KOREA POLICY

2026 | Volume 4 / Issue 1

The U.S.-South Korea Joint Fact Sheet: A Roadmap for the Future of the Alliance

KEI Editorial Board

KEI is registered under FARA on behalf of the Korea Institute for International Economic Policy.
Additional information is available at the Department of Justice, Washington, DC

Printed in the United States of America.
ISSN: 2837-4134

Korea Policy
Volume 4 : Issue 1

The U.S.-South Korea Joint Fact Sheet: A Roadmap for the Future of the Alliance

Preface

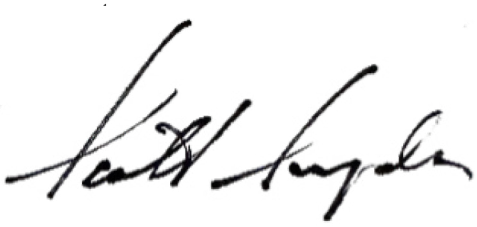
The Korea Economic Institute of America (KEI) is pleased to issue Vol. 4, Issue 1 of its new flagship journal, Korea Policy. Our new online journal carries forward the objective and spirit of KEI's previous publications, the Academic Paper Series' (APS) On Korea publication, and the Joint U.S.-Korea Academic Studies publication. Like our previous publications, Korea Policy identifies and explores the array of security, economic and political issues and policy trends related to Korea and the U.S.-Korea alliance. The journal offers academically rigorous and policy-relevant research.

Korea Policy papers are written by academic scholars and policy experts from the United States, South Korea, and around the globe. The objective is to provide opportunities for recognized specialists and new voices to present fresh research and innovative thinking on Korea, the region, and related international issues. Each issue covers a broad, unifying theme and is arranged into two sections of articles. Before publication, working papers of these articles are presented as part of our Korea Policy series at KEI's office in Washington, DC.

The papers in Vol. 4, Issue 1 exemplify the breadth and depth of policy issues relevant to Korea and the U.S.-Korea alliance. They are original pieces written exclusively for this issue over the last six months. KEI distributes the final publication to individuals in governments, the private sector, policy institutes, and educational communities around the world, and features the digital publication on the KEI website for the broader public.

Contributions in this issue fall under the theme: The U.S.-South Korea Joint Fact Sheet: A Roadmap for the Future of the Alliance. The first section explores U.S.-South Korea alliance modernization in new strategic frontiers by examining key issues in the U.S.-South Korea Joint Fact Sheet, such as alliance deterrence posture and transition of wartime operational control, and bilateral cooperation in the defense industry, nuclear-powered submarines, and the cyber domain. The second section focuses on alliance adaptation to an era of transformation. It revisits past and present issues in the alliance and proposes innovative ideas for South Korea's future economic development, the U.S.-South Korea civil nuclear partnership, and export controls on AI infrastructure.

For over 40 years, KEI has produced objective and informative analyses and highlighted important policy research on Korea. I hope you find this volume of Korea Policy to be a useful contribution.



Scott Snyder
President and CEO
Korea Economic Institute of America
June 2026

Table of Contents

KEI Board of Directors

Mr. Mark Fitzpatrick
International Institute for Strategic Studies - Americas

Dr. Stephan Haggard
University of California San Diego

Dr. Tae Soo Kang
Korea Advanced Institute of Science & Technology

Dr. Danny M. Leipziger
George Washington University

Dr. Kongdan “Katy” Oh
Independent Scholar

Ms. Tami Overby
DGA Group

Dr. Song E. Young
Sogang University

Mr. Scott Snyder
President and CEO, KEI

About KEI

The Korea Economic Institute of America (KEI) is a U.S. policy institute and public outreach organization dedicated to helping Americans understand the breadth and importance of the relationship with the Republic of Korea. Through publications, media, events, and outreach programs, KEI advances scholarship and understanding of Korea that informs policymakers and the American public about the security, economic, and political implications of U.S. ties to the Korean Peninsula.

For over 40 years, KEI has promoted dialogue and understanding between the United States and South Korea through in-depth analysis and conversation. KEI draws on the expertise of resident staff, provides a platform for leading voices from the United States, South Korea, and beyond, commissions original research and analysis, and hosts discussions among policymakers and opinion leaders.

KEI maintains strong ties with U.S. think tanks and academic institutions, generating cutting-edge research on the Korean Peninsula that reaches experts, students, and the broader public.

In today's digital age, KEI reaches a global audience by livestreaming events and providing online commentary, data, and scholastic research through its "Inside the Investment" video series, "Eye on Korea" podcast, and livestreamed and recorded programming.

The U.S.-Korea partnership is built on shared values, but it requires continued effort to sustain. KEI is proud to help uphold this relationship and ensure a safer and more prosperous world.

Introduction

How the U.S.-South Korea Joint Fact Sheet Lays the Future of the Alliance

By Gilbert Rozman

This issue of *Korea Policy* details recommendations for implementing the policy goals set forth in the U.S.-South Korea Joint Fact Sheet reaffirming the Korea Strategic Trade and Investment Deal approved at the summit between U.S. President Donald Trump and South Korean President Lee Jae Myung on October 29, 2025. There are two key sections: 1) new frontiers of cooperation between the two countries to include modernization of the security relationship, defense industrial cooperation, nuclear submarines, and cybersecurity; and 2) adapting the alliance amid global transformation on South Korea's economic development strategy, civil nuclear cooperation, and AI export controls. For compelling reasons explained in the seven articles, the state of the alliance hinges on the successful implementation of these policy goals.

Why is 2026 likely to go down as an unusually significant test of the U.S.-South Korea alliance? At least four reasons deserve close attention. First, it is well-known that South Korea stands on the front line of an increasingly bipolar Northeast Asia, with tensions exacerbated since 2022 as international peace and stability are being shaken. The issues raised in this issue reflect this deteriorating environment. Second, technological change has come to the fore as never before since the advent of nuclear weapons. One article after another cites the urgency of responding to these challenges. Third, the Trump factor must not be overlooked, given his penchant for unilateral action and pressure. Authors do not shy away from mentioning it. Finally, South Korea has emerged as a vital powerhouse for U.S. security and economic transformation. Its critical role emerges repeatedly in the recommendations for alliance transformation for the sake of both states and of the world.

Modernizing the U.S.-South Korea Alliance for New Strategic Frontiers

The four articles on new frontiers of cooperation highlight growing opportunities and risks for the U.S.-South Korea alliance. Reviewing past negotiations and agreements, they point to unfinished business and rapidly changing circumstances. Further delay would pose unprecedented risks.

Section One's articles clarify South Korean thinking at this critical juncture in the alliance. Together, they identify new opportunities resulting from the Joint Fact Sheet and warn of accelerating risks if agenda items are not implemented. The first article calls for deepening U.S.-South Korea coordination on crisis-management mechanisms, political and diplomatic signaling, and China policy to modernize the alliance and contribute to a more sustainable deterrence posture. The second article argues that multi-domain, high-technology hybrid war demands a

---

Gilbert Rozman is Emeritus Musgrave Professor of Sociology at Princeton University and the editor-in-chief of The Asan Forum, a bi-monthly, on-line journal on international relations in the Indo-Pacific region.

qualitative change in U.S.-South Korea defense industry cooperation. The third article explores how South Korea can strengthen its position when requesting the future development of more advanced nuclear-powered submarines (SSNs) by becoming a reliable U.S. partner in submarine maintenance, logistics support, infrastructure hosting, repair planning, and lifecycle services. The fourth article proposes a South Korean national cybersecurity strategy that aligns with U.S. priorities and serves as an anchor for alliance cooperation, reinforcing U.S. commitments to South Korea's defense and leveraging both countries' resources to strengthen private-sector investment in cybersecurity and foster cyber policy innovation.

In "The Path Forward for Alliance Modernization and Redesigning the U.S.-South Korea Alliance," In Hyo Seol warns that despite talk of alliance modernization, neither government has articulated an official definition, implementation plan, or transition roadmap. It notes that the Iran war is acting as a powerful catalyst for accelerating changes to the alliance posture and force deployment in the Indo-Pacific, elevating the discourse on alliance restructuring from an abstract strategic discussion to a concrete, lived reality for expert communities and the broader publics of both nations. Yet, modernizing the alliance entails formidable challenges. Unlike past iterations of burden-sharing discussions, which implied a negotiated redistribution of costs within a broadly unchanged framework, the Trump administration's new interpretation of burden-shifting entails a structural reallocation of responsibility. Allies are expected not merely to pay more but to assume fundamentally different roles—as primary defenders of their own territory, while the United States repositions itself as an enabler and backstop rather than a frontline protector.

The new division of labor portends changes to virtually every dimension of the combined defense posture. Successful modernization would serve as proof of concept for the broader U.S. global alliance restructuring strategy. Conversely, if South Korea—the most capable and best-prepared ally—fails to navigate modernization successfully, the signal sent to other U.S. allies would be deeply damaging. Failure to fundamentally update the alliance would be perilous, warns Seol.

Seol's chapter addresses the need to respond to the systematic application of "America First" principles to alliance restructuring. Strategic flexibility demands a fundamentally different kind of alliance management—based on joint planning and institutional preparation rather than post-hoc diplomatic accommodation. Structural changes could lead to a narrative of retreat, as the public in both countries loses confidence in the alliance and leaders face pressure to hedge against its decline. Among the risks are the coercive negotiating style characteristic of the Trump administration, given that South Korean public opinion on the alliance—while broadly positive—is sensitive to perceptions of unequal treatment and can rapidly shift when the alliance appears to impose costs without corresponding benefits. Also at risk is the prospect that adjustments to United States Forces Korea (USFK) and its physical presence on the Korean Peninsula will be misread as a weakening of extended deterrence. To minimize such risks, Seol calls for expert-level consultations.

In “The Future of U.S.-South Korea Defense Industry Cooperation on AI and Cybersecurity,” Eun-ho Kang emphasizes that “multi-domain, high-technology hybrid war,” in which conventional warfare, cyber warfare, information warfare, electronic warfare, and space warfare unfold simultaneously on a single integrated battlespace, is now a concrete reality on the battlefield. North Korea is rapidly accumulating real combat experience with advanced technologies such as drones and electronic warfare. Meanwhile, South Korea faces internal demographic constraints, and externally, the United States is demanding not only increased defense burden-sharing but also voluntary contributions from its allies. Kang’s article offers recommendations for U.S.-South Korea cooperation in physical AI and cybersecurity—applying these domains to defense shipbuilding.

Multi-domain, high-technology hybrid warfare demands a fundamental shift in South Korea’s force buildup and a qualitative change in U.S.-South Korea defense industry cooperation. The allies need a model of cooperation that combines U.S. advanced AI design capabilities with South Korea’s world-class manufacturing base—and the two countries should apply this model to the defense shipbuilding sector. As land, sea, and air domains are integrated with space, cyber, and electronic warfare into a single battlespace, inferiority in any one domain translates into paralysis of the entire operation. The boundary between peacetime and wartime has collapsed. Hybrid warfare integrates conventional warfare, irregular warfare, cyber warfare, information warfare, and economic coercion. Warfare has become a war of attrition. In addition, software supply-chain contamination is a major threat, as is North Korea’s evolving conventional forces and real-world experience.

The alliance is being redefined as a structure in which each country maintains a certain level of independent deterrence and response capability and operates in a complementary manner, building an integrated command-and-control system that connects land, sea, and air weapon systems with space, sensors, and command communications. The South Korean armed forces should reorganize around unmanned systems by applying physical AI technology and enabling manned-unmanned teaming, autonomous operation, and robotic/AI pilots. South Korea’s role in enhancing U.S.-South Korea defense cooperation will thus become more important moving forward.

Kang highlights that the shipbuilding industry is the optimal showcase for the future of U.S.-South Korea defense cooperation—one that simultaneously demands collaboration in physical AI and cybersecurity. South Korea’s strengths make partnering with it an irreplaceable option in rebuilding the U.S. shipbuilding industry. Defense shipbuilding cooperation goes beyond simple industrial cooperation; it serves as a powerful model of security cooperation that embeds alliance trust in industry and technology. Successful cooperation in this sector is expected to rapidly spread to other areas, such as aviation and ground weapons.

In “Pathways to Cooperation for South Korea’s Successful Nuclear-Powered Submarine Acquisition,” Jihoon Yu identifies the legal, political, and technological barriers to South Korea’s successful acquisition of nuclear submarines. Failure in this endeavor, launched through

Trump's October 2025 approval, could deepen distrust in Washington, raise concerns regarding proliferation, and damage bilateral relations. Nonproliferation commitments, export control rules, alliance equity concerns, and the strain on the U.S. submarine-industrial base all weigh heavily on the issue. Yu recommends a phased strategy, grounded in a clear alliance-centered rationale, a legally sound, nonproliferation-centric framework, an industrial and human-capital compact that also benefits the United States, a gradual and transparent approach to sustainment and fuel cycle issues, and a broader diplomatic narrative that presents a South Korean SSN as a stabilizing and defensive contribution to regional maritime security. A disciplined approach will be far more credible than one that appears designed to maximize fuel cycle freedom. The more Seoul presents itself as the ally pursuing the most nonproliferation-compatible route, the easier it becomes to justify engagement.

Yu, however, worries that South Korea may not handle the SSN negotiations well, which could deepen mistrust in Washington, raise nonproliferation concerns, and leave U.S. officials with the impression that Seoul is asking for the most sensitive form of support before demonstrating the political discipline and institutional preparation such support would require. Thus, the most promising path is gradual, alliance-centered, and institutionally serious. Seoul should begin the process by demonstrating restraint, nonproliferation responsibility, industrial usefulness, workforce commitment, and diplomatic maturity. Yu urges South Korea to anchor the SSN debate in combined deterrence rather than prestige, maritime burden-sharing rather than autonomy theatrics, safeguards-compatible discipline rather than ambiguity, and long-term alliance trust rather than short-term political pressure. Succeeding in SSN acquisition will test the alliance, but successful implementation will expand alliance cooperation to a new frontier.

In "Enhancing Strategic Alignment in Cyberspace Within the U.S.-South Korea Alliance," Sebastian Garcia observes that cybersecurity requires constant adaptation and agility to remain ahead of the latest threat capabilities. Technological disruptions, including the emergence of AI, and new geopolitical developments, such as the strengthening of North Korea-Russia ties, only shorten time horizons. Garcia's article proposes a South Korean national cybersecurity strategy that aligns with U.S. priorities, serving as a new anchor of alliance cooperation and stability, reinforcing credible U.S. commitments to South Korea's defense, and leveraging both countries' resources to strengthen private-sector investment in cybersecurity and foster cyber policy innovation. South Korea should work with the United States to seek alternative means of fostering shared interests between the public and private sectors without enacting stringent regulations that the United States will not countenance. This means formulating a new cybersecurity agenda to foster the development of a robust cyber insurance market, expand talent recruitment pipelines for the cyber policy and legal workforces, and deepen South Korea-Europe defense industrial partnerships in AI-enabled cyber capability research and development.

Central to the alliance's defense posture in cyberspace is deterring the North Korean cyber threat, which has grown bolder and more sophisticated over the past decade. Its use of cyber operations as a tool of intelligence gathering and irregular warfare poses significant security

threats. Garcia warns against moves that could undermine the U.S. strategic shift toward deregulation and recommends increasing public-private partnerships to maintain the U.S. technological advantage in cyberspace. The challenge is to demonstrate that South Korea is not a free rider in cyberspace but a proactive contributor to bolstering its own and other U.S. allies' cyber capabilities. While divergent methods for shaping public-private cooperation and an increased U.S. demand for burden-sharing in cyber defense could be points of contention, this moment yields an opportunity for renewed alignment, including deterrence of a bolder, more sophisticated North Korean cyber threat.

Alliance Adaptation in an Era of Transformation

The common theme across Section Two's articles is the application and impact of advanced technology, which present new opportunities for coordination. However, challenges include an unsustainable South Korean approach to economic development; shifts in U.S. political and commercial thinking on spent fuel recycling and implications for South Korea; and risk management for high-performance AI systems through infrastructure governance and joint export controls. The authors address these urgent needs with bold proposals.

In "South Korea's New External Economic Development Strategy," Taeho Bark and Dongchul Kwak warn that given U.S. prioritization of domestic production over foreign investment and international trade, South Korea needs a new external economic development strategy. Bark and Kwak argue that the global trade environment has been uprooted; states are pursuing unilateral and discretionary industrial and trade policies aimed at maximizing or protecting national interests. Forced, along with others, to conclude agreements requiring large-scale investments in the United States, South Korea must recognize that expanded exports and high-standard free trade agreements (FTAs) are insufficient. The authors call for leveraging overseas foreign direct investment (FDI) to enhance domestic industrial competitiveness, expand exports, create jobs, and minimize the risks of industrial hollowing-out. Optimism rests on the fact that South Korean firms possess world-class manufacturing capabilities in advanced technologies and core industries and that its large firms already have strong global competitiveness.

Bark and Kwak propose three pillars of South Korea's new external economic development strategy: 1) Expand exports linked to overseas investment by firms; 2) Lead in research and development (R&D) of advanced technology while continuously developing new technologies, attracting world-class foreign firms; and 3) Strengthen the international competitiveness of small and medium-sized enterprises (SMEs). In doing so, South Korea can overcome the challenges of the global trade environment and advance toward a more mature and resilient advanced economy.

For the first pillar, South Korea should transition from primarily producing final goods to becoming a global hub for exporting intermediate goods in advanced manufacturing, thereby supporting national strategic industries. Committed to investing USD 20 billion annually in the United States over the next decade, along with a USD 100 billion investment in U.S. shipbuilding, the South

Korean government should consult closely with South Korean firms and communicate with the U.S. government to ensure these investments serve mutual interests.

For the second pillar, R&D should be clearly defined as enhancing capabilities to develop new technologies, manufacturing products based on those technologies, and assessing their commercial viability. Systems must ensure a seamless transition from laboratory research to pilot testing, initial production, and eventually, mass production. South Korea should establish R&D-manufacturing clusters in strategic industries and attract leading foreign firms to establish R&D bases domestically by offering world-class standards in research autonomy, compensation, long-term visa options, and family settlement.

The third pillar would capitalize on the relocation of foreign firms from China to ASEAN countries and India, while prioritizing the mitigation of barriers faced by South Korean SMEs, such as information gaps, financial constraints, and weak overseas networks. The government should provide structured education and training programs for SME employees covering macro-level changes in the global trade environment, geopolitical risks, the AI-driven technological transition, and supply-chain disruptions, as well as practical knowledge related to overseas markets, international contracts, negotiations, and local management. SMEs should stop viewing overseas investment and exports as high risk.

In “Rethinking the U.S.-South Korea 123 Agreement in a New Strategic Era,” Kayla Orta cites geopolitical shifts in the global civil nuclear market, changing regional security dynamics, rising global energy demand driven by AI, next-generation technologies, and the increased market shares of Chinese and Russian firms as central motivations for capitalizing on the momentum in the United States and South Korea for new nuclear energy policies. Together, the two allies should respond by updating and expanding their 2015 123 Agreement, the author proposes. Near-term opportunities should focus on 1) AI-driven nuclear industry revitalization, 2) traditional and advanced nuclear fuel supplies, and 3) spent fuel management and long-term storage strategies. Industry leaders should not be left out in the planning for a revised framework. For both Washington and Seoul, nuclear energy policy is gaining new momentum; engagement presents a critical opportunity to expand the presence of both countries in global markets while also reinforcing high standards for nuclear safety, security, and nonproliferation.

Orta’s article points to a rising sense of urgency in South Korea that the cooperation framework is not currently meeting its intended goals, and that the U.S.-South Korea civil nuclear relationship remains locked in a cycle of frustration. Points of national security interest—including nuclear fuel import dependencies and limitations in spent fuel waste storage—have strained U.S.-South Korea civil nuclear cooperation. The prolonged hiatus of the High-Level Bilateral Commission has remained a source of frustration for the South Korean government. Another source of concern is that Chinese and Russian state-backed firms have captured significant market shares through competitive financing and rapid-deployment nuclear export packages. The 123 framework needs to be quickly updated.

In “Redefining National Security Governance Through Access and Compute: U.S.-South Korea Export Controls on AI Infrastructure,” ChangHee Kim explores how the rules for AI chip exports are in flux. In March 2026, the U.S. Department of Commerce drafted rules that would require licenses for virtually all AI chip exports, potentially conditioning transfers of more than 200,000 chips on recipient countries agreeing to build AI data centers in the United States. In South Korea, the AI Basic Act entered into force on January 22, 2026, establishing risk-management obligations for high-performance AI systems, with phased enforcement beginning in 2027. The government also began distributing the first tranche of a ten-thousand-unit national graphics processing unit (GPU) pool in March 2026.

Parallel policy imperatives—U.S. efforts to maintain technological leadership and South Korea’s ambitions to secure AI infrastructure capacity—create both opportunities for alignment and governance gaps. Given that AI infrastructure is no longer transferred primarily through the movement of hardware, export control regimes need to move beyond a perspective centered on physical equipment and technical documentation and consider computation and access as core units of control. What is needed is coordination on new AI infrastructure governance, redefining AI data centers as “borderless strategic assets” controlled through access rights—an alliance-based governance model built on compute quotas, Zero Trust, and real-time access control systems.

In place of export control systems structured around the cross-border movement of tangible items and technical documents, technology transfer in a borderless AI infrastructure environment is determined by who can access which compute resources and data, and with what entitlements. Specifically, Kim 1) shows that technology transfer in AI data centers is shifting from physical movement to access entitlement structures; 2) identifies a growing misalignment between data protection law, which has already codified access-based transfer concepts, and export control law, which remains physical and act-based; 3) proposes compute quota as a new policy control concept; and 4) links functional weaponization of AI directly to export and access control debates.

The center of gravity of national security risk is shifting from “What has moved?” to “Who can access which compute resources?” As AI data centers become more sophisticated, Kim argues that export control systems should be redesigned so that access entitlement structures, rather than physical borders, become the core unit of control. Compute quota—the combination of usage time, number of devices used in parallel, and intensity of workloads that yields functional capability—should become the object of control. U.S.-South Korea joint export control is emerging as a realistic alternative. This is not simply a matter of tightening existing rules, but of redesigning alliance-based national security governance by introducing access and compute as new units of control.

Conclusion

In the spring of 2026, a whirlwind of diplomacy centered on China and Iran diverted attention from the U.S.-South Korea alliance. Chinese President Xi Jinping hosted President Trump and Russian President Vladimir Putin before traveling to Pyongyang for a summit with North Korean leader Kim Jong Un. Trump's statements and posts took all the oxygen out of the room, leaving little room to focus on the alliance. Still, with little fanfare, the United States and South Korea continued exploring new frontiers of cooperation and adaptation for the alliance. The AI revolution accelerated these discussions, especially as its application to warfare, as seen in Ukraine and Iran, grew more compelling.

For the issues raised in this volume, a series of questions come to the forefront. 1) Would the "constructive strategic stability" Trump and Xi touted at their summit impact U.S. policy toward South Korea? 2) Would Xi's closer embrace of Kim reverberate in actions that would impact the U.S.-South Korea alliance? 3) Would the way the Iran war appeared to end with a memorandum of understanding affect Trump's foreign policy agenda? and 4) Would the United States pivot back to alliance-building in East Asia at a time when its alliance system was suffering unprecedented disruption? Answers are unlikely to come before the new rounds of diplomacy planned for the fall of 2026. Uncertainty clouds the initiatives discussed in what follows.

Section 1

Modernizing the U.S.-South Korea Alliance for New Strategic Frontiers

The Path Forward for Alliance Modernization and Redesigning the U.S.-South Korea Alliance

By In Hyo Seol

Since the inauguration of U.S. President Donald Trump's second term in January 2025, the restructuring of U.S. alliance relationships has accelerated on a global scale. Within NATO, the June 2025 Hague Summit Declaration committed allies to spend an unprecedented 5 percent of GDP on defense and defense-related investment by 2035. In the Indo-Pacific, the Trump administration has intensified pressure on allies to assume greater security responsibilities while signaling a willingness to recalibrate U.S. force posture. Within the U.S.-South Korea alliance, "alliance modernization" has emerged as the central concept encapsulating this transformation. The publication of the *National Security Strategy* (NSS) in November 2025 and the *National Defense Strategy* (NDS) in January 2026 has sharpened the strategic direction of the new U.S. alliance posture.[1]

As of yet, neither' the United States nor South Korea has formally defined the specific contents of alliance modernization. Given President Trump's negotiating style, which deliberately leverages ambiguity as a bargaining tool, it is likely to remain a fluid concept without a fixed definition.[2] Nevertheless, the broad strategic direction is already discernible. While the term "alliance modernization" has appeared intermittently in the past—most notably in the May 2003 U.S.-South Korea joint statement, in which the two countries agreed to "modernize" the alliance—its meaning under the second Trump administration is qualitatively different.[3] It represents the systematic application of America-First principles to alliance restructuring, an effort refined by a cohort of strategists since Trump's first term that reflects, in part, the deepening of U.S.-China strategic competition and the shifting military balance in the Indo-Pacific.[4]

In the U.S.-South Korea context, the concept gained official traction through a series of signals in 2025. That June, U.S. Chargé d'Affaires to South Korea Joseph Yun publicly expressed a desire to "modernize the alliance." In August, the U.S. Department of Defense characterized alliance modernization as ensuring "credible deterrence for the peninsula and beyond."[5] Most significantly, the November Security Consultative Meeting (SCM) communiqué pledged to "modernize the alliance in a future-oriented and mutually beneficial manner."[6] Yet as of early 2026, neither government has articulated an official definition, implementation plan, or transition roadmap.[7]

What is particularly noteworthy is that the Iran war, which erupted in late February 2026, is now acting as a powerful catalyst for accelerating changes to the United States' alliance

---

Dr. In Hyo Seol is Associate Professor in the Department of Strategic Studies at Korea National Defense University (KNDU). He also serves as Director of the New Security Research Center at KNDU's Research Institute for National Security Affairs.

posture and force deployment in the Indo-Pacific. The crisis has elevated the discourse on alliance restructuring from an abstract strategic discussion to a concrete, lived reality for expert communities and the broader public in both nations.

Alliance modernization entails formidable challenges. It implies fundamental changes to the way an alliance and the combined defense posture that has endured for decades actually operates. These matters have long remained hidden from public view for two reasons. First, many of the operational details have been classified. Second, there has been a persistent concern that open discussion of fundamental changes to the alliance could itself erode trust and credibility between the allies. Yet in a rapidly shifting security environment and evolving regional military balance, proceeding with such far-reaching changes without sufficient deliberation among experts from both countries risks generating unnecessary misunderstanding, controversy, and mutual distrust—an outcome that serves neither country's interests.

This article does not intend to advocate a particular national strategy for either country. Rather, it seeks to provide an analytical foundation upon which experts from both nations can build a shared understanding of the challenges and opportunities ahead. The article proceeds in four parts. The first section analyzes the strategic logic of alliance modernization as articulated in the NSS and NDS, examining its three constituent layers: political-security motivation, defense-strategic prioritization, and military-operational adaptation. The second section examines how the Iran war has transformed alliance modernization from an abstract concept into an urgent operational reality. The third section provides a balanced assessment of the risks and opportunities of pursuing alliance modernization, with particular attention to the structural convergence of military interests between the two countries. The article concludes with recommendations for the path forward, emphasizing the critical role of expert-level dialogue in ensuring a stable transition.

Alliance Modernization and Trump's Second-Term Alliance Strategy

The Essence of Alliance Modernization

The alliance restructuring agenda articulated during Trump's first term—expressed primarily through burden-sharing pressure and the conditionalization of security commitments—has evolved into a far more systematic program in the second term. Whereas the first term focused overwhelmingly on financial contributions, demanding exponential increases in South Korea's annual payment under the Special Measures Agreement and threatening to withdraw forces as leverage, the second term integrates theater-level operational concepts, force posture logic, and military deployment architecture into a comprehensive, redesigned framework.[8]

The two foundational strategy documents of the second term—the 2025 NSS and 2026 NDS—differ markedly from their predecessors in both form and substance. They are notably shorter and less systematically structured than the strategy documents of previous administrations, which aimed to provide overarching guidance to the vast national security apparatus and present a new vision of international order to allies and partners. The current documents are

more directly polemical, criticizing past strategies while making the case for a new direction to the American public. In exchange for this reduced scope, they articulate U.S. positions and demands with unusual directness and clarity.[9]

This evolution matters because it signals that alliance modernization under Trump's second term is not merely a rhetorical shift but a structural project backed by institutional momentum. The appointment of Elbridge Colby as U.S. Under Secretary of Defense for Policy—the same strategist who authored *The Strategy of Denial* and served as the lead architect of the 2018 NDS—ensures that the intellectual framework underpinning burden-shifting and denial-based deterrence is now embedded at the highest operational level of the Pentagon. Similarly, U.S. Deputy Assistant Secretary of Defense for East Asia John Noh has publicly called on Indo-Pacific allies to "dramatically" increase defense spending, prioritize capabilities that deny China's military objectives, and take greater responsibility for actively defending "critical terrain, sea lanes and infrastructure within their regions."[10] The pattern suggests an emerging logic increasingly translated into policy pressure and bureaucratic guidance, rather than a fully institutionalized doctrine.

Prioritization, Burden-Shifting, and Limited Support

The overarching principle animating both documents is prioritization. The NSS declares that the United States will no longer attempt to defend everything but will concentrate on its most vital interests. Homeland defense and the Western Hemisphere receive the highest priority, while secondary threats are to be addressed primarily through allies and partners. Past strategies are criticized as grandiose, while the new approach is characterized as "flexible realism."[11] This framing represents a significant departure from the expansive ambitions of previous administrations, which sought to maintain credible deterrence across all theaters simultaneously.[12]

More consequentially, the strategy documents move beyond the familiar language of burden-sharing to articulate what amounts to burden-shifting. The new formula assigns allies a "primary responsibility" for their own defense and for regional collective defense, while the United States commits to providing "critical but more limited support." The NDS explicitly states that "decades of the United States subsidizing their defense" have led allies to chronically underinvest in their own security—a condition it frames as both strategically unsustainable and economically unjust to U.S. taxpayers.[13] The implications are far-reaching. Unlike burden-sharing, which implies a negotiated redistribution of costs within a broadly unchanged framework, burden-shifting entails a structural reallocation of responsibility. Allies are expected not merely to pay more but to assume fundamentally different roles, becoming the primary defenders of their territory. At the same time, the United States repositions itself as an enabler and backstop rather than a frontline protector. For the U.S.-South Korea alliance, this distinction is not semantic; it portends changes to virtually every dimension of the combined defense posture, from command authority and operational planning to force structure and crisis management procedures.

The NDS offers a strikingly different diagnosis of the simultaneity problem—the challenge of multiple conflicts erupting concurrently across different theaters. The Joe Biden administration treated simultaneity as an inevitable byproduct of U.S.-China competition and responded with a policy of "integrated deterrence," which sought to leverage all instruments of national power in coordination with allies.[14] The 2026 NDS, by contrast, identifies the root cause not in the structural dynamics of great power competition but in allied free-riding. Its logic is straightforward: if allies were adequately fulfilling their defense responsibilities, regional conflicts would be deterred or contained locally, and U.S. intervention capacity would not be stretched across multiple theaters.[15] This diagnosis leads directly to the prescription: allies must assume primary responsibility for their own security, freeing U.S. resources for the highest-priority challenges.

To incentivize compliance rather than resistance, the NSS introduces a differentiated system of incentives and pressure. Allies that demonstrate exemplary commitment to burden-sharing may receive preferential treatment in trade, technology transfer, and arms sales, while those deemed insufficiently committed may face greater pressure or reduced priority.[16] The intent is to create competitive dynamics among allies, encouraging proactive role expansion. The United States also maintains its commitment to providing critical—if more limited—support, recognizing that its own interests are served by preserving allied sovereignty. However, if allies lack sufficient deterrence capability, they may abandon resistance and instead accommodate—or bandwagon with—potential adversaries, a prospect that would severely damage U.S. strategic interests.[17]

From Overwhelming Force to Denial: A Shift in Deterrence Posture

At the military-strategic level, alliance modernization is driven by the growing sophistication of China's anti-access/area denial (A2/AD) capabilities. These capabilities have turned large, fixed, and high-value targets near the first island chain—major bases, ports, command-and-control nodes, and logistics hubs—into increasingly vulnerable assets subject to long-range precision strikes.[18] This creates what might be called the "paradox of forward deployment": the same forward presence that provides deterrence through proximity and rapid response also creates vulnerability to preemptive attack and catastrophic paralysis.[19]

The envisioned response involves redistributing forces within the first island chain to positions along the second island chain, with an emphasis on survivability, mobility, and resilience. Simultaneously, the United States intends to support capacity building for allies within the first island chain so they can sustain deterrence with a reduced U.S. forward presence, while the United States maintains the ability to rapidly deploy forces when required.

This constitutes a fundamental shift in the deterrence paradigm—from deterrence by overwhelming force to deterrence by denial. Overwhelming deterrence, predicated on the forward deployment of massive forces capable of suppressing any crisis from the outset, risks giving adversaries the dangerous perception that a swift fait accompli is achievable by destroying concentrated forward forces in a preemptive strike. The concentration of high-value assets at a small number of known locations creates what strategists call a "target-rich environment" that rewards aggression—precisely the opposite of what deterrence is meant

to achieve. Deterrence by denial, by contrast, demonstrates that even after an initial strike, sufficient forces will survive, reconstitute, and frustrate the adversary's objectives, making aggression a losing proposition regardless of initial tactical success.[20]

From this perspective, alliance modernization could contribute to a more sustainable deterrence posture, but only if it is paired with credible crisis-management mechanisms, careful signaling, and close U.S.-South Korea coordination on China policy. Without such political and diplomatic management, a distributed and resilient posture could just as easily be perceived by Beijing as a more durable containment architecture rather than a path toward a "decent peace."[21] The critical caveat is that successful implementation remains uncertain. Force posture adjustments risk being perceived as a weakening of U.S. security commitments, and the inherent instability of the transition process could itself undermine existing deterrence arrangements before new ones are firmly in place.

The Iran War and the Acceleration of Alliance Modernization

Direct Impact on the Korean Peninsula

On February 28, 2026, the United States and Israel launched large-scale military strikes against Iran, initiating what has become the most significant U.S. military operation in the Middle East since the 2003 operation against Iraq. Responding to the ensuing Iranian retaliation—missile strikes against U.S. bases in the Persian Gulf, drone attacks across the region, and the closure of the Strait of Hormuz—has required an enormous concentration of U.S. military assets, including carrier strike groups, air defense systems, strategic bombers, and ground forces.[22]

The consequences for the Korean Peninsula have been direct and immediate. In March 2026, unusually frequent flights of Boeing C-17 Globemaster III and Lockheed C-5 Galaxy were observed at Osan Air Base—aircraft typically used to transport Patriot and THAAD missile defense components. U.S. media reports confirmed that components of the THAAD system were being relocated from South Korea to the Middle East and that Patriot interceptor missiles from the Indo-Pacific were being deployed to counter Iranian threats.[23]

South Korean President Lee Jae Myung acknowledged the situation at a cabinet meeting, stating, "USFK may dispatch some air defense systems abroad in accordance with its own military needs. While we have expressed opposition, the reality is that we cannot fully push through our position." He added that South Korea's own defenses were sufficient to deter North Korea. This redeployment was not without precedent: in 2025, the U.S. Air Defense Artillery Regiment returned to the Korean Peninsula after being deployed to the Middle East for approximately six months, confirming a pattern of treating peninsula-based assets as globally fungible reserves.[24]

The concept of "strategic flexibility"—the use of U.S. forces stationed in South Korea for off-peninsular operations—has been a point of contention in the alliance since at least the George W. Bush administration, when the United States declared it would withdraw forces from South

Korea for redeployment to Iraq. At that time, then South Korean President Roh Moo-hyun insisted that South Korea "will not be embroiled in any conflict in Northeast Asia against our will," and the allies papered over their differences with carefully worded mutual acknowledgments.[25] The Iran war demonstrates that strategic flexibility is no longer a diplomatic abstraction to be managed through creative language; it is an operational reality implemented unilaterally, in real time, and during live military conflict. This reality demands a fundamentally different kind of alliance management—one based on joint planning and institutional preparation rather than post-hoc diplomatic accommodation.

What the Iran War Reveals

The Iran crisis has highlighted several dynamics central to the logic of alliance modernization and with profound implications for the U.S.-South Korea alliance.

First, the redeployment of key U.S. assets from the Korean Peninsula to another theater is no longer a theoretical possibility but an operational reality. What had been discussed as an abstract contingency—the prospect of U.S. forces and critical defense systems being redirected from the peninsula during an external conflict—is now unfolding in real time. This constitutes a scaled-down preview of what could occur during a future U.S.-China confrontation or a Taiwan contingency, when the demands on U.S. military resources would be vastly greater than those imposed by the war in Iran.

Second, the war has demonstrated the vulnerability of forward-deployed, fixed assets. Reports that a low-cost Iranian drone destroyed a high-value THAAD radar in Jordan—valued at hundreds of millions of dollars—underscore the risks inherent in static forward deployment.[26] In the Indo-Pacific context, where China's A2/AD capabilities are far more sophisticated than those of Iran, the vulnerability of fixed assets within the first island chain would be exponentially greater. Additionally, the Center for Strategic and International Studies assessed that the United States expended a substantial number of THAAD interceptors during the Iran conflict, raising serious questions about the sustainability and replaceability of expensive air defense systems in high-intensity engagements.[27]

Third, the possibility of a simultaneity problem has only intensified. As the Middle East conflict consumes strategic resources, including high-demand, low-density air defense assets critical to Indo-Pacific deterrence, the tools available for the Indo-Pacific are further constrained. This dynamic may create opportunities for provocation by North Korea, which has historically exploited periods of U.S. strategic distraction.[28]

Fourth, and most fundamentally, the Iran war demands that both sides of the alliance confront the changed reality with open eyes. The question is whether Washington and Seoul will continue to grapple with the resulting uncertainty without joint deliberation or develop a shared vision and institutionalize a roadmap for managing the ongoing transformation. How this transition is framed—whether as a U.S. retreat from its security commitments or as the construction of a more survivable and sustainable deterrence architecture—will be decisive for public confidence

and alliance stability on both sides of the Pacific. The framing challenge is not merely a matter of public relations; it reflects a genuine analytical choice about how to interpret the structural changes underway. If the narrative of retreat dominates, it will become self-fulfilling, as the public in both countries loses confidence in the alliance and political leaders face pressures to hedge against its decline. If, however, the narrative of adaptation and resilience gains traction, supported by concrete evidence of continued deterrence capability, the transition can strengthen rather than weaken the alliance.

The Underdeveloped State of Alliance Modernization and Potential Risks

The Underdeveloped State of Alliance Modernization and Its Potential Risks

As of early 2026, the alliance modernization agenda remains underdeveloped. The strategic direction has been articulated through the NSS and NDS, but neither a concrete implementation plan nor a transition roadmap exists. Crucially, there has been insufficient deliberation among mainstream security experts in either country about the operational details of what modernization would actually entail. If wartime operational control (OPCON) transfer—which the fifty-seventh SCM affirmed would proceed through Full Operational Capability verification—moves forward in conjunction with alliance modernization, the combined scope and pace of change will be unprecedented, encompassing command structures, operational plans, force allocation, rules of engagement, and extended deterrence arrangements.[29] U.S. Secretary of Defense Pete Hegseth has publicly endorsed South Korea's pursuit of OPCON transfer as a "great" endeavor reflecting South Korea's growing military capability, while Under Secretary Colby has advocated reviewing the conditions for transfer, potentially lowering the bar for compliance.[30] This creates a situation in which political momentum toward rapid change may outpace the institutional preparation needed to ensure a stable transition.

Several specific risks demand careful attention. The first concerns the Trump administration's coercive negotiating style. The use of tariffs, economic pressure, and deliberate strategic uncertainty as bargaining leverage may yield short-term concessions, but risks eroding the predictability and trust that undergird alliance cohesion. Alliance theorists have long observed that the deliberate cultivation of uncertainty intensifies both abandonment and entrapment anxieties, creating a volatile dynamic in which rational expectations become difficult to sustain, and misperception becomes more likely.[31] In the U.S.-South Korea context, this dynamic is particularly dangerous because South Korean public opinion on the alliance—while broadly positive—is sensitive to perceptions of unequal treatment and can shift rapidly when the alliance appears to impose costs without corresponding benefits.[32]

The second risk lies in the insufficiently explored nature of the issues at stake. Force posture restructuring, changes to command arrangements, adjustments to extended deterrence operations, and revisions to crisis management protocols are complex, sensitive matters that demand intensive expert engagement. The problem is not that alliance modernization is moving too fast, but that the expert-level deliberation needed to support it has not yet begun in earnest. They must be launched immediately and proceed in parallel with the political and institutional

process. Without such concurrent deliberation, the risk is not that change happens too quickly, but that it happens without the shared understanding needed to prevent confusion, misperception, and a decline in mutual confidence. The history of alliance management demonstrates that the most dangerous moments are not disagreements over policy, but misunderstandings about intentions—precisely the condition that the absence of substantive expert dialogue creates.[33]

Third, adjustments to U.S. force posture risk being interpreted as a contraction of the U.S. defense commitment. In South Korea, the historical memory of the Acheson Line—U.S. Secretary of State Dean Acheson's January 1950 speech defining the U.S. defense perimeter in a way that excluded the Korean Peninsula, widely regarded as having contributed to North Korea's miscalculation in starting the Korean War—remains a powerful frame of reference.[34] Any perceived U.S. withdrawal or pullback is likely to trigger significant public anxiety in South Korea. These concerns were heightened when the November 2025 SCM communiqué notably omitted previous U.S. pledges to maintain U.S. Forces Korea (USFK) at current force levels and removed language stating that any North Korean nuclear attack would lead to the end of the North Korean regime.[35]

Fourth, there is the risk that adjustments to USFK's physical presence will be misread as a weakening of U.S. extended deterrence. USFK has long been perceived as the tangible guarantor of the U.S. nuclear umbrella: "the physical manifestation of the U.S. ironclad commitment to the U.S.-ROK mutual defense treaty," as the USFK commander himself has characterized it.[36] If its presence is reduced, concerns may arise that this signals a gradual withdrawal, ultimately eroding the U.S. nuclear assurance. The perception that the United States might weaken extended deterrence to reduce its military burden could fundamentally undermine deterrence against North Korea's nuclear threat, with cascading consequences for regional stability.

Structural Opportunities: Why Alliance Modernization Can Succeed

Alliance modernization also presents significant opportunities for both countries—opportunities that expert communities must work to identify, articulate, and maximize. A failure to recognize these opportunities risks ceding the narrative entirely to the risks, producing a self-fulfilling prophecy of alliance deterioration.

South Korea stands as one of the strongest candidates for a "model ally" in U.S. alliance restructuring, provided that Seoul can sustain a bipartisan commitment to deterrence, defense responsibility, and strategic coordination with Washington despite changes in domestic political leadership. It has invested in self-reliant defense capabilities more consistently and for a longer period than virtually any other U.S. ally. With one of the largest and most capable conventional forces among U.S. allies, an annual defense expenditure that ranks eleventh in the world, a defense spending ratio among the highest of U.S. allies relative to GDP at approximately 2.6 percent, and a defense industrial base ranked in the global top ten, South Korea possesses a strong foundation for assuming greater defense responsibility.[37] A successful modernization of the U.S.-South Korea alliance would serve as a proof of concept for the broader U.S. global alliance restructuring strategy, lending credibility to the entire enterprise. Conversely, if the

most capable and best-prepared ally fails to navigate modernization successfully, the signal sent to other U.S. allies would be deeply damaging.

Moreover, South Korea is structurally indispensable to the United States in its long-term competition with China. Its advanced semiconductor industry, world-class shipbuilding capacity, and growing role in global defense exports provide the United States with critical supply-chain resilience and industrial depth essential for sustained strategic competition. South Korea's defense industry has emerged as a major global exporter, with contracts spanning Europe, the Middle East, and Southeast Asia, demonstrating precisely the kind of allied capability development that the NDS's burden-shifting framework envisions.[38] This structural interdependence transcends any single transactional exchange and constitutes a durable basis for building modernized alliance arrangements. For both countries, the modernization process offers an opportunity to deepen cooperation in precisely those technological and industrial domains—semiconductors, advanced manufacturing, AI-enabled defense systems, and naval construction—that will determine the outcome of long-term great-power competition.

The Double Contingency Logic: Convergence of Military Interests

Perhaps the most consequential structural opportunity lies in the convergence of national security interests created by the double contingency problem. The global simultaneity challenge increasingly raises the probability of multiple crises erupting concurrently within the Indo-Pacific itself. At the regional level, the risk of a dual contingency—a Taiwan Strait crisis and a Korean Peninsula crisis occurring simultaneously or in close succession—has grown substantially.[39] Political-military tabletop exercises conducted by the Atlantic Council's Indo-Pacific Security Initiative have demonstrated that the region's security structure increasingly generates conditions in which simultaneous crises become plausible, and that these scenarios present extraordinarily complex challenges for U.S. decision-makers.[40]

The strategic implications are profound. Maintaining deterrence on the Korean Peninsula is essential to achieving the highest-priority U.S. strategic objective in the Indo-Pacific—preventing a Chinese fait accompli against Taiwan. If deterrence on the peninsula fails, the United States would be forced to contend with two simultaneous fronts, drastically complicating its ability to concentrate on the Taiwan contingency. North Korea, for its part, has a structural incentive to exploit a Taiwan crisis: Pyongyang could calculate that with U.S. attention and resources diverted to the Taiwan Strait, the window for coercive action on the peninsula would be wider than at any other time. The possibility of episodic coordination or opportunistic alignment among revisionist states—often captured in the CRINK framework—could further elevate this risk, although the Iran war also revealed limits to their ability or willingness to act in a tightly coordinated manner.[41]

Given these risks, it follows that if South Korea assumes primary responsibility for peninsular defense and the United States provides "critical but more limited support," then the United States retains a powerful structural incentive to ensure that this support is genuinely forthcoming. If the peninsula becomes unstable because U.S. support proves hollow, the entire Indo-

Pacific deterrence architecture unravels. This means that even under the new burden-shifting framework, the United States has compelling self-interested reasons—not merely altruistic or treaty-based ones—to invest in the success of Korean Peninsula deterrence. The logic also runs in the other direction: South Korea's demonstrated capability to maintain peninsular stability with reduced direct U.S. involvement frees U.S. resources for the Taiwan contingency, making the United States a more effective great power competitor and, paradoxically, a more reliable ally.

In other words, alliance modernization need not signify a contraction of the U.S. security commitment. Rather, it can be understood as a redistribution of roles on a foundation of converging military interests. The new division of labor, in which South Korea leads peninsular defense while the United States concentrates on the broader Indo-Pacific challenge, creates a structure in which both sides have strong incentives to fulfill their respective commitments, because the failure of either would undermine the security of both. This is a fundamentally different dynamic from a simple withdrawal or abandonment scenario, and it is essential that expert communities on both sides articulate this distinction clearly.

The Double Nuclear Contingency: Why Extended Deterrence Must Endure

The convergence of interests deepens further—and becomes even more urgent—when considering the nuclear dimension. In a simultaneous crisis involving the Taiwan Strait and the Korean Peninsula, both China and North Korea could employ the threat of tactical nuclear weapons—as Russia has done during its war in Ukraine—to deter U.S. intervention. Russia has demonstrated that nuclear threats, even when not carried out, can significantly constrain the scope and tempo of Western responses and create political paralysis among allied publics.[42] The war in Ukraine has, in effect, provided a real-world laboratory for the coercive use of nuclear threats below the threshold of actual employment. China and North Korea may well internalize this lesson and seek to replicate this dynamic in a future Indo-Pacific crisis, calculating that nuclear brinkmanship can deter or delay U.S. military response at the most critical moments.

North Korea's nuclear arsenal is particularly relevant in this context. Pyongyang has developed and tested a range of tactical nuclear delivery systems—including short-range ballistic missiles, submarine-launched ballistic missiles, and cruise missiles—and explicitly incorporated the use of tactical nuclear weapons into its declared military doctrine.[43] In a dual-contingency scenario, North Korea could threaten or carry out a limited nuclear strike against military targets in South Korea or Japan, calculating that even small-scale nuclear use would fundamentally alter the strategic calculus for the United States and its allies across the Indo-Pacific theater.

The Atlantic Council's Guardian Tiger tabletop exercises found that participants consistently judged that failure of deterrence on the Korean Peninsula in a dual-contingency scenario significantly complicated U.S. options for defending Taiwan.[44] Should nuclear deterrence fail on the Korean Peninsula, even limited North Korean nuclear use would lower the global threshold for nuclear employment. This would place the United States in an extraordinarily difficult position: attempting to defend Taiwan under Chinese nuclear coercion at a moment when the nuclear

taboo has already been breached in the same theater. The cascading effect on U.S. credibility, allied confidence, and the global nuclear nonproliferation order would be devastating.

The implication for alliance modernization is unambiguous. Maintaining credible extended deterrence on the Korean Peninsula is not merely a South Korean interest; it is integral to the viability of U.S. strategy for defending Taiwan and, more broadly, to the preservation of the global nuclear order. This structural logic demonstrates that in the course of alliance modernization, extended deterrence should not be weakened but rather institutionalized with greater precision and sophistication. The mechanisms for nuclear consultation, crisis communication, and escalation management between Washington and Seoul should be strengthened, not attenuated, as part of the modernization process.

The Taiwan Contingency and the Role of the Korean Peninsula

The Iran war has brought to the surface one of the most sensitive challenges embedded in alliance modernization: the question of entrapment and the alliance's out-of-theater role. If the conditions under which peninsula-based assets may be redirected to other contingencies are not addressed through the modernization process, this issue risks becoming a persistent source of friction that corrodes cooperation from within. The Taiwan contingency represents the most consequential version of this challenge. Any military confrontation over Taiwan would be fundamentally shaped by the fact that both the United States and China possess nuclear arsenals and have compelling reasons to prevent nuclear escalation. With Camp Humphreys located in close proximity to Beijing, the direct involvement of peninsula-based U.S. forces in offensive operations against China would risk transforming a Taiwan Strait conflict into a qualitatively different kind of confrontation—one that dramatically raises the threshold of nuclear escalation. It is reasonable to expect that both Washington and Beijing would have strong incentives to limit the Korean Peninsula's direct role in such a crisis, particularly at levels below a full-scale general war.

In practical terms, the most likely role for the Korean Peninsula in a Taiwan scenario would not be as a staging ground for offensive operations against China but as a theater where deterrence against North Korean opportunism must be firmly maintained. Ensuring that Pyongyang does not exploit a Taiwan crisis is a shared interest of the highest order. This logic reinforces the case for an alliance posture in which South Korea assumes primary responsibility for peninsular deterrence, the United States maintains enabler presence and rapiddeployment capabilities for credible support, and forces that would substantively contribute to Taiwan's deterrence are positioned at more dispersed and survivable locations along the second island chain.

Such a reconfiguration must proceed gradually, with the continued presence of USFK serving as the visible anchor of alliance credibility throughout the transition. Even as force composition evolves, the allies should jointly invest in strengthening missile defenses, integrating unmanned and autonomous systems, and incorporating other elements of future warfare that enhance deterrence while reducing the vulnerability of fixed installations. These efforts would alleviate public concerns by demonstrating that the alliance is not contracting but adapting and becoming

more resilient and operationally effective. Over the long term, the Korean Peninsula's strategic significance extends well beyond the current threat environment; as the Arctic emerges as a domain of great-power competition, the peninsula's geographic position will become even more valuable, reinforcing the case for a sustained, if transformed, U.S. commitment.[45]

Conclusion

Trust is the most valuable asset of any alliance. Over more than seven decades, the U.S.-South Korea alliance has accumulated a rich repository of experience and institutional mechanisms for aligning national interests that have not always been naturally convergent. The task of alliance modernization is to leverage this accumulated capital to expand future interest convergence, not to squander it through hasty or poorly considered changes.

Altering the institutional and conceptual foundations that the allies have maintained for decades is an inherently difficult undertaking for both countries. The existing body of preparatory research among expert communities on both sides is insufficient for the scope of change now being contemplated. If sweeping changes are driven primarily by political pressure in the absence of adequate deliberation, this may result in unnecessary friction, misunderstanding, and wasteful controversy that damages the bilateral relationship—precisely when the evolving strategic environment demands close coordination.

Expert dialogue cannot by itself reverse the political logic of the Trump administration or eliminate coercive bargaining. Its more realistic function is to reduce misperception, identify areas of practical convergence, and provide institutional guardrails against avoidable alliance friction. The double-contingency and double-nuclear-contingency analyses presented in this article illustrate one point of convergence: maintaining deterrence on the Korean Peninsula is closely tied to the viability of the broader U.S. regional strategy. Demonstrating the existence of such structural linkages—through rigorous and sustained expert engagement—is essential for instilling confidence among the publics of both nations that the alliance rests on a durable foundation of shared interests, one that endures beyond the fluctuations of any single administration.

For alliance modernization to proceed on stable footing, several concrete steps are needed. First, the specific content and operational conditions of OPCON transfer and "critical but more limited support" must be concretized, institutionalized, and empirically demonstrated through combined exercises, tabletop simulations, and other visible means. What does "critical but more limited support" look like in practice? What assets will the United States commit to providing, under what conditions, and through what mechanisms? These questions cannot be left to ad-hoc negotiation during a crisis; they must be answered in advance through rigorous joint planning. Second, extended deterrence consultation mechanisms, including the bilateral Nuclear Consultative Group (NCG), should be strengthened and expanded to address the new scenarios created by alliance modernization. Third, both countries should invest in joint research programs that bring together military, academic, and policy experts to develop shared analytical frameworks for understanding the transformed alliance. Such institutionalization and

publicization serve as the most persuasive mechanisms for assuring both countries' public that the alliance remains credible, capable, and robust—even as its operational architecture undergoes significant transformation.

Endnotes

[1] The White House, *National Security Strategy of the United States* (November 2025), https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf; U.S. Department of Defense, *National Defense Strategy* (January 2026), https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF. On NATO, see North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration.

[2] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Department of Defense, January 2018), 7, https://media.defense.gov/2020/May/18/2002302061/-1/-1/1/2018-NATIONAL-DEFENSE-STRATEGY-SUMMARY.PDF. The 2018 NDS articulated the principle of being "strategically predictable, but operationally unpredictable"—a stance carried into the second Trump term's alliance strategy.

[3] The White House, "Joint Statement Between the United States of America and the Republic of Korea," May 14, 2003, https://georgewbush-whitehouse.archives.gov/news/releases/2003/05/text/20030514-17.html.

[4] Elbridge A. Colby, *The Strategy of Denial: American Defense in an Age of Great Power Conflict* (Yale University Press, 2021); Fred Fleitz, ed., *An America First Approach to U.S. National Security* (America First Press, 2024); Alexander Velez-Green and Robert Peters, "The Prioritization Imperative: A Strategy to Defend America's Interests in a More Dangerous World," The Heritage Foundation, August 1, 2024, https://www.heritage.org/defense/report/the-prioritization-imperative-strategy-defend-americas-interests-more-dangerous; Dan Caldwell and Jennifer Kavanagh, "Aligning Global Military Posture with U.S. Interests," Defense Priorities, July 9, 2025, https://www.defensepriorities.org/explainers/aligning-global-military-posture-with-us-interests/.

[5] Sang-ho Song, "Alliance Modernization Seeks to Ensure Credible Deterrence on, 'Beyond' Korean Peninsula: Pentagon," Yonhap News Agency, August 8, 2025, https://en.yna.co.kr/view/AEN20250808009652315.

[6] U.S. Department of Defense, "57th Security Consultative Meeting Joint Communique," November 14, 2025, https://media.defense.gov/2025/Nov/14/2003820640/-1/-1/1/57-SECURITY-CONSULTATIVE-MEETING-JOINT-COMMUNIQUE.PDF.

[7] Derek Grossman, "The Devil Is in the Details: U.S. and ROK Seek Alliance Modernization, But How?" Seoul National University Institute for Peace and Unification Studies, August 2025, https://ipus.snu.ac.kr/eng/wp-content/uploads/sites/2/2025/09/ROK-US-POLICY-BRIEF-2025-AUG_ISSUE12.pdf; Jungsup Kim, "Modernizing the ROK–U.S. Alliance and Washington's Strategic Perspective," Sejong Institute, September 25, 2025, https://sejong.org/web/boad/22/egoread.php?bd=22&seq=12473.

[8] Bruce Klingner, "U.S.-South Korea Burden-Sharing Talks Remain Stuck. Here's How to Fix It," Heritage Foundation, April 13, 2020, https://www.heritage.org/china/commentary/us-south-korea-burden-sharing-talk-remain-stuck-heres-how-fix-it; Caldwell and Kavanagh, "Aligning Global Military Posture with U.S. Interests."

[9] James M. Acton et al., "Unpacking Trump's National Security Strategy," Carnegie Endowment for International Peace, January 21, 2026, https://carnegieendowment.org/emissary/2026/01/trump-national-security-strategy; Yang Gyu Kim, "'일차적 책임' 청구서와 '제한된 지원'의 역설: 2026 NDS와 한국의 선택 [The Invoice of 'Primary Responsibility' and the Paradox of 'Limited Support': The 2026 NDS and South Korea's Choices]," RINSA Security Review, no. 236, Research Institute for National Security Affairs, Korea National Defense University, April 30, 2026, https://www.kndu.ac.kr/bbs/rinsa/53/K_25452/artclView.do?layout=unknown.

[10] John Noh, "Advance Policy Questions for John Noh, Nominee to be Assistant Secretary of War for Indo-Pacific Security Affairs," Senate Armed Services Committee, October 2025, https://www.armed-services.senate.gov/noh-apq-responses.

[11] The White House, *National Security Strategy*, 9-10.

[12] The White House, *National Security Strategy of the United States of America* (October 2022), 22, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[13] U.S. Department of Defense, *National Defense Strategy*, 13-14.

[14] The White House, *National Security Strategy of the United States of America*.

[15] U.S. Department of Defense, *National Defense Strategy*, 13-14. The NDS lists the simultaneity problem and allied burden sharing as one of five key elements in its security environment assessment, alongside the homeland/Western Hemisphere, China, Russia, and Iran/North Korea.

[16] The White House, *National Security Strategy*, 12.

[17] U.S. Department of Defense, *National Defense Strategy*, 18-19.

[18] U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (2025), https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF.

[19] Thomas G. Mahnken et al., *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition* (Center for Strategic and Budgetary Assessments, 2020), https://csbaonline.org/research/publications/deterrence-by-detection-a-key-role-for-unmanned-aircraft-systems-in-great-power-competition. On the vulnerability of concentrated forward-deployed forces to Chinese precision strike, see also Evan Braden Montgomery, "Contested Primacy in the Western Pacific: China's Rise and the Future of U.S. Power Projection," *International Security* 38, no. 4 (Spring 2014): 115–149.

[20] Colby, *The Strategy of Denial*; Caldwell and Kavanagh, "Aligning Global Military Posture with U.S. Interests."

[21] U.S. Department of Defense, *National Defense Strategy*, 10.

[22] U.S. Central Command, "Operation Epic Fury Fact Sheet," April 6, 2026, https://www.centcom.mil/Portals/6/Documents/Publications/260406-FactSheet.pdf?ver=ezk_KiJvld1N84sCwrTJEg%3D%3D; Eve Sampson, "Iran War May Force US to Shift Missile Defenses from South Korea, Seoul Says," Defense News, March 11, 2026, https://www.defensenews.com/news/your-military/2026/03/11/iran-war-may-force-us-to-shift-missile-defenses-from-south-korea-seoul-says/.

[23] Heejin Kim and Kyu-Seok Shim, "South Korea Says Can Deter Threats if U.S. Weapons Redeployed to Middle East," Reuters, March 10, 2026, https://www.reuters.com/world/asia-pacific/south-korea-president-says-cant-stop-us-forces-redeploying-weapons-2026-03-10/; Sampson, "Iran War May Force U.S. to Shift Missile Defenses from South Korea, Seoul Says"; Seth Robson and Yoojin Lee, "South Korea Objects to U.S. Military Moving Air Defense System to Middle East," Stars and Stripes, March 11, 2026, https://www.stripes.com/theaters/asia_pacific/2026-03-11/thaad-south-korea-middle-east-iran-21025377.html; "U.S. Did Not Move Defense System from Korea, General Says," Reuters, April 21, 2026, https://www.reuters.com/business/aerospace-defense/us-did-not-move-defense-system-korea-general-says-2026-04-21/; Hui Jie Lim, "South Korea Opposed to U.S. Moving Air Defense Systems in the Country to Middle East: President Lee," CNBC, March 10, 2026, https://www.cnbc.com/2026/03/10/south-korea-patriot-transfer-iran-war-air-defenses.html.

[24] Robson and Lee, "South Korea Objects South Korea Objects to U.S. Military Moving Air Defense System to Middle East." The 2nd Battalion, 1st Air Defense Artillery Regiment returned to South Korea in October 2025 after a six-month deployment to the Middle East, confirming a recurring pattern of treating peninsula-based air defense assets as globally fungible reserves; Wes Rumbaugh, "The Depleting Missile Defense Interceptor Inventory," Center for Strategic and International Studies, December 5, 2025, https://www.csis.org/analysis/depleting-missile-defense-interceptor-inventory. Reports indicate the United States expended approximately 14 percent of its THAAD interceptor stockpile during operations against Iran.

[25] Roh Moo-hyun, "Address by President Roh Moo-hyun at the 53rd Commencement and Commissioning Ceremony of the Korean Air Force Academy," March 8, 2005, https://www.hri.co.kr/upload/board/AddressByPresidentRohMoohyun.PDF; U.S. Department of State, "United States and the Republic of Korea Launch Strategic Consultation for Allied Partnership," January 19, 2006, https://2001-2009.state.gov/r/pa/prs/ps/2006/59447.htm.

[26] Vivian Salama and Nancy A. Youssef, "Iran Is Hitting the Radars That Underpin U.S. Missile Defenses," *Wall Street Journal*, March 2026, https://www.wsj.com/world/iran-is-hitting-the-radars-that-underpin-u-s-missile-defenses-2edbfccc; "Iran Strikes Three Countries Targeting THAAD Missile Defenses," Militarnyi, March 6, 2026, https://militarnyi.com/en/news/iran-strikes-targets-thaad-missile-defenses/.

[27] Rumbaugh, "The Depleting Missile Defense Interceptor Inventory"; Karishma Vaswani, "South Korea Alarmed by US Military Shift," *Taipei Times*, March 21, 2026, https://www.taipeitimes.com/News/editorials/archives/2026/03/21/2003854198.

[28] Liang Tuang Nah, "With US Distracted in Iran, N Korea's Opportunistic, Not Suicidal," *Asia Times*, March 17, 2026, https://asiatimes.com/2026/03/with-us-distracted-in-iran-n-koreas-opportunistic-not-suicidal/; Sung-Yoon Lee, "North Korea's Latest Missile Provocation Was Entirely Predictable," The Conversation, September 15, 2021, https://theconversation.com/north-koreas-latest-missile-provocation-was-entirely-predictable-167942.

[29] Clint Work, "The Variables of OPCON: One Wartime OPCON Transition, Multiple Plans," *The Diplomat*, September 5, 2025, https://thediplomat.com/2025/09/the-variables-of-opcon-one-wartime-opcon-transition-multiple-plans/; Clint Work, "No More Delays: Why It's Time to Move Forward With Wartime OPCON Transition," Stimson Center, June 21, 2022, https://www.stimson.org/2022/no-more-delays-why-its-time-to-move-forward-with-wartime-opcon-transition/; J. James Kim, "Redefining the U.S.–ROK Alliance in an Era of Uncertainty," Stimson Center, January 30, 2026, https://www.stimson.org/2026/redefining-the-u-s-rok-alliance-in-an-era-of-uncertainty/.

[30] Sang-ho Song, "Pentagon Nominee Voices Support for Bolstering S. Korea's Role in Alliance over OPCON Transfer Question," Yonhap News Agency, March 5, 2025, https://en.yna.co.kr/view/AEN20250305000351315; Sang-ho Song, "Hegseth Calls S. Korea's Push for OPCON Transfer 'Great,' Depicts it as 'Combat Credible Partner,'" Yonhap News Agency, October 29, 2025, https://en.yna.co.kr/view/AEN20251029016900315.

[31] Glenn H. Snyder, "The Security Dilemma in Alliance Politics," *World Politics* 36, no. 4 (July 1984): 461–495; Robert Jervis, *Perception and Misperception in International Politics* (Princeton University Press, 1976), chap. 3.

[32] Karl Friedhoff, "Troop Withdrawal Likely to Undermine South Korean Confidence in U.S. Commitment," Chicago Council on Global Affairs, July 2020, https://globalaffairs.org/sites/default/files/2020-12/2020_sma_korea_brief_0.pdf; Lee Sang Sin, "South Korean Public Opinion on the ROK-U.S. Defense-Cost Sharing," Korea Institute for National Unification, July 2020, https://repo.kinu.or.kr/bitstream/2015.oak/11681/1/CO20-17%28e%29.pdf.

[33] Glenn H. Snyder, *Alliance Politics* (Cornell University Press, 1997), 180-214; Paul W. Schroeder, "Alliances, 1815–1945: Weapons of Power and Tools of Management," in Klaus Knorr, ed., *Historical Dimensions of National Security Problems* (University Press of Kansas, 1976), 227-262.

[34] Park Won-gon, "'제2의 애치슨 라인' 우려 키운 미 국방장관의 36분 연설 [Concerns Over a 'Second Acheson Line' Raised by the U.S. Defense Secretary's 36-Minute Speech]," *Joongang Ilbo*, June 9, 2025, https://www.joongang.co.kr/article/25342473.

[35] Bruce Klingner, "Divergent Priorities in Dangerous Times: The U.S.-South Korea Alliance Faces Uncertain Future," *Korea Policy* 3, no. 2 (December 2025): 15-34.

[36] Minji Lee, "USFK commander rejects speculation on troop cut in S. Korea, reaffirms commitment," Yonhap News Agency, May 28, 2025, https://en.yna.co.kr/view/AEN20250528004800315.

[37] Minkyeong Kim and Xiao Liang, "Can the Growth Trend in South Korea's Arms Industry Last," Stockholm International Peace Research Institute, December 10, 2025, https://www.sipri.org/commentary/topical-backgrounder/2025/can-growth-trend-south-koreas-arms-industry-last; Xiao Liang et al., "Trends in World Military Expenditure, 2024," SIPRI Fact Sheet, April 2025, https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf.

[38] Toby Dalton and Darcie Draudt-Véjares, "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.

[39] Markus Garlauskas et al., *A Rising Nuclear Double-Threat in East Asia: Insights from Our Guardian Tiger I and II Tabletop Exercises* (Atlantic Council, May 2025), https://www.atlanticcouncil.org/in-depth-research-reports/report/a-rising-nuclear-double-threat-in-east-asia-insights-from-our-guardian-tiger-i-and-ii-tabletop-exercises/; In Hyo Seol, "다중 전쟁 동시 지속 상황과 한국의 안보 전략 [Multi-War Simultaneity and South Korea's Security Strategy]," *Peace Studies* 32, no. 2 (2024): 43–72; "Extended Deterrence in the Indo-Pacific: A Regional Track 1.5 Dialogue," Center for Global Security Research, September 2024, https://cgsr.llnl.gov/sites/cgsr/files/2024-11/event_report_-_extended_deterrence_in_the_indo-pacific.pdf; Hal Brands and Michael Beckley, *Danger Zone: The Coming Conflict with China* (W. W. Norton & Company, 2022), chap. 5-6.

[40] Garlauskas et al., *A Rising Nuclear Double-Threat in East Asia*.

[41] d'Artis Kancs, "NATO Defence Readiness in Europe: A CRINK Scenario Analysis," *Security and Defence Quarterly* 53, no. 1 (2026), https://securityanddefence.pl/NATO-defence-readiness-in-Europe-A-CRINK-scenario-analysis,208926,0,2.html.

[42] Heather Williams et al., "Russian Nuclear Calibration in the War in Ukraine," Center for Strategic and International Studies, February 23, 2024, https://www.csis.org/analysis/russian-nuclear-calibration-war-ukraine; Hal Brands, "Assessing the U.S. Response to Russia's Manipulation of Risk," Johns Hopkins University, 2024, https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/escalation-management-ukraine-response-russias-manipulation-risk/.

[43] Vann H. Van Diepen, "North Korea's New Nuclear Law: What Does It Say and What Does It Mean?" 38 North, September 15, 2022, https://www.38north.org/2022/09/north-koreas-new-nuclear-law-what-does-it-say-and-what-does-it-mean/.

[44] Garlauskas et al., *A Rising Nuclear Double-Threat in East Asia*. The Guardian Tiger exercises found that failure of deterrence on the Korean Peninsula in a dual-contingency scenario significantly complicated U.S. options for defending Taiwan.

[45] Nima Khorrami, "The Arctic and the Future of the South Korea-US Alliance," The Diplomat, September 24, 2025, https://thediplomat.com/2025/09/the-arctic-and-the-future-of-the-south-korea-us-alliance/.

The Future of U.S.-South Korea Defense Industry Cooperation on AI and Cybersecurity

By Eun-ho Kang

The war between Russia and Ukraine, which dramatically intensified following Russia's full-scale invasion of Ukraine in February 2022, has demonstrated to the world that the paradigm of modern warfare has fundamentally changed. So-called "multi-domain, high-technology hybrid war," in which conventional warfare, cyber warfare, information warfare, electronic warfare (EW), and space warfare unfold simultaneously on a single integrated battlespace, is no longer a conceptual abstraction but a concrete reality on the battlefield.[1] The war in Ukraine carries direct implications for South Korean security as well. Externally, North Korea has deployed its special operations unit, the Storm Corps, to the Ukrainian front, where it is rapidly accumulating real combat experience with advanced technologies such as drones and EW.[2] Internally, South Korea faces demographic constraints that will inevitably reduce its standing forces to below 350,000 troops.[3] At the same time, the United States is demanding not only increased defense burden-sharing but also voluntary roles and contributions from its allies.[4]

Addressing these complex challenges requires solving two tasks simultaneously. The first is a fundamental transformation of South Korea's force structure to match the requirements of future battlefields. The second is the qualitative advancement of U.S.-South Korea defense industry cooperation, taking into account the evolving role of the U.S.-South Korea alliance, which is the cornerstone of South Korean security. In particular, AI, Physical AI, and cybersecurity represent critical domains that apply to both imperatives—force buildup and the enhancement of bilateral defense cooperation.

This paper aims to present a new direction for future U.S.-South Korea defense industry cooperation by connecting and analyzing these two tasks. To this end, it examines South Korea's force buildup by analyzing recent patterns of warfare, reviewing the history of U.S.-South Korea defense industry cooperation to identify principles and directions for future collaboration, and establishing specific plans for cooperation in AI, Physical AI, and cybersecurity—applying these to the defense shipbuilding sector to provide concrete policy recommendations.

Dr. Eun-ho Kang is Chair of the Department of Advanced Defense Industry Studies and Director of the Defense Industry Research Institute at Jeonbuk National University (JBNU). He concluded his public service as Commissioner of the Defense Acquisition Program Administration (DAPA) in late June 2022. The primary purpose of this article is to present practical and immediately applicable directions for advancing U.S.-South Korea defense industry cooperation, drawing on the author's experience of over thirty-one years in roles related to fostering South Korea's defense industry and strengthening U.S.-South Korea cooperation. Most materials used in preparing this article reference the latest non-public documents of the South Korean Ministry of National Defense and DAPA.

Analysis of Recent Patterns of Warfare

The wars between Russia and Ukraine, Israel and Hamas, and U.S.-Israel and Iran have empirically demonstrated three structural changes on the modern battlefield.[5]

First is the multi-domain expansion of the battlefield. As land, sea, and air domains are integrated with space, cyber, and EW into a single battlespace, inferiority in any one domain translates directly into total operational paralysis.

Second is the collapse of the boundary between peacetime and wartime. Hybrid warfare integrates conventional warfare, irregular warfare, cyber warfare, information warfare, and economic coercion, normalizing sub-threshold pressure and measures that make it difficult for the adversary to escalate to full-scale war.[6]

Third is the shifting balance of warfare toward wars of attrition. Extreme cost asymmetry has become routine: First-person view suicide drones costing tens of thousands of dollars destroy tanks worth hundreds of thousands, and interceptor missiles costing tens of millions must be deployed to defend against them.

The Drone Revolution and Civil-Military Technology Convergence

Drones have placed the battlefield under constant twenty-four-hour surveillance, fundamentally undermining traditional tactical concepts centered on concealment and maneuver—to the point of drone supremacism. However, observers such as General Sir Nick Carter, former UK Chief of the General Staff, have argued that drones themselves do not transform warfare; rather, it is the doctrine and operational concepts governing their employment that shape their strategic impact.[7]

Moreover, the war in Ukraine has demonstrated the decisive military role of civilian advanced technologies: SpaceX's Starlink, GIS Arta's artillery fire coordination application based on Uber's technology, and Clearview AI's facial recognition system are but a few potent examples. General John Jay Raymond, then Chief of Space Operations of the U.S. Space Force, described the Ukraine war as "the first war where commercial space capabilities have really played a significant role."[8]

Electronic and Cyber Warfare as Battlefield Prerequisites

EW is no longer merely a support function; it has become a prerequisite for combat. GPS jamming, communication disruption, and data-link interference simultaneously neutralize drones, precision-guided munitions, and command-and-control systems. A force that fails to dominate the electromagnetic spectrum is effectively a blind force.

Cyber warfare, in particular, functions as a prelude to military operations. Immediately before its full-scale invasion in February 2022, Russia launched cyberattacks against major Ukrainian institutions to sow social chaos. Even more threatening from South Korea's perspective is software supply chain contamination. A "digital Trojan horse," activated at the outset of hostilities

and capable of turning friendly weapon systems into bricks, can collapse defense capabilities before a single shot is fired—even if physical forces remain 100 percent intact.[9]

AI-Based Command Decision-Making and Multi-Layered Defense Challenges

AI is emerging as a key tool for compressing the time from detection to decision to strike. AI-based command decision-making systems that dramatically increase decision speed and accuracy are becoming decisive factors in warfare.[10]

On the defensive side, the cost asymmetry dilemma is acute. Responding to low-cost drones and rockets with high-cost interceptor missiles is unsustainable in a prolonged conflict. The air defense experiences of Saudi Arabia and the United Arab Emirates against Iranian missile and drone attacks, along with Israel's operation of the Iron Dome, illustrate this clearly.[11] Air defense must be redesigned as a multi-layered, composite defense system combining missiles, EW, lasers, interceptor drones, and anti-aircraft guns, and adequate stockpiles of air defense missiles and other munitions must be secured.

Direction of South Korea's Force Buildup

South Korea faces core threats along two axes. Externally, North Korea's threat is qualitatively evolving as the regime adds battle-tested conventional forces, real-world experience, and new technologies to its nuclear and missile capabilities. In Ukraine, Storm Corps is rapidly accumulating modern combat experience, including in drone operations and EW countermeasures, risking a deepening asymmetry between the North Korean military and a South Korean military that lacks combat experience.[12]

Internally, South Korea faces a rapid decline in military manpower. Assuming a standing force of approximately 350,000, it is impossible to conduct theater-level operations under the existing manpower-centric, platform-centric force structure.[13] Furthermore, the U.S.-South Korea alliance is no longer a safety net guaranteeing automatic U.S. intervention. The alliance is being redefined as a structure in which each country maintains a certain level of independent deterrence and response capability and operates in a complementary manner. The moment for South Korea to secure a minimum level of independent deterrence is now absolutely critical.

As such, there are several future capabilities critical for South Korean forces to properly develop to address the evolving threat theater. First, building a South Korean AI-integrated joint all-domain command and control (JADC2)—the Korea Integrated Command and Control (KICC)—that is interoperable with the U.S. JADC2 is the top priority.[14] The focus must shift away from systems dependent on individual weapon system capabilities and instead concentrate on building an integrated command-and-control system that connects land, sea, and air weapon systems with space (satellites), sensors, and command communications—enabling real-time (or near-real-time) detect-decide-strike operations.

Second, unless a cyber kill chain that can detect, isolate, and patch cyberattacks in real time at machine speed (milliseconds) without human intervention and trace attacks back to their origin

is established, key weapon systems such as missiles and satellites cannot function normally within the allied network.[15]

Furthermore, deterrence itself cannot be established without a system that guarantees anti-jamming, anti-spoofing-based positioning, navigation, and timing (PNT) integrity to ensure accurate spatiotemporal information even under extreme jamming conditions.[16] South Korea's Hyunmoo missiles, F-35s, Aegis destroyers, and virtually all precision-strike and command-and-control assets currently depend on PNT and network time synchronization.

Third, in response to an era of troop reductions already underway, South Korean forces must be reorganized around unmanned systems by broadly applying physical AI technologies across weapon systems, enabling manned-unmanned teaming, autonomous operation, and robotic/AI pilots.

Lastly, South Korea should establish a multi-layered defense system to counter North Korea's long-range artillery and drone threats.[17] This includes fielding tactical/operational suicide drones (unmanned aerial vehicles, unmanned surface vessels, and unmanned underwater vehicles), small precision-guided munitions, and cost-effective force packages incorporating decoys. On the defensive side, a system that combines soft-kill, hard-kill, directed energy, and anti-aircraft guns to neutralize swarm targets at low cost must be fielded rapidly.

Stages of Development and Future Direction of U.S.-South Korea Defense Industry Cooperation

U.S.-South Korea defense industry cooperation can be analyzed in five generations since the 1950s.[18]

Generation one (1950s–1980s) established the foundation of defense industry cooperation between the two countries. During and immediately after the Korean War, South Korea had virtually no defense industrial base. As such, the allies formed a thoroughly asymmetric structure in which the United States provided technology and funding while South Korea absorbed it. This dependency gradually improved after the South Korean government established the Agency for Defense Development (ADD) in August 1970 and began fostering a domestic defense industry. As U.S. technical assistance continued, South Korea's defense technology capabilities slowly grew. The joint development of the K1 tank (ROKIT) by Chrysler Defense and ADD/Hyundai Precision can be cited as the first official case of cooperation between the two countries' defense industries.

During generation two (1990–2006), the development of South Korea's defense industry—particularly its defense technology—was driven primarily by technology transfer obtained through offset trade. The 1990s were the most adventurous period for technological development in South Korea's defense industry; this was the era in which many of today's acclaimed weapon systems—the K9 self-propelled howitzer, the K2 main battle tank, the Cheongung-2 air defense system, various naval vessels, and the domestic fighter development program—were

developed. The most representative example of technology acquisition through offset trade is the T-50 trainer aircraft development project between Lockheed Martin and Korea Aerospace Industries (KAI), which was part of the F-16 purchase offset agreement. This was South Korea's first systematic acquisition of advanced aircraft technology, which has since become the technological foundation for the independent development of the KF-21 fighter aircraft.

The two allies began cooperating on defense production during generation three (2006–2019). In 2006, the South Korean government launched the Defense Acquisition Program Administration (DAPA) to strengthen the domestic defense technology base and secure international competitiveness. South Korea's defense industry subsequently experienced remarkable growth and began actively expanding into international markets. The most important issue that arose between the United States and South Korea during this process was how to protect the core technologies embedded in weapon systems. The U.S. side had a keen interest in ensuring core technologies transferred through offset trade and other means could be safely protected during the defense export process. In response, the South Korean government enacted the Defense Technology Protection Act in 2015, with advice from the U.S. Department of Defense, legally mandating equal protection for both independently developed core technologies and key technologies transferred from the United States. Additionally, the U.S. Naval Research Laboratory and South Korea's ADD/LIG Nex1 attempted to jointly develop the Lightweight Optical Guided Rocket Interceptor (LOGIR), which can be considered the first case in which both countries participated as equal technology partners.

Generation four (2019–2025) consisted of market expansion and supply chain cooperation. Triggered by major contracts, such as the K9 self-propelled howitzer deal with Australia in 2021 and the K2, K9, and FA-50 deals with Poland in 2022, South Korea emerged as a global defense supplier. The international community began to pay close attention to South Korea's defense industry, coining the term "K-Defense."[19] During this leap forward, the U.S. side supported South Korea by granting export license (EL) approvals for key components of South Korea's exported weapon systems with virtually no denials—thereby indirectly supporting South Korea's entry into international defense markets. In addition, U.S.-South Korea supply chain cooperation in the defense sector also strengthened, including the exclusion of Chinese-made components.[20]

The current generation five (2025–Future) has thus far focused on growing cooperation on advanced supply chains and high-technology development.[21] In June 2025, the newly inaugurated Lee Jae Myung administration outlined its policy objective of establishing the country's defense industry as a global arms exporter.[22] As such, the Lee administration significantly increased defense research and development (R&D) budgets and large-scale investment decisions in new technologies such as physical AI and semiconductors.[23] In addition, in line with the Donald Trump administration's national defense and security strategy, South Korea aims to increase its defense budget to approximately 3.5 percent of GDP within the next decade.[24] From the U.S. perspective, given the increasingly heavy burden of the twin fiscal and trade deficits, China's rapid technological advancement and military buildup, Russia's growing threat, and continued instability in the Middle East, South Korea's role in enhancing U.S.-South Korea defense

cooperation will become even more important. In particular, as seen in the concrete progress of U.S.-South Korea defense shipbuilding cooperation under the "MASGA" (Make American Shipbuilding Great Again) initiative, an equal partnership that combines the strengths of both countries is essential.[25] For a genuine U.S.-South Korea defense partnership to function, the allies must complete the establishment of a "production web," JADC2 integration, and joint technology and market development.[26]

Future Direction of Generation Five Cooperation

Fifth-generation defense cooperation is grounded in the historical experience and shared values of the U.S.-South Korea alliance, built over the past seventy-plus years. This goodwill must be accompanied by concrete expressions of trust, a genuine willingness to understand and seek solutions to both countries' technological and industrial challenges, and continued logistical support and operational capability enhancement even after contracts are signed.

The United States' strengths lie in AI algorithm and software design, systems architecture, advanced R&D, and access to global defense markets.[27] Meanwhile, South Korea's strengths include world-class manufacturing competitiveness, rapid weapons production and delivery speed, world-class industries such as shipbuilding, electronics, and semiconductors, and extensive experience with win-win localization cooperation.[28] The allies can combine these two strengths in a division-of-labor model in which the United States handles AI and systems design while South Korea handles platform manufacturing and production. This can be conceptualized as a production web— the construction of a global defense production cooperation network that organically integrates the industrial capabilities of both countries.

AI and cybersecurity represent the most fruitful and promising areas of fifth-generation cooperation. In the military domain, physical AI is realized in various forms, such as autonomous drones, unmanned ground vehicles, unmanned surface vessels, and autonomous combat robots.[29] Physical AI is developed to operate in real battlefield environments through Digital Twin environments and Sim-to-Real learning.[30] This will become the core foundational technology for manned-unmanned teaming in future military operations.[31] Physical AI development requires large-scale data, high-performance semiconductors, software technology, and the ability to integrate with actual weapon systems. It is difficult for a single country to pursue all of this independently—technological cooperation between allies is not a choice but a necessity.

South Korea's core strength lies in its world-class semiconductor technology and manufacturing industry. Combining U.S. AI algorithm and systems design capabilities with South Korea's semiconductor and manufacturing platform production capabilities would enable the construction of a powerful physical AI ecosystem that would surpass China's large-scale manufacturing base.

U.S.-South Korea physical AI cooperation can be advanced in the following manners: building a joint R&D platform that combines U.S. AI algorithm research capabilities with South Korea's hardware and platform production capabilities; mutually sharing joint training data, simulation

environments, and real-world operational data to improve the performance and reliability of AI models; building a cooperative model that combines U.S. systems design with South Korean platform manufacturing in areas such as drones, unmanned combat vehicles, and autonomous naval platforms; and establishing a cooperative channel for the architectural design stage to secure complete interoperability between the U.S. JADC2 and South Korean KICC. These cooperative structures are strategically significant as a new model of defense cooperation that combines U.S. AI technology with South Korea's manufacturing base, strengthening the technological and industrial competitiveness of both countries.

Cybersecurity represents the second growth area, as most of the data assets held by defense firms consist of sensitive defense-related information, including defense secrets, defense technologies, and national core technologies.[32]

Modern weapon systems are structured as a complex system of systems, integrating sensors, data links, software, and AI technology. While this enhances combat efficiency, it simultaneously increases vulnerability to cyberattacks. The F-35 program involves approximately 1,400 suppliers, and major South Korean shipbuilders have cooperative networks of approximately 1,300 to 2,400 partner firms; a single vulnerable link in the supply chain can threaten the entire system. Furthermore, the increase in international interest and demand for K-defense has led to a surge in cyber-hacking attempts, and the urgent development and application of anti-tampering technology to protect core technologies for exported weapon systems is critical.[33]

The United States has introduced the Cybersecurity Maturity Model Certification (CMMC) program to strengthen cybersecurity requirements for defense industrial base contractors and protect sensitive unclassified information in the defense supply chain. In parallel, the Department of Defense has adopted a Zero Trust cybersecurity strategy based on a "never trust, always verify" approach.[34] South Korean companies must meet the same standards—this is an essential condition for Stage 5 U.S.-South Korea defense cooperation.

U.S.-South Korea cybersecurity cooperation should be advanced in the following three-stage structure. Stage one consists of aligning cybersecurity standards by establishing a K-CMMC system aligned with CMMC, achieving mutual recognition of CMMC certifications, and integrating defense company security evaluation standards. DAPA should establish a Korean-style defense industry technology cybersecurity certification system in line with the phased implementation of CMMC in 2025 and implement a program to support the employment of information security professionals at small and medium-sized defense enterprises (covering up to 50 percent of standard salaries for three years).[35] Stage two should focus on building a joint cyber threat response system. This includes joint cyber threat information sharing, the establishment of a joint center to respond to cyberattacks on the defense industry, and the construction of a joint supply chain security monitoring system. The U.S.-South Korea Defense Technology Protection Council should be elevated to a more substantive and regular consultation channel.[36] During the third and final stage, joint R&D of cybersecurity technologies tailored to future battlefields must be undertaken, including security for AI weapon systems, swarm drone security, autonomous

weapons system security, space and satellite system security, and military cloud security. Furthermore, the construction of an integrated defense cloud system, which would overcome the limitations of network separation and serve as infrastructure enabling joint U.S.-South Korea R&D, must be pursued through a cloud-service-provider-based defense collaboration platform.[37]

A Concrete Model for Defense Shipbuilding Cooperation

The shipbuilding industry is the optimal showcase for U.S.-South Korea defense cooperation—one that simultaneously demands collaboration in physical AI and cybersecurity. The U.S. shipbuilding industry has experienced a sustained decline since World War II. The number of U.S. shipyards has declined sharply, and the United States now accounts for only about 0.1 percent of the global commercial shipbuilding market.[38]

This hollowing out of the U.S. shipbuilding industrial base is creating delays in U.S. Navy ship construction: DDG-51 destroyer maintenance has often taken longer than planned, while the lead FFG-62 frigate is forecasted to be delivered approximately thirty-six months later than initially planned. In addition, the U.S. Government Accountability Office (GAO) found that thirty-eight of fifty-one aircraft carrier and submarine maintenance periods, or 75 percent, were completed late from FY2015 to FY2019.[39] By contrast, China holds approximately 53 percent of global ship order volume, posing a direct challenge to the U.S. strategy of maintaining maritime supremacy. South Korea, meanwhile, possesses the world's second-largest shipbuilding industry, featuring a highly efficient production system centered on large shipyards and an extensive supply chain network. These South Korean strengths will serve as irreplaceable tools in rebuilding the U.S. shipbuilding industry.

The United States is pursuing maintenance and repair cooperation utilizing allied shipyards through its Regional Sustainment Framework (RSF) policy. Under this policy, South Korean shipyards are performing maintenance, repair, and overhaul (MRO) projects for vessels operated by the U.S. Military Sealift Command (MSC). Publicly reported examples include Hanwha Ocean's work on the USNS Wally Schirra, USNS Yukon, and USNS Charles Drew; HD Hyundai Heavy Industries' work on the USNS Alan Shepard and USNS Cesar Chavez; and HJ Shipbuilding & Construction's work on the USNS Amelia Earhart.[40] Based on these existing partnerships, the U.S. Navy is expected to expand cooperation with South Korea in vessel MRO and ship construction, and South Korean companies are pursuing U.S. shipyard investment and cooperation projects with this in mind.

However, the construction and maintenance of naval vessels involves the exchange of extremely sensitive information: hull design data, combat system software, communications and network system code, sensor and weapons system operational data, and maintenance history data. Because such data is directly linked to military operational capabilities, it becomes a prime target for cyberattacks.[41] During naval vessel MRO processes, persistent security risks exist: leakage of warship design data, hacking of combat system software, infiltration of maintenance

networks, and cyberattacks through the supply chain. As the SolarWinds hacking incident demonstrated, supply-chain-based cyberattacks can have a direct impact on national security.[42]

A Three-Stage Integrated Framework

AI-based ship construction and maintenance can serve as a concrete application of U.S.-South Korea physical AI cooperation. By combining U.S. AI systems design capabilities with South Korea's shipbuilding manufacturing capabilities, it is possible to advance digital twin-based ship design and construction, AI-based predictive maintenance, and the joint development of autonomous surface vessels and unmanned maritime systems.[43]

Additionally, the two countries should establish a cybersecurity certification system across the entire network of approximately 1,300 to 2,400 partner firms of major South Korean shipbuilders. Specifically, this requires establishing a defense supply chain security certification system (based on CMMC), introducing a partner firm cybersecurity evaluation system, and building a cyber threat information-sharing system.

Such efforts would be further strengthened by establishing an MRO security framework that encompasses warship maintenance network segmentation, an encrypted data exchange system, and a joint cybersecurity certification system. Furthermore, the United States and South Korea should set up a joint Defense Cybersecurity Cooperation Center and advance joint cyber threat response systems and cybersecurity R&D.

Strategic Implications of Defense Shipbuilding Cooperation

Defense shipbuilding cooperation goes beyond simple industrial cooperation; it serves as a powerful model of security cooperation that embeds alliance trust in industry and technology. The characteristics of the shipbuilding industry—complex global supply chain structures, production systems based on advanced digital technology, and direct linkage to military operational capabilities—make it an ideal test bed for physical AI and cybersecurity cooperation models. Successful cooperation in this sector is expected to rapidly spread to other areas, such as aviation and ground weapons, elevating U.S.-South Korea defense industry cooperation to a new dimension.

Conclusion

The United States and South Korea should elevate defense industry cooperation beyond weapon-systems collaboration to a technology partnership, with physical AI and cybersecurity as its twin pillars. To achieve this, the following policy recommendations are presented.

First, there is a need to establish a joint research platform that combines U.S. AI capabilities with South Korea's manufacturing platform and semiconductor technology. Through this, manned-unmanned teaming systems, autonomous drones, unmanned maritime systems, and other physical AI-based weapon systems can be jointly developed, and an ecosystem for developing advanced new technologies can be built.

Second, a South Korean-style defense industry technology cybersecurity certification system (K-CMMC) must be built to a level where mutual recognition with the U.S. CMMC is possible, and a U.S.-South Korea Defense Cyber Cooperation Center participated in by both governments and companies must be established. Expanding the program supporting the employment of information security professionals for small and medium-sized defense enterprises, and building an integrated defense cloud platform, should be pursued in parallel.

Third, the two countries should cooperate from the architecture-design stage to ensure interoperability between KICC and JADC2, while pursuing joint R&D on cyber kill chains and PNT integrity systems to strengthen shared deterrence.

Fourth, a global defense production cooperation network (production web) that integrates the industrial capabilities of both countries must be built in phases. In the defense shipbuilding sector, MRO cooperation should be expanded to encompass combat vessel construction, and this should be further developed into AI-based digital-twin ship design and joint development of unmanned maritime systems. In this process, applying the three-stage cybersecurity cooperation framework creates a virtuous cycle of security and cooperation.

Fifth, the two countries should focus on strengthening the defense technology protection system and developing human resources. In proportion to the expansion of K-defense exports, attempts at defense technology theft are also increasing. South Korea must pay particular attention to this area. Drawing on U.S. experience and know-how, the cybersecurity monitoring system covering the entire supply chain of defense companies must be expanded, and bold investment must be made in anti-tampering technology development—for which U.S. cooperation is indispensable.[44] Furthermore, to rapidly develop cyber professionals, a specialized cybersecurity training program encompassing operational technology (OT) cybersecurity, weapons-system software, and supply-chain security modules must be established. The establishment of a defense technology security system, including cybersecurity, must be proactively led by the South Korean side, and this is a prerequisite for enhancing fifth-generation cooperation, including U.S.-South Korea defense shipbuilding cooperation.

Additionally, the United States and South Korea should pursue the early conclusion of an RDP-A as an institutional mechanism to facilitate broader defense industrial cooperation, including shipbuilding, MRO, supply-chain resilience, and emerging technology collaboration.[45] Through this, South Korean companies will secure Buy American Act (BAA) exemptions in the U.S. defense market, and U.S. companies will be able to participate directly in major South Korean R&D projects.[46] In this process, the development of advanced new technologies and personnel exchanges will be activated, and U.S.-South Korea defense cooperation can unlock the full potential of fifth-generation cooperation.

The future of U.S.-South Korea defense industry cooperation hinges on a bold transition—from a mere transactional relationship to a genuine technology partnership. Cooperation that prioritizes physical AI and cybersecurity is not simply a matter of technological cooperation; it

will serve as the core axis of a new industrial and technological foundation for the U.S.-South Korea alliance.

Endnotes

[1] Eun-ho Kang, "전력구조, 2030 -2040년 우리에게 필요한 무기체계는 무엇인가? [Force Structure, What Weapon Systems Are Needed Over 2030-2040?]," 국방부 주관 국방개혁세미나 자료 - 스마트 강군, 새로운 국방개혁의 방향 [Materials form Defense Reform Seminar sponsored by the Ministry of National Defense], February 4, 2026.

[2] Heeyang Kwak and Seoyoung Kim, "국정원 북 '폭풍군단' 3000명 러시아로…드론 조종 등 훈련 중" [National Intelligence Service: 3,000 Troops from North Korea's 'Storm Corps' Sent to Russia… Undergoing Training Including Drone Piloting]," Kyunghyang Shinmun, October 23, 2024, https://www.khan.co.kr/article/202410232110045.

[3] YoonHae Kim, "스마트강군 구조개혁 [Structural Reform for a Smart and Strong Military]," 국방부 주관 국방개혁세미나 자료 - 스마트 강군, 새로운 국방개혁의 방향 [Materials form Defense Reform Seminar sponsored by the Ministry of National Defense], February 4, 2026.

[4] U.S. Department of Defense, *2026 National Defense Strategy of the United States of America* (Department of Defense, 2026), 4–5, 18–19, https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.pdf. The strategy states that the United States will urge and enable key regional allies and partners to do more for their collective defense, that allies in Europe and other theaters should take the lead with the United States offering critical but limited support, and that the Department of Defense will increase burden-sharing with U.S. allies and partners. See also The White House, *National Security Strategy* (2025), 15, https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf; North Atlantic Treaty Organization, "The Hague Summit Declaration," June 25, 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration.

[5] Eun-ho Kang, "한국 방산 수출의 지속적 증대 방안: 우크라이나 전쟁의 시사점과 선진 방산 전략을 위한 제언 [An Analysis and Evaluation of the Recent Surge in South Korean Defense Exports Following the Russia-Ukraine War]," 국방정책연구 *[Journal of Defense Policy Studies]* 39, no. 1 (2023): 22, http://doi.org/10.22883/jdps.2023.39.1.001.

[6] In this article, hybrid warfare refers to the coordinated use of military and non-military instruments—including conventional forces, cyber operations, disinformation, economic coercion, and political pressure—to achieve strategic objectives below or across the threshold of full-scale war. See North Atlantic Treaty Organization, "Countering Hybrid Threats," updated January 29, 2026, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats; Robert Person et al., "Back to the Future: The Persistent Problems of Hybrid War," *International Affairs* 100, no. 4 (2024): 1749–1761, https://doi.org/10.1093/ia/iiae131.

[7] Nick Carter, "A New Way of Warfare Requires More Than New Tech," War on the Rocks, January 5, 2026, https://warontherocks.com/2026/01/a-new-way-of-warfare-requires-more-than-new-tech/. Carter argues that Ukraine's drone experience should not be reduced to technology itself because "the drivers for real change are doctrine and concepts, not gadgets," and that drones must be integrated into doctrine, operational concepts, force design, and culture to generate a new way of warfare.

[8] Jonathan Beale, "Space, the Unseen Frontier in the War in Ukraine," BBC News, October 5, 2022, https://www.bbc.com/news/technology-63109532; UK House of Commons Defence Committee, *Defence Space: Through Adversity to the Stars?* Third Report of Session 2022–23, HC 182 (House of Commons, 2022), 27, https://publications.parliament.uk/pa/cm5803/cmselect/cmdfence/1031/report.html.

[9] Kang, "전력구조, 2030-2040년 우리에게 필요한 무기체계는 무엇인가? [Force Structure, What Weapon Systems Are Needed Over 2030-2040?]," 42.

[10] AI-enabled command-and-control systems support the rapid integration of sensor data and help compress the time from detection to decision and strike, a goal reflected in the U.S. Department of Defense's JADC2 concept. See U.S. Department of Defense, *Summary of the Joint All-Domain Command and Control (JADC2) Strategy* (2022), 2–5, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OFTHE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.

[11] "UAE Says Air Defences Engage Missiles, Drones as Flights Disrupted," Reuters, May 4, 2026, https://www.reuters.com/world/asia-pacific/fujairah-oil-zone-hit-by-fire-after-drone-attack-uae-says-it-intercepted-iran-2026-05-04/; Timour Azhari, "Saudi Arabia Has the Right to Take Military Action against Iran, Foreign Minister Says," Reuters, March 19, 2026, https://www.reuters.com/world/middle-east/riyadh-residents-receive-phone-alerts-first-time-warning-hostile-threat-2026-03-18/; "Saudi Arabia to Take All Necessary Measures to Defend Its Security, Cabinet Says," Reuters, March 3, 2026, https://www.reuters.com/world/middle-east/saudi-arabia-take-all-necessary-measures-defend-its-security-cabinet-says-2026-03-03/.

[12] Kang, "전력구조, 2030-2040년 우리에게 필요한 무기체계는 무엇인가? [Force Structure, What Weapon Systems Are Needed Over 2030-2040?]," 42–44. The author prepared the report through interviews and surveys with fifteen experts currently serving in South Korea's Ministry of National Defense, DAPA, and the defense academia, focusing on the direction of South Korea's force buildup in light of changes in the security environment, including recent patterns of warfare and the advancement of the North Korean nuclear threat. This was presented at the Ministry of National Defense-sponsored Defense Reform Seminar (February 4, 2026).

[13] Kim, "스마트강군 구조개혁 [Structural Reform for a Smart and Strong Military]," 24.

[14] JADC2 is intended to link sensors, shooters, and commanders across domains to improve decision speed, while South Korea's KICC modernization similarly focuses on AI-enabled command-and-control and interoperability with allied systems. See *Summary of the Joint All-Domain Command and Control (JADC2) Strategy*, 1–5; John R. Hoehn, *Joint All-Domain Command and Control (JADC2)*, CRS Report No. IF11493 (Congressional Research Service, 2022), https://www.congress.gov/crs-product/IF11493; Lee Seong-jin, "군, 2029년까지 AI 기반 지휘결심지원체계 구축 [South Korea to Deploy AI-Based Military Command Platform by 2029]," *Aju Press*, January 26, 2026, https://www.ajunews.com/view/20260126111158045.

[15] The cyber kill chain is a framework that describes the stages of a cyber intrusion, from reconnaissance and delivery to exploitation, command-and-control, and actions on objectives. See Eric M. Hutchins et al., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," in *6th International Conference on Information Warfare and Security 2011,* ed. Leigh Armistead (Curran Associates, 2011), 113–125.

[16] Joon Hyo Rhee et al., "Enhanced Accuracy Simulator for a Future Korean Nationwide eLoran System," *IEEE Access* 9, (2021): 115042-115052, doi: 10.1109/ACCESS.2021.3105063; Ji Da-gyum, "N. Korea Attempted to Disrupt GPS Signals on S. Korean Border Islands," *The Korea Herald*, March 8, 2024, https://www.koreaherald.com/article/3342351.

[17] A multilayered missile defense architecture uses complementary systems to intercept threats at different ranges and altitudes. See U.S. Department of Defense, *Missile Defense Review* (2019), 11–13, https://www.war.gov/portals/1/interactive/2018/11-2019-missile-defense-review/the%202019%20mdr_executive%20summary.pdf; "한국형 미사일방어체계 [Korea Air and Missile Defense]," Encyclopedia of Korean Culture, accessed May 30, 2026; Defense Agency for Technology and Quality, "보이지 않는 전장의 최상층, L-SAM" [L-SAM: The Upper Layer of the Invisible Battlefield]," Defense & Technology Quality, accessed May 30, 2026.

[18] The generation classification of U.S.-South Korea defense industrial cooperation used in this article is the author's own analytical framework. Representative cases for each stage are drawn in part from Won-jun Jang and Jae-pil Song, "한미 방산협력과 공급망 확대 전략에 관한 연구 - 한미 상호국방조달협정 (RDP-MOU)을 중심으로 [A Study on U.S.-South Korea Defense Industry Cooperation and Supply Chain Expansion Strategy: Focused on the U.S.-South Korea Reciprocal Defense Procurement Memorandum of Understanding (RDP-MOU)]," 한국국방경영분석학회지 [*Journal of the Korea Defense Management Analysis Society*] 48, no. 2 (2022): 39–55; Gyu-pyeong Jeong, "생산력 중심의 글로벌 방산협력 구상: 무기이전 신속성 분석을 중심으로 [Global Defense Cooperation Initiative Centered on Production Capacity: Focused on Analysis of Weapon Transfer Speed]," 한국산학기술학회논문지 [*Journal of the Korea Academia-Industrial Cooperation Society*] 25, no. 9 (2024): 821–829.

[19] Lee Jeong-gu, "K-Defense Industry Expands Win-Win Cooperation with Suppliers," *Chosun Ilbo*, March 10, 2026, https://www.chosun.com/english/industry-en/2026/03/10/R2QZUNAHDNFT5IWEB6BTUXILX4/; Chung Min Lee, *South Korea as a Rising Defence Exporter: Challenges and Opportunities* (International Institute for Strategic Studies, 2025), 3–7, https://www.iiss.org/research-paper/2025/12/south-korea-as-a-rising-defence-exporter-challenges-and-opportunities/.

[20] Author's firsthand observation based on policy measures undertaken during his tenure as Minister of the Defense Acquisition Program Administration (DAPA), including a comprehensive review of Chinese-origin components used in major defense systems and efforts to develop alternative sources.

[21] The designation of 2025 as the starting point of fifth-generation U.S.-South Korea defense cooperation is analytical rather than historical. While a formal fifth-generation framework has not yet emerged, this study uses 2025, coinciding with the inauguration of the Lee Jae Myung administration, as a baseline for conceptualizing and advancing future defense cooperation.

[22] South Korean Office of the President, "이 대통령 '방위산업 4대 강국, 결코 불가능한 꿈 아냐' [President Lee Says Becoming One of the World's Top Four Defense-Industry Powers Is Not an Impossible Dream]," Korea Policy Briefing, October 20, 2025, https://www.korea.kr/news/policyNewsView.do?newsId=148952420.

[23] South Korean Ministry of National Defense, "2026년 국방예산 전년 대비 7.5% 증가한 65조 8,642억원 확정 [2026 Defense Budget Finalized at KRW 65.8642 Trillion, Up 7.5 Percent Year-on-Year]," Korea Policy Briefing, December 5, 2025, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156733517; "국방연구개발 사업평가 [Evaluation of Defense R&D Programs]," South Korean National Assembly Budget Office, November 18, 2025, https://nabo.go.kr/ko/report/evaluationView.do?key=2509110003&idx=8984; South Korean Ministry of Science and ICT, "내년 R&D 예산 파격 투자…연구생태계 완전 복원, '진짜 성장' 실현 [Major Investment in Next Year's R&D Budget to Restore the Research Ecosystem and Realize 'Real Growth']," Korea Policy Briefing, August 22, 2025, https://www.korea.kr/news/policyNewsView.do?newsId=148948043; South Korean Ministry of Trade, Industry and Energy, "2026년 산업통상자원부 예산안 [2026 Budget Proposal of the Ministry of Trade, Industry and Energy]," Korea Policy Briefing, September 1, 2025, https://www.korea.kr/briefing/policyBriefingView.do?newsId=156721794.

[24] Yu-jung Lee, "Defense Spending to Hit $47 Billion as Sector Strives for 3.5% of GDP," *Joongang Ilbo*, September 3, 2025, https://koreajoongangdaily.joins.com/news/2025-09-03/national/defense/Defense-spending-to-hit-47-billion-as-sector-strives-for-35-of-GDP/2390380; Na-Ri Shin, "South Korea, U.S. Agree on Defense Spending Hike," *Donga Ilbo*, September 2, 2025, https://www.donga.com/en/article/all/20250902/5822053/1.

[25] South Korea proposed the "Make American Shipbuilding Great Again" (MASGA) initiative as a large-scale U.S.-South Korea shipbuilding cooperation package aimed at helping rebuild the U.S. shipbuilding industry through South Korean-led investment and industrial cooperation. See Ju-min Park and Jihoon Lee, "'Make America Shipbuilding Great Again' Package Key to Reaching Trade Deal, South Korea Says," Reuters, July 31, 2025, https://www.reuters.com/world/china/make-america-shipbuilding-great-again-package-key-reaching-trade-deal-south-2025-07-31/; Timothy W. Martin and Soobin Kim, "The New Acronym Driving South Korea's Summit With Trump," *Wall Street Journal*, August 24, 2025, https://www.wsj.com/world/asia/the-new-acronym-driving-south-koreas-summit-with-trump-masga-aed1aad9.

[26] "Production web" describes an analytical model of allied defense production and sustainment designed to strengthen supply chain resilience and wartime production capacity. See Bo Ram Kwon, "US–South Korea Defense Industrial Cooperation: Drivers, Developments, and Tasks Ahead," *Korea Policy* 2, no. 2 (2024): 175–77, https://keia.org/publication/us-south-korea-defense-industrial-cooperation-drivers-developments-and-tasks-ahead/; U.S. Department of Defense, *National Defense Industrial Strategy* (2024), 14–24.

[27] U.S. National Security Commission on Artificial Intelligence, *Final Report* (2021), 7–9, 35–38, https://www.govinfo.gov/app/details/GOVPUB-Y3-PURL-gpo153246; U.S. Department of Defense, *2023 National Defense Science and Technology Strategy* (2023), 4–8, https://www.cto.mil/wp-content/uploads/2024/05/2023-NDSTS.pdf; Mathew George et al., *Trends in International Arms Transfers, 2024* (Stockholm International Peace Research Institute, 2025), 2–3, https://www.sipri.org/publications/2025/sipri-fact-sheets/trends-international-arms-transfers-2024.

[28] South Korea's defense-industrial strengths are often linked to its advanced manufacturing base, fast production and delivery capacity, and willingness to combine exports with local production and technology-transfer arrangements. See Lee, *South Korea as a Rising Defence Exporter*; Won-Joon Jang and Hea Ji Park, "The Rise of Korea's Defense Industry in the New Global Order," *KIET Industrial Economic Review* 28, No. 6 (2023), https://www.kiet.re.kr/en/pub/ecoreviewDetailView?detail_no=1013; "South Korea and Poland to Upgrade Ties as Tusk Calls Seoul Key Ally after U.S.," Reuters, April 13, 2026, https://www.reuters.com/world/asia-pacific/south-korea-poland-upgrade-ties-comprehensive-strategic-partnership-media-2026-04-13/; Chung Min Lee, "The Future of K-Power: What South Korea Must Do After Peaking," Carnegie Endowment for International Peace, August 22, 2024, https://carnegieendowment.org/research/2024/08/the-future-of-k-power-what-south-korea-must-do-after-peaking.

[29] Physical AI is AI that enables machines to perceive, understand, and interact with the physical world. Physical AI in defense is reflected in autonomous and unmanned military systems, including "attritable autonomous systems" across multiple domains and "unmanned air, surface, and ground systems." See U.S. Defense Innovation Unit, "Implementing the Department of Defense Replicator Initiative to Accelerate All-Domain Attritable Autonomous Systems To Warfighters at Speed and Scale," November 30, 2023, https://www.diu.mil/latest/implementing-the-department-of-defense-replicator-initiative-to-accelerate; U.S. Department of the Navy, *Unmanned Campaign Framework* (2021), 7–9, https://www.govinfo.gov/app/details/GOVPUB-D201-PURL-gpo174216.

[30] NVIDIA defines a digital twin as "a virtual representation of a physical object or system." Sim-to-Real learning refers to training, testing, and validating AI systems in simulation before transferring them to operate in real-world environments. See "What Is a Digital Twin?" NVIDIA, accessed June 3, 2026, https://www.nvidia.com/en-us/glossary/digital-twin/; "NVIDIA Isaac Sim," NVIDIA, accessed June 3, 2026, https://developer.nvidia.com/isaac/sim?size=n_6_n&sort-field=featured&sort-direction=desc.

[31] Manned–unmanned teaming (MUM-T), or more broadly human–machine teaming, refers to the integration of soldiers with robotic and autonomous systems to increase combat effectiveness while reducing soldiers' exposure to dangerous tasks. The U.S. Army's *Robotic and Autonomous Systems Strategy* identifies increased "reach, persistence, lethality, survivability, and tempo" as key benefits of robotic and autonomous systems. See U.S. Army, *The U.S. Army Robotic and Autonomous Systems Strategy* (2017), 3–7, https://mronline.org/wp-content/uploads/2018/02/RAS_Strategy.pdf.

[32] Yeon-seung Ryu, "경제안보·기술안보 시대의 방위산업 안보 [The Era of Economic Security and Technology Security]," 국방외교저널 [*Journal of Defense Diplomacy*] (2024): 26.

[33] Ryu, "경제안보·기술안보 시대의 방위산업 안보 [The Era of Economic Security and Technology Security]," 26–27; Park Chan-Je, "[2023 국방안보방산포럼] '한·미·일 3각 협력 제도화 큰 성과…갈등 적은 분야부터 실행해야' [[2023 Defense Security Defense Forum] 'Great achievements in institutionalization of trilateral cooperation between South Korea, the U.S. and Japan...We need to start with areas with less conflict],'" *Aju Press*, November 16, 2023, https://www.ajunews.com/view/20231116140752717; Sang-Woo Lee, "류연승 명지대 교수 '방산 기술 보호에 정부 지원 늘려야' [Professor Ryu Yeon-seung of Myongji University, 'We need to increase government support to protect defense technology. Government Support for Defense Technology Protection Should Be Expanded],'" News Impact, June 21, 2024, https://www.newsimpact.co.kr/news/articleView.html?idxno=3269953.

[34] U.S. Department of Defense Chief Information Officer, "Cybersecurity Maturity Model Certification (CMMC)," accessed May 30, 2026, https://dodcio.defense.gov/CMMC/; U.S. Department of Defense, *DoD Zero Trust Strategy* (2022), 1–2, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf; Scott Rose et al., *Zero Trust Architecture*, Special Publication 800-207 (National Institute of Standards and Technology, 2020), 4, https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf.

[35] South Korean Defense Acquisition Program Administration (DAPA), unpublished internal document obtained by the author, 2025; Cybersecurity Maturity Model Certification (CMMC) Program, 32 C.F.R. 170 (2024), https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170.

[36] Defense technology protection and industrial security cooperation between South Korea and the United States have been discussed through bilateral defense acquisition and technology cooperation mechanisms, including the Defense Technology and Industrial Cooperation Committee (DTICC). South Korean Defense Acquisition Program Administration, "한미 방산기술협력위 5년만에 개최, 포괄적 파트너십 강화 협의 [Korea-U.S. Defense Technology Cooperation Committee Holds First Meeting in 5 Years to Discuss Strengthening Comprehensive Partnership]," Korea Policy Briefing, July 31, 2023, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156583125.

[37] The U.S. Department of Defense describes defense cloud infrastructure as providing "common data and infrastructure platforms" that "enable AI and Data Transparency" and "extend tactical support for the warfighter at the edge." The Joint Warfighting Cloud Capability (JWCC) further supports cloud services "from headquarters to the tactical edge" across different classification levels. See U.S. Department of Defense, *DoD Cloud Strategy* (2018), 2–5, https://media.defense.gov/2019/feb/04/2002085866/-1/-1/1/dod-cloud-strategy.pdf; U.S. Department of Defense, "Department of Defense Announces Joint Warfighting Cloud Capability Procurement," December 7, 2022, https://www.war.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/. As an example of Cloud Service Provider (CSP)-based defense collaboration, AWS describes its Integrated Homeland Defense cloud services as providing secure cloud infrastructure and technologies for "global networking, space integration, artificial intelligence (AI) and machine learning (ML), generative AI, digital twin, high-performance computing (HPC), security, and cross-domain operations." See "AWS Cloud: Ready to Power Integrated Homeland Defense," Amazon Web Services, accessed May 30, 2026, https://aws.amazon.com/federal/defense/integrated-homeland-defense/.

[38] Matthew P. Funaiole et al., "Are U.S. Policies Eroding China's Dominance in Shipbuilding?" Center for Strategic and International Studies, September 24, 2025, https://www.csis.org/analysis/are-us-policies-eroding-chinas-dominance-shipbuilding.

[39] See Congressional Budget Office, *Maintenance Delays for Conventional Navy Ships* (December 2025), 10–15, https://www.cbo.gov/publication/61507; Shelby S. Oakley et al., *Navy Frigate: Unstable Design Has Stalled Construction and Compromised Delivery Schedules*, GAO-24-106546 (Government Accountability Office, 2024), 1–2, https://www.gao.gov/products/gao-24-106546; Diana Maurer et al., *Navy Shipyards: Actions Needed to Address the Main Factors Causing Maintenance Delays for Aircraft Carriers and Submarines*, GAO-20-588 (Government Accountability Office, 2020), https://www.gao.gov/products/gao-20-588.

[40] Grady T. Fontana, "USNS Wally Schirra Completes Major Maintenance at South Korean Shipyard," U.S. Pacific Fleet, March 13, 2025, https://www.cpf.navy.mil/Newsroom/News/Article/4119656/usns-wally-schirra-completes-major-maintenance-at-south-korean-shipyard/; Boram Kim, "Hanwha Ocean Wins 2nd Maintenance Deal from U.S. Navy," Yonhap News Agency, November 12, 2024, https://en.yna.co.kr/view/AEN20241112008100320; Suk-yee Jung, "Hanwha Ocean Lands Third U.S. Navy MRO Contract," Business Korea, July 9, 2025, https://www.businesskorea.co.kr/news/articleView.html?idxno=246680; "HD HHI Secures MRO Contract for USNS Alan Shepard," Naval News, August 7, 2025, https://www.navalnews.com/naval-news/2025/08/hd-hhi-secures-mro-contract-for-usns-alan-shepard/; Eunhyuk Cha, "HD HHI Secures Regular Overhaul Contract for USNS Cesar Chavez," Naval News, January 8, 2026; "Korea's HJ Shipbuilding Wins MRO Contract for U.S. Navy Vessel," The Korea Times, December 15, 2025, https://www.koreatimes.co.kr/business/companies/20251215/koreas-hj-shipbuilding-wins-mro-contract-for-us-navy-vessel.

[41] Dong-seon Kim and Yeon-seung Ryu, "미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구 [A Study on Improving the Integrated Inspection System to Respond to the U.S. CMMC Regime]," 한국방위산업학회지 [*Journal of the Korea Defense Industry Association*] 29, no. 3 (2022): pp. 1–2.

[42] The SolarWinds incident was a major supply chain cyberattack in which malicious code was inserted into SolarWinds software updates, compromising multiple U.S. federal agencies and critical national security networks. See U.S. Cybersecurity and Infrastructure Security Agency, "Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," last updated April 15, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a; Vijay A. D'Souza, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," Government Accountability Office, April 22, 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[43] See Bai-Qiao Chen et al., "Review of Digital Twin of Ships and Offshore Structures," in *Developments in Maritime Technology and Engineering 5 Volume 1*, ed. Carlos Guedes Soares (CRC Press, 2021); Remigiusz Iwańkowicz and Radosław Rutkowski, "Digital Twin of Shipbuilding Process in Shipyard 4.0," *Sustainability* 15, no. 12 (2023): 9733.

[44] A strong U.S. example of defense technology protection is the Defense Technology Security Administration (DTSA)'s defense technology security review process. DTSA reviews international transfers of controlled defense technology and may require a Technology Security Plan (TSP) or Technology Transfer Control Plan (TTCP) to mitigate risks in Direct Commercial Sales (DCS) or Foreign Military Sales (FMS). These plans help foreign recipients and companies establish procedures to comply with export laws, license conditions, and technology-transfer controls. See U.S. Defense Technology and Security Administration, "Defense Technology Security Reviews," accessed June 4, 2026, https://www.dtsa.mil/SitePages/assessing-and-managing-risk/defense-technology-security-reviews.aspx.

[45] Chan Yang et al., "국방상호조달협정(RDP-A)이 대미 방산 수출입에 미치는 영향 분석: 도구변수 활용을 중심으로 [The Impact of the Reciprocal Defense Procurement Agreement (RDP-A) on Defense Trade with the United States: An Instrumental Variable Approach]," 한국방위산업학회지 [*Journal of the Korea Association of Defense Industry Studies*] 32, no. 3 (2025): 52–53, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART003291301.

[46] The BAA can function as a procurement barrier because it gives preference to U.S.-made goods in federal acquisition, making it harder for foreign defense suppliers to compete in U.S. defense contracts. In the RDP-A context, the U.S. Department of Defense explains that reciprocal defense procurement agreements are designed to "remove barriers" to purchases of supplies and services from the other country; accordingly, an RDP-A could reduce BAA-related barriers and facilitate U.S.-South Korea defense-industrial cooperation. See Yang et al., "국방상호조달협정(RDP-A)이 대미 방산 수출입에 미치는 영향 분석 [The Impact of the Reciprocal Defense Procurement Agreement (RDP-A) on Defense Trade with the United States]."

Pathways to Cooperation for South Korea's Successful Nuclear-Powered Submarine Acquisition

By Jihoon Yu

South Korea's interest in a conventionally armed, nuclear-powered attack submarine (SSN) is no longer a distant strategic aspiration. It has become a live policy issue. Recent U.S.-South Korea summit-level discussions have placed the question of nuclear-powered submarines within a broader alliance agenda that also includes civil nuclear cooperation, shipbuilding, and maritime industrial capacity.[1] The U.S.-South Korea Joint Fact Sheet released by the White House after the summit meeting stated that the United States had "given approval for the ROK to build nuclear-powered attack submarines" and would work with South Korea to advance requirements for the project, including fuel sourcing options.[2]

That language did not settle the issue. It did, however, move South Korea's SSN debate from the realm of aspiration to the realm of alliance management and structured policy follow-up discussions. Since the summit, the Lee Jae Myung administration has established an interagency task force to support working-level talks with the Donald Trump administration on nuclear-powered submarines, civil nuclear cooperation, and other related issues. U.S. and South Korean officials have also begun follow-up discussions on how to turn language in the Joint Fact Sheet into practical requirements. These developments do not make an SSN program inevitable, but they underscore that the issue has become concrete enough that both countries must decide how to manage it responsibly.

The more important question, then, is not whether South Korea can articulate a strategic case for nuclear-powered submarines. The harder question is whether the two countries can build a pathway that is politically credible, legally defensible, technologically manageable, industrially useful, and strategically stabilizing. A South Korean SSN capability would never be purely for its own national security. From the outset, it would be bound up with the U.S.-South Korea alliance, U.S. nonproliferation policy, export-control rules, congressional oversight, and the condition of the U.S. submarine industrial base.

From Washington's perspective, this issue is not simply about whether Seoul wants a more capable submarine. It is about how a major U.S. ally can modernize its maritime capabilities without weakening global nonproliferation norms, straining the U.S. submarine industrial base, or creating new doubts about alliance cohesion. Just as importantly, U.S. policymakers will want to understand how a South Korean SSN capability could serve U.S. strategic interests, strengthening allied undersea deterrence, improving burden-sharing in the Indo-Pacific, relieving pressure on U.S. naval assets, and contributing to a more resilient maritime balance.

Dr. Jihoon Yu is Research Fellow at the Korea Institute for Defense Analyses (KIDA), where he previously served as a Director of External Cooperation. He served in the Republic of Korea Navy for 27 years as a submarine officer and strategic planning officer.

For Seoul, the lesson is equally important: strategic logic alone will not carry the case in Washington. South Korea will need to show not only why an SSN capability matters for its own security, but also how it can reinforce the alliance, support U.S. regional strategy, and remain compatible with nonproliferation norms. That is why the most promising course is not a demand for a submarine transfer or an immediate AUKUS-style exception. It should be a phased strategy built around an alliance-centered rationale, a nonproliferation-compatible framework, and industrial and human capital cooperation that also benefits the United States. In addition, South Korea should pursue a sustainment-first approach, with a disciplined, diplomatic narrative that presents a South Korean SSN as a stabilizing contribution to Indo-Pacific maritime security. Even if both governments can build that pathway, meaningful U.S. cooperation will still be difficult. But it will become more plausible over time.

Why South Korea Wants SSN Capabilities

South Korea operates in a demanding maritime environment, as North Korea continues to diversify its missile arsenal, deepen its undersea ambitions, and harden its military posture.[3] Beyond the peninsula, the Indo-Pacific maritime environment is growing more contested. Sea lines of communication (SLOC) are under greater pressure, undersea competition is intensifying, and the premium on survivable, persistent, and long-range undersea operations is only increasing.[4]

Advanced conventional submarines still matter, including those with air-independent propulsion. However, their limitations in endurance, speed, and sustained operational flexibility remain.[5] An SSN offers a different set of advantages: faster deployment, longer submerged endurance, greater freedom of maneuver, more persistent intelligence and surveillance missions, and a stronger capacity to complicate an adversary's targeting and operational planning.[6] For South Korea, those advantages matter not only in a wartime scenario on the Korean Peninsula but also in alliance missions involving sea lane security, anti-submarine warfare, undersea domain awareness, and the defense of maritime approaches.

However, the case for a South Korean SSN cannot be built around prestige or slogans about autonomy. In Washington, that kind of framing would likely raise skepticism rather than build support. If SSNs are presented as symbols of status or as tools for reducing South Korea's dependence on the alliance, suspicion may arise. The more persuasive case is an alliance case. A South Korean SSN capability would carry more weight in Washington if it is framed as a force multiplier for combined deterrence and maritime security, strengthening undersea surveillance near the peninsula, improving burden-sharing in Northeast Asia, supporting anti-submarine and anti-surface operations, and contributing to the defense of vital sea lanes in a more dangerous regional environment.

That framing matters because the United States has already shown a willingness to share extraordinary forms of naval nuclear propulsion technology under tightly controlled conditions. The 2023 AUKUS "optimal pathway" was not built around a quick transfer of boats. Rather, it was built around time, personnel integration, infrastructure development, rotational presence,

and eventually capability transfer.[7] The takeaway for South Korea is that the United States cooperates on highly sensitive issues only when strategic trust is high, long-term political alignment is clear, and the project is structured to reinforce rather than weaken U.S. force posture and industrial resilience. Therefore, South Korea should highlight the benefits of its SSN capability for the alliance's maritime strategy.

The First Pathway: Build an Alliance-Centered Strategic Narrative

Any serious South Korean effort should begin with narrative discipline. Too often, SSN debates drift toward maximalist language: strategic autonomy, prestige, latent nuclear status, or the idea that Seoul should possess what "advanced countries" possess.[8] That language may have domestic appeal, but it is politically counterproductive in Washington. It quickly creates the impression that undersea capability is only part of the story, and that nuclear hedging may be the larger objective.[9]

The first pathway, then, is conceptual. South Korea should define the mission of a future SSN capability narrowly, carefully, and responsibly. The most persuasive missions are those that align with U.S.-South Korea alliance priorities and with regional stability: countering North Korean undersea and missile threats, protecting critical maritime approaches, supporting anti-submarine and intelligence missions, escorting naval task groups, and contributing to maritime commons security with allies.[10] Therefore, a South Korean SSN should be described as conventionally armed, unrelated to nuclear weapons, and defensive in nature.

That matters because the United States will judge South Korea's intentions as much as its technical competence. The basic question will be straightforward: is Seoul seeking a capability that fits within allied deterrence, or one that signals eventual strategic divergence? If South Korea wants U.S. cooperation, it needs to remove ambiguity on that point.

The alliance-centered narrative should also stress complementarity rather than duplication. South Korea does not need to mirror the global mission profile of the U.S. Navy. A smaller South Korean SSN force tailored to regional contingencies could instead free U.S. assets for broader missions while improving the resilience of allied undersea operations in Northeast Asia. The argument for South Korean SSNs should focus on the alliance needing a more capable and persistent division of labor in the undersea domain, rather than on the fact that major powers have them.

Related to this, Seoul should avoid fusing the SSN debate with arguments for indigenous nuclear weapons. Under the Nuclear Nonproliferation Treaty (NPT), non-nuclear-weapon states remain bound by safeguards obligations, and the International Atomic Energy Agency (IAEA) continues to treat safeguards as central to verifying the peaceful use of nuclear material.[11] Once SSNs are rhetorically tied to nuclear armament, practical U.S. cooperation becomes harder to defend. Seoul's message has to remain disciplined: this is about naval propulsion, maritime defense, and alliance burden-sharing, not nuclear weapons.

The Second Pathway: Use the Existing Nuclear Cooperation Framework More Creatively

Law and politics matter just as much as strategy. The 2015 U.S.-South Korea Agreement for Peaceful Nuclear Cooperation renewed the bilateral "123 Agreement" framework for civil nuclear cooperation and created the High-Level Bilateral Commission as an institutional setting for senior-level dialogue on peaceful nuclear and strategic cooperation.[12] That framework was not built for naval propulsion; still, it remains the most important political and institutional platform through which the two governments can begin structured discussions on issues that would eventually shape any SSN path.

For that reason, South Korea should not dismiss the 123 framework as irrelevant simply because it is civilian in nature. In practice, that existing structure can help build the habits of transparency, technical dialogue, regulatory confidence, and fuel cycle trust that Washington would want to see long before entertaining anything more sensitive.[13] Seoul should use existing bilateral nuclear mechanisms to deepen cooperation on nuclear safety and safeguards, fuel-cycle transparency, and export-control compliance. None of those steps would authorize a South Korean SSN, but together they would address one of Washington's central anxieties: that Seoul wants the outcome without first building the trust architecture needed to support it.

There is also a wider nonproliferation issue. Naval nuclear propulsion occupies an unusually sensitive space because it intersects with safeguard obligations in ways that require special treatment. The IAEA has continued to engage states on safeguards questions related to naval propulsion, including Brazil's proposal concerning special procedures for nuclear material used in naval propulsion.[14] South Korea should study those developments carefully, not because Brazil offers a ready-made model, but because any future South Korean path will require early thinking about how to reconcile alliance cooperation, reactor fuel arrangements, and confidence in international verification.

That leads to a basic strategic principle: South Korea should default to a low-enriched uranium (LEU), transparency-first approach. LEU would not eliminate safeguards concerns because naval propulsion still involves nuclear material that may require special safeguards treatment. But it would be a more credible nonproliferation marker than highly enriched uranium (HEU) because LEU is not directly usable in nuclear weapons without further enrichment and would make Seoul's program easier to present as proliferation-resistant, verifiable, and compatible with alliance oversight.[15] Fuel choice and perceptions of safeguards will weigh heavily in determining whether the United States supports a South Korean SSN pathway. A visibly disciplined approach, anchored in verifiability, proliferation resistance, and alliance oversight, will be far more credible than one that appears designed to maximize fuel cycle freedom. The more Seoul presents itself as the ally pursuing the most nonproliferation-compatible route, the easier it becomes for U.S. officials and legislators to justify close nuclear partnership.

The Third Pathway: Make South Korean SSN Cooperation a U.S. Industrial Base Opportunity

One of the most overlooked aspects of the SSN question is industrial politics. Washington's immediate problem is not a lack of appreciation for alliance cooperation; it is capacity. The U.S. submarine and maritime industrial base is under serious strain, and U.S. officials have repeatedly pointed to workforce shortages, maintenance delays, and the difficulty of meeting ambitious shipbuilding and readiness goals as the root causes.[16] The U.S. Navy's messaging on the maritime industrial base has emphasized the need to use submarine-focused efforts as a springboard for broader maritime industrial integration, while public statements continue to highlight workforce bottlenecks and production constraints.[17]

That reality means South Korea should not approach the United States with a proposal that sounds like a zero-sum demand on scarce U.S. capacity. A better approach is to make South Korean SSN cooperation part of the answer to U.S. maritime industrial stress. South Korea remains one of the world's leading shipbuilding powers. It has a large-scale shipyard capacity, advanced digital shipbuilding capabilities, a sophisticated supplier network, and experience in complex naval construction and maintenance.[18] None of that automatically translates into naval nuclear propulsion competence, but it does mean Seoul has something tangible to bring to the alliance conversation.

The key is sequencing. Before requesting the most sensitive technology transfers, Seoul should expand bilateral industrial cooperation in areas useful to the U.S. Navy and politically easier to support in Washington. Initial focus should be on less sensitive domains where South Korea can add immediate value: non-nuclear maintenance and repair, digital shipyard and workforce cooperation, and supply-chain resilience for key maritime components. Such cooperation would build a practical, credible track record of contribution before Seoul seeks deeper cooperation in more sensitive areas.

Such cooperation would do at least three things. First, it would show that South Korea is investing in allied industrial resilience. Second, it would build practical relationships among South Korean firms, U.S. shipyards, and naval program offices. Third, it would gradually socialize the South Korean industry into the disciplines that any future SSN-related work would demand: rigorous quality assurance, cybersecurity, security compliance, and a culture aligned with the exacting standards of nuclear programs.[19]

This is where Seoul should draw the right lesson from AUKUS. Australia did not begin by asking for finished boats but after years of integrating people, infrastructure, and industrial planning.[20] The United States, the United Kingdom, and Australia also moved to reduce barriers to defense trade through export control reform; in 2024, Washington implemented new International Traffic in Arms Regulations (ITAR) exemptions and related measures to facilitate deeper defense trade integration with Australia and the United Kingdom.[21] South Korea should not expect identical treatment anytime soon. Yet, it should seek a South Korean version of defense-industrial

streamlining in less sensitive areas to build a record that could eventually justify tailored treatment in more sensitive domains.

The message to the United States should be clear and practical: helping South Korea prepare for an eventual SSN capability can reinforce the U.S. maritime industrial ecosystem rather than drain it.

The Fourth Pathway: Invest in People Before Platforms

No country acquires an SSN capability simply by purchasing reactors or drawing up hull designs. It does so by building a generational ecosystem of trained operators, technical experts, regulators, and industrial personnel who can meet the demanding standards of naval nuclear propulsion over decades.

This is where South Korea should move fastest, as human capital cooperation is strategically valuable and politically more feasible than early platform transfers. A serious U.S.-South Korea pathway should begin with personnel embedding, education, and long-term training. Again, AUKUS offers a useful precedent: it places heavy emphasis on embedding Australian military and civilian personnel within the U.S. Navy and the Royal Navy, as well as supporting industrial bases.[22]

For South Korea, a parallel effort could take several forms. Washington and Seoul could build on existing patterns of naval training and industrial education cooperation by expanding educational and observational exchanges in areas such as submarine operations, shipyard management, quality assurance, and lifecycle sustainment. Recent bilateral naval exercises have already included in-port academics, liaison officer exchanges, and anti-submarine warfare training, while the two countries have also begun shipbuilding education initiatives that could provide a foundation for broader workforce cooperation.[23]

Over time, those exchanges could expand into more specialized training for South Korean officers, engineers, regulators, and industrial personnel in nuclear safety culture, systems engineering, maintenance planning, and oversight. South Korean shipyards could also develop joint workforce programs with U.S. counterparts focused on demanding naval standards. More ambitiously, the alliance could establish a dedicated U.S.-South Korea maritime nuclear talent initiative under a broader defense-industrial cooperation framework.

This matters for two reasons. First, it addresses the most basic truth about SSNs: the real bottleneck is often trust in people and institutions, not money or steel. Second, it provides an early-success model. Even if platform-level cooperation remains politically difficult for some time, training and personnel cooperation can still move the alliance forward while strengthening the long-term foundation for an SSN pathway.

South Korea should also build its own domestic institutional architecture in parallel. An SSN capability cannot depend solely on naval enthusiasm; it requires interagency alignment across defense, foreign affairs, industry, energy, export controls, nuclear regulation, and legislative

oversight for maximum efficacy. Washington will want to see that Seoul has moved beyond conceptual ambition and is building the bureaucratic foundation needed for a program of exceptional sensitivity.

The Fifth Pathway: Pursue a Sustainment-First Model

A sustainment-first model deserves separate attention because sustainment is not simply another form of industrial cooperation. It is where operational trust is tested over time. Building a submarine is one challenge; keeping it deployable, safe, secure, and integrated into allied operations over decades is another. For a capability as sensitive as naval nuclear propulsion, Washington will care not only about whether Seoul can eventually acquire platforms but also about whether South Korean institutions can sustain the long-term disciplines of maintenance planning, configuration control, safety oversight, security compliance, and lifecycle accountability.

This is why South Korea should avoid defining success too narrowly as indigenous construction from the outset. A more realistic path would begin with sustainment roles that are politically easier to support and operationally useful to the alliance. These could include non-nuclear maintenance support, dockside infrastructure cooperation, spare-parts resilience, digital sustainment tools, and selected lifecycle support functions for allied maritime forces. Such activities would not resolve the most sensitive propulsion questions, but they would help South Korea demonstrate reliability in the daily work that makes undersea operations viable.

The value of this approach is cumulative. Sustainment cooperation would allow South Korean shipyards, naval personnel, and regulators to build habits of precision, documentation, security, and schedule discipline in practical settings. It would also give U.S. officials a record of performance to evaluate before considering more sensitive forms of cooperation. In Washington, confidence is rarely built through abstract assurances alone. It is built through repeated evidence that a partner can meet demanding standards under real operational conditions.

A sustainment-first model, therefore, creates a ladder of credibility. It shifts the question from whether the United States should make an immediate exception for South Korea to whether South Korea has already become a dependable contributor to allied maritime readiness. Over time, that record could make deeper SSN-related cooperation appear less like a speculative political favor and more like the next step in an established alliance practice. Sustainment, in this sense, is not a lesser goal. It is the practical foundation on which any more ambitious SSN pathway would have to rest.

The Sixth Pathway: Keep the Program Conventionally Armed and Strategically Bounded

Washington's concerns are not solely legal or technical—they are also geopolitical. U.S. officials may worry about how China interprets South Korea's SSN path, how other allies react, and whether a South Korean SSN sets precedents that complicate U.S. nonproliferation diplomacy elsewhere.[24] More specifically, they will want reassurance that South Korea's SSN effort does

not blur the line between allied naval modernization and a broader regional conversation about nuclear latency or strategic autonomy. Seoul cannot remove all of those concerns, but it can reduce them through consistent signaling and careful policy design.

The most important step is self-limitation. South Korea should repeatedly affirm that any future SSN capability would be conventionally armed and tightly bounded in mission, force structure, and doctrine. It should reject any narrative that presents an SSN as a stepping stone to nuclear weapons, a shortcut to latent nuclear status, or an instrument of independent strategic coercion. Instead, Seoul should emphasize deterrence, defense, maritime surveillance, anti-submarine warfare, protection of critical SLOC, and support for the maritime commons in coordination with allies. The narrower and more disciplined the stated mission, the easier it will be to present the program as stabilizing rather than escalatory.

This message is not just for Washington but for the wider region as well. South Korea should clarify that an SSN capability would not be designed for power projection detached from alliance obligations, let alone to change the regional nuclear order. It should be explained as a defensive maritime capability shaped by a demanding strategic environment, not as a prestige platform or a symbol of geopolitical ambition. That distinction will affect how much diplomatic friction the program creates over time.

The more Seoul frames the program as a disciplined, alliance-based contribution to stability, under strong safeguards and close alliance coordination, the more manageable the diplomatic environment becomes. Strategic restraint in this instance is not a concession but a condition for political feasibility.

The Seventh Pathway: Build Political Support in Washington Before Seeking Policy Breakthroughs

No South Korean SSN pathway will succeed if Seoul focuses only on the executive branch. The U.S. Congress matters, as evidenced by the defense trade reforms linked to AUKUS.[25] Legislative authorities, export controls, budget politics, and industrial oversight all shape what Washington can and cannot do.[26] South Korea, therefore, needs a long game in Washington that extends beyond the White House to Congress, think tanks, naval communities, industrial stakeholders, former defense officials, and the broader nonproliferation policy world. Without that wider political groundwork, even a strategically sensible proposal could stall.

This means patient coalition-building. Seoul should engage not only those already inclined toward stronger alliance burden-sharing, but also skeptics concerned about precedent, proliferation, industrial strain, or regional escalation. The goal should be to normalize serious discussion of a future pathway as legitimate, strategically rational, and compatible with nonproliferation instead of securing an immediate endorsement of a South Korean SSN. In Washington, major new ideas usually have to become discussable before they become possible.

That requires answering hard questions directly and repeatedly. Why is an SSN necessary as opposed to advanced conventional submarines? How would safeguards concerns be handled? How would Seoul avoid burdening U.S. industry? How would the program strengthen rather than dilute U.S. deterrence? How would it be sequenced? What guardrails should be in place to prevent mission creep or political misinterpretation? These are the questions that South Korea must answer if it wants serious support.

The more specific and restrained South Korea's answers are, the more persuasive they will be. Ambition without sequencing will fail, and sequencing without political outreach will fail. A steady campaign of explanation in Washington does not guarantee success, but it would gradually lower the barriers to future cooperation. In alliance politics, breakthroughs are usually prepared long before they are announced.

What South Korea Should Not Do

A practical pathway also requires clarity about what to avoid. In a project as politically sensitive as naval nuclear propulsion, poor framing can be as damaging as poor policy. South Korea should develop both a positive roadmap and a clear sense of what arguments and tactics are most likely to backfire in Washington.

First, Seoul should not publicly demand immediate access to the AUKUS model. Australia's pathway rests on a unique trilateral structure, decades of nuclear stewardship trust with the United States and the United Kingdom, and a very specific political setting. Treating AUKUS as an entitlement benchmark would likely provoke backlash in Washington and reinforce the impression that Seoul is seeking shortcuts on a highly sensitive issue. The better course is to study AUKUS carefully and adapt the parts of it that matter most: personnel embedding, industrial integration, long timelines, and strict alliance framing.

Second, South Korea should not allow domestic debates to blur the line between SSNs and nuclear weapons. The more those two issues are fused in public rhetoric, the harder it becomes for U.S. officials to defend even exploratory cooperation. Once SSNs are folded into a broader argument about nuclear sovereignty or armament, the political cost of supporting South Korea rises sharply.

Third, Seoul should not present the program as an abrupt sovereign leap. The United States will be much more receptive to a phased pathway than to a symbolic declaration unsupported by institutional preparation. Large strategic announcements may work in domestic politics, but in Washington, they often raise doubts about seriousness and sequencing.

Fourth, South Korea should not underestimate the compliance burden that comes with sensitive defense cooperation. Even modest growth in defense trade integration would require Seoul to demonstrate that it can protect classified information, manage controlled technologies, and operate within U.S. export-control rules. For Washington, political will alone will not be enough.

Confidence will depend on whether South Korean institutions and firms can meet exacting standards consistently over time.

Finally, Seoul should not assume that strategic logic alone will carry the argument. Even if the military case for a South Korean SSN strengthens, U.S. support will still depend on whether South Korea appears politically disciplined, nonproliferation-responsible, and industrially useful. In alliance politics, legitimacy has to be built as carefully as capability.[27]

A Realistic Roadmap

If South Korea wants a successful long-term outcome, the roadmap should be sequential. The point is not to force an immediate breakthrough on the most sensitive issue but to structure the pathway in stages so that each step strengthens the political and institutional basis for the next. The success of that strategy will depend on the alliance's ability to gradually build trust, habits of cooperation, and concrete evidence of South Korea's seriousness.

In the near term, Seoul should focus on narrative discipline, mission definition, and political engagement in Washington. It should make clear that a future South Korean SSN capability would be conventionally armed, alliance-centered, strategically bounded, and nonproliferation-responsible. At the same time, it should expand maritime industrial cooperation in non-nuclear domains and invest heavily in human capital, nuclear governance preparation, export control trust, and submarine sustainment cooperation. Quiet but technical consultations on safeguards, fuel cycle perceptions, and regulatory requirements should begin early, even if they remain largely out of public view. The near-term objective is not to force a decision but to make South Korea look disciplined, useful, and credible.

In the medium term, South Korea should seek a more formalized U.S.-South Korea maritime strategic cooperation track centered on undersea deterrence, industrial integration, workforce development, and alliance resilience. That could include embedded personnel, expanded submarine education and observation programs, more ambitious MRO cooperation, joint workforce initiatives, and limited but meaningful technical exchanges. At this stage, Seoul's goal should be to make itself indispensable to allied maritime resilience in Northeast Asia. The more South Korea is seen as helping solve operational and industrial problems, the more plausible SSN-related cooperation will become.

Only in the long term, after years of trust-building and demonstrated performance, should Seoul seek decisions on the most sensitive dimensions of SSN cooperation: reactor arrangements, fuel pathways, deeper technology access, and possible construction or acquisition models. By then, the question in Washington should focus on responsibly structuring the next step.

Table 1. A Phased Roadmap for U.S.-South Korea SSN Cooperation

Phase	Main Objective	Priority Actions	Strategic Effect
Near Term	Build credibility before asking for sensitive concessions	Clarify mission definition; maintain conventionally armed framing; expand Washington outreach; begin safeguards, fuel-cycle, and regulatory consultations; deepen non-nuclear maritime industrial cooperation.	Makes South Korea appear disciplined, useful, and nonproliferation-responsible.
Medium Term	Make South Korea indispensable to allied maritime resilience	Formalize a U.S.-South Korea maritime cooperation track; expand personnel embedding; develop submarine education programs; broaden MRO and workforce cooperation; strengthen export-control and industrial-security trust.	Builds practical performance records and lowers political resistance to deeper cooperation.
Long Term	Structure sensitive SSN cooperation responsibly	Consider reactor arrangements, fuel pathways, deeper technology access, and construction or acquisition models only after years of demonstrated performance and institutional trust.	Turns a politically difficult request into the next step in a proven alliance relationship.

A realistic roadmap is not gradual for the sake of caution alone. It is gradual because the issue itself is unusually sensitive. Naval nuclear propulsion sits at the intersection of alliance politics, nonproliferation, industrial capacity, legal authority, and regional strategy. Any effort to accelerate every dimension simultaneously would likely provoke resistance. A phased approach lowers that risk by ensuring that political support, institutional preparation, industrial cooperation, and diplomatic messaging evolve together rather than at cross-purposes. In this sense, sequencing is what makes an otherwise implausible objective strategically imaginable.

Conclusion

If South Korea ever acquires an SSN capability, it will not be because of a single dramatic negotiation or a bold political decision: it will be the result of patient alliance statecraft. The decisive question is not whether Seoul can make a strategic case for nuclear-powered submarines, but whether South Korea can persuade the United States that helping it move in that direction would strengthen the alliance, reinforce nonproliferation discipline, ease maritime industrial strain, and contribute to Indo-Pacific stability.

That is why the most promising path is gradual, alliance-centered, and institutionally serious. Seoul should begin by demonstrating restraint, nonproliferation responsibility, and a credible record of practical contribution to the alliance. It should anchor the SSN debate in combined deterrence rather than prestige, in maritime burden-sharing rather than autonomy theatrics, in safeguards-compatible discipline rather than ambiguity, and in long-term alliance trust rather than short-term political pressure.

Even if South Korea follows that course, U.S. cooperation will not be easy. However, it will become thinkable. And in alliance politics, that is often where major change begins.

Endnotes

[1] Jihoon Yu, "Game Changer: Trump Approves South Korea's Nuclear Submarine Ambition," The Diplomat, October 31, 2025, https://thediplomat.com/2025/10/game-changer-trump-approves-south-koreas-nuclear-submarine-ambition/.

[2] The White House, "Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung," November 13, 2025, https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/.

[3] "North Korea Submarine Capabilities," Nuclear Threat Initiative, August 19, 2024, https://www.nti.org/analysis/articles/north-korea-submarine-capabilities/.

[4] "Navigating Security Dilemmas in Indo-Pacific Waters," Stockholm International Peace Research Institute, June 2024, https://www.sipri.org/sites/default/files/2024-06/indo_pacific.pdf.

[5] Karen Elphick, "The Deterrence Advantage of Nuclear-Powered Submarines," Australian Parliamentary Library, March 4, 2025, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/Research_Papers/2024-25/The_deterrence_advantage_of_nuclear_powered_submarines.

[6] Jihoon Yu, "South Korea Should Lean into Nuclear-Powered Submarines," War on the Rocks, February 17, 2025, https://warontherocks.com/south-korea-should-lean-into-nuclear-powered-submarines/.

[7] Government of the United Kingdom, "Fact Sheet: Trilateral Australia-UK-US Partnership on Nuclear-Powered Submarines," March 13, 2023, https://www.gov.uk/government/publications/joint-leaders-statement-on-aukus-13-march-2023/fact-sheet-trilateral-australia-uk-us-partnership-on-nuclear-powered-submarines.

[8] Tom Corben, "AUKUS versus ROKUS: Lessons for South Korea from Australia's Experience," Korea On Point, December 10, 2025, https://koreaonpoint.org/articles/article_detail.php?idx=512.

[9] Lami Kim, "South Korea's Nuclear Latency Dilemma," War on the Rocks, September 19, 2024, https://warontherocks.com/south-koreas-nuclear-latency-dilemma.

[10] Jihoon Yu and Erik French, "The U.S.-ROK Alliance as an Indo-Pacific Maritime Partnership," U.S. Naval Institute, May 2022, https://www.usni.org/magazines/proceedings/2022/may/us-rok-alliance-indo-pacific-maritime-partnership.

[11] International Atomic Energy Agency, *Legal Framework for IAEA Safeguards* (2013), https://www.iaea.org/publications/10388/legal-framework-for-iaea-safeguards.

[12] U.S. Department of State, "Joint Statement of the 2016 United States-Republic of Korea Foreign and Defense Ministers' Meeting," October 19, 2016, https://2009-2017.state.gov/r/pa/prs/ps/2016/10/263340.htm.

[13] "Agreement for Cooperation Between the Government of the Republic of Korea and the Government of the United States of America Concerning Peaceful Uses of Nuclear Energy," June 15, 2015, https://fissilematerials.org/library/kr123.pdf.

[14] International Atomic Energy Agency, "Naval Nuclear Propulsion: Brazil," November 12, 2025, https://www.iaea.org/sites/default/files/govinf2025-13.pdf.

[15] James M. Acton, "Why the AUKUS Submarine Deal Is Bad for Nonproliferation—And What to Do About It," Carnegie Endowment for International Peace, September 21, 2021, https://carnegieendowment.org/posts/2021/09/why-the-aukus-submarine-deal-is-bad-for-nonproliferationand-what-to-do-about-it.

[16] "Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program: Background and Issues for Congress," Congressional Research Service, December 4, 2025, https://www.congress.gov/crs-product/R41129.

[17] Eric J. Labs, "Testimony on The Navy's 2025 Shipbuilding Plan and Its Implications for the Shipbuilding Industrial Base," Congressional Budget Office, March 11, 2025, https://www.cbo.gov/publication/61240.

[18] Namyeon Kwon, "Don't Miss the Boat: Considerations for U.S.-South Korea Maritime Cooperation," Center for Strategic and International Studies, June 12, 2025, https://www.csis.org/analysis/dont-miss-boat-considerations-us-south-korea-maritime-cooperation.

[19] *The AUKUS Nuclear-Powered Submarine Pathway: A Partnership for the Future* (Australian Department of Defence, March 2023), https://www.asa.gov.au/sites/default/files/documents/2024-10/00.%20Public%20Report.pdf.

[20] Australian Submarine Agency, "Submarine Rotational Force-West," https://www.asa.gov.au/aukus/submarine-rotational-force-west.

[21] U.S. Department of State, "International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation Among Australia, the United Kingdom, and the United States," *Federal Register* 89, no. 85 (May 1, 2024), https://www.federalregister.gov/documents/2024/05/01/2024-08829/international-traffic-in-arms-regulations-exemption-for-defense-trade-and-cooperation-among.

[22] "Fact Sheet: Trilateral Australia-UK-US Partnership on Nuclear-Powered Submarines," The American Presidency Project, March 13, 2023, https://www.presidency.ucsb.edu/documents/fact-sheet-trilateral-australia-uk-us-partnership-nuclear-powered-submarines.

[23] Victor Murkowski, "U.S., Republic of Korea Conduct Maritime Counter Special Operations Forces Exercise," United States Navy, November 21, 2025, https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4339775/us-republic-of-korea-conduct-maritime-counter-special-operations-forces-exercise.

[24] Ariel (Eli) Levite and Toby Dalton, "How the United States Can Use AUKUS to Strengthen Nuclear Nonproliferation," Carnegie Endowment for International Peace, December 16, 2021, https://carnegieendowment.org/research/2021/12/how-the-united-states-can-use-aukus-to-strengthen-nuclear-nonproliferation.

[25] Paul K. Kerr, "U.S. Arms Transfer Restrictions and AUKUS Cooperation," Congressional Research Service, August 9, 2024, https://www.congress.gov/crs-product/IF12483.

[26] Philip Johnson et al, "Export Control Changes for the AUKUS Partnership," U.S. Department of Commerce, March 18, 2025, https://www.bis.gov/media/documents/aukus.pdf.

[27] Osman Sabri Kiratli, "The Politics of Alliance Cohesion: Experimental Evidence on American Attitudes Toward Corrective Measures in Security Partnerships," *Perspectives on Politics* (October 2025): 1–16.

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?”

Section 2

Alliance Adaptation in an Era of Transformation

South Korea's New External Economic Development Strategy

By Taeho Bark and Dongchul Kwak

The global trade environment has been undergoing a significant transformation since the establishment of the General Agreement on Tariffs and Trade (GATT) system, driven primarily by the United States' shift in policy stance from a focus on free trade to prioritizing domestic production over foreign imports and global supply chains. Particularly since the inauguration of the first Donald Trump administration, the U.S. government has implemented various policies to promote domestic industries based on the belief that overseas investment by U.S. firms and imports from foreign countries deprive domestic workers of jobs and exacerbate income inequality.[1] These policies directly contradict international trade theory, which is grounded in productivity and efficiency.

Under the second Trump administration, the United States has gone so far as to completely disregard the most-favored-nation (MFN) principle it has upheld for decades, instead adopting discretionary tariff policies that discriminate against foreign countries under various U.S. trade laws.[2] Since the April 2 announcement of "Liberation Day" tariffs, the United States has begun using tariffs as a policy instrument to compel the European Union, Japan, South Korea, and other partners to conclude agreements requiring large-scale investments in the United States.[3] The Lee Jae Myung administration immediately initiated negotiations with the Trump administration to complete a "Package Deal" involving tariff adjustments in exchange for massive investment commitments in the United States, along with additional support for the reconstruction of the U.S. shipbuilding industry.[4]

Although the U.S. Supreme Court ruled on February 20, 2026, that the Trump administration's reciprocal tariffs imposed under the International Emergency Economic Powers Act (IEEPA) were unlawful, Trump strongly opposed the decision. His administration immediately introduced a new 10 percent global tariff under Section 122 of the Trade Act of 1974 and initiated Section 301 investigations into unfair trade practices against several trading partners.[5]

Taking into account these dramatic developments in tariff measures, Trump's policy objectives can be broadly divided into two dimensions. First, he seeks to increase U.S. tariff revenues and reduce the trade deficit by imposing tariffs. Second, through tariff negotiations, he aims to

---

Dr. Taeho Bark is President of the Seoul Forum for International Affairs (SFIA) and Professor Emeritus at the Graduate School of International Studies (GSIS) of Seoul National University. He served as the Minister for Trade of the Republic of Korea from 2011-2013.

Dr. Dongchul Kwak is Associate Professor at the School of Economics and Trade and Head of the Research Center for Digital Economy and Trade of Kyungpook National University, Daegu, Republic of Korea.

boost inward investment and revive U.S. manufacturing industries, including semiconductors, energy, shipbuilding, and nuclear power. However, whether these objectives could be achieved smoothly remains to be seen.

The fundamental problem is that policies prioritizing domestic firms and industries are proliferating across major economies, while international norms governing such policies remain unclear. In particular, international rules regarding industrial subsidies, tariffs imposed on national security grounds, and countermeasures against unfair trade practices have not been clearly established, and the World Trade Organization (WTO)—the institution responsible for addressing these issues—is no longer functioning effectively.[6] Even more troubling is the likelihood that this situation will persist for the foreseeable future; countries around the world are expected to continue pursuing unilateral and discretionary industrial and trade policies aimed at maximizing or protecting national interests. For example, Canada imposed 25 percent tariffs on USD 108 billion in U.S. goods, and the European Union announced but then delayed its plan to reimpose the 2018 and 2020 retaliatory tariffs against the United States.[7]

South Korea has pursued an external economic policy focused on expanding export markets. To this end, South Korea has respected the WTO-centered multilateral trading system while simultaneously concluding high-standard free trade agreements (FTAs) with major economies such as the United States, China, and the European Union.[8] However, the recent increase in volatility in import tariffs, coupled with growing pressure to invest locally rather than export, poses serious challenges for South Korea. Moreover, if overseas investment by South Korean firms continues to expand, it could potentially inflict serious damage on the South Korean economy. Domestically, concerns have been raised that large-scale overseas investment by South Korean firms may lead to industrial hollowing-out, reducing exports and employment at home.[9]

Given the relatively small size of its domestic market, South Korea has no choice but to rely on external economic activities—such as exports and overseas investment—to sustain economic growth. This paper seeks to explore a new external economic development strategy for South Korea that links overseas investment to exports, along with corresponding policy directions. The paper first reviews the relationship between international trade and foreign direct investment (FDI) in the existing literature and then empirically analyzes how the relationship between South Korean firms' overseas investment and exports has evolved over time. Based on this analysis, the paper proposes a new external economic development strategy focused on maximizing exports of intermediate goods produced through FDI and presents policy measures to implement this strategy effectively.

FDI and International Trade

The relationship between FDI and international trade has long been a central topic in international economics. Early theoretical studies distinguished between horizontal FDI, which involves establishing overseas production bases to access foreign markets, and vertical FDI, which takes advantage of cross-country differences in production costs to procure intermediate

inputs more efficiently. These studies argued that horizontal FDI tends to substitute for exports because it targets foreign markets directly, whereas vertical FDI does not because it increases cross-border trade in intermediate goods between headquarters and overseas affiliates.[10]

In practice, however, various forms of FDI are observed depending on firms' circumstances, producing outcomes that differ from early theoretical expectations. For example, a firm may undertake FDI in a developing country with low productive factor costs, source most intermediate inputs from the home country, assemble or produce final goods locally, and export them to third-country markets. Alternatively, a firm may invest in a developed country with a large market, source high value-added intermediate inputs from the home country, and assemble or produce final goods for sale in the host country market. While the former case represents vertical FDI that increases intermediate-goods trade but may reduce home-country exports to third markets, the latter represents horizontal FDI that substitutes for final-goods exports but can expand intermediate-goods exports, potentially increasing overall trade. Thus, firms strategically choose between exports and FDI depending on their circumstances.

Most empirical studies to date conclude that overseas FDI and exports are complementary.[11] That is, in nearly all cases, the expansion of intermediate-goods exports outweighs the substitution effect on final-goods exports. This is particularly evident in manufacturing industries characterized by fragmented production, where parent firms significantly increase exports of intermediate goods to their overseas affiliates after undertaking FDI. Furthermore, studies show that even when firms relocate final-goods production overseas, high value-added upstream production processes tend to remain in the home country.[12] This suggests that by continuously expanding exports of high value-added intermediate goods, home countries can maintain domestic production of these goods despite outward FDI.

Nevertheless, concerns about industrial hollowing-out have risen in countries with large manufacturing sectors as overseas FDI expands.[13] Some empirical studies show that overseas FDI does not directly reduce domestic production or employment, but instead restructures domestic industries toward higher value-added activities.[14] OECD emphasizes that the risk of industrial hollowing-out depends less on the scale of outward FDI and more on a country's ability to upgrade its position within global value chains.[15] Accordingly, it is increasingly important to devise strategies that leverage overseas FDI to enhance domestic industrial competitiveness, expand exports, and create jobs while minimizing the risks of hollowing-out.

Structural Changes in South Korea's Exports and Linkages With Overseas Investment

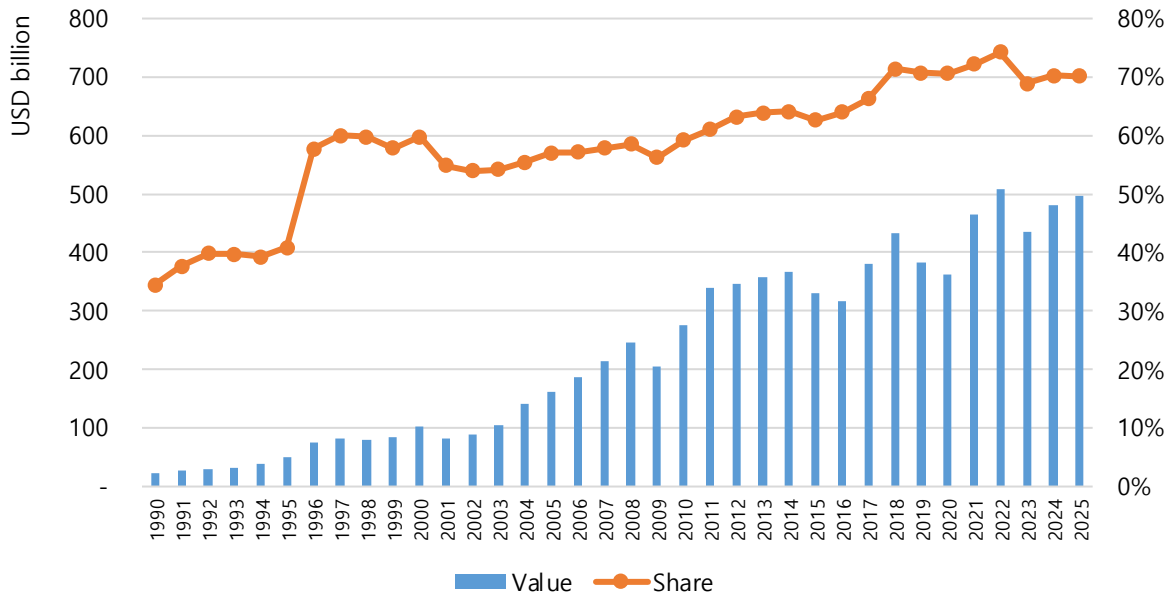
In the early 1960s, South Korea was one of the poorest countries in the world, with per capita income below USD 100.[16] At the time, the South Korean government concluded that exports were the only viable path to economic development for a country lacking natural resources and technology, and it devoted substantial efforts to export promotion. Initially, the government encouraged exports of labor-intensive goods and, in the 1970s, began fostering heavy and chemical industries.[17] Although South Korea faced the risk of overinvestment, excess capacity,

and excessive debt, the global economic boom of the mid-1980s enabled heavy industry and chemical products to become major export items, helping the country overcome these challenges and sustain rapid economic growth.

On the back of export-led growth, South Korea achieved remarkable economic development, ranking thirteenth globally in GDP, seventh in total trade, and sixth in exports by 2024.[18] South Korea has pursued a trade policy centered on export market expansion by simultaneously promoting the multilateral trading system and regional trade agreements. As of 2024, South Korea has concluded and implemented twenty-two FTAs with fifty-nine countries. The combined GDP of these FTA partners exceeds 85 percent of global GDP, giving South Korea the world's third-largest FTA network after Singapore and China.[19]

South Korea initially exported labor-intensive consumer goods, but the share of intermediate goods in total exports has steadily increased over time. As shown in Figure 1, intermediate goods now account for more than 70 percent of South Korea's exports in 2025. This shift reflects South Korean firms' strategic choice to specialize in exporting productivity-enhancing, internationally competitive intermediate goods rather than producing final goods domestically, as rising wages reduced the profitability of domestic production of final goods.

Figure 1. South Korea's Intermediate Goods Exports and Their Share in Total Exports, 1990–2025

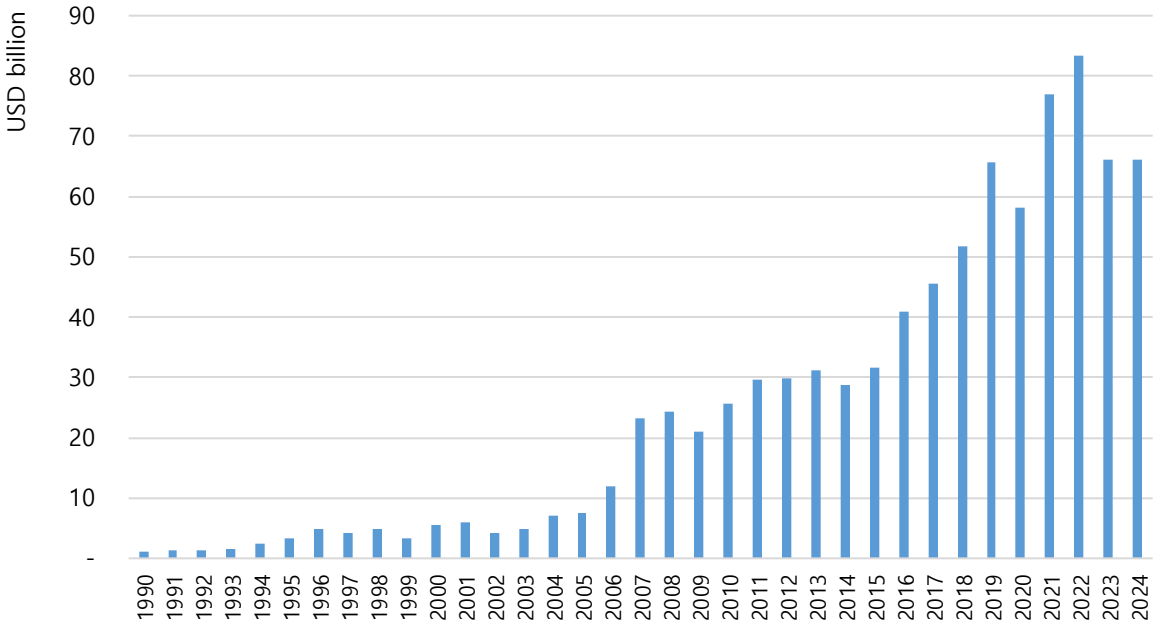


Source: "K-stat," Korea International Trade Association.

South Korean firms have invested in countries with low production costs to produce consumer goods and intermediate inputs for export to global markets, including the United States.[20] For instance, after South Korea normalized diplomatic relations with China in 1992, many South Korean firms established subsidiaries in China, attracted by low wages and inexpensive land.[21] These subsidiaries sourced intermediate goods from parent companies in South Korea, utilized Chinese labor to produce consumer and intermediate goods, and exported them globally. During

this period, South Korea's exports to China consisted largely of intermediate goods supplied to South Korean affiliates located in China.[22] As shown in Figure 2, overseas investment by South Korean firms steadily increased over time, reaching a record USD 83.5 billion in 2022 and remaining above USD 60 billion thereafter.

Figure 2. South Korea's Total Outward Foreign Direct Investment, 1990–2024



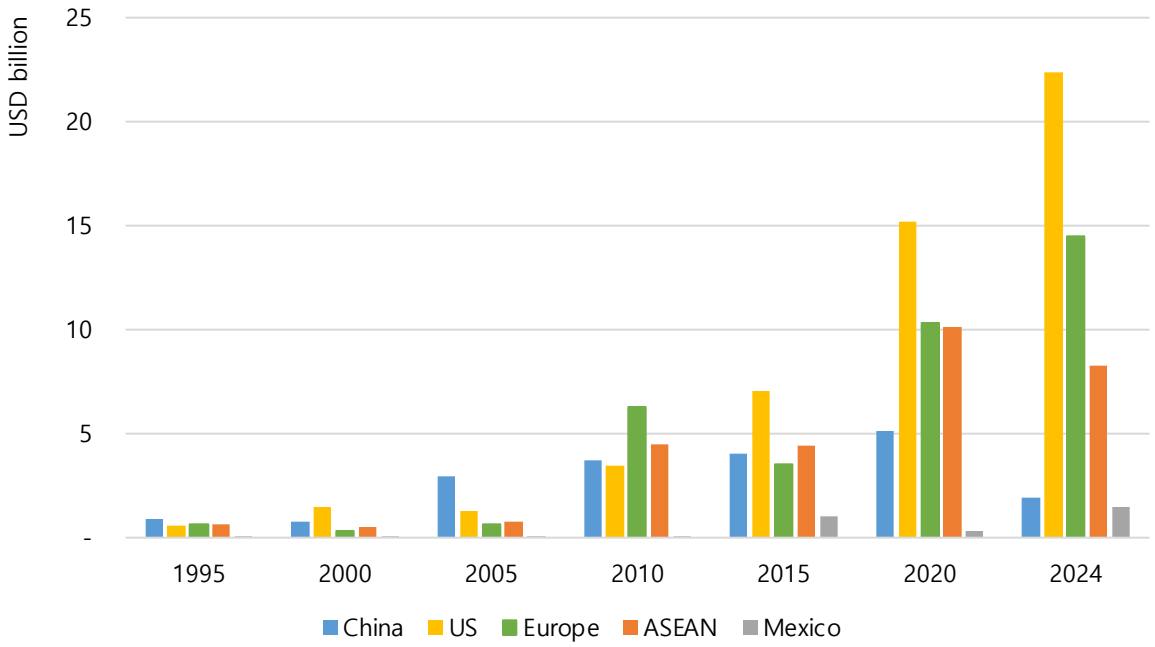
Source: Korea EXIM Bank.

All in all, South Korean firms' FDI strategies have evolved through three stages. Initially, firms favored vertical FDI aimed at producing final goods in low-cost locations for export to third-country markets. Over time, however, they expanded into horizontal FDI aimed at penetrating local markets in advanced or rapidly growing economies. Up until 2025, South Korean firms pursued vertical, horizontal, or hybrid forms of FDI tailored to their specific corporate strategies. However, some manufacturing firms that have invested heavily in Mexico to exploit competitive labor costs, geographic proximity to the United States, and preferential tariff access under the United States-Mexico-Canada Agreement (USMCA) now face significant uncertainty under the second Trump administration.

Trump's "America First" trade policy has the potential to reshape not only the global trading system but also South Korean firms' supply chains and overseas investment strategies. Figure 3 illustrates trends in South Korean firms' overseas investment by region. Investment in China expanded steadily until 2020. However, from 2010 onward, investment in ASEAN member countries surpassed investment in China, reflecting rising labor and land costs in China and heightened U.S.-China tensions. South Korean firms judged it more advantageous to establish production bases in ASEAN countries such as Vietnam and Indonesia. While the primary objective remains exporting goods produced in Southeast Asia to global markets,

investment aimed at local market entry has recently increased as ASEAN economies grow.[23] Notably, South Korean firms' investment in China dropped sharply between 2020 and 2024.

Figure 3. South Korea's Outward FDI by Major Destination, 1995–2024

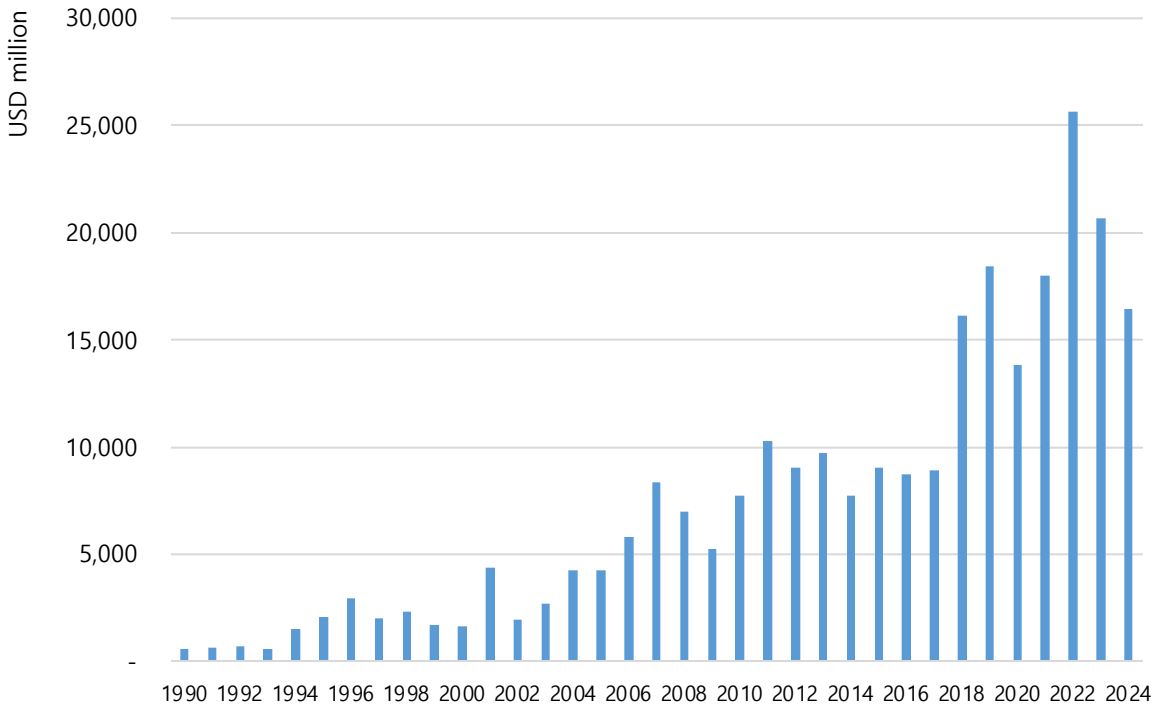


Source: The Export-Import Bank of Korea.

Overseas investment in the United States and Europe has also increased markedly since 2010, with investment in the United States accelerating after 2015. In 2024, the United States ranked first, followed by Europe, ASEAN, and China, as top destinations for South Korean outbound FDI. Since 2020, investment in advanced economies has largely focused on local market entry, driven by host-country incentives such as manufacturing subsidies and by U.S. pressure to invest domestically through tariff threats.[24] Given continued large-scale investment commitments by major South Korean firms, this trend is expected to persist.[25]

In addition, the sectoral focus of FDI has changed over time. As shown in Figure 4, South Korean firms have significantly increased manufacturing FDI after 2000, exceeding USD 15 billion annually from 2018 onward and peaking at USD 25 billion in 2022. In the 1990s, food and apparel accounted for a large share of manufacturing FDI.[26] Since the 2000s, investments have shifted toward high-tech sectors such as electronic components, computers, and communications equipment. Investment in chemicals and automobiles also expanded from the 2010s onward, with electrical equipment—including secondary batteries, power transformers, and energy storage systems—emerging as the largest sector by 2024.[27]

Figure 4. South Korea's Outward Foreign Direct Investment in the Manufacturing Sector, 1990–2024

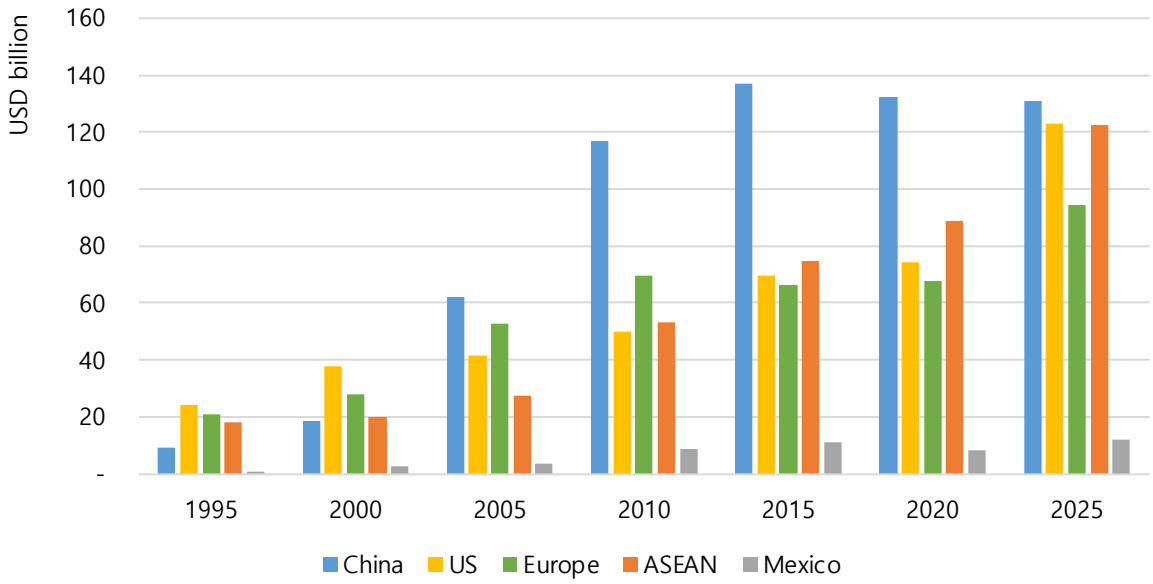


Source: The Export-Import Bank of Korea.

South Korean manufacturing firms' investment patterns vary significantly depending on the destination country. Investment in the United States initially focused on automobiles, chemicals, and electronics, but has concentrated primarily on electrical equipment since 2020.[28] Investment in China began with automobiles and apparel, and later shifted toward electronics and communications equipment, with electrical equipment rising in importance after 2015.[29] Investment in ASEAN countries has been dominated by electronics-related sectors, while investment in Mexico has focused on automobiles and metal products.[30]

There is a strong correlation between South Korean exports and the outward FDI of South Korean firms. As Figure 5 shows, South Korean exports to countries and regions that receive more FDI from South Korean firms have also increased. Exports to China surged between 2000 and 2015, when investment in the country was high, and exports to ASEAN and the United States grew substantially after 2015 as investment shifted to those regions.[31]

Figure 5. South Korea's Total Exports to Major Trading Partners, 1995–2025



Source: "K-stat," Korea International Trade Association.

With intermediate goods accounting for over 70 percent of South Korean exports, this trend reflects increased exports of intermediate inputs supplied by parent firms to their overseas affiliates. Table 1 shows a strong positive correlation between overseas investment and intermediate goods exports globally, including ASEAN, China, Mexico, and the United States.

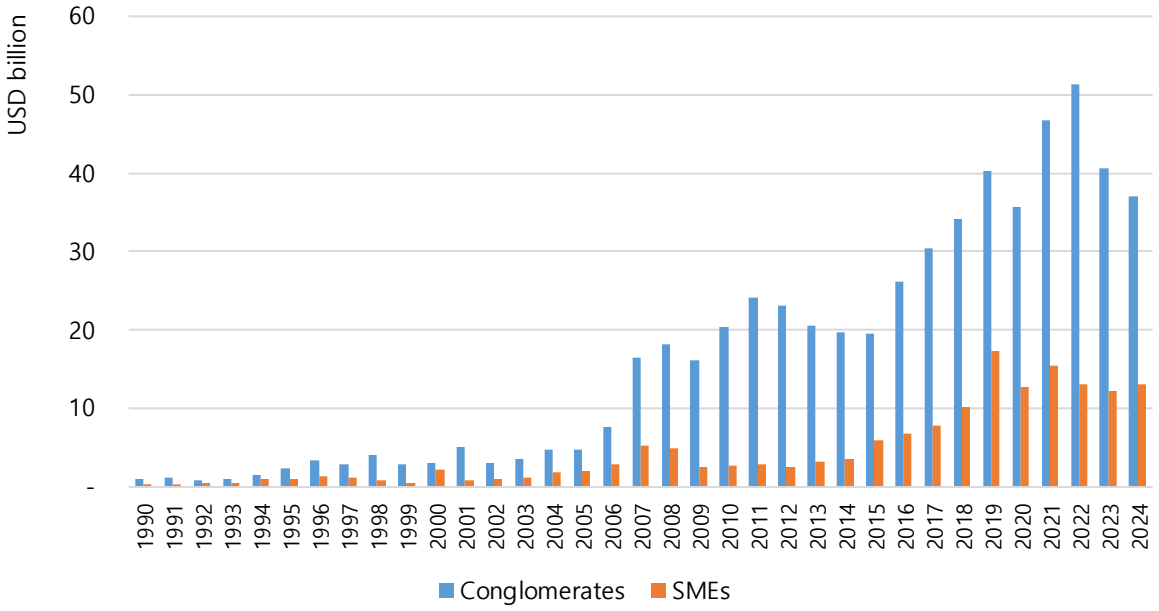
Table 1. Correlation Between South Korea's Intermediate Goods Exports and Outward FDI, 1990–2024

ASEAN	China	Mexico	United States	World
0.941	0.842	0.773	0.940	0.941

Source: Author's calculation based on data by the Export-Import Bank of Korea and the Korea International Trade Association.

As shown in Figure 6 and Table 2, manufacturing FDI is led by large South Korean firms with strong global competitiveness. These conglomerates are usually concentrated in high-tech sectors such as electronics, automobiles, and, especially, electrical equipment.[32] Given the strong correlation between FDI and intermediate goods exports, most exports from these large firms consist of intermediate goods supplied to their overseas affiliates. As overseas investment by South Korean conglomerates expands further in advanced manufacturing sectors, exports of high-tech intermediate goods are also expected to grow.

Figure 6. South Korea's Outward Foreign Direct Investment by Firm Size, 1990–2024



Source: The Export-Import Bank of Korea.

Table 2. South Korean Conglomerates' Outward Foreign Direct Investment by Manufacturing Subsector, 2020–2024 (Unit: USD Million)

Sector	2020	2021	2022	2023	2024
Electrical Equipment	2,244 (20.6%)	2,967 (20.5%)	5,237 (23.8%)	6,512 (38.4%)	5,653 (48.1%)
Motor Vehicles	1,804 (16.6%)	1,972 (13.6%)	1,941 (8.8%)	1,745 (10.3%)	1,380 (11.7%)
Electronic Components	3,186 (29.2%)	5,612 (38.7%)	8,229 (37.5%)	3,599 (21.2%)	1,089 (9.3%)
Chemicals	806 (7.4%)	494 (3.4%)	3,020 (13.7%)	986 (5.8%)	933 (7.9%)
Primary Metal	608 (5.6%)	543 (3.7%)	896 (4.1%)	1,606 (9.5%)	681 (5.8%)

Source: The Export-Import Bank of Korea.

New External Economic Development Strategy and Recommendations for Implementation

Recent changes in the global trade environment are likely to disadvantage South Korea, which has relied heavily on export-led growth. Advanced economies, including the United States, are

adopting policies to protect domestic industries and expand domestic production by attracting both domestic and foreign firms.[33] At the same time, large-scale overseas investment by South Korean firms has raised concerns domestically about declining exports and employment. South Korea must now devise a new external economic development strategy to navigate these challenges.

Given its small domestic market, South Korea must remain deeply integrated into the global economy through exports and overseas investment to achieve sustained growth. Fortunately, South Korean firms possess world-class manufacturing capabilities in advanced technologies such as semiconductors, batteries, and robotics, as well as in core manufacturing industries such as automobiles, shipbuilding, and steel. As demonstrated earlier, overseas investment by South Korean firms is closely linked to South Korea's export performance.

Building on these strengths, this paper proposes a new external economic development strategy organized around three pillars: 1) expanding exports of advanced intermediate goods linked to overseas investment by South Korean firms; 2) positioning and promoting South Korea as a global hub for research and development (R&D) in future advanced technologies; and 3) strengthening the international competitiveness of South Korean small and medium-sized enterprises (SMEs).

Expanding Exports Linked to Overseas Investment by South Korean Firms

The first pillar of this strategy is to expand exports linked to overseas investment by South Korean firms. In essence, South Korea should transition from being a primary producer of final goods to a global exporter of intermediate goods, such as materials, components, and equipment, in advanced manufacturing industries. This shift aims to ensure that both South Korean firms operating abroad and multinational corporations increasingly rely on South Korean-made intermediate goods. This approach would not only increase South Korean exports but also upgrade its export structure toward advanced industries and create high-quality jobs. The South Korean government must clearly articulate this strategic objective and provide consistent policy support.

To implement this strategy effectively, close cooperation between the government and the private sector is essential. In particular, the South Korean government must identify manufacturing sectors where South Korean firms already possess world-class production capabilities and advanced technology sectors with strong potential to become future strategic industries. Examples include semiconductors, automobiles and auto parts, electric vehicle (EV) batteries, quantum computing, AI, robotics, biotechnology, small modular reactors (SMRs), shipbuilding, defense industries, and power systems. The government should actively support these sectors as national strategic industries through targeted policy instruments, such as enhanced tax incentives for R&D and facilities, state-backed mega funds, regulatory sandboxes, and targeted immigration and retention incentives.

As noted earlier, overseas affiliates of South Korean firms constitute a stable and expanding demand base for South Korea's advanced intermediate goods. Accordingly, South Korea must make effective use of outbound FDI. Under the recent U.S.-South Korea investment agreement, the South Korean government committed to facilitating approximately USD 20 billion in annual investment in the United States over the next decade, along with a separate commitment of USD 150 billion in the U.S. shipbuilding sector.[34] The South Korean government should select investment projects that support South Korean firms already operating in the United States, as well as other firms planning future investments.

Although the current U.S. investment procedures require South Korean investments to align with sectors prioritized by the U.S. government, South Korea has a clear understanding of the manufacturing sectors the Trump administration seeks to revitalize. The South Korean government must engage in close consultations with South Korean firms and maintain active communication with the U.S. government to ensure that South Korean investments serve the mutual interests of both countries.

Furthermore, when investments are carried out under the U.S.-South Korea joint investment framework, South Korea should seek to prevent the imposition of unfavorable tariffs on South Korean exports of intermediate goods to U.S.-based investment projects. In such cases, the South Korean government should request the application of tariff rates guaranteed under the Korea-U.S. Free Trade Agreement (KORUS FTA).[35] In addition, for projects that require South Korean personnel, South Korea should request appropriate visas that allow South Korean professionals to work in the United States for a reasonable period. South Korea should maintain dialogue through the U.S.-Republic of Korea Business Travel and Visa Working Group to ensure that the United States clarifies its visa application rules and follows through on implementing the new "specialized trainers" category added to the B-1 Temporary Business Visitor visa. Although the B-1 visa is an imperfect fit for the nature of the work, the U.S. Department of State has broadened the definition of work permitted under the visa to make it easier for South Korean professionals to apply and qualify for travel and work in the United States.[36]

Geopolitical risks have recently disrupted the stable supply of key raw materials and intermediate inputs, potentially constraining South Korea's production and export of intermediate goods.[37] To address this risk, the South Korean government, in cooperation with the private sector and partner countries, has been working to reduce dependence on specific countries and diversify supply sources.[38] Going forward, South Korea should build on its complementary relationship with countries rich in critical minerals—such as the United States, Australia, and Canada—by concluding supply chain agreements that enable South Korean firms to engage in direct investment and corporate partnerships. At the same time, South Korea should systematically expand domestic efforts to secure critical minerals, including through recycling and extraction from industrial waste.[39]

South Korean firms should also actively leverage the country's extensive FTA network to stabilize supply chains for critical minerals. In addition, the South Korean government should

pursue South Korea's accession to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) at an early stage. Membership in the CPTPP would not only expand export markets for South Korean firms but also significantly help them secure stable supplies of critical minerals, materials, and components.[40] Given persistent geopolitical risks and the dysfunction of the WTO-based multilateral trading system, South Korea's accession to CPTPP would offer substantial benefits to South Korean firms. Moreover, South Korea already has bilateral FTAs with all CPTPP members except Japan and Mexico, so accession would impose limited additional burdens while reinforcing free trade principles and trade rules in the Asia-Pacific region, particularly given South Korea's status as one of the world's top trading nations.

Finally, the United States has recently announced that imports of products made with forced labor may be subject to investigations under Section 301 of the U.S. Trade Act of 1974, on the grounds that such imports disadvantage U.S. products.[41] The Uyghur Forced Labor Prevention Act (UFLPA) is already in effect, prohibiting imports of goods produced using forced labor.[42] The South Korean government should ensure South Korean firms are well aware of these developments and work with them to develop appropriate compliance measures.

Positioning South Korea as a Global R&D Hub for Advanced Technology

The second pillar of the new external economic development strategy is to position South Korea as a global R&D hub for future advanced technologies. This implies attracting world-leading researchers and firms from abroad to conduct advanced technology R&D in South Korea. A global R&D hub does not merely conduct research across multiple fields; it is a location capable of developing new technologies, manufacturing products based on those technologies, and testing their commercial viability.[43] South Korea possesses strong potential in this regard, with globally competitive firms in advanced manufacturing, a relatively large domestic market, and high consumer demand capable of supporting integrated activities ranging from technology development to commercialization.[44]

To implement this strategy, South Korea must fundamentally redefine the objectives and nature of its R&D policies. Historically, South Korea's R&D evaluation system has emphasized quantitative indicators, such as the number of academic papers or patents produced, while insufficient consideration has been given to whether research outcomes translate into competitive industrial production.[45] Going forward, the ultimate goal of R&D must be clearly defined as enhancing national capabilities to develop new technologies, manufacture products based on those technologies, and achieve the commercial viability of those products. Systems must be built to ensure a seamless transition from laboratory research to pilot testing, initial production, and eventually mass production.

Achieving this shift requires the spatial integration of advanced technology R&D and pilot manufacturing. Globally recognized R&D hubs share a common feature: research institutes and production facilities are physically proximate, enabling rapid experimentation, iteration, and learning through failure.[46] South Korea should establish R&D-manufacturing clusters in strategic industries such as batteries, AI, robotics, biotechnology, SMRs, shipbuilding, defense, and

power systems, where research, experimentation, pilot production, and mass manufacturing can occur within a single integrated ecosystem.[47]

To become a global R&D hub, South Korea must also attract leading foreign firms to establish R&D bases domestically. When deciding on R&D locations, global firms prioritize proximity to capable partners, availability of skilled talent and experimental infrastructure, and the ease of technology transfer and joint research. Accordingly, South Korea must provide credible assurances that foreign firms can engage in joint research with domestic institutions and collaborate closely with globally competitive South Korean manufacturers.[48]

South Korea's success as an advanced technology R&D hub hinges on its ability to attract and retain top-tier researchers and engineers. Competition in advanced technologies is, at its core, a battle for talent. Highly skilled researchers choose locations based on both research environments and living conditions. To attract global talent, South Korea must offer world-class standards in research autonomy, compensation, long-term visa options, and family settlement conditions.[49] It is equally important to allow researchers to move freely among universities, firms, and research institutions within South Korea. Without these conditions, South Korea's competitiveness as a global R&D hub will face inevitable limits.

More broadly, South Korea must create an open and integrated ecosystem that organically connects leading domestic and foreign firms and talents across research, technology development, manufacturing, and commercialization. This requires the government to closely integrate policies across science and technology, industry, trade, security, and international talent mobility. The government and the private sector should also consider tailored approaches to invite leading foreign firms and research institutions to South Korea, allowing them to choose between establishing independent R&D centers or joint R&D facilities with South Korean firms. ASML's decision to establish a next-generation semiconductor manufacturing R&D center in South Korea with Samsung Electronics serves as a notable example of joint R&D.[50]

Strengthening the International Competitiveness of South Korean SMEs

The third pillar is to strengthen the international capabilities of domestic SMEs. South Korean SMEs have traditionally been concentrated in labor-intensive, low-tech industries such as textiles and footwear—a pattern largely attributable to South Korea's chaebol-centered economic development strategy. Rather than undertaking high-risk FDI, SMEs have predominantly served as domestic subcontractors, supplying components to large conglomerates.

However, the recent acceleration of outward expansion by South Korean conglomerates is expected to drive a corresponding increase in SME outward investment, as suppliers follow their principal buyers abroad. Furthermore, as rising wages and land costs erode China's role as the "world's factory," labor-intensive, low-tech production is increasingly relocating to ASEAN countries and India, where labor costs and business conditions are more favorable.[51] This shift generates additional investment opportunities for South Korean SMEs, which retain accumulated production expertise and competitive advantage in these sectors. Beyond following

South Korean conglomerates abroad, SMEs are also well positioned to supply competitive core components locally to global manufacturers operating in advanced economies such as the United States and the European Union, particularly in the semiconductor and EV battery sectors.

Whereas large firms have historically led participation in global value chains, SMEs now have greater opportunities to participate through overseas investment and exports. Yet many South Korean SMEs continue to face barriers, including information gaps, financial constraints, and weak overseas networks.[52] Given the increasingly challenging global trade environment, systematic government support is essential to facilitate SME participation in global value chains.

South Korean SMEs often perceive overseas investment and exports as high-risk endeavors.[53] However, in today's environment, these activities serve strategic functions such as market development, securing resilient supply chains, and building global partnerships. SMEs must therefore reassess their perceptions of overseas activities, and the government should strengthen policy support to facilitate this shift. Institutional recognition of small-scale, phased overseas investments and enhanced support to reduce initial costs related to legal compliance, taxation, and licensing are particularly important.

Given the limitations SMEs face when entering global value chains independently, greater emphasis should be placed on joint overseas expansion with large South Korean firms. By leveraging large firms' overseas production bases, research facilities, and supply chain networks, SMEs can participate in overseas activities as partner firms or technology collaborators while reducing risk. The government should develop comprehensive support packages—including financing, guarantees, insurance, and administrative assistance—for SMEs engaging in joint overseas expansion with large firms.

Meaningful participation in global value chains also requires SMEs to compete based on technology and expertise, rather than simply on production or subcontracting. The government should support the technological upgrading of SMEs to enable their participation as independent firms with competitive capabilities in processes, core components, software, or services. This involves providing assistance in obtaining internationally recognized patents, certifications, and standards that allow SME technologies to be commercially utilized through overseas investment and exports.

Another major challenge for SMEs is the lack of information about overseas markets and partners. The government should support SMEs in accessing information on local demand, regulatory environments, and potential partners through embassies, trade associations, and KOTRA.[54] Establishing networking platforms that link SMEs with South Korean firms and experts operating abroad would further reduce trial-and-error costs during market entry.

Finally, successful participation in global value chains requires SMEs to develop global organizational capabilities. Without personnel with overseas business experience and organizational capacity for global operations, sustained success is difficult. The government should therefore provide structured education and training programs for SME employees.

These training programs should cover macro-level changes in the global trade environment, geopolitical risks, the AI-driven technological transition, and supply-chain disruptions. Training programs should focus on providing practical knowledge related to overseas markets, international contracts, negotiations, and local management. Such support should be viewed as a form of public investment in strengthening the international competitiveness of South Korean SMEs.

Taken together, the three pillars proposed in this paper constitute a coherent and mutually reinforcing external economic development strategy tailored to the realities of a more protectionist and geopolitically fragmented global economy. By advancing these three pillars in an integrated and consistent manner, South Korea can transform the current external challenges into an opportunity to upgrade its growth model from an export-led economy centered on final goods produced domestically by large firms to a globally embedded innovation hub in which advanced intermediate goods, frontier technologies, and competitive SMEs collectively sustain long-term prosperity.

Endnotes

1 This line of logic and rationale is meticulously described in Robert Lighthizer, *No Trade Is Free: Changing Course, Taking on China, and Helping America's Workers* (Broadside Books, 2023). The first and second Trump administrations share some similarities but also differ in many respects. For instance, the first administration was heavily centered on China, whereas the second administration is broader in geographic scope targeting both China and key U.S. allies and partners. Furthermore, if the first administration focused on tariffs on specific imported goods or industries, the second employs a more expansive tariff program, including reciprocal and baseline tariffs. For more on the differences between the trade policies of the first and second Trump administrations, see Chad Bown, "Chad P. Bown on the Difference between Trump 1.0 and 2.0 Trade Policy," presentation video at the PIIE Global Economic Prospects, April 15, 2025, https://www.piie.com/newsroom/short-videos/2025/chad-p-bown-difference-between-trump-10-and-20-trade-policy.

2 Josh Boak, "Trump Announces Sweeping New Tariffs to Promote US Manufacturing, Risking Inflation and Trade Wars," Associated Press, April 3, 2025, https://apnews.com/article/trump-tariffs-liberation-day-2a031b3c16120a5672a6ddd01da09933.

3 Inu Manak, "Tracking Trump's Trade Deals," Council on Foreign Relations, March 17, 2026, https://www.cfr.org/articles/tracking-trumps-trade-deals.

4 The White House, "Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung," November 13, 2025, https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/.

5 Sunhyung Lee, "The Trump Administration's Next Trade Moves After IEEPA Ruling," Korea Economic Institute of America, February 27, 2026, https://keia.org/the-peninsula/the-trump-administrations-next-trade-moves-after-ieepa-ruling/.

6 Zdenek Drabek, "Is the WTO Terminally Ill? Threats to the International Trading System," *Asia and the Global Economy* 4, no. 1 (2024): 1–19.

7 For more on how other countries reacted to Trump's unilateral tariffs, see Christopher Shim and Will Merrow, "Here's How Countries Are Retaliating Against Trump's Tariffs," Council on Foreign Relations, March 21, 2025, https://www.cfr.org/articles/heres-how-countries-are-retaliating-against-trumps-tariffs; "EU to suspend 93 billion euro retaliatory trade package against US for 6 months," Reuters, January 23, 2026, https://www.reuters.com/business/eu-suspend-93-billion-euro-retaliatory-trade-package-against-us-6-months-2026-01-23/.

8 Soojung Cho, "Korea's Trade Policy Beyond Free Trade Agreements," *Journal of World Trade* 58, no. 2 (2024): 273–294.

9 Je-u Chae, "Korean Economy Faces Triple Threat in 2026," *Chosun Ilbo*, November 1, 2025, https://www.chosun.com/english/market-money-en/2025/10/30/JJF7NHLMAREJ3IRWO5S54M7WAI/.

[10] S. Lael Brainard, "An Empirical Assessment of the Proximity-Concentration Trade-off between Multinational Sales and Trade," *American Economic Review* 87, no. 4 (1997): 520–44; Bruce A. Blonigen, "In Search of Substitution between Foreign Production and Exports," *Journal of International Economics* 53, no. 1 (2001): 81-104; Elhanan Helpman et al., "Export versus FDI with Heterogeneous Firms," *American Economic Review* 94, no. 1 (2004): 300–16.

[11] Lionel Fontagné, *Foreign Direct Investment and International Trade: Complements or Substitutes?* OECD STI Working Papers (1999/3) (1999); Valeriano Martínez, et. al., "Foreign Direct Investment and Trade: Complements or Substitutes? Empirical Evidence for the European Union," *Technology and Investment* 3, no. 2 (2012): 105–12; Jean-Charles Bricongne et al., "The Proximity-Concentration Trade-Off with Multi-Product Firms: Are Exports and FDI Complements or Substitutes?" *The World Economy* 46, no. 5 (2023): 1264–89.

[12] Mihir A. Desai et al., "Domestic Effects of the Foreign Activities of US Multinationals," *American Economic Journal: Economic Policy* 1, no. 1 (2009): 181–203.

[13] Ann Harrison and Margaret McMillan, "Offshoring Jobs? Multinationals and US Manufacturing Employment," *Review of Economics and Statistics* 93, no. 3 (2011): 857–75.

[14] Dani Rodrik, "Premature Deindustrialization," *Journal of Economic Growth* 21 (2016): 1–33; Hyunbae Chun et. al., "Hollowing Out or Filling in? The Effects of Multinational Enterprises on Domestic Plant Turnover and Job Growth in Factory Asia," *Korean Economic Review* 36 (2020): 285–317.

[15] Organization for Economic Cooperation and Development, *Interconnected Economies: Benefiting from Global Value Chains* (2013).

[16] World Bank, "World Development Indicators," accessed May 20, 2026, https://databank.worldbank.org/source/world-development-indicators.

[17] Nathan Lane, "Manufacturing Revolutions: Industrial Policy and Industrialization in South Korea," *The Quarterly Journal of Economics* 140, no. 3 (2025): 1683–1741.

[18] World Bank, "World Development Indicators," accessed May 20, 2026, https://databank.worldbank.org/source/world-development-indicators; World Trade Organization, "World Trade Statistics," last updated March 19, 2025, https://www.wto.org/english/res_e/statis_e/world_trade_statistics_e.htm.

[19] Ministry of Trade and Industry of the Republic of Korea, "체결현황 [Current FTA Conclusion Status]," last updated April 2026, https://fta.motir.go.kr/ftamain/kfta/ov/; Lowy Institute Asia Power Index, "Global FTAs: Bilateral and Multilateral Free Trade Agreements Concluded by Index Countries with Other Countries (2024)," https://power.lowyinstitute.org/data/economic-relationships/economic-diplomacy/global-ftas/.

[20] According to KITA K-stat data, two of the largest intermediate export items in 1990 were semiconductors and woven fabrics. By 2025, semiconductors still accounted for the largest share of total intermediate exports, followed by petroleum products. KITA K-stat, "국내통계 [National Statistics]," accessed May 20, 2026, https://stat.kita.net/stat/kts/sum/SumImpExpTotalList.screen?utm_source=kita.net&utm_medium=kita&utm_campaign=service_local&utm_content=banner_gnb.

[21] Hongsuk Kim, "Toward Adjusting Korea's FDI Strategies in China," *KIET Industrial Economic Review* (1997): 18–20, https://www.kiet.re.kr/en/pub/ecoreviewDetailView?detail_no=71.

[22] According to KITA K-stat, intermediate goods exports to China reached a record high of USD 130.2 billion in 2022. By 2024, the share of intermediate goods in South Korea's total exports to China surged to an all-time peak of 85.9 percent. Regarding the trade balance, the surplus with China surpassed the USD 10 billion threshold in 2003 and subsequently culminated in a historical maximum of USD 62.8 billion in 2013. KITA K-stat, "가공단계 수출입 [Export and Import by Processing Stage]," accessed May 20, 2026, https://stat.kita.net/stat/kts/use/BecList.screen.

[23] "Korean Businesses Venture into ASEAN in Search of New Opportunities," *The Korea Herald*, October 15, 2018, https://www.koreaherald.com/article/1808382.

[24] John Towfighi, "South Korea Is Going Big on American Manufacturing: The Battery Belt Could Benefit the Most," *Business Insider*, September 23, 2024, https://www.businessinsider.com/south-korea-companies-jobs-manufacturing-evs-chips-batteries-2024-9.

[25] Anna J. Park and Hyun-woo Nam, "Seoul and Washington Agree on Details of Tariff Deal," *The Korea Times*, October 29, 2025, https://www.koreatimes.co.kr/foreignaffairs/20251029/seoul-and-washington-agree-on-details-of-tariff-deal; Tong-Hyung Kim, "South Korean Lawmakers Pass Law to Manage Seoul's Pledge of $350 Billion in US Investments," Associated Press, March 12, 2026, https://apnews.com/article/south-korea-us-investments-tariffs-3bf0f709d9066d62b1b8f6e36e48638e.

[26] According to the Korea EXIM Bank, in 1990, outward FDI (OFDI) in the food, apparel, and textiles sectors totaled USD 141 million, accounting for approximately 24 percent of the aggregate manufacturing OFDI. Korea EXIM Bank, "해외직접투자통계 [Foreign Direct Investment Statistics]," accessed May 20, 2026, https://stats.koreaexim.go.kr/sub/detailedCondition.do.

[27] According to the Korea EXIM Bank, in 2001, OFDI in the electronics-related sectors totaled USD 3.2 billion, accounting for nearly 74 percent of the total manufacturing OFDI. The chemicals sector's share reached 21.6 percent in 2010–the highest in twenty years–while the automotive sector's share reached 21.8 percent in 2018. In 2023 and 2024, OFDI in the electrical equipment sector totaled USD 6.7 billion and USD 5.9 billion, respectively, marking the highest levels in history. Korea EXIM Bank, "해외직접투자통계 [Foreign Direct Investment Statistics]," accessed May 20, 2026, https://stats.koreaexim.go.kr/sub/detailedCondition.do.

[28] According to the Korea EXIM Bank, investment in the automotive industry toward the United States in 1990 amounted to USD 85 million, representing 44.4 percent of South Korea's total investment in U.S. manufacturing sector. By 2000, the combined investment in the chemicals and electronic components sectors—including computers and telecommunications equipment—reached USD 340 million, accounting for approximately 60 percent of the total investment directed to the U.S. manufacturing sector. Korea EXIM Bank, "해외직접투자통계 [Foreign Direct Investment Statistics]," accessed May 20, 2026, https://stats.koreaexim.go.kr/sub/detailedCondition.do.

[29] According to the Korea EXIM Bank, investment in the electronic components industry toward China in 2010 amounted to USD 1.4 billion, representing 48.6 percent of South Korea's total manufacturing investment in the country. By 2020, investment in this sector reached USD 2.1 billion, accounting for 46 percent of South Korea's total investment directed to China's manufacturing industry. Although the investment scale for this industry declined to USD 761 million in 2024, its share of total investment in China's manufacturing industry remained significant at 45.2 percent, continuing to overwhelm other industrial sectors. Korea EXIM Bank, "해외직접투자통계 [Foreign Direct Investment Statistics]," accessed May 20, 2026, https://stats.koreaexim.go.kr/sub/detailedCondition.do.

[30] According to the Korea EXIM Bank, in 2000, investment in the electronics-related industry in ASEAN countries accounted for more than 30 percent of South Korea's total investment in the region's manufacturing sector. By 2024, investment in the electronics and electrical equipment industries surpassed USD 1 billion, representing 34.8 percent of the aggregate investment in ASEAN's manufacturing sector. Meanwhile, in 2015, investment in the automotive industry in Mexico exceeded USD 790 million, representing 87.4 percent of South Korea's total investment in the country's manufacturing industry. By 2024, although the investment scale declined to USD 400 million, it still accounted for a substantial 61.5 percent of the aggregate manufacturing investment in Mexico. Korea EXIM Bank, "해외직접투자통계 [Foreign Direct Investment Statistics]," accessed May 20, 2026, https://stats.koreaexim.go.kr/sub/detailedCondition.do. Given that the majority of goods produced by South Korean subsidiaries in Mexico are destined for the U.S. market, South Korean firms have expressed significant concern regarding the Trump administration's recent pressure to increase tariffs on Mexican-origin imports. Ashley Song, "Korean Firms in Mexico Brace for Continued Uncertainty Despite U.S. Tariff Delay," *Korea Bizwire*, February 4, 2025, http://koreabizwire.com/korean-firms-in-mexico-brace-for-continued-uncertainty-despite-u-s-tariff-delay/305535#google_vignette.

[31] According to KITA K-stat, South Korea's trade surplus with China, which stood at USD 4.8 billion in 1999, saw a substantial increase, peaking at USD 62.8 billion in 2013. Subsequently, this surplus contracted to USD 1.2 billion by 2022, before shifting into a trade deficit of USD 18 billion in 2023—marking the first such deficit since 1992. In contrast, South Korea's trade surplus with the United States, which was a mere USD 2.4 billion in 1998, rose to USD 25.8 billion in 2015 and reached a historical high of USD 55.6 billion in 2024. KITA K-stat, "국가 수출입 [Export and Import by Country]," accessed May 20, 2026, https://stat.kita.net/stat/kts/ctr/CtrTotalImpExpList.screen.

[32] South Korean SMEs have traditionally been concentrated in labor-intensive, low-tech industries; therefore, they were unable to undertake high-risk foreign direct investment until recently.

[33] International Monetary Fund, *World Economic Outlook: War Sets Back the Global Recovery* (April 2022).

[34] Ju-min Park and Kanishka Singh, "US, South Korea Unveil Details on Shipbuilding Investment and Sub in Trade Deal," Reuters, November 14, 2025, https://www.reuters.com/world/asia-pacific/us-south-korea-release-details-deal-including-korean-investment-shipbuilding-2025-11-14/.

[35] Under KORUS FTA, nearly all bilateral trade in consumer and industrial products has become duty-free ten years after the agreement came into force. U.S. Department of State, "South Korea Free Trade Agreement," accessed May 20, 2025, https://2017-2021.state.gov/trade-agreements/south-korea-free-trade-agreement/.

[36] Ryan Mosser, "B-1 Visa Updates: New Specialized Trainers Category for Foreign Nationals," Ogletree Deakins, March 4, 2026, https://ogletree.com/insights-resources/blog-posts/b-1-visa-updates-new-specialized-trainers-category-for-foreign-nationals/.

[37] James Bowen, "The Raw Materials of Economic Security: South Korea's Evolving Energy and Critical Minerals Policies in an Era of Disruption," *Korea Policy* 1, no. 3 (2024): 108–131.

[38] In 2024, South Korea was elected as the inaugural chair of the Crisis Response Network under the Indo-Pacific Economic Framework for Prosperity, indicating that South Korea's experience and policy know-how in supply chain emergency response were highly appraised. South Korean Ministry of Trade, Industry and Energy, "Korea Elected as Inaugural Chair of IPEF Crisis Response Network," July 30, 2024, https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=7523&type=O.

[39] International Energy Agency, *Recycling of Critical Minerals: Strategies to Scale Up Recycling and Urban Mining* (December 2025).

[40] Cecilia Malmström and Han-koo Yeo, "The European Union and South Korea Should Join the Transpacific Trade Pact," *Peterson Institute for International Economics*, May 20, 2025, https://www.piie.com/blogs/realtime-economics/2025/european-union-and-south-korea-should-join-transpacific-trade-pact.

[41] Office of the United States Trade Representative, "USTR Initiates 60 Section 301 Investigations Relating to Failures to Take Action on Forced Labor," March 12, 2026, https://ustr.gov/about/policy-offices/press-office/press-releases/2026/march/ustr-initiates-60-section-301-investigations-relating-failures-take-action-forced-labor.

[42] United States Congress, "An Act to Ensure that Goods Made with Forced Labor in the Xinjiang Uyghur Autonomous Region of the People's Republic of China Do Not Enter the United States," *Public Law* 117-78, 117th Congress (2021–2022).

[43] Giorgia Ponti and Raffaele Trapasso, "Regional Impact of Public R&D Organisations: Insights and International Comparisons for Innovation Diffusion in the United Kingdom," *OECD SME and Entrepreneurship Papers* (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/regional-impact-of-public-r-d-organisations_3a4d4c0a/587d7e6c-en.pdf.

[44] South Korea 2025: Shifts and Explorations (Ipsos Flair Collection, December 2024), https://www.ipsos.com/sites/default/files/ct/publication/documents/2025-04/ipsos-flair-south-korea-2025-en.pdf.

[45] Organisation for Economic Cooperation and Development, *Industry and Technology Policies in Korea*, (2014), https://www.oecd.org/content/dam/oecd/en/publications/reports/2014/05/industry-and-technology-policies-in-korea_g1g423d8/9789264213227-en.pdf.

[46] Cameron Davis et al., "Building Innovation Ecosystems: Accelerating Tech Hub Growth," McKinsey & Company, February 28, 2023, https://www.mckinsey.com/industries/public-sector/our-insights/building-innovation-ecosystems-accelerating-tech-hub-growth.

[47] Under the South Korean government's Strategy to Foster the National High-Tech Industry, the world's largest cluster for advanced logic semiconductor manufacturing and R&D will be constructed in Gyeonggi Province by 2042. Korea Trade-Investment Promotion Agency, "Strategy to Foster the National High-Tech Industry," accessed May 20, 2026, https://www.investkorea.org/ik-en/cntnts/i-3010/web.do.

[48] For instance, Luxembourg leverages fiscal sector synergies, tax incentives, and open migration policies to attract AI talent, building on its NVIDIA partnership to position itself as Europe's AI research hub. Luxembourg Government, "Luxembourg to Be the First European Country to Create an Artificial Intelligence (AI) Partnership with NVIDIA," January 30, 2019, https://gouvernement.lu/en/actualites/toutes_actualites/communiques/2019/01-janvier/30-bettel-partenariat-nvidia.html.

[49] Sari Pekkala Kerr et al., "Global Talent Flows," World Bank Group Policy Research Working Paper 7582, October 17, 2016, https://openknowledge.worldbank.org/entities/publication/9857bef7-6d40-5d14-a5ce-c194e58d35fe.

[50] Dong-hwan Ko, "Samsung, ASML to Invest W1 Trillion to Build Research Fab in Korea," December 13, 2023, *The Korea Times*, https://www.koreatimes.co.kr/business/companies/20231213/samsung-asml-to-invest-w1-trillion-to-build-research-fab-in-korea.

[51] Joe Cash, "Western Firms Shift Investment from China to India as Worries Mount," Reuters, September 13, 2023, https://www.reuters.com/markets/western-firms-shift-investment-china-india-worries-mount-2023-09-13/; ASEAN Secretariat and United Nations Trade and Development, *ASEAN Investment Report 2025: Foreign Direct Investment and Supply Chain Development* (October 2025), https://asean.org/wp-content/uploads/2025/10/AIR2025_rev17-Okt.pdf.

[52] Sang-uk Jung and Jia-qi Tian, "Strategic SME Responses to Non-Tariff Barriers: Korean Adaptation to the US MoCRA and FSVP," *Global Trade and Customs Journal* 21, no. 3/4 (2026): 234–243.

[53] "SMEs Seeking Overseas Expansion amid Difficulties at Home: Poll," *The Korea Herald*, April 22, 2018, https://www.koreaherald.com/article/1652336.

[54] For instance, KOTRA offers AI-based information services—"Intelligent Trade and Investment Platform"—and big-data platforms like TriBIG and BuyKOREA, which allow SMEs to search for target-market entry strategies, promising overseas partners, and real-time trade-data-driven insights. See Korea Trade-Investment Promotion Agency, "KOTRA Expands Export Opportunities for SMEs and Mid-Sized Companies with AI," August 22, 2025, https://www.investkorea.org/ik-en/bbs/i-5074/detail.do?ntt_sn=491434.

Rethinking the U.S.-South Korea 123 Agreement in a New Strategic Era

By Kayla T. Orta

On November 25, 2015, the United States and South Korea's joint civil nuclear technology agreement, also known as the "Section 123 Agreement," entered into force, establishing a twenty-year framework for the two nations' bilateral cooperation.[1] A decade later, geopolitical shifts in the global civil nuclear market, alongside changing regional security dynamics, are driving a careful reconsideration—and potential expansion—of the current structure of the U.S.-South Korea nuclear technology partnership.

Both Washington and Seoul have long emphasized the importance of the bilateral partnership on peaceful-use nuclear technologies. What makes this a critical moment for the U.S.-South Korea nuclear partnership is that recent discussions have increasingly commingled civil nuclear cooperation with hitherto unexplored nuclear technology for security and defense applications. In October 2025, U.S. President Donald Trump traveled to South Korea for his first state visit since his reelection and second diplomatic summit with South Korean President Lee Jae Myung on the sidelines of the Asia-Pacific Economic Cooperation (APEC) leaders' summit. While the Trump-Lee summit focused on bilateral trade, economic security, and technology-focused partnerships, Trump's post-summit announcement on October 29 granting his approval for South Korea to build nuclear-powered submarines (SSNs) took many foreign policy and military analysts by surprise.[2] South Korea has long argued for the benefit of SSNs in its force posture against North Korea's rising nuclear weapons and missiles programs. Over the years, Washington has been hesitant and, at times, largely skeptical of South Korea's intentions, due to potential regional nuclear proliferation implications.[3]

The post-summit Trump-Lee Joint Fact Sheet, announced in November 2025, also seemed to open the door to renewed bilateral discussion on "the ROK's civil uranium enrichment and spent fuel reprocessing for peaceful uses," in accordance with preexisting agreements and legal guidelines.[4] From Seoul's perspective, the Trump administration's willingness to include civil uranium enrichment and reprocessing (ENR) technologies in last year's Joint Fact Sheet indicates a shift in U.S. policy thinking, potentially signaling that the time is right for South Korea to expand its domestic nuclear technology capabilities.[5] Readying to meet at the negotiation table, the Lee administration speedily assembled an intra-government team to explore greater flexibility for South Korean civil-use nuclear activities.[6]

Kayla T. Orta is Nonresident Fellow at the Atlantic Council's Indo-Pacific Security Initiative. She also holds concurrent nonresident fellowships at George Washington University's Institute for Korean Studies (GWIKS) and the University of Vienna's European Centre for North Korean Studies (ECNK).

From Washington, however, the policy response has been less enthusiastic. Hesitancy among U.S. policymakers to change long-standing positions on high-risk proliferation technologies signals that, though renegotiation talks may occur, the outcomes for U.S.-South Korea civil nuclear relations remain uncertain.[7] Overall, South Korea's bid to expand nuclear fuel cycle technologies, alongside the potential for South Korean-built SSNs in the Indo-Pacific region, calls for deeper consideration of the historical foundations and future-oriented pathways of the U.S.-South Korean bilateral nuclear partnership. As Washington and Seoul explore options to restart nuclear-focused discussions, this paper explores the key drivers of nuclear cooperation—from within and outside of the U.S.-South Korea bilateral partnership—reviews the history of today's ongoing debate, and stresses near-term political and industry-driven opportunities for both nations.

Historical Legacy: U.S.-South Korea Civil Nuclear Cooperation

Under what circumstances did the United States and South Korea first establish bilateral civil nuclear relations? And how has the partnership grown to be a pivotal discussion point in the U.S.-South Korea diplomatic and security relationship? In order to explore future pathways for U.S.-South Korea nuclear cooperation, it is important to first understand the historical context of the over seventy-year-old partnership.[8] U.S.-South Korea civil nuclear cooperation dates back to the post-Korean War (1950-1953) period, when South Korea was seeking secure and reliable energy sources to reconstruct its national economy. Under President Dwight Eisenhower's "Atoms for Peace" initiative, the United States and South Korea signed a joint Agreement on Cooperation Concerning Civil Uses of Atomic Energy in 1956, which effectively launched their long-term relationship on the peaceful development of nuclear energy.[9]

Building on this bilateral cooperation, South Korea institutionalized its national commitment to international nonproliferation norms by joining the International Atomic Energy Agency (IAEA) in August 1957. Within South Korea's domestic legal system, the passage of the 1958 Atomic Energy Act and the establishment of the Office of Atomic Energy in 1959 laid the groundwork for a national nuclear governance structure.[10] Within three years of establishing regulatory frameworks, South Korea, aided and guided by U.S. technical expertise, constructed its first research reactor, KRR-1, which reached criticality in 1962.[11] This technical achievement marked South Korea's official entry into the technical field of atomic energy research and development (R&D).

By the late 1960s, South Korea's rising energy demand and regional security pressures prompted further cooperation with the United States and, by extension, the IAEA. In 1967, the United States, South Korea, and the IAEA concluded an additional safeguards agreement, facilitating the successful construction of South Korea's second research reactor (KRR-2) and marking the nation's first implementation of international nuclear safeguards.[12] These early cooperative projects not only assisted the early expansion of South Korea's civilian nuclear R&D capacity but also reinforced IAEA-led nonproliferation and safeguards norms as a central pillar of the U.S.-South Korean bilateral partnership.

In the following decades, the United States and South Korea continued to expand their bilateral civil nuclear cooperation. In the 1970s, however, new geopolitical tensions briefly threatened to derail South Korea's focus on peaceful applications of nuclear technology.[13] Concerns over North Korea's rising security threat and the potential removal of U.S. troops from the Korean Peninsula led then President Park Chung-hee to explore possible avenues for developing an indigenous nuclear weapons program. Seoul's attempts to acquire sensitive nuclear technologies from foreign suppliers raised significant concerns in Washington. In response, the United States leveraged the continuation of U.S.-South Korea technical cooperation as a means to ensure South Korea's reaffirmation of its commitment to peaceful nuclear development.[14] As a result, both nations signed a revised bilateral "123 Agreement" in 1974, and South Korea reinforced its nonproliferation commitments by joining the Nuclear Non-Proliferation Treaty (NPT) in 1975. These actions marked a decisive turning point, firmly anchoring South Korea within the global nonproliferation regime.

Following its accession to the NPT, South Korea undertook additional steps to demonstrate its strong commitment to nuclear safety, security, and nonproliferation transparency, including ratifying the Convention on the Physical Protection of Nuclear Material (1982), signing the Comprehensive Nuclear-Test-Ban Treaty (1999), and adopting the IAEA Additional Protocol in 1999 (ratified in 2004).[15] Furthermore, beginning in the 1970s, the South Korean government implemented a State System of Accounting for and Control of Nuclear Materials (SSAC), in line with IAEA requirements. Institutional developments followed, including the establishment of the Technology Center for Nuclear Control (TCNC) in 1994 and its successor, the Korea Institute of Nuclear Nonproliferation and Control (KINAC) in 2006, which enhanced the independence and effectiveness of safeguards implementation. Collectively, South Korea's international agreements and national-level systems for regulation and accountability reinforced international confidence in South Korea's adherence to peaceful-use nuclear practices.[16]

Over time, U.S.-South Korea nuclear cooperation has evolved beyond one-way technical assistance into a mature partnership characterized by both collaboration and competition in global nuclear markets. Rising rapidly through the ranks, South Korea now stands as the fifth-largest civil nuclear energy producer in the world—only outpaced by the United States, China, France, and Russia.[17] Today, South Korea's state-owned companies, including Korea Electric Power Corporation (KEPCO) and Korea Hydro & Nuclear Power (KHNP), operate twenty-six reactors in-country, accounting for nearly 30 percent of the nation's energy mix.[18] The nation's R&D institutions, such as the Korea Atomic Energy Research Institute (KAERI), alongside private industry leaders, including Doosan Enerbility, Hyundai Engineering and Construction (E&C), and Samsung C&T, are driving the next generation of advanced nuclear reactor technologies at home and abroad.

As a whole, the historical trajectory of U.S.-South Korea nuclear cooperation was founded upon and has benefited from the dynamic interplay of diplomatic engagement, industry-to-industry relations, and, crucially, shared civil nuclear technical and industrial know-how. Emerging from postwar reconstruction to become a globally recognized leader, South Korea's civil nuclear

program has been deeply shaped by its sustained U.S. partnership. Amid this growth, the bilateral Section 123 Agreement, most recently revised in 2015, has served as a pivotal guiding line for U.S.-South Korean civil nuclear cooperation, underscoring shared commitments to advancing peaceful-use nuclear technology in accordance with safety, security, and nonproliferation standards.

Nuclear Agendas: U.S. and South Korean Policies

For both Washington and Seoul, nuclear energy policy is gaining momentum. Under the second Trump administration, the United States aims to quadruple its domestic nuclear energy capacity to 400 gigawatts electric (GWe) by 2050.[19] Since returning to the White House, Trump has launched a reinvigoration of the U.S. nuclear industry through a series of executive orders calling on the U.S. government to "accelerate the secure and responsible development, demonstration, deployment, and export of United States designed advanced nuclear technologies."[20] At present, the United States operates ninety-four commercial reactors across twenty-eight states, amounting to a net generating capacity of 97 GWe.[21] Domestically, the U.S. government has enacted policies to upscale innovation for existing reactors and provide both financial and regulatory support for building new reactors and diversifying fuel supply chains.[22] Beyond this, the Trump administration aims to expand U.S. commercial relevance in the global market, proposing a goal of "at least 20 new 123 Agreements" with partner countries by early 2029.[23]

Despite temporary rollbacks, South Korea's nuclear energy policy is also undergoing sustained revitalization, with reactors under construction at home and abroad.[24] The country operates twenty-six reactors, with another three large-scale APR-1400 reactors under construction.[25] On February 21, 2025, the South Korean National Assembly approved South Korea's Eleventh Basic Plan for Electricity Supply and Demand, which includes plans for the construction of at least two traditional large-scale reactors—with a combined electricity production of 2.8 GWe—and a first-of-a-kind 700 megawatt (MW) small modular reactor (SMR) by the late 2030s.[26] South Korea's nuclear industry—often referred to as "Team Korea"—comprises leading research institutions and private engineering and manufacturing firms, representing over seventy years of technical expertise.[27] Beyond the Korean Peninsula, South Korea is leveraging this strong industrial base to actively expand its nuclear export opportunities. After completing construction of four APR-1400 reactors at the Barakah nuclear power plant in the United Arab Emirates, South Korea's more recent success in securing a nuclear export project to the Czech Republic reflects its growing role in global nuclear energy deployment.[28]

Geopolitical Trends and Global Nuclear Energy Markets

Rising global energy demand—driven in part by the development of energy-intensive technologies such as AI—is accelerating advancements in civil nuclear technologies and driving newcomer nations to politically and financially invest in partnerships with leading nuclear exporters, including the United States and South Korea.[29]

Around the world, the nuclear energy sector is experiencing renewed momentum, marked by increased political support for and rising investments in traditional large-scale nuclear reactors and next-generation technologies, including SMRs and advanced modular reactors (AMRs).[30] Estimates from the U.S. Department of Commerce project that the global market for new reactors could reach USD 500–740 billion by 2030.[31] Longer-term projections from the IAEA forecast that global nuclear capacity could expand to upwards of 992 GWe by mid-century—roughly a 2.6-fold increase over 2024 global capacity levels.[32] As the global nuclear energy market evolves, Washington and Seoul are well positioned to leverage their advanced civil nuclear industries, established regulatory frameworks, and decades of operational expertise to capture emerging opportunities.

Several key geopolitical trends are shaping this evolving nuclear landscape. First, the global nuclear landscape is expanding as more countries pursue civil nuclear programs. Interest spans both emerging and established economies, with nuclear power viewed as a viable solution to meet rising energy demands and advance decarbonization goals. Following the United Nations Climate Change Conference (COP28), over thirty nations have declared their intentions to triple nuclear energy capacity by 2050.[33] Similarly, the World Nuclear Association reports that over thirty nuclear newcomer countries are currently considering, planning, or initiating nuclear energy projects.[34]

Second, the geographic center of gravity for nuclear energy development is shifting toward the Indo-Pacific region. While historically led by the United States, Canada, and Europe, future large-scale and SMR reactor construction projects are concentrated in Asia. With nearly forty reactors under construction, China aims to reach 110 GWe of nuclear capacity by 2030, while India has announced at least seven new reactor projects for the same period.[35] Russia's state-owned Rosatom claims to be constructing forty-eight nuclear-related facilities, including multiple export projects across six countries.[36] This regional concentration reflects broader trends in economic growth and energy demand, underscoring the strategic importance of the Indo-Pacific in shaping the global nuclear energy landscape.

Third, the global nuclear market is becoming more competitive, with major suppliers seeking to secure export contracts, shape regulatory norms, and expand geopolitical influence. Chinese and Russian state-backed firms have captured significant market shares through large-scale domestic deployment and can offer competitive financing for nuclear export projects.[37] Against this backdrop, the United States and South Korea—both as collaborative partners and, at times, as competitors—are leveraging advanced technologies, trusted regulatory standards, and industrial capacity to offer credible alternatives. Coordinated U.S.-South Korean engagement presents a critical opportunity to expand their presence in global markets while reinforcing high standards for nuclear safety, security, and nonproliferation.[38]

Finally, technical innovation and design diversification are reshaping the nuclear sector. AMRs and SMRs offer the potential for greater flexibility, lower upfront costs, and enhanced safety features compared to traditional large-scale reactors.[39] As a result, a growing number of

countries are advancing civil nuclear technologies, driving increased global investment and a growing pipeline of first-of-a-kind projects scheduled for the coming decades.

Together, these global trends point to a dynamic—and, increasingly, competitive—nuclear energy market, with significant implications for international cooperation and technological leadership. For the United States and South Korea, these changes present time-sensitive opportunities to advance domestic industries and expand participation in third-country nuclear projects.

Repeating Cycles: The U.S.-South Korea Renegotiation Debate

The U.S.-South Korean 123 Agreement, revised in 2015, established pathways to capitalize on such opportunities. To address long-standing and future challenges in the partnership, the reciprocal agreement laid the crucial legal basis for more substantial, interdependent nuclear industry cooperation.[40] As is common in diplomatic negotiations, however, the resulting agreement encapsulated both collaborative successes and structural weaknesses. To some extent, the outcomes of previous negotiations were designed to push difficult issues down the road for future discussions. Unfortunately, over ten years later, the road is looking much the same as before. Now past the midpoint of the agreement—initially set to run until November 25, 2035, with an additional five-year extension clause—there is a growing sense of urgency in South Korea that the U.S.-South Korean cooperation framework is not reaching its intended goals.[41] Because of this, the United States and South Korea are once again discussing avenues to "advance nuclear cooperation initiatives," and, if agreed upon, expanded options for the 123 Agreement.[42]

The restart of U.S.-South Korean bilateral nuclear discussions is, in many ways, an echo of past challenges. These issues date back to the initial five-year-long renegotiations in the 2010s, which resulted in the current 123 Agreement. Previously, U.S. and South Korean negotiators, ahead of the 1974 agreement's March 2014 expiration, began consultations on its renewal in October 2010. Both sides felt the importance of the renegotiation, as the two nations aimed to redefine the nuclear partnership from one historically rooted in South Korea's dependence on U.S. technology to a more balanced partnership that acknowledged South Korea's rising global status as a mature civil nuclear energy producer. As then chief negotiator Robert J. Einhorn stated, both sides wanted a "successor agreement that will expand the level of cooperation… in the civil nuclear energy area and that will reflect the increased importance that the Republic of Korea is playing in the global nuclear energy arena."[43]

Reportedly, the main challenges of the negotiations centered around sensitive technologies that could lead to the production of fissile material for nuclear weapons. South Korea expressed a desire to expand its civil nuclear fuel cycle—including both uranium enrichment and spent fuel reprocessing capabilities—seeking advance approval from Washington to proceed.[44] From South Korea's perspective, these technologies would provide much-needed solutions for its advancing national nuclear energy program by removing dependence on enriched uranium imports, offsetting limited spent-fuel storage capacity, and enhancing the competitiveness of the nation's nuclear export bid. Furthermore, South Korea argued that the U.S.-Japan 123

Agreement, which includes a provision for comprehensive, "long-term consent" for Japanese reprocessing technologies, set an unfair precedent for which U.S. allies were allowed to pursue back-end fuel cycle technologies—an argument that continues to be made today.[45]

Washington, however, raised concerns over regional example-setting for these higher-risk proliferation technologies.[46] Especially in the case of the Korean Peninsula, U.S. policymakers feared that if South Korea pursued ENR technologies, it would effectively dissolve the 1992 Joint Declaration on the Denuclearization of the Korean Peninsula, which stated that neither North Korea nor South Korea would possess "nuclear reprocessing and uranium enrichment facilities."[47] Clearly, North Korea—utilizing ENR capabilities for its nuclear weapons program—had repeatedly violated the agreement; however, the prevailing U.S. policy thought at the time stressed the importance of the 1992 inter-Korean agreement in the eventuality that North Korea returned to denuclearization talks.[48]

Despite consultations in Washington and Seoul, negotiators struggled for years to balance both sides' interests, requirements, and limitations. At the conclusion, the proposed agreement aimed to address South Korea's nuclear aspirations within the bounds of U.S. nonproliferation policies by designing and implementing a bilateral cooperative framework to explore—and potentially open the door to—U.S. approval of South Korea's development of ENR capabilities. As Einhorn stated during a speech in October 2013, the U.S. government's stance on South Korea's pursuit of ENR technologies was not a permanent "no, never" but rather a statement of "not now."[49] As agreed upon in the 2015 123 Agreement, the route to future capabilities would run through the newly established High-Level Bilateral Commission (HLBC), which would act as the official bilateral channel for regular discussions, and a ten-year Joint Fuel Cycle Study on spent fuel storage and reprocessing technologies, including electrochemical processes such as pyroprocessing.[50]

This point was well emphasized by U.S. Assistant Secretary of State for International Security and Nonproliferation Thomas M. Countryman during his statement before the U.S. Senate Committee on Foreign Relations in October 2015. He said that the renewed 123 Agreement "contains a set of pathways toward possible U.S. Government decisions in the future on whether to grant advance consent to the ROK to enrich or reprocess U.S. obligated nuclear material."[51] Critically, details as to when, where, and how these technologies would be jointly developed in the future were not specified, though the prevailing assumption was that if joint studies resulted favorably, then any advancements in commercial ENR technologies would be pursued jointly and likely under U.S. leadership and oversight.

As such, the 2015 123 Agreement exemplified mutual compromise, balancing U.S. nuclear nonproliferation concerns and South Korean nuclear industry ambitions. However, the agreement's much-praised strengths could also be seen as its greatest weaknesses. By focusing on reaching a diplomatic win for both sides, the negotiations resulted in kicking the conversation on ENR capabilities down the road.[52] For Washington, negotiators emphasized that the United States had not given prior consent for proliferation-sensitive technologies, while

South Korean policymakers, in turn, championed the deal as a step in the right policy direction, laying out the requisite pathway toward the future development of ENR capabilities.[53]

Since June 2015, the gaps in U.S. and South Korean thinking on the 123 Agreement have only widened. Additionally, weaknesses in the joint implementation of the pact, as well as rifts in leading U.S. and South Korean nuclear companies, placed increasing pressure on the civil nuclear partnership. Officially launched in Seoul in 2016, the HLBC aimed to facilitate two-way agency-level engagement for "strategic cooperation between the parties and ongoing dialogue regarding areas of mutual interest in civil nuclear energy, including the civil nuclear fuel cycle" and initially focused on four working group areas of critical interest and cooperation: 1) spent fuel management, 2) promotion of nuclear exports and export controls cooperation, 3) assured fuel supply, and 4) nuclear security.[54] Steered by the working groups, the HLBC convened at the intersection of both nations' diplomatic, technical, and regulatory expertise. Though the HLBC successfully convened in April 2016, January 2017, and August 2018, regular meetings soon ceased.[55] As industry tensions rose over the Westinghouse-KHNP intellectual property rights dispute, both U.S. and South Korean diplomatic capital turned toward seeking cooperative solutions to the corporate disagreement, which hampered progress on expanding U.S.-South Korean joint nuclear reactor export projects. The "prolonged hiatus" of the HLBC has remained a source of frustration for the South Korean government's nuclear-focused agencies.[56]

Moreover, the planned deadline for the ten-year Joint Fuel Cycle Study—launched in 2011—also quietly passed without large-scale public disclosure of its findings. According to the 123 Agreement, the study intended to explore the technical feasibility, economic viability, and nonproliferation acceptability of spent fuel management and disposition technologies, including reprocessing. Overall, the joint study was highly unique in form, requiring a specialized Technology Transfer Agreement (TTA) for cooperation between the U.S. Department of Energy's Idaho National Laboratory (INL) and KAERI.[57] In 2021, South Korea's Ministry of Science and ICT reported that the ten-year project's findings were largely inconclusive regarding the feasibility of pyroprocessing and required further research.[58]

Overall, the lack of perceived progress across these key pillars of the 123 Agreement has locked the U.S.-South Korean civil nuclear relationship in a looping cycle of frustration.[59] Apparent inaction on issue areas that South Korea increasingly views as points of national security interest—including nuclear fuel import dependencies and limitations in spent fuel waste storage—has caused strain on U.S.-South Korean civil nuclear cooperation. Conversely, U.S. policymakers' thinking on the necessity of nonproliferation constraints has not changed, but rather been reinforced over the last decade.[60] While the argument for a return to the initially agreed-upon processes and frameworks—including restarting the HLBC—is reasonable, the possibility of receiving a different outcome to the brokered 2015 agreement on advance U.S. approval for ENR technologies at this time seems unlikely.

That being said, near-term prospects for industry-to-industry relations on these topics may be improving. U.S.-based commercial entities—driven in part by the revitalization of the U.S.

nuclear industry—are seeking to expand domestic uranium enrichment and, contrary to past U.S. thinking, launching commercial-level spent fuel recycling projects with U.S. government support.[61] Further shifts in U.S. political and commercial thinking on spent fuel recycling could be on the horizon. On the sidelines of U.S.-South Korean diplomatic engagement, there may be opportunities for South Korea to have a stake in early-stage enterprises for traditional and advanced fuel production.

The process and potential outcomes from a current bilateral discussion over renegotiating the U.S.-South Korean civil nuclear cooperative framework remain uncertain. Despite this, there are clear pathways forward for the United States and South Korea to reestablish a more future-oriented and successful partnership.

U.S.-South Korean "Future-Oriented" Nuclear Partnership

As Washington and Seoul explore strategies to reaffirm and strengthen the existing—or, potentially, renewed—framework for the U.S.-South Korean partnership on civil nuclear energy, they should take into consideration several areas of near-term opportunity, including 1) AI-driven nuclear industry revitalization, 2) traditional and advanced nuclear fuel supplies, and 3) spent fuel management and long-term storage strategies.

AI-Driven Nuclear Energy Revitalization

Amid the U.S.-China race for global AI leadership, Washington is gradually positioning nuclear energy as a much-needed solution to providing a high-intensity, reliable energy supply for data centers. Increasingly, the U.S. government and large technology firms are exploring "civil nuclear energy to fill the critical gap in wattage for AI development" and deployment.[62] As nuclear energy is reframed as essential for the U.S. national AI agenda, there are timely and important opportunities for the U.S.-South Korea nuclear partnership to play a critical role in the rising AI-nuclear nexus.[63]

The Trump administration has explicitly emphasized the need for new nuclear reactors, either traditional large-scale or SMRs, to provide baseload energy for AI-related infrastructure.[64] To accomplish fast-paced nuclear reactor construction, the U.S. commercial nuclear industry will turn to trusted vendors to ensure a reliable supply chain for critical reactor components, including South Korean companies. For example, South Korean firm Doosan Enerbility has supplied major nuclear equipment, including steam generators, for the Vogtle nuclear power plant's Westinghouse-designed AP-1000 reactor units 3 and 4—the United States' most recent large-scale nuclear construction projects.[65] Similarly, Fermi America launched a cooperative partnership with Doosan Enerbility and Hyundai E&C to construct four AP-1000 reactors as part of the company's planned 11 GWe Project Matador initiative in Amarillo, Texas, with construction planned for 2027.[66]

Additionally, as more U.S. big tech companies, such as Amazon, Google, Meta, and Microsoft, target nuclear energy for on-the-grid or behind-the-meter energy solutions for data centers,

South Korean companies have a window of opportunity to participate in early-mover market engagement, particularly for first-of-a-kind SMRs and advanced nuclear fuel projects.[67] In August 2025, X-energy, Amazon, KHNP, and Doosan Enerbility signed a strategic collaboration agreement in support of the construction of generation-IV Xe-100 SMRs and TRISO-X fuel production in the United States.[68]

Looking ahead, Washington and Seoul should continue to capitalize on near-term opportunities for new AI-driven nuclear initiatives, strengthening industry-to-industry partnerships. These are but a few examples of how South Korea's key public institutions and private firms—including KHNP, Doosan Enerbility, Hyundai E&C, and Samsung C&T—are actively contributing to the development of next-generation nuclear energy technologies in the United States.[69] Such trusted technology partnerships will be indispensable for ensuring the timely, on-budget buildup of the U.S. nuclear industry. For South Korea, early buy-in to U.S. nuclear projects can serve to reinforce South Korean companies' international position as globally trusted nuclear technology innovators.

Traditional and Advanced Nuclear Fuel Supplies

As the United States and South Korea target rapid, innovative timelines for growing their domestic nuclear fleets, while simultaneously eyeing openings for international nuclear export deals, the importance of long-term availability and reliability of supply for traditional nuclear fuels, including low-enriched uranium (LEU, LEU+), as well as advanced fuel types such as high-assay low-enriched uranium (HALEU), is ever more pressing.

Notably, South Korea, despite being the world's fifth-largest nuclear energy producer, does not operate industrial-scale facilities for uranium enrichment—a vital first step in nuclear fuel production.[70] Because of this, South Korea's reactor fleet depends entirely on imported enriched uranium. Previously, South Korea's dependency on imported LEU represented little concern, due to the wide availability of natural uranium and the nation's long-time export-import partnerships with key LEU suppliers. However, geopolitical challenges—triggered by Russia's invasion of Ukraine and the international community's efforts to move away from Russian-produced LEU—have caused South Korea to reevaluate its LEU import strategies.[71] In 2024, the country imported roughly 1,209,340 kilograms of enriched uranium from major suppliers, including Russia (45 percent), Canada (17 percent), Australia (15 percent), and France (7 percent), among others.[72] Since the United States enacted the Prohibiting Russian Uranium Imports Act on May 13, 2024, South Korea has started to shift the trajectory of its own LEU import plans, including by sourcing less from Russia.[73] In this context, South Korea is increasingly comparing its LEU import dependency to supply vulnerabilities associated with fossil fuel imports, leaving the nation potentially exposed to geopolitical risks and supply disruptions.[74]

To address fuel cycle insecurities, the United States and South Korea should explore routes to advance commercial fuel supply assurances for both traditional and emerging nuclear fuel types. Already, steps are moving in the right direction. On February 4, 2025, Centrus Energy—one of the fastest-growing uranium enrichment companies in the United States—and KHNP signed a

ten-year purchasing contract for LEU shipments from Centrus Energy's American Centrifuge Plant in Piketon, Ohio.[75] Expanding the partnership, KHNP and POSCO International signed a non-binding memorandum of understanding (MOU) with Centrus Energy to explore investment opportunities to expand U.S. enrichment capabilities and to pursue additional purchasing agreements for LEU and HALEU.[76] Additionally, the U.S. Export-Import Bank's announcement to provide up to USD 1.8 billion to South Korean nuclear operators to purchase LEU from General Matters signals continued market opportunities for the U.S.-South Korea nuclear partnership.[77]

Lastly, the Trump administration's reassessment of U.S.-based recycling of spent nuclear fuel is also leading to an uptick in public-private R&D, as well as interest and investment in commercial reprocessing in the United States.[78] With support from the U.S. Department of Energy's Advanced Research Projects Agency-Energy (ARPA-E) program, U.S. company Curio, in partnership with U.S. national laboratories, has completed laboratory-scale demonstrations of its NuCycle technology aimed at recycling spent nuclear fuel.[79] At the commercial level, Oklo announced plans in September 2025 to build a USD 1.68 billion commercial nuclear fuel recycling facility for operation by the early 2030s in Oak Ridge, Tennessee.[80] As the U.S. commercial sector continues to explore recycling projects, there may be opportunities for public-private engagement with South Korean industry, similar to existing LEU purchasing partnerships.

Moving forward, any revisions to the U.S.-South Korean 123 Agreement—and, potentially, by extension to the HLBC—will need to reconcile South Korea's legitimate priorities for energy resilience and industrial growth with longstanding U.S. commitments to nonproliferation leadership. Maintaining this balance will be critical for both parties to jointly advance nuclear energy industries that are secure, sustainable, and resistant to proliferation risks.

Spent Fuel Management and Long-Term Storage

As large-scale nuclear energy producers, the United States and South Korea have a vested interest in the safe, secure, and reliable long-term storage of spent nuclear fuel (SNF). Neither country possesses final storage solutions for SNF, relying on short-to-medium-term storage in reactor spent fuel pools (wet storage) or on onsite dry casks designed to contain radiation for several decades.[81] As Seoul grapples with growing challenges in spent fuel management, Washington's extensive regulatory and technical expertise provides a strong basis for expanded collaboration.

Over the years, South Korea has increasingly sounded the alarm on the nation's dwindling capacity for SNF short- and long-term storage. In September 2025, the National Assembly received reports from KHNP that South Korea's oldest reactor plants, Kori and Hanbit, will reach storage capacity limits by the early 2030s.[82] Based on reports, South Korea's stored SNF was estimated at approximately 19,110 metric tons (MT) of uranium across its five commercial nuclear power plants in 2024.[83] In the United States, approximately 95,000 MT of SNF are stored at seventy-nine licensed sites across the country; however, South Korea's limited landmass and smaller number of nuclear power plants create constraints on storage capacity, raising the urgency for near-term management and long-term disposal solutions.[84]

In addition to commercial nuclear waste, South Korea's research and medical industries have produced a total of 137,864 drums (sized at 200 liters each) of radioactive waste.[85] Following the example of other nuclear-producing nations, South Korea established a low- and intermediate-level radioactive waste (LILW) disposal center, the Korea Radioactive Waste Agency (KORAD) in January 2009. Of the 137,864 drums of solid radioactive waste, only 32,475 drums as of March 2024 met the criteria for LILW and were transported to KORAD for permanent disposal.[86] Boasting a total capacity of 100,000 drums of LILW solid waste storage, KORAD addresses South Korea's LILW storage needs; however, the complex is not rated for high-level nuclear waste such as spent reactor fuel. On February 27, 2025, the National Assembly passed the High-Level Radioactive Waste Special Act to address the growing need for high-level waste storage.[87] The special act includes specified timelines for the construction and operation of an interim nuclear waste storage and permanent disposal storage facilities by 2050 and 2060, respectively.[88]

As South Korea's commercial nuclear industry is under increasing pressure to find a solution to the waste storage problem, there is an opportunity for the United States and South Korea to develop and invest in near-term options. In 2015, Doosan, partnering with NAC International under a technology cooperation agreement, developed an SNF storage system for use in South Korea, and later became the first South Korean company to export dry casks to the United States in 2021.[89] Additionally, Orano TN (a U.S. subsidiary of a French-owned nuclear fuel cycle company), SeAH Besteel, and KEPCO Engineering & Construction signed an MOU for collaboration on the safe, secure management of South Korea's used nuclear fuel in dry storage.[90] Recently, KHNP selected Doosan Enerbility and NAC International to jointly design an indigenous dry cask storage system in South Korea, aiming for regulatory approval by 2027.[91] Building on these industry-to-industry partnerships, the United States and South Korea can focus on near-term SNF management and storage solutions, targeting swift technology development and sector buildup to address South Korea's SNF capacity limitations.

Dual-Use Challenges on the Horizon

As mentioned above, the U.S.-South Korea nuclear partnership is facing new challenges in the form of overlapping agendas on the civil nuclear front and the newly introduced potential of South Korean-built SSNs. On November 13, 2025, the White House's Joint Fact Sheet gave "approval for the ROK to build nuclear-powered attack submarines."[92] Even more interestingly, the statement specified that "The United States will work closely with the ROK to advance requirements for this shipbuilding project, including avenues to source fuel."[93] The injection of military-use nuclear technologies complicates the overall partnership—blurring the lines that were previously clearly delineated under the U.S.-South Korean civilian nuclear partnership.

For the Lee administration, the news was a welcome surprise, but one that produced more questions than answers. On the sidelines of APEC, Lee had requested U.S. support for acquiring nuclear fuel for submarines as part of South Korea's plans for a defense buildup to address North Korea's expanding weapons of mass destruction (WMD) program.[94] Trump's endorsement

of South Korea's independent pursuit of SSNs instead has raised questions in Washington and in Seoul over what this would mean in practice. Unlike the U.S. AUKUS Pillar I agreement with the United Kingdom and Australia, this would not be a technology transfer agreement for U.S.-built SSNs and the highly enriched uranium (HEU) fuel necessary for their operation.[95] Rather, this statement seems to indicate overarching approval for South Korea's independent pursuit of nuclear-propulsion submarines.[96] However, under the current U.S.-South Korean 123 Agreement, South Korea cannot pursue HEU fuel production, limiting future SSN designs to LEU or as yet untested HALEU fuel systems.[97] Furthermore, Trump's statement that South Korean SSNs would be built at the U.S. Philly Shipyard has raised additional concerns over the lead time necessary to upgrade the decades-old shipyard for SSN manufacturing.[98]

Implementing the White House's statement may prove difficult legally, as the agreement would necessitate a completely new type of nuclear cooperation between the two countries. Under the 2015 123 Agreement, the United States and South Korea are limited to cooperating on peaceful uses of nuclear technologies. According to Article 13 of the agreement, "Nuclear material, moderator material, equipment and components transferred… shall not be used for a nuclear weapon or any nuclear explosive device, for research on or development of any nuclear explosive device, or for any military purpose."[99] As such, both countries would not be able to leverage the existing nuclear agreement for SSN development—even if South Korea were to pursue a French-style SSN design powered by LEU, as some in the Lee administration have suggested.[100]

To move forward on SSN-related collaboration, the United States and South Korea will need to establish separate tracks for peaceful- versus military-use nuclear cooperation—each necessitating different political and legal frameworks.[101] Depending on the nature of the joint SSN project, the United States would have to establish new technology and fuel transfer agreements, which could include discussions on U.S.-produced LEU, HEU, or even HALEU fuel as well as legal structures for the transfer of U.S.-produced materials and equipment. Beyond this, South Korea would also need to modify its IAEA Comprehensive Safeguards Agreement, adding the inclusion of an Article 14 provision for IAEA verification that nuclear material is not being diverted to a nuclear weapons program.

Overall, the recent U.S.-South Korean SSN discussions add another layer of complexity to the evolution of the nuclear partnership. Though not insurmountable, both nations should exercise caution moving forward, especially given how this development will relate to South Korea's preexisting political and legal obligations for civil nuclear cooperation.

Looking Down the Road

The United States and South Korea's recent refocusing on the bilateral 123 Agreement demonstrates the strategic importance—to both states—of the cooperative nuclear partnership. Over the past decade, the U.S.-South Korea nuclear partnership has continued to grow, capitalizing on critical opportunities of importance to both parties.

As U.S. and South Korean negotiators reenter conversations over areas of improvement for the 2015 123 Agreement, both sides should approach the issues with clear eyes, evaluating strengths in equal measure to perceived weaknesses. Restarting regular, high-level working groups—whether in the form of the HLBC or a newly designed official coordination body—should rank high on the agenda. Most importantly, future U.S.-South Korean bilateral consultations should incorporate public-private partnerships: to be successful, industry leaders should not be left out of the conversation. Additionally, there should be clarification regarding the timeline for the U.S.-South Korean Joint Fuel Cycle Study and the feasibility—politically, economically, and in terms of nonproliferation—of reprocessing technologies. Lessons from the United States' recent uptick in private-sector leadership on spent fuel recycling technologies could feed into these discussions.

The pursuit of improvements, however, should not overshadow the foundational frameworks currently in place to strengthen the U.S.-South Korean nuclear cooperative partnership in the long run. Moreover, as the long-term political dimensions are readdressed, both sides should not overlook the near-term commercial successes and yet unexplored opportunities that lie ahead for the U.S.-South Korea nuclear partnership.

Endnotes

[1] *Text of Proposed Agreement for Cooperation Between the Government of the U.S. and the Government of the Republic of Korea Concerning Peaceful Uses of Nuclear Energy* (U.S. Government Publishing Office, 2015), https://www.govinfo.gov/content/pkg/CDOC-114hdoc43/pdf/CDOC-114hdoc43.pdf.

[2] Kayla Orta, "How South Korea Advanced its Trade and Technology Agenda at the APEC Summit," Atlantic Council, November 6, 2025, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-south-korea-advanced-its-trade-and-technology-agenda-at-the-apec-summit/.

[3] Sang-Hun Choe, "Trump Gives Legs to South Korea's Dream for Nuclear-Powered Subs," *New York Times*, November 17, 2025, https://www.nytimes.com/2025/11/17/world/asia/trump-south-korea-nuclear-submarines.html.

[4] The White House, "Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung," November 13, 2025, https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/.

[5] The White House, "Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung."

[6] Hyun-bin Kim, "Korean Negotiators to Visit Washington for Talks on Nuclear Energy Pact," *The Korea Times*, March 6, 2026, https://www.koreatimes.co.kr/foreignaffairs/20260306/korean-negotiators-to-visit-washington-for-talks-on-nuclear-energy-pact; Dong-ha Kim, "South Korea-U.S. Nuclear Cooperation Task Force Coordinates Expanded Rights Negotiations," *Chosun Ilbo*, January 19, 2026, https://www.chosun.com/english/national-en/2026/01/19/TAQTRL64KVEN5PBGZXVSAS5EIU/.

[7] On January 30, 2026, Senators Edward J. Markey (D-MA) and Jeff Merkley (D-OR), co-chairs of the Nuclear Weapons and Arms Control Working Group, along with Senators Chris Van Hollen (D-MD) and Ron Wyden (D-OR), wrote a joint letter to President Trump expressing concerns over Trump's "support for South Korea to enrich uranium and separate plutonium." The letter stated that the Trump administration's actions are a "[reversal of] Washington's long-standing bipartisan policy to prevent the spread of enrichment and reprocessing technologies to limit the risk that those capabilities could be used to produce fissile materials for weapons." See "Markey, Merkley, Van Hollen, Wyden Urge Trump to Keep Longstanding Ban on South Korean Nuclear Enrichment, Reprocessing," January 30, 2026, https://www.markey.senate.gov/news/press-releases/markey-merkley-van-hollen-wyden-urge-trump-to-keep-longstanding-ban-on-south-korean-nuclear-enrichment-reprocessing.

[8] Kayla Orta, "Atoms for Peace or Strategic Power? Re-aligning U.S.-South Korea's Nuclear Nonproliferation Agendas," *2025 International Joint Research Project* (Research Institute for National Security Affairs, Korea National Defense University, January 2026).

[9] Orta, "Atoms for Peace or Strategic Power?"; Kayla Orta and Kyung-joo Jeon, "Strength in Partnership: Elevating U.S.-ROK Cooperation in Nuclear Energy," *The National Interest*, April 15, 2025, https://nationalinterest.org/blog/energy-world/strength-in-partnership-elevating-u-s-rok-cooperation-in-nuclear-energy.

[10] Atomic Energy Act (S. Kor.), amended by Act No. 10909, July 25, 2011, translated in Korea Law Translation Center's online database, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=23918&type=sogan&key=2.

[11] Orta, “Atoms for Peace or Strategic Power?”

[12] Orta, “Atoms for Peace or Strategic Power?”; “Agreement Between the International Atomic Energy Agency, the Government of the Republic of Korea and the Government of the United States of America for the Application of Safeguards” (INFCIRC/111), International Atomic Energy Agency, April 9, 1968, archived at https://www.iaea.org/sites/default/files/infcirc111.pdf.

[13] Orta, “Atoms for Peace or Strategic Power?”

[14] For a review of historical documentation, see William Burr (ed.), “Stopping Korea from Going Nuclear, Part I,” National Security Archive, Briefing Book No. 582, March 22, 2017, https://nsarchive.gwu.edu/briefing-book/henry-kissinger-nuclear-vault/2017-03-22/stopping-korea-going-nuclear-part-i; William Burr (ed.), “Stopping Korea from Going Nuclear, Part II,” National Security Archive, Briefing Book No. 584, April 12, 2017, https://nsarchive.gwu.edu/briefing-book/henry-kissinger-nuclear-vault/2017-04-12/stopping-korea-going-nuclear-part-ii.

[15] Orta, “Atoms for Peace or Strategic Power?”

[16] Orta, “Atoms for Peace or Strategic Power?”

[17] U.S. Energy Information Administration, “Five Countries Account for 71% of the World’s Nuclear Generation Capacity,” August 11, 2025, https://www.eia.gov/todayinenergy/detail.php?id=65904.

[18] “Nuclear Power in South Korea,” World Nuclear Association, last updated March 6, 2026, https://world-nuclear.org/information-library/country-profiles/countries-o-s/south-korea.

[19] U.S. Department of Energy, “Fact Sheet: The Energy Department Is Delivering On Accelerating The Deployment Of Nuclear Power,” January 19, 2026, https://www.energy.gov/articles/fact-sheet-energy-department-delivering-accelerating-deployment-nuclear-power.

[20] The White House, “Deploying Advanced Nuclear Reactor Technologies for National Security,” May 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/05/deploying-advanced-nuclear-reactor-technologies-for-national-security/.

[21] U.S. Energy Information Administration, “The United States Operates the World’s Largest Nuclear Power Plant Fleet,” April 24, 2025, https://www.eia.gov/todayinenergy/detail.php?id=65104; U.S. Nuclear Regulatory Commission, “Operating Nuclear Power Reactors (by Location or Name),” last updated August 6, 2025, https://www.nrc.gov/info-finder/reactors/index.

[22] U.S. Office of Nuclear Energy, “The Nation’s Nuclear Reactor Fleet Is on the Rise,” U.S. Department of Energy, March 12, 2026, https://www.energy.gov/ne/articles/nations-nuclear-reactor-fleet-rise; U.S. Department of Energy, “Fact Sheet: The Energy Department Is Delivering On Accelerating.”

[23] The White House, “Deploying Advanced Nuclear Reactor Technologies.”

[24] Kayla Orta, “US-South Korean Civil Nuclear Exports Are a Winning Strategy,” *The National Interest*, September 29, 2025, https://nationalinterest.org/blog/energy-world/us-south-korean-civil-nuclear-exports-are-a-winning-strategy.

[25] World Nuclear Association, "Nuclear Power in South Korea."

[26] "Plans for Two New Reactors Confirmed by South Korea," World Nuclear News, January 26, 2026, https://www.world-nuclear-news.org/articles/plans-for-two-new-reactors-confirmed-by-south-korea.

[27] Frequently, the term "Team Korea" refers to both government-owned and private companies within South Korea's broader civil nuclear industry. See "TEAM KOREA Brochure," Korea Nuclear Association, accessed June 12, 2026, https://www.e-kna.org/mobile_e/DownLoad.php?file=Attachment._TEAM_KOREA_Brochure.pdf.

[28] World Nuclear Association, "Nuclear Power in South Korea."

[29] Kayla Orta, "Artificial Intelligence Needs Nuclear Power – And Allied Cooperation," *The National Interest*, March 26, 2026, https://nationalinterest.org/blog/techland/artificial-intelligence-needs-nuclear-power-and-allied-cooperation.

[30] For more information on advanced reactor designs, see "Advanced Reactor Information System (ARIS)," International Atomic Energy Agency, accessed June 5, 2026, https://aris.iaea.org/.

[31] See Nuclear Fuel Working Group, *Restoring America's Competitive Nuclear Energy Advantage: A Strategy to Assure U.S. National Security* (U.S. Department of Energy, 2020), https://www.energy.gov/articles/restoring-americas-competitive-nuclear-energy-advantage.

[32] See International Atomic Energy Agency, *Energy, Electricity and Nuclear Power Estimates for the Period up to 2050,* IAEA Reference Data Series no. 1, September 2025, https://doi.org/10.61092/iaea.gwov-o544.

[33] See "Four More Countries Endorse Global Declaration to Triple Nuclear Energy," World Nuclear Association, March 10, 2026, https://world-nuclear.org/news-and-media/press-statements/four-more-countries-endorse-global-declaration-to-triple-nuclear-energy; Mary Albon, "Two More Countries Join Global Pledge to Triple Nuclear Energy by 2050," International Atomic Energy Agency, November 24, 2025, https://www.iaea.org/newscenter/news/two-more-countries-join-global-pledge-to-triple-nuclear-energy-by-2050.

[34] "Emerging Nuclear Energy Countries," World Nuclear Association, last updated May 27, 2026, https://world-nuclear.org/information-library/country-profiles/others/emerging-nuclear-energy-countries; U.S. Department of Energy, "At COP28, Countries Launch Declaration to Triple Nuclear Energy Capacity by 2050, Recognizing the Key Role of Nuclear Energy in Reaching Net Zero," December 1, 2023, https://www.energy.gov/articles/cop28-countries-launch-declaration-triple-nuclear-energy-capacity-2050-recognizing-key.

[35] See Brad Plumer and Harry Stevens, "China is Outpacing the U.S. on Nuclear Power, an American Invention," *The New York Times*, October 22, 2025, https://www.nytimes.com/interactive/2025/10/22/climate/china-us-nuclear-energy-race.html; "China Keeps Pushing Nuclear Power With Ambitious Growth Target," Bloomberg News, March 8, 2026, https://www.bloomberg.com/news/articles/2026-03-09/china-keeps-pushing-nuclear-power-with-ambitious-growth-target; "Nuclear Power in China," World Nuclear Association, last updated March 23, 2026, https://world-nuclear.org/information-library/country-profiles/countries-a-f/china-nuclear-power; "Nuclear Power in India," World Nuclear Association, last updated January 20, 2026, https://world-nuclear.org/information-library/country-profiles/countries-g-n/india.

[36] See "Projects," Rosatom, accessed March 31, 2026, https://rosatom.ru/en/investors/projects/.

[37] See Shunsuke Tabeta et al., "China and Russia Dominate Nuclear Power Push with 90% of New Reactors," *Nikkei Asia*, January 18, 2026, https://asia.nikkei.com/business/energy/china-and-russia-dominate-nuclear-power-push-with-90-of-new-reactors.

[38] See Orta, "US-South Korean Civil Nuclear Exports."

[39] Robin Gaster, "Small Modular Reactors: A Realist Approach to the Future of Nuclear Power," Information Technology & Innovation Foundation, April 14, 2025, https://itif.org/publications/2025/04/14/small-modular-reactors-a-realist-approach-to-the-future-of-nuclear-power/.

[40] See Fred McGoldrick, "The New Peaceful Nuclear Cooperation Agreement Between South Korea and the United States: From Dependence to Parity," Korea Economic Institute of America, August 31, 2015, https://keia.org/publication/the-new-peaceful-nuclear-cooperation-agreement-between-south-korea-and-the-united-states-from-dependence-to-parity/; Duyeon Kim and Mark Hibbs, "What the New U.S.–South Korea Civil Nuclear Cooperation Agreement Means," Carnegie Endowment for International Peace, April 13, 2015, https://carnegieendowment.org/posts/2015/04/what-the-new-us-south-korea-civil-nuclear-cooperation-agreement-means.

[41] See Seung-Yeon Kim, "S. Korea to Soon Begin Talks with U.S. on Revising Nuclear Energy Pact: FM Cho," Yonhap News Agency, October 23, 2025, https://en.yna.co.kr/view/AEN20251023003100315.

[42] The U.S. Department of State announced that Under Secretary of State for Political Affairs Allison Hooker's planned visit to South Korea on June 1–3, 2026 will include discussions on efforts to "advance nuclear cooperation initiatives" between the two nations. See U.S. Department of State, "Under Secretary Hooker's Travel to the Republic of Korea," May 28, 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/05/under-secretary-hookers-travel-to-the-republic-of-korea/; Sang-Ho Song, "S. Korea, U.S. to launch talks on security initiatives from summit agreements next week," Yonhap News Agency, May 29, 2026, https://en.yna.co.kr/view/AEN20260529001351315.

[43] Sang-Hun Choe, "South Korea and U.S. Differ on Nuclear Enrichment," *The New York Times*, December 5, 2011, https://www.nytimes.com/2011/12/06/world/asia/south-korea-and-us-differ-on-nuclear-enrichment.html?ref=asia&_r=0.

[44] Seongho Sheen, "Nuclear Sovereignty versus Nuclear Security: Renewing the ROK-U.S. Atomic Energy Agreement," *The Korean Journal of Defense Analysis* 23, no. 2 (2011): 273–288, https://www.brookings.edu/wp-content/uploads/2016/06/08_nuclear_korea_sheen.pdf.

[45] *Text of Proposed Agreement Between the United States and Japan Concerning Peaceful Uses of Nuclear Energy* (U.S. Government Printing Office, 1987), https://www.nrc.gov/docs/ML0413/ML041350444.pdf; for South Korea's perspective, see Sung Chull Kim, "Endangering Alliance or Risking Proliferation?: US-Japan and US-Korea Nuclear Energy Cooperation Agreements," *The Pacific Review* 30, no. 5 (2017): 692–709, http://dx.doi.org/10.1080/09512748.2017.1293715; for more information on U.S. policy thinking during the U.S.-Japan 123 Agreement (1987) negotiations, see William Burr (ed.), "Japan Plutonium Overhang Origins and Dangers Debated by U.S. Officials," National Security Archive, Briefing Book No. 597, updated August 1, 2018, https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2017-06-08/japan-plutonium-overhang-origins-dangers-debated-us-officials.

[46] Sang-Hun Choe, "U.S. and South Korea Reach Revised Nuclear Deal," *The New York Times*, April 22, 2015, https://www.nytimes.com/2015/04/23/world/asia/us-and-south-korea-reach-revised-nuclear-deal.html.

[47] "Joint Declaration of the Denuclearization of the Korean Peninsula," conclusion date: January 20, 1992, S. Korea-N. Korea, https://peacemaker.un.org/sites/default/files/document/files/2024/05/kr20kp920120jointdeclarationdenuclearizationkoreanpeninsula.pdf.

[48] Robert Einhorn, "U.S.-ROK Civil Nuclear Cooperation Agreement: Overcoming the Impasse," The Brookings Institution, October 11, 2013, https://www.brookings.edu/articles/u-s-rok-civil-nuclear-cooperation-agreement-overcoming-the-impasse/.

[49] Einhorn, "U.S.-ROK Civil Nuclear Cooperation Agreement: Overcoming the Impasse."

[50] In the Agreed Minutes submitted to the U.S. Congress alongside the 2015 123 Agreement, section 6 on "Arrangements for Spent Fuel Management and Disposition" detailed the role of the HLBC and Joint Fuel Cycle Study in determining long-term feasibility, viability, and acceptability for reprocessing technologies. See *Text of Proposed Agreement for Cooperation Between the Government of the U.S. and the Government of the Republic of Korea Concerning Peaceful Uses of Nuclear Energy*.

[51] U.S. Congress, Senate, Committee on Foreign Relations, Hearing on Reviewing the Civil nuclear Agreement in South Korea, 114th Cong., 1st sess., October 1, 2015, https://www.foreign.senate.gov/imo/media/doc/10%2001%2015%20Reviewing%20the%20Civil%20Nuclear%20Agreement%20with%20the%20Republic%20of%20Korea.pdf.

[52] Daniel Horner, "S. Korea, U.S. Sign Civil Nuclear Pact," Arms Control Association, July/ August 2015, https://www.armscontrol.org/act/2015-07/news/s-korea-us-sign-civil-nuclear-pact.

[53] ROK-US Nuclear Agreement Task Force, "한미 원자력협정 전명 개정 – 과거를 벗고 현재를 풀며 미래를 열다 [Complete Revision of the ROK-US Nuclear Agreement – Shedding the Past, Resolving the Present, Opening the Future]," South Korean Ministry of Foreign Affairs, April 22, 2015, https://www.mofa.go.kr/www/brd/m_4076/view.do?seq=354697&page=1.

[54] See *Text of Proposed Agreement for Cooperation Between the Government of the U.S. and the Government of the Republic of Korea*.

[55] See U.S. Department of Energy, "Co-Chairs of the United States-Republic of Korea High Level Bilateral Commission Convene in Washington," January 11, 2017, https://www.energy.gov/articles/co-chairs-united-states-republic-korea-high-level-bilateral-commission-convene-washington; U.S. Department of Energy, "Deputy Secretary Brouillette Hosts U.S.-Republic of Korea High Level Bilateral Commission Meeting," August 17, 2018, https://www.energy.gov/articles/deputy-secretary-brouillette-hosts-us-republic-korea-high-level-bilateral-commission.

[56] Eunju Jun, "Beyond the 123 Agreement: A Strategy for a Substantive ROK-U.S. Nuclear Partnership," Korea on Point, October 30, 2025, https://koreaonpoint.org/articles/article_detail.php?idx=478.

[57] Einhorn, "U.S.-ROK Civil Nuclear Cooperation Agreement."

[58] Bong-su Kim, "Official Approval of Korea-US Joint Research Report on Spent Nuclear Fuel Reprocessing Technology," *Asia Business Daily*, September 1, 2021, https://www.asiae.co.kr/en/print.htm?idxno=2021090121190805878.

[59] Jun, "Beyond the 123 Agreement."

[60] See "Markey, Merkley, Van Hollen, Wyden Urge Trump to Keep Longstanding Ban on South Korean Nuclear Enrichment, Reprocessing."

[61] See Office of Nuclear Energy, "DOE's Office of Nuclear Energy Awards $19 Million to Advance Recycling of Used Nuclear Fuel," U.S. Department of Energy, February 5, 2026, https://www.energy.gov/ne/articles/does-office-nuclear-energy-awards-19-million-advance-recycling-used-nuclear-fuel.

[62] Orta, "Artificial Intelligence Needs Nuclear Power."

[63] See Kayla Orta, "High-Tech Alliances: South Korea, the G7 and the Future of AI and Nuclear Innovation," *Istituto Affari Internazionali Papers* 25, no. 26 (October 2025), https://www.iai.it/en/publications/c03/high-tech-alliances-south-korea-g7-and-future-ai-and-nuclear-innovation.

[64] The White House, "Deploying Advanced Nuclear Reactor Technologies."

[65] See, "Doosan Awarded Further Contract by Westinghouse," World Nuclear News, June 5, 2008, https://www.world-nuclear-news.org/Articles/Doosan-awarded-further-contract-by-Westinghouse.

[66] "Fermi Enlists Korean Firms for Texan Reactors," World Nuclear News, October 28, 2025, https://www.world-nuclear-news.org/articles/fermi-enlists-korean-firms-for-texan-reactors; Neul-bit Ha, "Hyundai E&C Becomes First Korean Builder to Design Large-Scale Nuclear Plants in US," *The Korea Herald*, October 26, 2025, https://www.koreaherald.com/article/10601378.

[67] Orta, "Artificial Intelligence Needs Nuclear Power."

[68] "X-energy, Amazon, Korea Hydro & Nuclear Power, and Doosan Enerbility Announce Partnership to Scale Advanced Nuclear Energy for AI Infrastructure," X-Energy, August 25, 2025, https://x-energy.com/news/x-energy-amazon-korea-hydro-amp-nuclear-power-and-doosan-enerbility-announce-partnership-to-scale-advanced-nuclear-energy-for-ai-infrastructure/.

[69] See World Nuclear News, "Fermi Enlists Korean Firms."

[70] Kayla Orta, "How the US and South Korea Can Secure Nuclear Supply Chains," *The National Interest*, April 16, 2026, https://nationalinterest.org/blog/energy-world/how-the-us-and-south-korea-can-secure-nuclear-supply-chains.

[71] Jae-hyun Ju, "원전 연료 러 의존 줄인다…한수원, 美 센트루스와 10년 공급 계약 [Reducing Reliance on Russia for Nuclear Fuel… KHNP Signs 10-year Contract with U.S. Centrus]," *Seoul Economic Daily*, February 5, 2025, https://m.sedaily.com/amparticle/14023795; Dae-un Cha, "한·러 관계 얼어붙는데…원전연료 러시아 의존도 30% 넘어 [As South Korea-Russia Relations Freeze… Dependence on Russia for Nuclear Fuel Exceeds 30%]," Yonhap News Agency, September 16, 2024, https://www.yna.co.kr/view/AKR20240911153800003.

[72] "Korea, Rep. Enriched Uranium and Plutonium and their Compou Imports by Country in 2024," World Integrated Trade Solution, accessed March 30, 2026, https://wits.worldbank.org/trade/comtrade/en/country/KOR/year/2024/tradeflow/Imports/partner/ALL/product/284420.

[73] See U.S. Nuclear Regulatory Commission, "Backgrounder on Uranium Import Ban," last updated October 31, 2024, https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/uranium-import-ban; Prohibiting Russian Uranium Imports Act, Pub. L. No. 118-62, 138 Stat. 1022 (2024), https://www.congress.gov/bill/118th-congress/house-bill/1042; Dae-un Cha, "원전연료 러 의존 소폭 줄었다…서방권 비중 높여갈 듯" [Dependence on Russia for Nuclear Fuel Has Decreased Slightly… Western Reliance Is Expected to Increase], Yonhap News Agency, January 1, 2025, https://www.yna.co.kr/view/AKR20250124144200003.

[74] Kayla Orta, "The Iran Crisis Is Fueling South Korea's Drive for Nuclear Energy," The Diplomat, March 12, 2026, https://thediplomat.com/2026/03/the-iran-crisis-is-fueling-south-koreas-drive-for-nuclear-energy/.

[75] "Centrus Awarded Korean Contract for Enriched Uranium," World Nuclear News, February 5, 2025, https://www.world-nuclear-news.org/articles/centrus-awarded-korean-contract-for-enriched-uranium.

[76] "Centrus Signs Agreement with KHNP and POSCO International for Potential Investment in American Uranium Enrichment," Centrus Energy, August 25, 2025, https://investors.centrusenergy.com/news-releases/news-release-details/centrus-signs-agreement-khnp-and-posco-international-potential.

[77] Jennifer A. Dlouhy, "Japan, South Korea Nuclear Operators Get US Ex-Im Bank Support," Bloomberg News, March 15, 2026, https://www.bloomberg.com/news/articles/2026-03-15/japan-south-korea-nuclear-operators-get-us-ex-im-bank-support.

[78] The White House, "Reinvigorating the Nuclear Industrial Base," May 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/05/reinvigorating-the-nuclear-industrial-base/.

[79] "U.S. Nuclear Fuel Recycling Takes Two Steps Forward," Nuclear Newswire, September 8, 2025, https://www.ans.org/news/2025-09-08/article-7348/us-nuclear-fuel-recycling-takes-two-steps-forward/.

[80] See "Oklo Announces Fuel Recycling Facility as First Phase of up to $1.68 Billion Advanced Fuel Center in Tennessee," Oklo, September 4, 2025, https://oklo.com/newsroom/news-details/2025/Oklo-Announces-Fuel-Recycling-Facility-as-First-Phase-of-up-to-1-68-Billion-Advanced-Fuel-Center-in-Tennessee/default.aspx; Office of Environmental Management, "EM Cleanup Paves Way for $1.7 Billion Energy Investment in Oak Ridge," U.S. Department of Energy, September 23, 2025, https://www.energy.gov/em/articles/em-cleanup-paves-way-17-billion-energy-investment-oak-ridge.

[81] "Storage and Disposal of Radioactive Waste," World Nuclear Association, last updated March 23, 2026, https://world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-waste/storage-and-disposal-of-radioactive-waste#interim-waste-storage-and-transport; U.S. Nuclear Regulatory Commission, "Backgrounder on Dry Cask Storage of Spent Nuclear Fuel," last updated June 12, 2023, https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dry-cask-storage.

[82] Hyeong-won Kim, "Gori Nuclear Plant's Spent Fuel Storage Nears 95% Saturation," *Chosun Ilbo*, September 15, 2025, https://www.chosun.com/english/national-en/2025/09/14/K5QI3MWRIFEBVKS6GY7J3JRB5E/.

[83] International Atomic Energy Agency, *The 8th National Report (Republic of Korea) under the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management* (2024), https://www.iaea.org/sites/default/files/2025-08/korea_rep_of-national-report-8rm.pdf.

[84] Office of Nuclear Energy, "Inside One of the Nation's Biggest Research Projects on Spent Nuclear Fuel," U.S. Department of Energy, July 7, 2025, https://www.energy.gov/ne/articles/inside-one-nations-biggest-research-projects-spent-nuclear-fuel; See 사용후핵연료 안전관리 분과(2분과) 보고서 [*Spent Nuclear Fuel Safety Management Subcommittee, (Subcommittee 2) Report*], Korean Nuclear Society, March 2025, https://www.kns.org/boards/download/29199.

[85] See International Atomic Energy Agency, *The 8th National Report (Republic of Korea)*.

[86] See International Atomic Energy Agency, *The 8th National Report (Republic of Korea)*.

[87] "South Korea Enacts Legislation on High-Level Waste," World Nuclear News, March 4, 2025, https://www.world-nuclear-news.org/articles/south-korea-enacts-legislation-on-high-level-waste.

[88] 고준위 방사성폐기물 관리에 관한 특별법 [Special Act on the Management of High-Level Radio Active Waste] (S. Kor.), https://www.law.go.kr/법령/고준위방사성폐기물관리에관한특별법/(20843,20250325).

[89] See "Doosan Heavy Industries and NAC International, Inc. form Technology Alliance on Development of CASK Storage for Spent Nuclear Fuel," NAC International, October 26, 2015, https://www.nacintl.com/newsroom/nac-news/doosan-heavy-industries-and-nac-international-inc-form-technology-alliance-on-development-of-cask-storage-for-spent-nuclear-fuel; "Doosan Enerbility to Design Used Fuel Storage System," World Nuclear News, November 6, 2023, https://www.world-nuclear-news.org/Articles/Doosan-Enerbility-to-design-used-fuel-storage-syst.

[90] "Orano Signs MOU for Developing Used Nuclear Fuel Dry Storage in Korea," Orano, May 23, 2022, https://www.orano.group/usa/en/our-news/news-releases/2022/may/orano-signs-mou-for-developing-used-nuclear-fuel-dry-storage-in-korea.

[91] "Doosan Enerbility Wins Spent Nuclear Fuel Cask Project With its Homegrown Technology," Doosan, November 2, 2023, https://www.doosanenerbility.com/en/about/news_board_view?id=21000582&page=0&pageSize=9; "Doosan Enerbility Teams with NAC International to Win Used Fuel Storage Design Work for KHNP," NAC International, November 7, 2023, https://www.nacintl.com/newsroom/nac-news/doosan-enerbility-teams-with-nac-international-to-win-used-fuel-storage-design-work-for-khnp; Ha-nee Shin, "Doosan Enerbility Signs Dry Cask MOU with 8 Companies," *Joongang Ilbo*, August 30, 2022, https://koreajoongangdaily.joins.com/2022/08/30/business/industry/Korea-Doosan-Enerbility-Nuclear-energy/20220830171140042.html.

[92] The White House, "Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung."

[93] The White House, "Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae Myung."

[94] Eun-jung Kim, "[APEC 2025] Lee Asks Trump to Allow S. Korea to Have Fuel for Nuclear-powered Submarines," Yonhap News Agency, October 29, 2025, https://en.yna.co.kr/view/AEN20251029009853315.

[95] Derek E. Mix and Jared G. Tupuola, *AUKUS and Indo-Pacific Security*, CRS Report No. IF12113 (Congressional Research Service, 2025), https://www.congress.gov/crs-product/IF12113.

[96] Ji-ho Yang and Han-kook Jung, "South Korea Poised to build Nuclear-powered Submarines in a Decade," *Chosun Ilbo*, October 31, 2025, https://www.chosun.com/english/national-en/2025/10/31/36P7BPTM7ZBOJJ4A2SU7YQGDCQ/.

[97] Brian Persons et al., "Why Korea's Nuclear-Powered Submarine Matters to U.S. Strategy," RAND, February 12, 2026, https://www.rand.org/pubs/commentary/2026/02/why-koreas-nuclear-powered-submarine-matters-to-us.html.

[98] "Editorial: Build Lead Nuclear Submarine in Korea, Subsequent Ones in U.S.," *Chosun Ilbo*, November 1, 2025, https://www.chosun.com/english/opinion-en/2025/11/01/OQOPKGMFMBFJLICLWNP3UPRMKU/.

[99] See *Text of Proposed Agreement for Cooperation Between the Government of the U.S. and the Government of the Republic of Korea*.

[100] Hyun-kyung Kang, "Untangling South Korea's Quest for Nuclear-Powered Submarines," *The Korea Times*, November 20, 2025, https://www.koreatimes.co.kr/foreignaffairs/northkorea/20251120/untangling-south-koreas-quest-for-nuclear-powered-submarines; for a review of French LEU-fuel nuclear-powered submarines, see Alain Tournyol du Clos, *France's Choice for Naval Nuclear Propulsion: Why Low-Enriched Uranium Was Chosen* (Federation of American Scientists, 2016), https://fas.org/publication/frances-choice-for-naval-nuclear-propulsion-why-low-enriched-uranium-was-chosen/.

[101] See Lowell H. Schwartz, "Legal and Policy Options for a U.S-South Korea Nuclear Submarine Program," Just Security, December 8, 2025, https://www.justsecurity.org/126497/us-south-korea-nuclear-submarine/.

Redefining National Security Governance through Access and Compute: U.S.-South Korea Export Controls on AI Infrastructure

By ChangHee Kim

AI has emerged as a core strategic asset, and its performance depends less on the models themselves than on the data centers and high-performance compute resources—the total computational power, measured in graphics processing unit (GPU) hours, used to train and operate AI systems—that support them. Such infrastructure can enable the diffusion of technology through mere access, without any physical transfer of equipment, creating a structural challenge for export control regimes designed on the premise of physical exports.

The U.S. and South Korean export control systems remain structured around the cross-border movement of tangible items and technical documents. In a borderless AI infrastructure environment, however, the actual route of technology transfer is determined less by where servers are located than by who can access which compute resources and data, and with what entitlements. Current export control regimes do not adequately capture this reality.

South Korean companies making large-scale investments in AI infrastructure in the United States are simultaneously subject to U.S. export rules, which treat the release of controlled technology to foreign persons within the United States as an export, and to South Korea's strategic technology control system. In this process, the same behavior—for example, a South Korean engineer remotely accessing a U.S. data center—can be interpreted differently under the two systems, amplifying regulatory uncertainty and investment risk.

This paper argues for a transition from hardware-centric export controls to compute-centric export governance. It proposes redefining AI data centers not as assets located inside or outside physical borders, but as "borderless strategic assets" managed through access entitlement structures. It discusses how Zero Trust—a cybersecurity principle that requires identity verification and authorization at each access point—and real-time access control can apply to

---

ChangHee Kim is a global trade compliance professional with over 20 years of experience specializing in U.S. and South Korean export controls (ITAR/EAR and Korean strategic items regulations), reexport compliance, and national security governance.

The author is grateful to Attorney Sejin Jung of Lee & Ko for helpful comments on legal and policy issues related to U.S. export controls and South Korean strategic technology regulations. Attorney Jung is a leading expert in Korean digital and data law, with particular expertise in the AI Basic Act and data governance legislation, and has contributed to shaping Korea's AI governance discourse through his published work in the field. Any remaining errors are the author's own.

national security governance. Specifically, the paper: 1) shows that technology transfers in AI data centers are shifting from physical movement to access entitlement structures; 2) identifies a growing misalignment between data protection law and export control law; 3) proposes compute quota and risk-tiered Zero Trust-based access governance as new policy control concepts; and 4) links functional weaponization of AI to export and access control debates.

Recent policy developments in both countries emphasize the importance of these policy questions. In March 2026, the U.S. Department of Commerce drafted rules that would require licenses for virtually all AI chip exports globally, adding conditions to transfers of more than 200,000 chips on recipient countries agreeing to build AI data centers in the United States.[1] In South Korea, the AI Basic Act entered into force on January 22, 2026, establishing risk management obligations for high-performance AI systems, with phased enforcement beginning in 2027.[2] Seoul also began distributing the first tranche of a 10,000-unit national GPU pool in March 2026.[3] Taken together, these developments create new opportunities for policy coordination between the United States and South Korea, but also expose governance gaps that neither side is yet well-positioned to manage alone.

The End of Physical Borders and the Rise of Compute

The problem of AI governance fundamentally clashes with assumptions about technology transfer on which traditional export control systems were built. Those systems evolved on the premise that strategic technologies physically cross borders. From the Coordinating Committee for Multilateral Export Controls—the informal multilateral export control regime of the Cold War—to the post-Cold War Wassenaar Arrangement, multilateral regimes have focused on controlling the movement of physical equipment and technical documents.[4] Semiconductors, precision machinery, and telecommunications equipment remain among the key controlled items today.

This challenge has taken on new urgency under the current policy environment. In January 2025, the Donald Trump administration issued an executive order prioritizing U.S. leadership in AI infrastructure, signaling a continued emphasis on compute access within U.S. national security policy.[5] In South Korea, the Lee Jae Myung administration has similarly identified AI and semiconductor supply chains as strategic priorities, pursuing domestic AI capability development while deepening investment ties with U.S. cloud and data center ecosystems.[6] These parallel policy imperatives—U.S. efforts to maintain technological leadership and South Korea's ambitions to secure AI infrastructure capacity—create both alignment opportunities and governance gaps.

The spread of AI technologies is now substantively shaking the physical-transfer premise of export control regimes. Today, strategic AI capabilities can rapidly diffuse without physical transfers, through access to compute resources and data. For example, if an actor has long-term access to a high-performance GPU cluster—an array of specialized processors optimized for the parallel computations required to train and run AI models—and continuously uses it to train and refine models, it can accumulate strategic AI capabilities without any movement of hardware.

In this environment, the central axis of national security risk is shifting from the question of "What has moved?" to "Who can access which compute resources?" Consider the case of 100 identical GPUs. If they are shared among research institutions in multiple allied countries, rather than being monopolized by a single organization in one location, the physical configuration may be the same, but the security implications can be very different. The real risk is determined by how much compute a particular actor can concentrate and for how long. (For a more detailed explanation, see Appendix A.)

As the AI market grows, data centers and high-performance compute infrastructure have become core elements of strategic competition. South Korean firms have become major investors and operators in the U.S. AI ecosystem, yet current export control systems were not designed to address compute access as a new channel for technology diffusion.[7]

This paper is informed by broader compliance and policy debates in export control and AI governance. Policy discussions and compliance commentary increasingly highlight deep uncertainty in cloud-based AI infrastructure environments that cannot be easily addressed using traditional metrics such as server location or equipment counts, with growing concern that legitimate technical activities may fall into a regulatory gray zone.[8] The purpose of this paper is therefore not to offer a final institutional blueprint but to identify the policy questions that now require closer U.S.-South Korea coordination. In particular, it seeks to explore a new governance framework that allows security and industrial innovation to coexist by focusing on two axes: access rights and compute quotas.

The paper makes three main points. First, AI infrastructure is no longer transferred primarily through the movement of hardware, but through access. High-end AI capabilities can spread across borders solely via remote access to data center resources and compute—without the physical relocation of equipment.

Second, simply allowing long-term, repeated use of compute resources can enable the transfer and accumulation of strategic capabilities, even in the absence of any formal provision or disclosure of the underlying technology. Even with identical hardware configurations, an actor's cumulative use of compute over time can yield a qualitatively different level of functional AI capability.

Third, in response to these changes, export control regimes should move beyond a perspective centered on physical equipment and technical documentation, and reconsider computation and access as core units of control. The argument here is not that existing systems should be replaced, but that they no longer fully capture the security risks and compliance uncertainties posed by AI infrastructure environments.

In practice, the current export regime appears markedly less effective at capturing computation- and access-based risks in cloud and multi-tenant environments—where different organizations share the same physical infrastructure but are logically separated through virtualization and access controls—than in traditional on-premises settings.

AI Data Centers and the Borderless Nature of Access-Based Transfers

In AI infrastructure environments, technology transfer can no longer be adequately described in terms of physical movement or the transmission of documents alone. In large-scale AI data centers and cloud-based computing infrastructures, it is not the physical location of servers but rather who can access which compute resources and datasets, and with what kind of authorization, that effectively determines the scope of the "transfer."

In the case of multinational enterprises, data centers operated by the U.S. affiliate of a South Korean organization may be located either in South Korea or in the United States, and the nationality and residence of personnel with access rights to those data centers are highly diverse.[9] In these settings, the actual pathways through which technology and data move are defined by access-control structures rather than national borders, and usage patterns and associated risks are difficult to understand based solely on physical location.

The Prior Evolution of Data Protection Law

Data protection law in some countries has already incorporated this reality to a significant extent. Both the European Union's General Data Protection Regulation (GDPR) and South Korea's Personal Information Protection Act (PIPA) interpret cross-border transfers of personal data as encompassing not only the physical transmission of data, but also conduct that makes data accessible from abroad.[10] Even if servers are located domestically, supervisory authorities generally apply regulations governing cross-border transfers if overseas personnel can remotely view or process personal data.[11]

This regulatory logic is not confined to data protection. It is gradually being extended to other regulatory regimes that govern the transfer of technology and industrial capabilities.[12]

Moreover, under the U.S. export control system, this kind of access-based use is discussed as a core issue in determining how technology should be controlled.[13] For example, consider a scenario in which an AI model developed and trained on a server in Seoul is remotely accessed by an affiliate researcher in Silicon Valley via a virtual private network (VPN) to analyze its architecture or conduct additional training. Even if the AI model and associated know-how are not physically transferred abroad, there is a question of whether export control rules treat this as a transfer of technology if foreign personnel can, in practice, access and utilize that technology. Ultimately, in AI infrastructure environments, the criteria for technology transfer are shifting from the storage location of technology or the routing of data flows toward who can access and exploit that technology.

Structural Limitations of Export Control Regimes

By contrast, the U.S. Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR), as well as South Korea's systems for controlling strategic goods and strategic technologies, remain grounded in a traditional concept of technology provision and disclosure and do not fully reflect today's reality.[14] The U.S. export regime similarly treats the

"release" of controlled technology to foreign persons in the United States as an export, but its regulatory focus lies on whether the substantive contents of the technology or software have been disclosed.[15]

As a result, there are interpretive gaps regarding how to distinguish and regulate access to high-performance GPU resources, on the one hand, and the transfer of controlled technical information, on the other. These ambiguities leave room for regulatory arbitrage and create burdens on both policymakers and industry by undermining companies' ability to predict what levels of access and collaboration are permitted.

South Korea's regime is also framed primarily around active conduct, such as the provision, transmission, and teaching of technology, and does not explicitly capture access-based usage patterns as a distinct regulatory unit. For example, whether the act of a South Korean engineer utilizing GPUs in a U.S. data center via Application Programming Interface (API) calls—standardized requests sent over a network to access and trigger specific functions in a remote system—constitutes the provision of a controlled strategic technology is, under the current text of the law, open to interpretive dispute.

Furthermore, both traditional forms of remote access, such as encrypted Secure Shell (SSH) connections or console logins, and API calls that expose high-risk functions can amount to substantive access to compute in AI infrastructure environments.[16] For instance, if a South Korean engineer can repeatedly invoke APIs such as "/train," "/fine-tune," or "/target-detection" against a model deployed in a U.S. data center to perform military- or security-related AI functions, this could result in a significant level of functional capability being transferred to and concentrated in a particular actor, even in the absence of any transfer of technical documentation. Nevertheless, current export control rules do not explicitly treat such API-based access to computation as an independent regulatory category, creating a gray area that will require dedicated discussion to design U.S.-South Korea joint governance mechanisms.[17]

Consequently, while an access-rights-based notion of transfer has been substantially codified in the field of data protection, the export control space remains anchored in a physical and act-based framework, creating potential regulatory misalignment. This misalignment should be addressed through close policy and governance coordination within the U.S.-South Korea alliance.

Compute Quotas: A New Policy Control Concept and Its Institutional Implications

Current export control regimes focus on acts of providing or disclosing technology and on the physical movement of equipment. The actual amount of compute used is not yet treated as an independent regulatory unit. Existing debates have mainly emphasized the number of GPUs and the performance of individual devices, but in practice, AI capability is determined by the cumulative compute quota—the total amount of AI compute resources that a particular actor uses over a specified period—consumed over time.[18]

Here, compute quota refers to the combination of usage time, the number of devices used in parallel, and workload intensity that yields functional capability. It is this capability that must become the object of control if the United States and South Korea are to manage substantive technology transfer and capability accumulation in a borderless infrastructure environment.

For example, assume that an identical configuration of 100 H100 GPUs is available. If one organization runs them for only two days on an experimental basis, while another organization uses the same configuration almost every day for six months to train large-scale models, the visible hardware is the same, but the magnitude and character of the AI capability accumulated are completely different. The former is likely to remain at the level of short performance tests or demos, whereas the latter can repeatedly train and refine massive models, rapidly building strategic-level AI capabilities that can be directly deployed for military and security missions such as precise target identification, situational awareness, and cyber operations automation.

This paper treats compute quota not simply as a technical measure, but as a policy concept that may help define the upper bound of permitted AI capability accumulation. Rather than controlling individual equipment movements, the idea is to manage the upper bound of AI functionality that a particular actor may accumulate. Instead of focusing solely on controlling physical transfers, the key question for export licensing and joint governance centers on how much AI compute will be permitted. Once compute quota is introduced as a concept, policymakers can move beyond asking about the destination and quantity of GPU exports and focus instead on how much countries, organizations, and projects use AI compute. This can serve as a useful policy tool for preventing specific countries or actors from concentrating and accumulating strategic AI capabilities over long periods.

At the same time, compute alone does not determine the quality or significance of a technology transfer. In practice, strategic AI capability also depends on model architecture, data quality and availability, engineering expertise, organizational learning, and the operational context in which systems are deployed. Compute quota should therefore not be understood as a universal proxy for all forms of AI risk, but as a policy handle that is most informative where sustained access to high-performance compute is coupled with frontier model training, capability concentration, and high-risk functional deployment. In other domains, such as narrow, data-limited applications or environments where talent and organizational capacity are the binding constraints, compute-centric controls should be supplemented by other regulatory instruments and risk indicators.

Institutional Gaps in U.S.-South Korea Export Controls

The export control systems of the United States and South Korea increasingly recognize that high-performance computing resources are a key determinant of AI capability. However, neither country has yet to institutionalize compute quotas as an independent control concept. The United States indirectly controls compute capacity through export restrictions on high-end GPUs and data center equipment, but regulations focus on performance thresholds and quantity limits for individual hardware items.[19] South Korea's system likewise centers on the

provision and transfer of technology, making it difficult to systematically capture the cumulative and continuous use of compute.[20]

As a result, if an actor maintains the same hardware configuration but conducts large-scale cumulative compute over an extended period, it can accumulate strategic AI capabilities within a regulatory gray zone. Even if GPUs are imported under an export license and then used to provide compute to a specific actor that far exceeds what was initially anticipated, current regimes have limited ability to detect or manage that change.

The compute quota concept addresses these gray areas and offers a starting point for U.S.-South Korea joint governance discussions. Concretely, this would mean shifting the regulatory focus from whether equipment has been brought in to who is continuously using how much compute, and incorporating compute quotas as a core variable in licensing, notification, and reporting frameworks. For allied countries, a tiered structure could be designed in which higher ceilings and more flexible operation are permitted, creating an institutional basis for the United States and South Korea to jointly monitor and manage the concentration of sensitive compute resources.

Borderless Strategic Assets and Zero Trust as a Policy Logic

Current export control systems rely primarily on *ex ante* regulation, through document submissions and licensing reviews, combined with *ex post* reporting and audits. This approach can be effective for controlling imports and exports of physical equipment, but it faces clear limitations in cloud-based AI infrastructure, where access to compute can shift rapidly. Once a license is approved, it is difficult to track and adjust, in real time, who is actually using how much compute under which conditions.

In the United States and Europe, regulators have already begun tightening controls on high-end AI chips and related technical data, while introducing requirements for companies to systematically retain and manage access logs and usage records for such data.[21] U.S. rules still focus heavily on whether technology has been provided or disclosed and whether license conditions have been complied with, so logs are commonly used for *ex post* audits and compliance checks.[22] Deemed export rules and interpretations on cloud and remote access likewise hinge on whether technical data has been "released," and therefore do not fully capture newer risks, such as API-based compute access or large-scale concentration of compute.[23]

The U.S. AI Diffusion Rule reflected some awareness of these access- and compute-based risks. The framework's conditions on transfers of advanced computing hardware included measures such as Validated End-User (VEU) status, clustering limitations, ongoing security and logging obligations, and restrictions on certain forms of model training and infrastructure use for non-allied destinations. These measures implicitly address aspects of AI infrastructure by tying hardware exports to monitoring, acceptable-use controls, and access management for a limited group of trusted countries, including South Korea. However, they remain fundamentally anchored in hardware export licensing and do not yet treat access-permission structures

and cumulative compute quotas as primary units of control in their own right. The approach proposed in this paper is therefore not a rejection of the framework, but an attempt to extend its logic by making access and compute explicit, first-order variables in U.S.-South Korea joint governance of AI infrastructure.

This paper draws on the Zero Trust concept from cybersecurity and applies it as a policy framework for export control and national security governance.[24] Zero Trust is the principle of not presuming that any person or organization is trustworthy, but instead verifying identity and authorization at each point of access and granting only the minimum privileges necessary for the task at hand. In this paper, Zero Trust serves as a conceptual framework for articulating where access should be allowed and where it should be restricted in a borderless AI environment.

Zero Trust's most stringent forms—continuous verification, fine-grained attribute-based policies, real-time enforcement, and strict compute ceilings—are particularly appropriate where access involves sensitive models, high-end training functions, defense-related applications, or high-risk APIs. By contrast, lower-risk collaborative research among trusted institutions in allied countries may warrant lighter application of the same principles, with greater reliance on *ex post* auditing and institutional safeguards. A risk-tiered application of Zero Trust thus offers a more realistic path for embedding access-centric controls into existing export control systems without imposing disproportionate burdens on benign innovation.

This perspective makes it possible to consider real-time access control as a new policy option, alongside existing document-based licensing. Incorporating real-time access control does not mean abolishing the existing licensing and reporting framework, but rather embedding the principles agreed at the licensing stage directly into data center access control and logging systems. This could involve: 1) assigning attributes such as nationality, affiliation, and project purpose to each account and role; 2) defining policies based on those attributes—for example, "Accounts of specified nationalities may not access training functions on high-end GPU clusters," or "Allied public research project accounts may use up to X GPU-hours per month"; and 3) recording and monitoring all access and compute usage in real time, so that access is automatically blocked and alerts triggered if predefined thresholds are exceeded. In such a system, principles agreed upon by regulators and companies are automatically enforced in data center operations.

As AI data centers become more sophisticated, U.S.-South Korea export control systems must be redesigned so that access entitlement structures, rather than physical borders, become the core unit of control. Building on existing document- and license-based systems, a step-by-step integration of Zero Trust and real-time access control offers a realistic and implementable policy pathway for dealing with AI infrastructure.

Expanding Export Control Norms to Reflect AI Functional Weaponization Risks

AI weaponization is not confined to software embedded in physical weapon systems such as autonomous lethal weapons. From the moment AI begins performing a range of military and security functions—such as target identification, situational awareness, decision support, and cyber operations automation—it functionally acquires a weapon-like character.[25]

Of course, physical weapon platforms such as autonomous unmanned aerial vehicles (UAVs) and ballistic missile systems have long been treated as core controlled items under existing export control regimes, including ITAR and EAR.[26] What this paper emphasizes, however, is that actors can use essential weapon functions such as target identification, route planning, and situational awareness solely through access to high-performance compute and sensitive data, negating the need for systems embedded in hardware. At this point, compute quotas and access-permission structures emerge as a new axis for controlling weaponization.

This kind of functional weaponization is possible even without transferring the source code or the model itself, relying instead only on access to compute resources and the operating environment. For example, if an actor merely secures access to an AI analysis system linked to sensitive sensor data, it can use that system to analyze and predict an adversary's military activities.[27] This is difficult to fully capture within the traditional export control regime, which is structured around the transfer of physical items and technical documentation.

Compute access, model deployment locations, and the degree of integration with military and intelligence systems must be examined as new control points. In other words, where a given model is deployed and who can use it should be treated as core variables in assessing functional weaponization risk. By doing so, debates on AI weaponization need not remain at the abstract level of ethics and norms; instead, the concepts of compute quota and access-permission structures can be directly connected to the concrete design of export-control and access-control mechanisms.

Conclusion and Policy Questions

As technologies and compute resources diffuse across borders, a U.S.-South Korea joint export control system—policy alignment plus joint governance—serves as a realistic alternative to effective AI export control.

From a compliance-practice perspective, a U.S.-South Korea joint approach can both mitigate AI weaponization risks and help reduce investment uncertainty for companies in allied countries. To this end, a new governance direction centered on compute quotas, access permissions, Zero Trust, and real-time access control can serve as a foundation for establishing future joint working groups and step-by-step policy alignment.

As a practical first step, the two countries should establish a joint working group to develop common standards for access logging, compute-usage monitoring (see Appendix B), and the

identification of high-risk AI functions in cross-border data center environments. A second priority should be to pilot a compute-quota-based governance model in a limited set of high-risk domains—such as military-relevant model training, critical-infrastructure AI systems, or dual-use intelligence applications—before considering broader deployment across other allied countries. These pilots would allow regulators and industry to test different logging architectures, threshold definitions, and enforcement mechanisms in a controlled setting, generating the empirical and institutional experience needed to scale up joint governance of AI infrastructure over time.

On this basis, there are several policy questions that policymakers and practitioners should consider in relation to U.S.-South Korea joint export control. In which domains and for which targets should the shift to compute-centric control be examined first? What criteria (roles, purposes, nationality, risk grades) are needed to treat access-permission structures, rather than physical borders, as the primary units of control? Under what conditions are access control using Zero Trust and real-time access enforcement implementable, and where do technological and legal limitations arise? If compute quotas are introduced as a policy variable, what thresholds, time periods, and project units are appropriate, and how should these be differentiated between allies and countries of concern? What could a U.S.-South Korea joint working group pilot first (for example, log standards, compute monitoring, criteria for identifying high-risk APIs)?

In short, as AI data centers advance, U.S.-South Korea export control laws should also be updated. This is not simply a matter of tightening existing rules, but of redesigning alliance-based national security governance by introducing access and compute as new units of control.

Appendix A. Explanatory Note on the Security Implications of GPU Counts and Compute Quotas

A.1. Why "The Same One Hundred GPUs" Can Mean Very Different Things

In the main text, this paper points out that the security implications differ between a scenario in which one hundred identical GPUs are distributed across multiple allied research institutions and one in which a single organization monopolizes them over a long period. The difference arises not from the physical number of devices, but from how compute is distributed or concentrated.

When 100 GPUs are shared among public research institutes or universities across several allied countries, the compute capacity available to each institution is limited, and research tends to be more diversified. In this case, total compute is distributed across many actors, so the likelihood that any single organization's strategic AI capabilities will leap forward rapidly is relatively low. By contrast, when the same 100 GPUs are concentrated for an extended period in a particular military agency, intelligence service, or state-owned research institute and repeatedly used to train frontier-level models, compute accumulates with a single actor, enabling the rapid development of large-scale models that can be directly applied to military missions such as target identification, situational awareness, and cyber operations.

A.2. "How Many Units" Versus "Who Uses How Much, and for How Long"

Traditional export control asks: "How many GPUs of what performance were exported to which country?" However, AI capability is better explained by the total compute used for a training run and the cumulative compute quota an organization uses over time. The key question thus shifts from "How many GPUs are there?" to "Which actor is using how much compute, for how long?"

A.3. Implications for the Design of U.S.-South Korea Export Control Regimes

This distinction suggests two main directions for the design of U.S.-South Korea export control regimes. First, regulations that focus solely on device counts and performance are insufficient to fully capture actual patterns of compute concentration in cloud-based and multi-tenant environments. Second, if compute quotas and their distribution are introduced as policy variables, it becomes possible to design more fine-grained ceilings on the strategic AI capabilities permitted to allies, friendly states, and countries of concern. Ultimately, even for the same 100 GPUs, security implications and policy responses must vary depending on whose hands they are in, what usage patterns they follow, and how long they are concentrated.

Appendix B. International Regulatory Trends on Logging, Compute Quotas, and Real-Time Control

B.1. Institutionalization of Logging and Record Management: Trends in Europe and the United States

In EU AI regulatory discussions, the EU AI Act (Regulation (EU) 2024/1689) requires providers of high-risk AI systems to automatically generate and retain logs of inputs, outputs, and system behavior, with the aim of ensuring traceability and explainability. The recordkeeping provisions of the U.S. EAR (15 CFR Part 762) impose broad retention duties that extend to electronic records and system-generated logs. For companies that handle controlled technical data in cloud or remote-access environments, the systematic management of access logs—showing who accessed which data, under what conditions, and when—is recognized as a key compliance element.

B.2. Limitations of the U.S. System and Directions for Improvement

Current deemed export rules and the EAR's concept of "release" largely preserve a traditional structure focused on the "transfer of knowledge" and the "disclosure of technology."[28] While this framework works reasonably well for regulating situations in which foreign persons gain access to technology through documents and source code, it is increasingly insufficient to capture AI-related risks that manifest in cloud environments primarily through execution and compute—especially high-risk API-based functional access and large-scale concentration of compute.

Recently, the Trump administration and major research institutions have been discussing ways to impose notification and reporting obligations on training runs for large models that use compute above certain thresholds, and to use such reports as a basis for monitoring AI capabilities. These discussions could be integrated with export licensing conditions so that compute quotas exceeding specific thresholds are subject to more stringent review, reporting, and restrictions. These directions should not be seen as a purely U.S. domestic matter but as issues for joint discussion within a U.S.–South Korea governance framework.

B.3. EAR Provisions on the Transfer ("Release") of Technical Data

Under 15 CFR § 734.15, technology is "released" to a foreign person when that person is permitted to inspect or receive it, including through access information such as passwords or decryption keys. Under 15 CFR § 734.19, transferring such access information may itself constitute a licensable activity. These provisions indicate that existing law already recognizes certain forms of access-enabled release but does not yet provide a sufficiently clear framework for AI-specific compute access scenarios, such as high-risk API-based functional use or large-scale compute concentration.

B.4. ITAR Provisions on Technical Data and Release

Under 22 CFR § 120.33, ITAR broadly defines technical data and treats the provision of access credentials to encrypted defense technical data as a potential release. This framework presupposes the importance of access logs and underscores that providing the means of access—not merely the data itself—can trigger export control obligations. The policy implication is that AI-specific access controls must be designed with this interpretive risk in mind.

B.5. Provisions on Technology Transfer Under South Korean Export Control Law and Their Implications

South Korea's export control regime—anchored in the Foreign Trade Act and the Public Notice on the Export and Import of Strategic Items—defines technology provision primarily in terms of active acts such as transfer of materials, training, and technical guidance. This framework has not yet explicitly captured access-based usage modes such as cloud access, remote API calls, or cumulative compute utilization as distinct regulatory units. Refinement is needed in three areas: 1) clear criteria for when cloud- and API-based usage constitutes strategic technology provision; 2) guidelines for managing access logs and compute-usage records for AI infrastructure; and 3) introduction of compute scale and access patterns as explicit variables in licensing and monitoring frameworks.

Endnotes

[1] Alexandra Alper and Stephen Nellis, "US Mulls New Rules for AI Chip Exports, Including Requiring US Investments by Foreign Firms," Reuters, March 5, 2026, https://www.reuters.com/world/us-mulls-new-rules-ai-chip-exports-including-requiring-investments-by-foreign-2026-03-05; Mackenzie Hawkins, "US Considers Requiring Permits for Nvidia, AMD Global AI Chip Sales," *Bloomberg*, March 5, 2026, https://www.bloomberg.com/news/articles/2026-03-05/us-drafts-rules-for-sweeping-power-over-nvidia-s-global-sales.

[2] South Korean Ministry of Science and ICT, "The AI Basic Act Comes into Force to Lay the Foundation for Korea to Become an AI G3," January 22, 2026, https://www.msit.go.kr/eng/bbs/view.do%3Bjsessionid%3DZT0iXB7mAiF9kdAY5Ak7c74gZdsb4OTVG2h47Huj.AP_msit_1?bbsSeqNo=42&mId=4&mPid=2&nttSeqNo=1214&sCode=eng.

[3] "S. Korea Begins GPU Rollout to Boost AI Research, Industry," United Press International, March 3, 2026, https://www.upi.com/Top_News/World-News/2026/03/03/gpu-distribution-industry-academia-research-institutions/9711772587666.

[4] Xiaoyang Zhang, "From COCOM to Wassenaar: Is It Still Our Way Ahead?" *Drexel Law Review* 15, no. 1 (2023): 47–119, https://drexel.edu/~/media/Files/law/law%20review/v15-1/Zhang%2047.ashx; "The Wassenaar Arrangement at a Glance," Arms Control Association, last updated February 2022, https://www.armscontrol.org/fact-sheets/wassenaar; *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies Volume I: Founding Documents* (Wassenaar Arrangement Secretariat, 2019), https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf.

[5] "Removing Barriers to American Leadership in Artificial Intelligence," January 31, 2025, https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence; The White House, *Winning the Race: America's AI Action Plan* (2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

[6] Ministry of Science and ICT, "National AI Strategy Policy Directions," September 26, 2024, https://www.msit.go.kr/eng/bbs/view.do?bbsSeqNo=42&mId=4&mPid=2&nttSeqNo=1040&pageIndex&sCode=eng&searchOpt=ALL&searchTxt; Government of the Republic of Korea, State Affairs Planning Committee, "National Agenda: Five-Year Plan of State Administration," June 2025, https://www.korea.kr/govVision/; "NVIDIA, South Korea Government and Industrial Giants Build AI Infrastructure and Ecosystem to Fuel Korea Innovation, Industries and Jobs," NVIDIA, October 31, 2025, https://investor.nvidia.com/news/press-release-details/2025/NVIDIA-South-Korea-Government-and-Industrial-Giants-Build-AI-Infrastructure-and-Ecosystem-to-Fuel-Korea-Innovation-Industries-and-Jobs/default.aspx.

[7] For examples of cross-border access patterns in multinational data center environments, see major cloud providers' regional infrastructure documentation, e.g., Amazon Web Services, Microsoft Azure, and Google Cloud's regional deployment and access control guides.

[8] European Data Protection Supervisor, "International Transfers," accessed April 28, 2026, https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en; "Data Protection Laws in

South Korea," DLA Piper, last updated January 20, 2025, https://www.dlapiperdataprotection.com/index.html?c=KR&t=law; "Understanding Korean PIPA: A Guide for Foreign Businesses," VeraSafe, July 31, 2024, https://verasafe.com/blog/understanding-korean-pipa-a-guide-for-foreign-businesses.

[9] See European Data Protection Supervisor, "International Transfers"; "Data Protection Laws in South Korea," DLA Piper.

[10] U.S. Bureau of Industry and Security, 15 C.F.R. §§ 730–774 (2026), https://www.ecfr.gov/current/title-15/part-730; International Traffic in Arms Regulations, 22 C.F.R. §§ 120–130 (2026), https://www.ecfr.gov/current/title-22/part-120; Foreign Trade Act, art. 19, amended by Act No. 13838 (January 27, 2016), https://elaw.klri.re.kr/eng_service/lawView.do?hseq=37529&lang=ENG; South Korean Ministry of Trade, Industry and Energy, "Public Notice on Export and Import of Strategic Items."

[11] For a definition of "release" of technology, see U.S. Bureau of Industry and Security, 15 C.F.R. § 734.15, https://www.ecfr.gov/current/title-15/section-734.15; Adnan Masood, "Export Controls and Advanced AI Systems in the United States," Medium, February 25, 2026, https://medium.com/@adnanmasood/export-controls-and-advanced-ai-systems-in-the-united-states-ear-itar-ofac-risk-in-models-cloud-35769edcdeaa; Bruce H. Leeds, "Storing Export Controlled Data in the Cloud: What's the Latest?" Braumiller Law Group, accessed April 28, 2026, https://www.braumillerlaw.com/storing-export-controlled-data-in-the-cloud-whats-the-latest.

[12] Masood, "Export Controls and Advanced AI Systems in the United States"; Leeds, "Storing Export Controlled Data in the Cloud: What's the Latest?"; Hanna Dohmen et al., "Controlling Access to Advanced Compute via the Cloud: Options for U.S. Policymakers," Center for Security and Emerging Technology, May 15, 2023, https://cset.georgetown.edu/article/controlling-access-to-advanced-compute-via-the-cloud/.

[13] As of early 2026, neither the U.S. EAR/ITAR nor South Korean strategic technology law explicitly defines API-based access to computation as a distinct regulatory category. See 15 C.F.R. § 734.15; 15 C.F.R. § 734.19; Dohmen et al., "Controlling Access to Advanced Compute via the Cloud: Options for U.S. Policymakers"; South Korean Ministry of Trade, Industry and Energy, "전략물자수출입고시 [Public Notice on Export and Import of Strategic Items]," MOTIE Notice No. 2025-37 (effective Dec. 31, 2025), https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A0%84%EB%9E%B5%EB%AC%BC%EC%9E%90%20%EC%88%98%EC%B6%9C%EC%9E%85%EA%B3%A0%EC%8B%9C.

[14] Masood, "Export Controls and Advanced AI Systems in the United States"; Leeds, "Storing Export Controlled Data in the Cloud: What's the Latest?"

[15] U.S. Department of Commerce, "Framework for Artificial Intelligence Diffusion," January 15, 2025, https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion; "Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024," 2024 O.J. (L 2024/1689) 1, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

[16] U.S. Department of Commerce, "Framework for Artificial Intelligence Diffusion"; U.S. Cybersecurity and Infrastructure Security Agency, "Executive Order on Improving the Nation's Cybersecurity," accessed April 28, 2026, https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity; "Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024."

[17] See C. Randall Pratt, "Cloud Computing and Deemed Exports," U.S. Bureau of Industry and Security, Advisory Opinion, January 11, 2011, https://www.bis.gov/media/1352.

[18] For EAR recordkeeping requirements, see U.S. Bureau of Industry and Security, 15 C.F.R. pt. 762, https://www.ecfr.gov/current/title-15/part-762; U.S. Bureau of Industry and Security, *Export Compliance Guidelines: The Elements of an Effective Export Compliance Program* (2017), https://www.bis.gov/sites/default/files/documents/ECP_0.pdf.

[19] U.S. Bureau of Industry and Security, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," October 13, 2022, https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor; U.S. Bureau of Industry and Security, "Framework for Artificial Intelligence Diffusion."

[20] Foreign Trade Act, art. 19; Ministry of Trade, Industry and Energy, "전략물자 수출입고시 [Public Notice on Export and Import of Strategic Items]," Notice No. 2023-231 (2023).

[21] "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024," Art. 12 (logging obligations for high-risk AI systems), Art. 19 (retention of logs), 2024 O.J. (L 2024/1689) 1, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng; U.S. Bureau of Industry and Security, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification"; U.S. Bureau of Industry and Security, "Framework for Artificial Intelligence Diffusion."

[22] U.S. Bureau of Industry and Security, 15 C.F.R. pt. 762 (EAR recordkeeping requirements); U.S. Bureau of Industry and Security, *Export Compliance Guidelines: The Elements of an Effective Export Compliance Program*.

[23] U.S. Bureau of Industry and Security, 15 C.F.R. § 734.15 (defining "release" of technology), https://www.ecfr.gov/current/title-15/section-734.15; 15 C.F.R. § 734.13(b) (deemed export—release of controlled technology to a foreign person within the United States); Masood, "Export Controls and Advanced AI Systems in the United States"; Leeds, "Storing Export Controlled Data in the Cloud."

[24] Scott Rose et al., *Zero Trust Architecture* (National Institute of Standards and Technology, 2020), https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf; Cybersecurity and Infrastructure Security Agency, "Executive Order on Improving the Nation's Cybersecurity," accessed April 28, 2026, https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

[25] Will Shumate et al., *Export Controls on Artificial Intelligence and Uncrewed Aircraft Systems* (RAND, February 2026), https://www.rand.org/pubs/research_reports/RRA3296-1.html; Mark Bromley and Giovanna Maletta, *The Militarization of Technology: Preventing Diversion and Misuse Through Export Controls* (Stockholm International Peace Research Institute, 2025), https://www.sipri.org/sites/default/files/2025-11/rpp_2025_11_miltech.pdf.

[26] U.S. Department of State, 22 C.F.R. § 121 (2026), https://www.ecfr.gov/current/title-22/part-121 (Category VIII: Aircraft and Related Articles, including UAVs); U.S. Bureau of Industry and Security, 15 C.F.R. § 774 (2026), https://www.ecfr.gov/current/title-15/part-774 (ECCN 9A012: UAVs and related systems); "Missile Technology Control Regime Equipment, Software and Technology Annex," Missile Technology Control Regime, https://www.mtcr.info/en/mtcr-annex.

[27] Shumate et al., *Export Controls on Artificial Intelligence and Uncrewed Aircraft Systems*; Bromley and Maletta, *The Militarization of Technology: Preventing Diversion and Misuse Through Export Controls.*

[28] 15 C.F.R. § 734.15 ("release" of technology or software to a foreign person); 15 C.F.R. § 734.13 (export of technology and software); Export Administration Regulations (EAR), 15 C.F.R. pt. 734 (scope of the EAR, including definitions of "release" and "transfer").