https://www.chosun.com/english/north-korea-en/2024/05/13/ECYM6BGMWNFSPFWIVYMZ36XXIE/.

[10] Sean Lyngass, "North Korean hackers bug software used by thousands of US companies in potential crypto heist attempt," CNN, March 31, 2026, https://www.cnn.com/2026/03/31/politics/north-korea-hacking-crypto; A.J. Vicens, "North Korea-linked hack hits largely invisible software that powers online services," Reuters, April 1, 2026, https://www.reuters.com/sustainability/boards-policy-regulation/north-korea-linked-hack-hits-largely-invisible-software-that-powers-online-2026-03-31/; "North Korea-Nexus Threat Actor Compromises Widely Used Axios NPM Package in Supply Chain Attack," Google Threat Intelligence Group, March 31, 2026, https://cloud.google.com/blog/topics/threat-intelligence/north-korea-threat-actor-targets-axios-npm-package.

[11] Michael Barnhart, "North Korea's Integration of AI Across Cyber, Economic, and Military Domains," 38 North, February 27, 2026, https://www.38north.org/2026/02/north-koreas-integration-of-ai-across-cyber-economic-and-military-domains/.

[12] Esther In, "Modern Cyber Warfare and International Law," Cornell Law Review, August 20, 2025, https://publications.lawschool.cornell.edu/lawreview/2025/08/20/modern-cyber-warfare-and-international-law/.

[13] Sean Lyngaas, "Pro-Iran hackers claim cyberattack on major US medical device maker," CNN, March 15, 2026, https://www.cnn.com/2026/03/11/politics/pro-iran-hackers-cyberattack-medical-device-maker.

[14] Anton Sokolin and Shreyas Reddy, "North Korean, Russian cybercriminals join forces for first time: Report," NK News, November 24, 2025, https://www.nknews.org/2025/11/north-korean-russian-cybercriminals-join-forces-for-first-time-report/; Pia Hüsch and Joseph Jarnecki, "DPRK and Russian Collaboration in Cyberspace as a Driver for UK-ROK Cyber Cooperation," 38 North, March 4, 2026, https://www.38north.org/2026/03/dprk-and-russian-collaboration-in-cyberspace-as-a-driver-for-uk-rok-cyber-cooperation/.

[15] Seongeun Lee, "Coupang's Data Breach and the Urgency of Data Governance Reform in South Korea," The Diplomat, March 7, 2026, https://thediplomat.com/2026/03/coupangs-data-breach-and-the-urgency-of-data-governance-reform-in-south-korea/; Ji-won Choi, "Lotte Card hack exposes data of 3 million users," *The Korea Herald,* September 18, 2025, https://www.koreaherald.com/article/10578647.

[16] Vaibhav Garg et al., "National Cyber Security Strategies: The Past, Present, and Future," Usenix, July 31, 2025, https://www.usenix.org/publications/loginonline/national-cyber-security-strategies-past-present-and-future.

[17] The White House, "National Cybersecurity Strategy," March 2023, 25, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[18] The White House, "President Trump's Cyber Strategy for America," March 2026, https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

[19] A-ri Choi, "Government Unveils Comprehensive Cybersecurity Strategy," *Chosun Ilbo*, October 22, 2025, https://www.chosun.com/english/industry-en/2025/10/22/2UFKFNC44ZCRFD4KFHHIYKHKDY/.

[20] "National Cybersecurity Strategy," South Korean National Security Office, April 2019, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf.

[21] Joohui Park and Donghee Kim, "Forging Forward: South Korea's Proactive Cyber Defense and Strategic Cooperation with the United States," Center for Strategic and International Studies, July 10, 2025, https://www.csis.org/analysis/forging-forward-south-koreas-proactive-cyber-defense-and-strategic-cooperation-united; E.D. Ivanov, "The Cybersecurity Policy of the Republic of Korea 2017–2025," *Herald of the Russian Academy of sciences* 6 (2025): 20–33, https://kazanmedjournal.ru/0131-2812/article/view/698887.

[22] Natasha Wood, "South Korea's 2024 Cyber Strategy: A Primer," Center for Strategic and International Studies, August 2, 2024, https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer.

[23] Choi, “Government Unveils Comprehensive Cybersecurity Strategy.”

[24] Choi, “Government Unveils Comprehensive Cybersecurity Strategy.”

[25] Hüsch and Jarnecki, “DPRK and Russian Collaboration in Cyberspace.”

[26] “Top 10 Countries Hit Hardest by Cybercrime in 2025,” CloudSEK, February 13, 2026, https://www.cloudsek.com/knowledge-base/countries-most-targeted-by-cyberattacks.

[27] “Cyber Operations Tracker,” Council on Foreign Relations, accessed May 13, 2026, https://www.cfr.org/cyber-operations/.

[28] Julian E. Barnes and Anatoly Kurmanaev, “Cyberattack in Venezuela Demonstrated Precision of U.S. Capabilities,” *New York Times*, January 15, 2026, https://www.nytimes.com/2026/01/15/us/politics/cyberattack-venezuela-military.html.

[29] White House, “President Trump’s Cyber Strategy for America.”

[30] “Defense chief urges efforts to back Korea’s goal of No. 4 arms exporter,” *Korea Times*, January 14, 2026, https://www.koreatimes.co.kr/southkorea/defense/20260114/defense-chief-urges-efforts-to-back-koreas-goal-of-no-4-arms-exporter.

[31] Jae-eun Lee, “Government Invests 12 Billion Won to Foster AI Security Firms,” *Chosun Ilbo*, May 8, 2026, https://www.chosun.com/english/industry-en/2026/05/08/ZX53QD5Z7VB3NONONO7S47KHR4/.

[32] Madeline Carr, “Public–Private Partnerships in National Cyber-Security Strategies,” *International Affairs (Royal Institute of International Affairs 1944-)* 92, no. 1 (2016): 43–62, http://www.jstor.org/stable/24757834.

[33] Carr, “Public–Private Partnerships in National Cyber-Security Strategies,” 61–62.

[34] VA Greiman, “Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration,” *Journal of Information Warfare* 14, no. 3 (2015): 30–42, https://www.jstor.org/stable/26502729.

[35] The White House, “President Trump’s Cyber Strategy for America,” 4.

[36] Fred Heiding et al., “Cybersecurity Strategy Scorecard,” *Belfer Center for Science and International Affairs,* March 27, 2025, 54, https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard.

[37] Heiding et al., “Cybersecurity Strategy Scorecard,” 37.

[38] Heiding et al., “Cybersecurity Strategy Scorecard,” 53.

[39] Cooper J. Attig and Eric J. Pennesi, “Cybersecurity Insurance – A Burgeoning Global Market,” Morgan Lewis, October 10, 2025, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/10/cybersecurity-insurance-a-burgeoning-global-market.

[40] Heiding et al., “Cybersecurity Strategy Scorecard,” 53.

[41] Heiding et al., “Cybersecurity Strategy Scorecard,” 19–20.

[42] Adam Segal, "South Korea and the U.S.-China Competition over Cyberspace," in *Between the Eagle and the Dragon: Challenges and Opportunities for South Korea in the U.S.-China Competition,* ed. Sue Mi Terry (The Wilson Center, 2022), 37, https://diplomacy21-adelphi.wilsoncenter.org/publication/between-eagle-and-dragon-essays.

[43] White House, "President Trump's Cyber Strategy for America," 6.

[44] Monica Ricci and Jessica Gulick, "Cybersecurity Games: Building Tomorrow's Workforce," *Journal of Law & Cyber Warfare* 5, no. 2 (2017): 183–224, http://www.jstor.org/stable/26441274.

[45] Tim Maurer and Arthur Nelson, "Priority #4: Cybersecurity Workforce Challenges," in *International Strategy to Better Protect the Financial System Against Cyber Threats,* Carnegie Endowment for International Peace, 2020, 114, http://www.jstor.org/stable/resrep26915.10.

[46] Heiding et al., "Cybersecurity Strategy Scorecard," 55–56.

[47] NATO Parliamentary Assembly, "Korea's Defence Ambitions and Cutting-Edge Tech Take Centre Stage in NATO Parliamentary Visit," December 5, 2025, https://www.nato-pa.int/news/koreas-defence-ambitions-and-cutting-edge-tech-take-centre-stage-nato-parliamentary-visit; "Gov't discusses ways to expand cybersecurity cooperation with NATO members," *The Korea Herald,* March 17, 2026, https://www.koreaherald.com/article/10696533.

[48] Chung Min Lee, "Are Long-Term NATO–South Korea Defense Ties Possible? Transitioning From an Arms Exporter to a Trusted Defense Partner," Carnegie Endowment for International Peace, February 18, 2026, https://carnegieendowment.org/research/2026/02/are-long-term-nato-south-korea-defense-ties-possible-transitioning-from-an-arms-exporter-to-a-trusted-defense-partner.

[49] Pia Hüsch and Joseph Jarnecki, "DPRK and Russian Collaboration in Cyberspace as a Driver for UK-ROK Cyber Cooperation," 38 North, March 4, 2026, https://www.38north.org/2026/03/dprk-and-russian-collaboration-in-cyberspace-as-a-driver-for-uk-rok-cyber-cooperation/.

[50] Joo-young Hwang, "S. Korea joins US-led multinational cyber defense drill," *The Korea Herald,* July 21, 2025, https://www.koreaherald.com/article/10536160; U.S. Indo-Pacific Command Public Affairs, "TRILATERAL STATEMENT: First Execution of Multi-Domain Japan - ROK - U.S. Exercise FREEDOM EDGE," June 27, 2024, https://www.navy.mil/Press-Office/News-Stories/Article/3819224/trilateral-statement-first-execution-of-multi-domain-japan-rok-us-exercise-free/; NATO, "Relations with the Republic of Korea," July 9, 2025, https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-the-republic-of-korea.

[51] Hyun-soo Kim, "S. Korea, NATO hold high-level talks on cybersecurity cooperation," Yonhap News Agency, September 12, 2025, https://m-en.yna.co.kr/view/AEN20250912003300315?section=national/diplomacy.

[52] Lee, "Are Long-Term NATO–South Korea Defense Ties Possible?"

[53] Lee, "Are Long-Term NATO–South Korea Defense Ties Possible?"

[54] White House, "President Trump's Cyber Strategy for America," 5.

[55] Lee, “Are Long-Term NATO–South Korea Defense Ties Possible?”