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]."