July 2023

Strengthening ROK-US Critical Technologies Cooperation: Progress and Path Forward

Authors and Editors:
Mark Bryan Manantan and Soyoung Kwon, Ph.D.

Sungmin Cho, Ph.D.
June Park, Ph.D.
Lami Kim, Ph.D.
Alexandra Seymour
Boyoung Kim, Ph.D.

PACIFIC FORUM INTERNATIONAL

GEORGE MASON UNIVERSITY
Korea

July 2023

Strengthening ROK-US Critical Technologies Cooperation: Progress and Path Forward

Authors and Editors:
Mark Bryan Manantan and Soyoung Kwon, Ph.D.

Sungmin Cho, Ph.D.
June Park, Ph.D.
Lami Kim, Ph.D.
Alexandra Seymour
Boyoung Kim, Ph.D.

PACIFIC FORUM
INTERNATIONAL

GEORGE MASON UNIVERSITY
Korea

About the Pacific Forum

Based in Honolulu, the Pacific Forum is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, the Pacific Forum collaborates with a broad network of research institutes from around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region. The Forum's programs encompass current and emerging political, security, economic, maritime, and technology policy issues, and work to help stimulate cooperative policies through rigorous research, analyses, and dialogue.

All facts, positions, and perspectives contained in this report are the sole responsibility of its authors and do not reflect the institutional views of the Pacific Forum or its board, staff, or supporters.

The Pacific Forum

Web: www.pacforum.org
Facebook: Pacific Forum
Twitter: @PacificForum
Instagram: @pacforum
Podcast: Indo-Pacific Current
Email: pacificforum@pacforum.org

Acknowledgements

Pacific Forum is grateful to the experts and practitioners for participating in the US-ROK Science and Tech Collaboration in Critical Technologies Dialogue (2022) supported by the Republic of Korea (ROK) Consulate-General of Honolulu, Hawaii, USA. This publication was made possible by the Center for Security Policy Studies, George Mason University Korea.

SCHAR SCHOOL OF POLICY AND GOVERNMENT
Center for Security Policy Studies
at George Mason University

About Center for Security Policy Studies – Korea (CSPS-K)

The Center for Security Policy Studies (CSPS) of Schar School of Policy and Government at George Mason University is a research center and academic hub that seeks solutions to today's pressing security challenges and educate tomorrow's security policy makers. Located at Mason's Arlington campus, CSPS provides unique access to defense and security experts, government officials, prominent think tank analysts and scholars.

Launched in 2019 at George Mason University's Korea campus, the Center for Security Policy Studies – Korea (CSPS-K) serves as a branch institute to liaise the policy world of Washington and Seoul and to provide diversified perspectives on both traditional and non-traditional security issues that warrant global attention. Every year, CSPS-K takes a different theme ranging from traditional security issues such as interstate conflict, regional security relations, and nuclear proliferation to non-traditional issues such as climate change, refugee crises, gender, human rights, and pandemics. This year's CSPS- K theme explores the <the challenges of New Technologies and the future of the US-ROK Alliance>.

Center for Security Policy Studies-Korea

George Mason University Korea
G636, 119-4 Songdomunhwa-ro, Yeonsu-gu
Incheon, Korea 21985
Email: csps2018@gmail.com
Website: https://csps.gmu.edu/csps-korea/

Table of Contents

About the Authors

Soyoung Kwon, PhD EDITOR

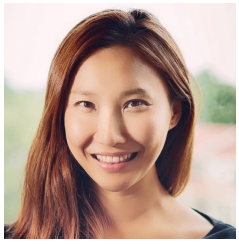
Dr. Soyoung Kwon is Associate Professor of Global affairs and Director of Security Policy Studies Korea at George Mason University. Prior to joining George Mason University Korea, she taught at Graduate School of International Studies at Kyung Hee University, Chunbuk National University, and Yonsei University. She began her academic career as a research associate fellow at the East Asia Institute of Cambridge University and a Shorenstein fellow at the Asia Pacific Research Center of Stanford University. Dr. Kwon then moved on to the government and policy sectors to serve as a spokesperson for foreign correspondents at the Ministry of Unification of Republic of Korea and as a Korea specialist and advisor on the EU-Korea relations at the European Parliament in Brussels. Dr. Kwon holds a B.A. in political science and diplomacy from Ewha Woman's University and a M.Phil and Ph.D. from the University of Cambridge.

Sungmin Cho, PhD

Dr. Sungmin Cho is a professor at the Asia-Pacific Center for Security Studies (APCSS), an academic institute of the US Department of Defense. His area of expertise covers US-China competition, Chinese politics, and the geopolitics of Northeast Asia. Dr. Cho has published articles in peer-reviewed journals, including World Politics, Journal of Contemporary China, The China Journal, Asian Security, Journal of Indo-Pacific Affairs, and Korea Observer. His policy analysis also appeared in Foreign Affairs, The Washington Quarterly, and War on the Rocks. Dr. Cho contributed commentaries at the invitations of CSIS, Brookings and other think tanks. Prior to his academic career, Dr. Cho served in the Korean Army as an intelligence officer for three years, including a seven-month deployment to Iraq. He earned Ph.D. in Government from Georgetown University, M.A. in International Relations from Peking University, and B.A. in Political Science from Korea University.

June Park, PhD

Dr. June Park is a political economist (PhD in Political Science, Boston University, 2015) working on the geoeconomics of conflict in the digital economy, observing East Asia, the US, Europe and the Gulf. She focuses on trade, energy and tech conflicts among nation states as they navigate their distinctive paths into the digital future. Her current work pertains to geoeconomic conflicts in emerging technology, i.e., semiconductors, EVs/batteries, digital currencies and AI. She is an inaugural Asia Fellow of the International Strategy Forum at Schmidt Futures, finalizing her first book manuscript, DIGITAL TRADE WARS & CURRENCY CONFLICT: China, South Korea and Japan's Responses to US Protectionism since COVID-19, and an external expert for the Center on East Asia Policy Studies (CEAP) of the Foreign Policy Program at the Brookings Institution. She served as a 2021-2022 Fung Global Fellow at the Princeton Institute for International and Regional Studies (PIIRS) at Princeton University.



Lami Kim, PhD

Dr. Lami Kim is former Assistant Professor at the US Army War College and an adjunct fellow at Pacific Forum. Her research interests include the intersection between civil and military uses of nuclear energy, China's nonproliferation and nuclear export policy, and politics and security on the Korean Peninsula and in East Asia. Previously, Lami served as a South Korean diplomat and a research fellow at Harvard's Belfer Center, Pacific Forum, Stimson Center and Seoul National University Asia Center. She has taught at Harvard University and Boston College. Her works have been published in The Washington Quarterly, the Bulletin of the Atomic Scientists, The Diplomat, PacNet, and Stimson Center, among others. Lami holds a master's and PhD in international affairs from the Fletcher School of Law and Diplomacy at Tufts University and a master's degree in Middle Eastern studies from Harvard University.

About the Authors

Alexandra Seymour

Alexandra Seymour was previously an Associate Fellow for the Technology and National Security Program at the Center for a New American Security. Her work focused on artificial intelligence (AI), defense innovation, semiconductors, 5G/6G, and workforce issues. Prior, Seymour was Chief of Staff at CalypsoAI, an AI security startup. She also served in the Pentagon as Speechwriter to the Deputy Secretary of Defense and in OSD(Policy), as well as on the National Security Council. Seymour's analysis and commentary have appeared in publications such as The Financial Times, BBC News, WIRED, USA Today, The Hill, DefenseScoop, The Diplomat, RealClearPolicy, National Journal, South China Morning Post, and Voice of America, and she has made media appearances on CBS News and NewsNation, among other outlets. Seymour is also a Visiting Fellow at the National Security Institute at George Mason University.

Boyoung Kim, PhD

Dr. Boyoung Kim is a research professor at the Center for Security Policy Studies-Korea, George Mason University Korea. Dr. Kim's research background is in cognitive and social psychology, with the main focus on moral judgments and decision-making. In her interdisciplinary work, she investigates ethical issues related to the advancement and application of emerging technologies, including Artificial Intelligence, social robots, and autonomous vehicles. She was a postdoctoral researcher at the United States Air Force Academy's Warfighter Effectiveness Research Center and George Mason University's Department of Psychology. Dr. Kim received a Ph.D. in Psychology from Brown University, a Master of Science in Experimental Psychology and a Bachelor of Arts in Psychology Intensive Program from Korea University.

Mark Bryan Manantan EDITOR

Mark Bryan Manantan is the Director of Cybersecurity and Critical Technologies at the Pacific Forum. At the Forum, he currently leads the Cyber ASEAN initiative, and the US Cyber, Technology, and Security partnerships with Japan, Australia, Taiwan, and South Korea. Mr. Manantan is also a non-resident fellow at the Center for Southeast Asian Studies, National Chengchi University, Taiwan, and formerly a research consultant at the Asia Society Policy Institute, Washington, DC. He has held visiting fellowships at the Japan Foundation, the Center for Rule-Making Strategies at Tama University in Tokyo, Japan, and the East-West Center, Washington, DC. Prior to that, he was a media, public relations, and advertising executive for Procter & Gamble, Wells Fargo, Aboitiz Equity Ventures, and UNICEF.

Introduction

The US–South Korea Relations: Strengthening Science and Tech Collaboration Amid Turbulent Times

Mark Bryan Manantan and Soyoung Kwon, PhD

It was the nightcap treat that nobody quite expected. Donning a black bow tie and tuxedo jacket, South Korean President Yoon Suk Yeol got the mic and sang his own rendition of the popular Don Mclean song, American Pie, at the White House State Dinner hosted by US President Joe Biden.[1] The mood was celebratory, after all, the United States-Republic of Korea (ROK) alliance has survived and continues to show signs of progress after 70 years since the Mutual Defense Treaty between Washington and Seoul was inked after the Korean war.

The milestones were not just symbolic. Practical outcomes resulted from President Yoon's six-day visit to the US, which include the deployment of nuclear-armed submarines to South Korea to deter Kim Jong Un's nuclear threats and ironing out wrinkles within the alliance. After much-protracted negotiations, Biden and Yoon finally straightened a new cost-sharing arrangement. This serves as an upgrade for the bilateral relations, transforming the perceived asymmetry between the US and ROK where the latter acquires equal status and responsibility. Getting the house in order is warranted for Washington and Seoul as the alliance adjusts to the unpredictable headwinds of economic and political fragmentation driven largely by great power rivalry. As the US goes full-throttle to confront China far beyond the military domain to include critical industries that will define the fourth industrial revolution, a gradual wholesale shift in the US-ROK alliance is on the horizon.

The Biden administration's passage of the Science Act and Chips Act certainly affirms the revival of old-fashioned industrial policy aimed to restrain China's ascent to global technological

dominance. As the US partially walks away from the rule-based economic order and inadvertently blurs the clear-cut distinction between protectionism and national security, South Korea is faced with stark choices: decoupling from China and /or joining the US-led chorus of onshoring and friend-shoring campaign.

Granted that the US can delay China's acquisition of advanced tech capabilities at least in the short-to-medium term using export controls and draconian industrial policies, particularly on semiconductors, South Korea is confronted with a plethora of uncomfortable scenarios. The confluence of political security and economic realities now suggest that South Korea must navigate two treacherous terrains: on the one hand backing US protectionist policies aimed to stifle China's technological upgrade while on the other, shielding its industries from possible Chinese economic retaliatory measures that have skin in the game.

While the US has put its unilateral bet on decoupling and onshoring, South Korea is still in a bind with Chinese coercive economic statecraft. Like most economies in East Asia, Seoul's hands are tied given the close complementary of its industries to China. Although South Korea has started to lessen its exposure to the Chinese market by relocating some of its supply chains to Southeast Asia and India, this will still take time. But considering the high stakes for closer cooperation between the US and South Korea following the revitalization of the alliance, the pertinent question, therefore, are

- **How can the US and South Korea arrive at a state of equilibrium to pursue mutual goals given their highly entrenched economic interdependence with China?**
- **Looking more closely, how should policymakers recalibrate the pace and dynamics of the US-South Korea alliance when economic security and technological disruptions intertwine further with existing geostrategic challenges?**
- **Furthermore, how can the US and South Korea tap into the opportunities and overcome challenges to achieve technological collaboration in critical and emerging technologies?**

Taking stock of these three-interrelated questions, Pacific Forum, in partnership with the Consulate of the Republic of Korea, Honolulu and the Center for Security Policy Studies of George Mason University convened a roundtable meeting among Korean, American, and regional experts to reflect on the opportunities and challenges of the renewed US-ROK bilateral relations against the larger geostrategic backdrop characterized by the rapidly deteriorating international

trade environment and the emerging geo-technological competition. Building on cross-cutting deliberations and key outcomes of the two-day closed-door workshop, "US-South Korea: Strengthening Science and Tech Collaboration" held in Honolulu, Hawaii in November 2022, this edited volume seeks to complement ongoing deliberations to carve practical pathways for US and South Korea's renewed cooperation. To tackle such a huge policy challenge, authors were encouraged to calculate the trade-offs of a closer US-South Korea tech collaboration as overtures of decoupling and friend-shoring incite enthusiasm and optimism for a new trusted trade or tech bloc to prosper that obviously cuts China. Authors were also tasked to formulate new configurations of alliance cooperation in new territories—particularly in critical and emerging technologies—that emphasize the comparative advantages of Washington and Seoul but also possible sources of friction that may damage trust. Throughout this concerted thinking, authors were to be mindful of the larger geostrategic powerplay and the shadow of North Korea's imminent and evolving threat.

Setting the tone for the entire publication, Dr. Soyoung Kwon leads the edited volume by mapping the evolution of the US-ROK relations over the past seventy years. Beyond just taking readers down memory lane, Kwon's essay takes a forward-leaning approach by revisiting the past and present of the security relationship. Kwon challenges the US-ROK alliance to be nimble and agile by expanding the purpose of the alliance beyond just deterring North Korea to incorporate the unprecedented challenges of non-traditional security issues from energy security, supply chain resilience, and critical technologies like AI and cybersecurity.

Dr. Sungmin Cho and Dr. June Park ride the wave of Kwon's challenge for agility as they dive deeper into the murky issue of friend-shoring or onshoring with particular attention devoted to semiconductors and the formation of a US, Japan, South Korea, and Taiwan coalition on the prized chips dubbed as Chip 4. The two authors offer distinct yet complementary perspectives.

Cho argues that the trend of decoupling especially in the high-tech sector is irreversible and that middle-power countries like South Korea must either thrive or perish. For its part, South Korea is still on a high-balancing wire because China remains an important source of raw materials and a market for its semiconductors. But Cho sheds light on why South Korea may soon be pulled closer to the US orbit of tech alliances such as Chip 4 despite its dependence on China. His argument is based on the following observation: First, the US is still perceived as the leader in setting standards in cutting-edge technology although China is still catching-up. Second, China, over time, has grown more dependent on South Korea's semiconductor juggernauts like Samsung and SK Hynix despite its push to develop its national chip champions.

Any punishment from Beijing may hurt Chinese companies too. Cho's contribution thus inspires confidence that conditions are ripe for decoupling and that South Korea is fully on board with the eventual formation of Chip 4.

Park's argument, however, heeds for prudence to assess the true merits of Chip 4 and whether it can truly deliver equal partnerships. For Park, the issue lies in the "disillusions of expected synergy" between US and South Korean firms. That the overriding principles of free and fair trade are still paramount. To persuade South Korean firms to be truly on-board Chip 4, US policymakers should ensure that protectionism and national security do not trump commercial interests. Cho and Park in unison advance the need for greater consultation between Washington and Seoul to improve transparency and trust to avoid unintended consequences that may damage ongoing collaboration. Park further adds that a review of the subsidy eligibility criteria and conditions of the CHIPS and Science Act should be a priority and a good starting point to make such a partnership a reality.

Diving into the specifics and feasibility of stronger US-ROK Science and Tech collaboration, Dr. Lami Kim, Dr. Alexandra Seymour, and Dr. Boyoung Kim tackle the progress and prospects of Washington and Seoul in critical fields of Fifth Generation Wireless Technology (5G), AI, and Robotics.

Kim sounds the alarm on the urgency for the US and South Korea to compete with China's dominant footprint in the 5G market. Her primary concern is that if China continues to gain clout in 5G it will soon build most of the Global South's digital infrastructure, which serves as the backbone of the emerging data-driven global economy. Kim lauds the efforts of the US and South Korea to promote the Open-Radio Access Network (RAN) as an alternative but contends that more needs to be done. To catch up with China's first-mover advantage in 5G, the US and South Korea's policy interventions should focus on developing talents and international technical standard-setting.

Echoing Kim's recommendations, Alexandra Seymour's writing on AI collaboration is premised on three important steps: harnessing the US and South Korea's comparative advantages in innovation capacity and talent pools; leading global discussion on the adoption of AI norms and standards anchored on democratic governance frameworks and; implementing or operationalizing often nebulous terms or concepts of AI governance like AI trustworthiness or AI explanability through actual and rigorous training and evaluation models. Extending the positive outcomes of the Biden-Yoon summit, Seymour signs off with tangible recommendations on AI cooperation, including the need for a data-sharing agreement for AI-enabled military applications.

Boyoung Kim's exploratory paper on US-ROK cooperation on Robotics goes beyond the conventional application of robotics in the military setting. She contends the need to look elsewhere for inspiration if the US and South Korea genuinely intend to have a fruitful and sustainable collaboration in the field of robotics. As a psychologist, she offers theories of trust in human-robot interaction as one of the possible bedrocks to establishing strategic collaborations in research & development, deployment, and evaluation of robotics. Kim welcomes the recent outcomes of the Biden-Yoon summit as a positive step that highlighted the role of autonomous robots as a field of critical technology, and suggests further expansion of current channels of collaboration at the technical, policy, and strategic levels.

Finally, rounding up the edited volume is Mark Bryan Manantan's article on North Korea's cybercrime and its role in funding Pyongyang's Weapons of Mass Destruction programs—a key observation made during the Biden and Yoon summit. Noting that North Korea is intentionally finding innovative means to access high-value technologies, Manantan investigates how North Korea's tech-savviness in repurposing and refining its cyber arsenal to launch ransomware attacks in exchange for cryptocurrencies fuels its military technology development. He specifically examines North Korea's integration of AI-enabled cyber capabilities that has the potential to further disrupt, degrade and even compromise supply chains. With such new and improved capabilities, North Korea does not only threaten the current momentum of US-ROK cooperation in critical technologies but also the entire innovation ecosystem.

As US and South Korean policymakers grapple with the enormity of the challenges, the modest aim of our edited volume is to offer insightful and cross-cutting ideas to implement the aspirations of the alliance. Each author offers actionable policy recommendations anchored on the pragmatic and collaborative themes of trust and transparency to guide Washington, Seoul, as well as other allies and partners in the Indo-Pacific to achieve technical, policy, and strategic equilibrium. With the alliance embarking on a new chapter, a different breed of US-ROK alliance is now needed—one that is future-proof to steer clear of the turbulent times ahead.

[1] Mary Yang, "Nuclear Deterrence by day, noraebang by Night. This head of state does both", NPR News, April 27, 2023. https://www.npr.org/2023/04/27/1172613834/yoon-suk-yeol-south-korea-president-united-states-visit-biden-musk

The US-ROK alliance: Past, Present, and Future

Soyoung Kwon, PhD

The US-ROK alliance is a key partnership between the United States and South Korea for promoting regional stability and security in Northeast Asia. It is primarily based on the Mutual Defense Treaty, signed in October 1953 following the Korean War. This bilateral security alliance, though asymmetrical, worked as a security guarantee for South Korea against the spread of communism and aggression of North Korea and China. The strong and firm security relationship, featuring stationed US troops, US-Korea joint training, and the US nuclear umbrella in South Korea, worked as an effective deterrence against North Korea's attack.

Since the 1990s, there has been growing demand for autonomy in security as well as conflicting progressive or conservative discourse in Korea over the US-ROK alliance. A change of administration with different political orientations would view the US-ROK relationship and inter-Korea relations differently, which directly affected the perception of threat and the level of reliance on the US. The division of opinion has manifested over the issues of the wartime operational control, negotiations for cost-sharing of the US Forces stationed in Korea, the combined defense posture, and relocation of the US bases. Yet, it never shook the core purpose of the alliance and its foundation based on common vision, values, and purpose.

The US-ROK alliance at 70 faces a new security environment that features the US-China rivalry, the rise of competition in critical and emerging technologies, and a revolution in military affairs based on artificial intelligence as seen in the Ukraine war. Since the new trends obscure the distinction between security and economic interests and between the areas of competition and cooperation, the common interests in the US-ROK alliance need to be redefined.

Addressing the question of "why alliances endure or collapse?", Stephen Walt points out four critical factors: 1) common interests and goals, 2) dependability and credibility in commitments,

3) equity in benefits and costs of the alliance, and 4) domestic politics with strong domestic support.[2] The status of the US-ROK alliance shows some signs of challenges in these areas. Divergent interests that lead to disagreements over policy and trade imbalances can undermine the security commitment based on common interests. Mixed messages, misguiding gestures, and unclear conversations can undermine the dependability and credibility of the allies. The financial pressure can also pose questions on the benefits and costs of the alliance. The new security issues add uncertainty to existing dynamics in the relationship. The endurance or collapse of an alliance depends on a complex interplay of the factors mentioned, and there is no simple formula for predicting the outcomes. However, by understanding these factors, policymakers can work to strengthen the relationship and mitigate the risks of collapse. The US-ROK alliance is at a historic juncture to rethink opportunities and challenges, through which it can navigate towards future-oriented cooperation.

The Origin and Evolution of the US–ROK alliance: Common Interests

The history of the US-ROK alliance could be traced back to the 1950s when the US recognized the strategic importance of the Korean peninsula in the Northeast Asia region as the testing ground for its capability to stop communist expansion. Following the 1953 Armistice Agreement that brought about a ceasefire in the Korean War, the Mutual Defense Treaty was signed between the US and ROK, with both states agreeing to protect each other in case of external attacks or aggressions.[3] During the Cold War, it was vital for the US to establish a bilateral alliance with countries in the East Asian region as "pacts of restraint."[4] The geopolitical strategic importance of East Asia served the purpose of the US alliance system in deterring communist aggression and maintaining regional stability.

The security environment in Northeast Asia rapidly changed after the Cold War. The focus of the alliance soon changed from blockading communism to impeding China from growing to be a regional hegemon.[5] Washington saw that China would be enlarging its military capabilities and engaging in overt conflict against its neighboring states to pursue regional hegemony, which can potentially destabilize regional peace and weaken US influence over the region.[6] North Korea's military provocations and nuclear proliferation further fomented an unpredictable and vulnerable security environment in the region. The Joint Vision between the US and South Korea affirmed their commitment to build a constructive alliance based on "common values, trust, and peace" to bring security, stability, and prosperity in the East Asian region.[7]

The US-Korea alliance, however, has gone through some dramatic changes during the Trump-Moon administration (2017-2020). The Trump administration stated: "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity." and "North Korea's continued provocations would prompt neighboring countries and the United States to further strengthen security bonds and take additional measures to protect themselves."[8] South Korea, on the other hand, saw China as an important economic partner rather than a security threat. The perception towards North Korea changed positively by the Moon Jae-In administration that advocated peace initiatives and improved inter-Korea relations. As a result, South Korea was hesitant in sharing the vision of the US Indo-Pacific strategy or the Quad. Caught between the Chinese economy with the United States, ROK was stuck with two difficult choices.

While the US position over its strategic interest and purpose of the alliance remained fairly constant, South Korea's perception of the alliance has fluctuated due to domestic politics. The turning point was the inter-Korean summit of 2000, where leaders of the two Koreas met for the first time in history. Scott Snyder noted: "Upon Kim Dae-Jung's return from the North, he declared that his visit had forestalled the possibility of war on the Korean peninsula. Although this statement was widely regarded as overoptimistic, it served to both validate and facilitate a transformation of South Korean public perceptions of the North from the image of the enemy to that of brother-in-need. Such a transformation carried with it a subtle implication for South Korean public perceptions of the US force presence in the ROK from that of necessity to extravagance or even a legacy of the past era of inter-Korean conflict."[9]

The main issues of contention have been the equity in the relationship and the credibility of the US commitment. The progressive governments (2003-2007; 2017-2022) asked for some adjustments in the US-ROK alliance including downsizing the US troops, relocation of US bases in Korea, and a transfer of wartime operational control (OPCON) from the Combined Forces Command (CFC) to the ROK Joint Chief of Staff.[10] This aligned with Korea's desire to achieve self-defense and a symmetric alliance. The conservative governments (2008-2012; 2013-2017) prioritized consolidation of the US-ROK alliance reaffirming the intent to restore based on established friendship. These administrations also advocated an agreement on the condition-based transition of wartime operational control, negotiations for cost-sharing of US Forces Korea, and upgrading the alliance's combined defense posture. In 2014, the Park Geun-Hye administration declared "the indefinite delay of OPCON transfer until some point in the mid-2020s" and made decision to retain a US-ROK Combined Division and the US counter-fire forces north of the Han River."[11] The Moon administration called for a retake of wartime operational control and relocation of CFC. The CFC finally moved from Seoul to a military complex in Pyeongtaek, 65 kilometers south of Seoul. The OPCON transfer, originally scheduled for 2022, did not happen.

The alliance quickly deteriorated over the cost-sharing agreement for US military presence in South Korea. The controversies over the Special Measures Agreement (SMA), which is a bilateral negotiation platform between the US and ROK to discuss cost sharing of USFK, intensified in 2019 when the Trump administration demanded South Korea to pay US$5 billion for USFK's stationery. This was an unprecedented fivefold increase from the previous year. With both sides failing to reach an agreement, 4,000 Korean employees in USFK bases had to take unpaid leave in April 2020. In the wake of the SMA controversy, leftist media outlets in South Korea questioned the role of the US-ROK alliance and presence of US troops in the country.[12] This issue became a source of tension in the alliance and a loss of credibility in US intent and commitment. Trump's claims on possible withdrawal of US troops from Korea, scaling back joint exercises, and burden-sharing pressure adversely affected the public's views of the US and the credibility of the US-Korea alliance as a security guarantee.[13] To make matters worse, the US overture to North Korea by the Trump Administration was not fully coordinated with South Korea, nor aligned with its approach. The Moon administration's National Security Strategy once gain accentuated South Korea's autonomy on self-defense capability and peace settlement in the Korean peninsula, creating a discourse of strategic alliance that calls for partnership rather than asymmetrical alliance.[14]

The US-ROK alliance has remained in Cold War premises, structures, and patterns of interaction, but no serious effort had been made to review and update the strategic framework. South Korea's demands for equity and autonomy as well as call for transforming asymmetric alliance into strategic partnership (i.e. Israel) invite inquiry on the existing framework of the security relationship.

Security Issues and Challenges: Old & New

The long-standing dispute over the cost of US military presence in South Korea was finally settled in 2021 by President Biden and the incumbent South Korean President Yoon Suk Yeol, as the two countries signed a new cost-sharing agreement. The Biden-Yoon administration is coordinating the security relationship within the context of the Indo-Pacific strategy to meet the changing international order and changing nature of threats. The South Korean public's view on the need for the US-Korea alliance, the US troops stationed in Korea, and confidence in US defense has been strongly positive.[16] The alliance is strengthened in recent years through enhanced joint military exercises and intelligence sharing, along with increased economic and diplomatic cooperation. Building on such positive momentum, the Biden-Yoon summit last May boosted the alliance, giving South Korea equal status.

Charting a Path Forward

While the alliance remains strong and important for both the United States and South Korea, there are new issues to be addressed to advance the future-oriented US-ROK alliance. First, the focus needs to expand beyond the traditional purpose of the alliance - deterring North Korea and China - or the extended deterrence based on the US nuclear umbrella. It needs to incorporate non-traditional security issues that are becoming increasingly important in the region and the world. These issues include AI, cyber security, supply chain, energy security, climate change, etc. They have a direct impact on stability and security of the region, as they can lead to conflict with the neighbors or with the great powers. In the case of the Korean Peninsula, both hard security and non-traditional security are at play, which proves that the alliance must be more alert in defining what is in the security policy topics. By prioritizing non-traditional security topics and global agendas, cooperation between the two countries will likely encourage more equal security partnership based on mutual respect and benefits.

Another area where the alliance could develop its cooperation includes emerging sectors such as technology and clean energy. New security issues related to critical and emerging technologies (CETs) invite a new agenda for the future of the US-ROK alliance. China has become a serious competitor in the emerging technologies to the US with increased capacity and opportunities. The technological rise of China has changed the US' threat perception as reflected on its national security goals. In the midst of technological competition in the region, where China invests heavily in AI, 5G networks, and quantum computing, the US-ROK alliance should find measures to work together to develop capabilities to maintain strategic edge and effective cybersecurity measures.

In commemorating the 70th Anniversary of the US-Korea Mutual Defense Treaty, the key question is how the two allies can better improve technical, policy, and strategic collaboration as equal partners in the field of science and technology. A new referent object of security always accompanies unprecedented challenges and opportunities. And the nature of novelty pushes us to place the issues within the traditional realist thinking of security until the stakeholders find the need for cooperation. High-tech cooperation, therefore, will take time to find a common ground in science and technology partnerships within the existing frame of alliance.

Recommendations

The US-ROK alliance should take a collaborative and forward-thinking approach to new security issues including emerging and critical technologies. Identifying the areas that can facilitate collaboration and tech cooperation is the first step. It can be summarized as follows:

- Joint Research and Development (R&D): the US and ROK can invest in joint R&D of emerging and critical technologies such as AI, quantum computing, and 5G networks. This would allow the two countries to share expertise and resources and accelerate innovation in these areas to advance their capabilities.
- Shared standards and regulatory frameworks: the US and ROK can work together to establish global standards for CETs and shared regulatory frameworks which will help ensure that these technologies are interoperable, safe, and secure without being misused.
- Joint cybersecurity measures: the US and ROK can work together to enhance their cybersecurity cooperation, particularly in the areas of critical infrastructure protection, information sharing, and joint cyber exercises.
- Technology supply chains: the US and ROK should coordinate to strengthen their technology supply chains, calibrate dependence to China while ensuring secure and reliable access to critical technologies.

The spill-over effects of the US-China rivalry and the recalibration of the traditional alliance system on tech cooperation may create more problems than solutions. The intensifying US-China tech competition for influence and hegemony has created diplomatic and economic challenges to the countries in the region that are pressured to join the technology alliances and decoupling policy to exclude China from its high-tech supply chain. There is also a deep-seated concern that the tech cooperation is framed within the asymmetrical security relationship between the US and Korea. The new paradigm of cooperation such as Chip 4 alliance is blurring the balance between security and economic interests, thus causing economic insecurity and technological nationalism. It also raises questions of trust and credibility, which could adversely impact the US-Japan-Korea relations.

Conventional International relations assert that an alliance endures when there is a common threat perception, shared goals, mutual trust, and domestic political support. But the formation of tech alliances or let alone tech partnerships are far more complicated and requires complex preconditions for such arrangements to transpire. This strikes at the heart of the viability of friend-shoring considering the US, South Korea, Japan, and Taiwan have tech companies

and enterprises competing for profit and innovation. The challenge is finding a pragmatic and sound approach between competition and cooperation to ensure that all players reap the benefits and minimize risks or frictions. Therefore, it is necessary to understand the divergent interests and discuss how to compensate for each other's weaknesses. For this, there must be better coordination and communication, particularly from the US, to clarify the purpose and objectives of the high-tech alliance rather than imposing 'friend-shoring". Building trust among the stakeholders is very much needed for tech cooperation to move forward within or even outside the traditional framework of security alliance while still mindful of countering China's threat. Providing incentives to compensate for revenue losses or investing in capacity can be an effective way to strengthen mutual trust and practice equal partnership.

The proceeding chapters will provide more in-depth recommendations on how to advance US-ROK cooperation in critical technologies. Each article examines the path forward for the US-ROK bilateral relations by undertaking two steps. First, adopting a pragmatic and sensible approach to learning by doing. This necessitates sharing best practices and lessons learned through testing and evaluation in a timely fashion.

Second, viewing collaboration as a spectrum rather than as one-size fits all. Such a realistic pathway reduces friction and reinforces trust. Such a proposition can be achieved through upgrading or setting-up new channels of communication to facilitate open and transparent consultative processes that enjoin key stakeholders. The US-ROK dialogue at the technical, policy and strategic levels must be sustained to find positive-sum areas for cooperation that are more feasible and less conflictual. The major key takeaways summarize in the proceeding papers offer new possibilities to achieve these endeavors.

2. Stephen M. Walt, "Why Alliances Endure or Collapse," Survival 39, no. 1 (March 1997): 156–79, https://doi.org/10.1080/00396339708442901.; Stephen M. Walt, The Origins of Alliances (Cornell University Press, 1990).
3. David Kang and Paul Chamberlain. "A History of US-ROK Relations to 2002," in Strategic Sentiment: South Korean Views of the United States and the US-ROK Alliance, ed. Derek Mitchell (Washington D.C.: Center for Strategic and International Studies, 1996), 15.
4. Victor D. Cha, "Powerplay: Origins of the U.S. Alliance System in Asia," International Security 34, no. 3 (January 2010): 163, https://doi.org/10.1162/isec.2010.34.3.158.
5. Zbigniew Brzezinski, Lee Hamilton and Richard Lugar. "Foreign Policy into the 21st Century: The U.S. Leadership Challenge," (Washington D.C.: The Center for Strategic and International Studies, 1996).

6. The National Security Strategy papers of the US administrations clearly indicate the change in threat perception and the rationales for the strategic importance of alliances in the Asia Pacific Region. For instance, see: White House, National Security Strategy of the United States of America (Washington D.C.: White House, 2017), 46, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

7. Scott Snyder, The US-South Korea Alliance (Boulder: Lynne Rienner Publishers, 2012). Also see Sang-Hyun Lee, "ROK-US Relations in Lee Myung-Bak Government: Toward a Vision of a 21st Century Strategic Alliance," The Journal of East Asian Affairs 22, no. 1 (2008): 1–32, https://www.jstor.org/stable/23257872.

8. White House, National Security Strategy of the United States of America (Washington D.C.: White House, 2017), 7.

9. Scott Snyder, "Excerpt: The US–South Korea Alliance," Council on Foreign Relations, 2009, https://www.cfr.org/excerpt-us-south-korea-alliance.

10. Roh government further attempted to achieve "realignment of USFK [including] a planned one-third reduction amounting to 12,500 troops, removal of US forces positioned in several camps along the DMZ to a central camp north of Seoul, and the redeployment of one of two US combat brigades from South Korea to Iraq, with the South Korean military taking over the major roles and missions near or at the DMZ." See Snyder, "Excerpt: The US–South Korea Alliance".

11. Clint Work and D.A. Pinkston, "Park Geun-Hye's Visit and the US-ROK Alliance," thediplomat.com, October 26, 2015, https://thediplomat.com/2015/10/park-geun-hyes-visit-and-the-us-rok-alliance/.

12. Man-yeol Lee, "[Column] Time for S. Korea to Show Some Backbone amid US Demands," english.hani.co.kr, January 27, 2020, https://english.hani.co.kr/arti/english_edition/english_editorials/925754.html.

13. Scott Snyder et al., "South Korean Attitudes toward the U.S.-ROK Alliance and USFK," JSTOR, 2019, https://www.jstor.org/stable/resrep20674.; Lee, Sang Shine et al., KINU 2020 Unification Consciousness Report, Korean Institute for National Unification, 2020, pp.22-37

14. Blue House, National Security Strategy of Moon Jae In's administration, (Seoul: Blue House, 2018).

15. Snyder, "Excerpt: The US–South Korea Alliance".

16. According to a public poll, 60.2% of South Koreans supported the idea of developing the US-ROK alliance with fundamental values, like human rights and democracy. Support for US Forces Korea (USFK) rated 82.1%; Support for USFK was much higher in the past due to a rise in North Korean provocations. Overall, nearly 88.3% of South Koreans were optimistic about US-ROK relations and South Koreans believe that the relationship between both countries will improve in the future based on trust in the alliance. J. James Kim, Chungku Ku, and Ham Geon Hee, "South Korean Public Opinion on ROK-US Bilateral Ties" (Seoul: Asan Institute, May 2022).

The Geopolitics of Semiconductor Cooperation among the United States, South Korea and China

Sungmin Cho, PhD

Among the various areas of technological cooperation between the United States and South Korea, the semiconductor sector is the area where the two countries have pursued the most extensive and in-depth collaboration. China has responded to this partnership with the most sensitivity. It is commonly believed that South Korea has been hesitant to fully participate in the US-led efforts to rebuild the global semiconductor supply chain due to its economic interests in China. However, South Korean experts and business communities have increasingly expressed their support for the country's participation in "Chip 4," which would involve cooperation with the United States, Taiwan, and Japan in semiconductor production."

This article explains South Korea's cost-benefit analysis regarding its semiconductor cooperation with the United States, as well as China's dilemma in dealing with South Korea. It also explains why the trend of technological decoupling between China and South Korea is likely to persist for some time, and how Seoul and Washington should be ready to deal with China's potential economic coercion.

South Korea–US cooperation on semiconductor and China's Response

In recent years, South Korea and the United States have expanded their cooperation on semiconductors in both bilateral and multilateral frameworks. For instance, in December 2021, South Korea's Ministry of Trade and Industry and the US Department of Commerce launched the "Semiconductor Partnership Dialogue."[17] Samsung Electronics also decided to construct a new semiconductor manufacturing facility in Texas, investing approximately 17 billion US dollars, which marks the company's largest-ever investment in the United States. South Korea and the US have made progress in their collaboration within the multilateral framework of "Chip 4," along with Japan and Taiwan. In February 2023, the first meeting of Chip 4 was held, and representatives from South Korea's Ministries of Foreign Affairs and Industry took part.[18] Although the Ministry of Foreign Affairs acknowledged its participation, it did not release an official statement on the event. Apparently, the South Korean government wanted to keep a low profile while joining the formal meeting on semiconductors with the United States, Japan, and Taiwan."

China's response has exhibited a mixed pattern of pressure and persuasion. Initially, Beijing cautioned Seoul by reminding South Korea of its reliance on the Chinese economy. In July 2022, the state-affiliated Global Times published an editorial that warned, "decoupling South Korea's economy from the vast market of China is equivalent to committing commercial suicide."[19] A month later, the Chinese Ministry of Foreign Affairs also pointed out that approximately 60% of South Korea's semiconductor exports went to China in 2021.[20] However, Chinese authorities later moderated their stance: in August 2022, the Global Times published another editorial that stated "the international community expects South Korea to play a balancing role in correcting the mistake" if it were to join the US-led Chip 4 partnership.[21] During a meeting with his South Korean counterpart in August 2022, Chinese Foreign Minister Wang Yi similarly called on South Korea to "make sound judgments."[22] South Korean analysts interpret that Beijing was trying to persuade Seoul to resist US pressure to isolate China by joining Chip 4 and conveying Chinese concerns internally. [23]

The dynamic interactions between South Korea and China raise several questions that require further analysis. How have South Koreans internally discussed the US's calls for South Korea to join Chip 4? Why has China exhibited a mixed response of threats and persuasion? What are the strategic dilemmas that each country faces in semiconductor cooperation?

South Korea's Dilemma vs. China's Dilemma

South Korea's dilemma stems from the fact that the country has a significant economic interest in the Chinese market while also seeking to expand technological cooperation with the United States. South Korean companies have produced a considerable proportion of their semiconductors in China, with Samsung manufacturing around 40% of NAND flash memory chips from its Shaanxi facility in 2022, and about 50% of SK Hynix's Dynamic Random Access Memory (DRAM) being produced from its Chinese facility.[24] China is also South Korea's largest market, with around 60% of the country's total memory chip exports being sold in China in 2022.[25] Recognizing China's significant importance to South Korea's chip-making industry, the US government granted Samsung and SK Hynix a one-year exemption when it announced a ban on exports of advanced chips and equipment that use American technologies to China.[26] However, many South Korean experts suspect that the US government will not extend the exemption beyond October 2023.[27] They argue that South Korea should choose to work more closely with the United States because, ultimately, it is the US that will set the standard for the next generation of cutting-edge technology in semiconductors.[28]

China's dilemma is that, even with knowledge of South Korea's cost-benefit calculus, it cannot effectively threaten retaliation in the semiconductor sector. South Korea's chip-making industry depends on the demand from the Chinese market, but this also means that China depends on South Korea's supply of semiconductors for economic growth. Although China is the largest market for chip-making equipment in the world, Chinese-owned production accounted for only 5% in 2022.[29] If China retaliates against Samsung or SK Hynix for their cooperation with the US government, Chinese companies will lose profits because they are the main customers of South Korean companies.[30] Knowing this vulnerability well, the Chinese government has invested in developing indigenous chip-making capabilities for years. However, Chinese companies' track records do not inspire much confidence: Tsinghua Unigroup, once seen as China's hope for boosting semiconductor self-reliance, faced bankruptcy in 2021.[31] Fujian Jinhua, another major Chinese chip-making company, tried to develop its own technology for DRAM production, but the project was suspended in 2019 while being sued by the US memory chipmaker Micron for stealing trade secrets.[32] As such, China is unlikely to have a substitute supplier for DRAM memory chips other than Samsung and SK Hynix for the foreseeable future.[33]

Based on these trends, it is likely that South Korea will gradually decouple from China in the semiconductor sector. Even before the US-led initiatives to re-build the semiconductor supply chain, South Korean companies have already felt the need to move their production lines out of

China for economic reasons. The cost of doing business in China, as well as competition with Chinese companies, has significantly increased in recent years. As a result, Samsung Electronics shifted much of its communication equipment production from Shenzhen in 2018 and from Tianjin in 2019, and its personal computer plant from Suzhou in 2020 to other emerging countries like Vietnam or India.[34] South Korean analysts argue that South Korean chip-makers still have time to shift out of China while maintaining a comparative advantage over Chinese competitors.[35] Given the bigger potential loss for China in case of decoupling, China is unlikely to launch economic retaliation targeting the semiconductor sector easily.[36] Perhaps for these reasons, most South Korean companies support South Korea's joining Chip 4.[37]

China still possesses many tools of economic coercion in the sectors other than semiconductor. For example, South Korea imported 83.5 % of lithium hydroxide, a key material used to make rechargeable batteries, and 100% of magnesium, which is used for vehicle light panels, from China in 2021.[38] These statistics imply that China can significantly hurt South Korea's major industries by banning the exports of these key materials. Beijing has signaled its willingness to adopt such measures. The editorial of Global Times explicitly warned that "South Korea's joining the US-led "anti-China camp"...will only damage South Korea's vital interests and destroy its economic outlook."[39] After the US-South Korea summit in May 2022, another Global Times editorial wrote, "The Yoon administration must be fully aware that China has many means to counteract South Korea...,it will be [Seoul] which will ultimately pay the price."[40] South Korea's chip-makers may not be the direct target of China's economic coercion, but the South Korean government still has to worry about China's retaliatory measures in other sectors.

Therefore, to expand cooperation on semiconductors, Seoul and Washington need to prepare countermeasures for potential retaliation from China. The South Korean people have experienced China's economic retaliation over the deployment of the US THAAD (Terminal High Altitude Area Defense) equipment in South Korea.[41] The lesson of 2017 was that South Korea alone cannot deal with China's sanctions. To deter China's economic retaliation, it is necessary for South Korea, and many other countries that share similar concerns, to develop a mechanism for collective response. As Victor Cha argues, the United States, its allies, and like-minded countries can develop a club that "threatens to cut off China's access to vital goods whenever Beijing acts against any single member."[42] To activate such a strategy of collective resilience, Washington needs to show leadership in banding together its allies and partners, including South Korea. In turn, Seoul needs to show commitment to the coalition of the willing against China's coercive statecraft.

Challenges Ahead and Way forward

Critics may argue that policies aimed at restricting China's access to advanced semiconductor technology would damage the liberal order of free trade and globalization.[43] From an economic perspective, the trend of decoupling in semiconductors between the two largest economies in the world would harm the efficiency of global productivity that could otherwise be maintained. However, the unfortunate reality of great power competition is that every country in the middle, including South Korea, has to cope with it. As tensions in geopolitics escalate, economic interests no longer work to temper security and military competitions among states. The Trump administration criticized China for committing acts of "economic aggression," such as the forced transfer of foreign technology or illegal theft of intellectual property.[44] The Biden administration shares this assessment.[45] China's response to Russia's invasion of Ukraine only hardened the negative assessment: European countries and Japan have shown an even stronger will to cooperate with the United States on semiconductor development, as Beijing provided chips to Russia that could be used to develop missiles and weapons.[45]

Regarding the next steps for US semiconductor policy, two caveats are in order. First, Washington needs to consult more closely with allies and partners in the policymaking process.[46] The new US guidelines for the application of subsidies, published in February 2023, require subsidized companies to participate in US research and development projects and share excess profits with the US government.[47] South Korean companies immediately responded that such measures are equivalent to demanding access to their technological secrets and forcefully taking away their profits.[48] Chosun Ilbo, generally a pro-US conservative press in South Korea, published an article unusually critical of the United States as a "semiconductor bullying" country.[49] Taiwan and European countries have also expressed similar concerns.[50] While the US government has all the rights to demand returns from subsidizing foreign companies, it is also advised to pay closer attention to the concerns of foreign companies.

In this context, it is worth noting that during South Korean President Yoon's visit to the United States in April 2023, US President Biden took this issue seriously. Both leaders agreed to minimize uncertainties and business burdens for South Korean chipmakers operating in the US regarding the Chips and Science Act.[51] During the summit, the US Department of Commerce released a paper on the National Semiconductor Technology Center (NSTC) and announced that South Korean companies such as Samsung and SK Hynix can participate in its research projects. The NSTC is a government-civilian consortium that the US government will fund with $11 billion to support the Chips Act.[52] South Korean experts are optimistic that Korean companies

can maintain their edge in the next generation of technology with more opportunities for joint research and development programs through the NSTC channel.[53]

Second, Washington and Seoul need to consider the unintended impacts of its semiconductor policies on the Chinese people in general. As Jude Blanchett of the Center for Strategic and International Studies recently pointed out, "keeping China a generation behind on technology has functional impacts on the livelihoods of Chinese people."[54] In the area of public health, for example, Chinese people's access to an advanced medical technology and better healthcare will be hindered as a result of the US wholesale restriction against China's access to advanced semiconductor. The same can be said about other non-security areas like education and food production. There is no doubt that the US needs to deny China's access to advanced semiconductors that go into missiles which will target the United States, its allies and Taiwan. As a next step, it would be ideal if the US and its allies can find a way to minimize the policy's impacts on ordinary Chinese citizens who have virtually no influence over China's military policies and behaviors.

The reality is that Washington must make difficult choices until it becomes technologically possible to selectively restrict China's chip-making capacities solely in military and security sectors, and South Korea most likely will expand cooperation with the United States despite Chinese opposition.

17. "Korea, U.S. Launch New Dialogue on Semiconductor Partnership," Korea Joongang Daily, December 9, 2021, https://koreajoongangdaily.joins.com/2021/12/09/business/tech/semiconductor-US-Korea/20211209182241330.html.
18. 조의준, "한국·미국·일본·대만 '칩4' 가동 본격화," 조선일보, February 24, 2023, https://www.chosun.com/politics/diplomacy-defense/2023/02/25/ZQYHWQXDYFHJXISBLEAHSKKC3I/.
19. "社评：韩国应有勇气对美国胁迫行为说 '不,' " 环球网, July 20, 2022, https://m.huanqiu.com/article/48uEl4JUSyX.
20. "2022年7月26日外交部□言人□立□主持例行□者□_中□人民共和□外交部," www.fmprc.gov.cn, July 26, 2022, https://

www.fmprc.gov.cn/web/fyrbt_673021/jzhsl_673025/202207/t20220726_10728257.shtml.
21. Global Times, "South Korea Naturally Wins Respect When It Adheres to Independent Diplomacy: Global Times Editorial - Global Times," www.globaltimes.cn, August 8, 2022, https://www.globaltimes.cn/page/202208/1272532.shtml.
22. Esther Chung, "Park Tries to Assuage Wang on Chips in Qingdao," koreajoongangdaily.joins.com, August 10, 2022, https://koreajoongangdaily.joins.com/2022/08/10/national/diplomacy/korea-china-semiconductor/20220810170408001.html.
23. 조준형, "중국서 '韓 칩4 가입 못막는다면 활용하자' 목소리," 연합뉴스, August 9, 2022, https://www.yna.co.kr/view/AKR20220809064600083.
24. 신지혜, "중국, '칩4' 대응전략 바꿨나...왕이 '한국 판단 기대,'" KBS , August 10, 2022, https://news.kbs.co.kr/news/view.do?ncd=5529209.
25. 김성민, "中서 삼성 낸드 40%, SK D램 40% 만드는데... 美 규제땐 직격탄," 조선일보, February 24, 2023, https://www.chosun.com/economy/tech_it/2023/02/25/KACPOVVZA5DDZJISFKOLHZ54QM/.
26. 오문영, "칩4 동맹 본격 가동...中 노골적 압박에 삼성·SK 속앓이," 머니투데이, September 30, 2022, https://news.mt.co.kr/mtview.php?no=2022092914072017930.
27. Laura Dobberstein, "SK Hynix given One-Year Reprieve for China Chip Restrictions," www.theregister.com, October 13, 2022, https://www.theregister.com/2022/10/13/sk_hynix_china_chip_reprieve/.
28. 권석준, "[권석준 칼럼] 10월 이후 삼성전자, SK하이닉스에 무슨 일이? | 피렌체의 식탁," Firenzedt, February 19, 2023, https://firenzedt.com/26117.
29. 최지희, "'하고 싶은 거 다해' 대만·美·日, 반도체 지원 경쟁 가속...한국만 뒤처졌다," 조선비즈, January 10, 2023, https://biz.chosun.com/it-science/ict/2023/01/11/IVEBUJZCNVFWXLDI3MRMD4LOTA/.
30. Jeff Pao, "China's Chip Sector Enters a 'Dark Forest' Era," Asia Times, February 21, 2023, https://asiatimes.com/2023/02/chinas-chip-sector-enters-a-dark-forest-era/.
31. 안하늘, "한미 밀착에 中 반도체 보복?...'자살골 될 것,'" 한국일보, May 24, 2022, https://www.hankookilbo.com/News/Read/A2022052314260003694.
32. Che Pan, "SK Hynix Says DRAM Operations 'Normal' despite China Lockdowns," South China Morning Post, July 27, 2022, https://www.scmp.com/tech/tech-trends/article/3186747/south-korean-chip-maker-sk-hynix-reports-record-revenue-despite.
33. Masha Borak, "Chip Maker Tsinghua Unigroup Facing Bankruptcy after Creditor Action," South China Morning Post, July 11, 2021, https://www.scmp.com/tech/tech-trends/article/3140678/chinese-chip-maker-tsinghua-unigroup-faces-bankruptcy.
34. Debby Wu, "Engineers Found Guilty of Stealing Micron Secrets for China," Bloomberg.com, June 12, 2020, https://www.bloomberg.com/news/articles/2020-06-12/chip-engineers-found-guilty-of-stealing-micron-secrets-for-china.
35. 머니투데이 and 오문영, "칩4 동맹 본격 가동...中 노골적 압박에 삼성·SK 속앓이," 머니투데이, September 30, 2022, https://news.mt.co.kr/mtview.php?no=2022092914072017930.
36. Ye-eun Jie, "Samsung, LG Shift Away from China toward India as Production Base," The Korea Herald, February 9, 2023, https://www.koreaherald.com/view.php?ud=20230209000664.
37. https://www.joongang.co.kr and 한우덕, "한국 반도체, 중국 위협할 '한 방' 될까?," 중앙일보, June 16, 2021, https://www.joongang.co.kr/article/24084003.
38. 박종관, "'中, 韓반도체 대상 보복 어렵다'...점차 무게 실리는 '칩4' 참여론," 노컷뉴스, August 25, 2022, https://www.nocutnews.co.kr/news/5806950.

39. Ibid. According to a 2022 survey with some 300 South Korean companies, only 5.3 percent of respondents opposed South Korea's participation in Chip 4, while the absolute majority of 95% (53.4 % to join now and 41.3 % later) supported it.
40. "코참넷," www.korcham.net, August 18, 2022, http://www.korcham.net/nCham/Service/Economy/appl/KcciReportDetail.asp?CHAM_CD=B001&SEQ_NO_C010=20120935433.
41. 이관범 [Lee Guan-bum], "급한 불'은 꺼도 '中의존' 여전...수입국 다변화로 재발 막아야 [Put the fire, but still economic dependency on China remains large. South Korea should diversify trade]," 문화일보 [Munhwa Ilbo], November 10, 2021, https://www.munhwa.com/news/view.html?no=2021111001070203011001.
42. 9 损害韩国的切身利益，破坏韩国的经济发展势头. "社评：对华关系，尹锡悦最有望处理好的事 [Editorial: Yoon Sukyeol most likely to handle relations with China well]," 环球时报 [Global Times], May 10, 2022, https://opinion.huanqiu.com/article/47wVcvsJU4X.
43. "Yoon unlikely to make waves on Taiwan question after Biden visit," Global Times (Eng.). May 22, 2022. https://www.globaltimes.cn/page/202205/1266279.html.
44. The Chinese authorities went after the South Korean companies operating in China, imposing regulatory punishments such as prolonged tax investigations, fines, delayed licensing approval, and property seizure. South Korea's tourism sector was the hardest hit with the banning of local tour packages to South. According to a report by the Hyundai Research Institute, South Korea's losses due to these anti-THAAD measures amounted to roughly US$7 billion. See Darren Lim, "Chinese Economic Coercion during the THAAD Dispute," Open Forum, Asian Institute for Policy Studies, December 28, 2019, http://www.theasanforum.org/chinese-economiccoercion-during-the-thaad-dispute/.
45. Victor Cha, "How to Stop Chinese Coercion," Foreign Affairs, December 14, 2022, https://www.foreignaffairs.com/world/how-stop-china-coercion-collective-resilience-victor-cha. / Antony J. Blinken, "The Administration's Approach to the People's Republic of China," US State Department, May 26, 2022, https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/.
46. Certainly, the Chinese authorities accuse the US policy as evidence of the American "abuse of hegemony," and "these unilateral, egoistic and regressive hegemonic practices have drawn growing, intense criticism and opposition from the international community. See "US Hegemony and Its Perils," www.fmprc.gov.cn (Ministry of Foreign Affairs of the People's Republic of China, February 2023), https://www.fmprc.gov.cn/mfa_eng/wjbxw/202302/t20230220_11027664.html.
47. 'How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World,' Office of Trade & Manufacturing Policy, U.S. Department of Commerce. June 19, 2018. https://trumpwhitehouse.archives.gov/briefings-statements/office-trade-manufacturing-policy-report-chinas-economic-aggression-threatens-technologies-intellectual-property-united-states-world/.
48. Amanda Lee, "Stymied by West, Russia's Top Trade Partners Include Mainland China, Hong Kong," South China Morning Post, February 3, 2023, https://www.scmp.com/economy/china-economy/article/3209034/stymied-west-russia-getting-critical-semiconductors-mainland-china-hong-kong.
49. Jo He-rim, "Samsung, SK Breathe Tentative Sigh of Relief over US Chip Subsidy Rules," The Korea Herald, March 22, 2023, https://www.koreaherald.com/view.php?ud=20230322000640.
50. 김지헌 and 김민지, "'쌩큐 삼성·SK' 외쳤던 바이든인데...돈 앞에 '반도체 동맹' 와르르 위기 [비즈360],"

헤럴드경제, March 3, 2023, http://news.heraldcorp.com/view.php?ud=20230303000340.
51. Yonhap, "S. Korea, US to Discuss 'Concerns' over US Chips Act: Trade Minister," The Korea Herald, March 9, 2023, https://www.koreaherald.com/view.php?ud=20230309000129.
52. LINK BROKEN: news.koreadaily.com/2023/04/28/economy/economygeneral/20230428220032968.html
53. Choi Kyong-ae, "Yoon-Biden Summit Paves Way for Bilateral Semiconductor Partnership," Yonhap News Agency, April 30, 2023, https://en.yna.co.kr/view/AEN20230430002100320.
54. Choi Kyong-ae, "Yoon-Biden Summit Paves Way for Bilateral Semiconductor Partnership," Yonhap News Agency, April 30, 2023, https://en.yna.co.kr/view/AEN20230430002100320.
55. 김홍수, "[만물상] 이번엔 '반도체 깡패' 되려는 미국.
56. 권석준, "[권석준 칼럼] 윤 대통령, '한국 반도체'를 위해 바이든에 무엇을 얘기해야 하나 | 피렌체의 식탁," Firenzedt, April 2, 2023, https://firenzedt.com/26639/.
57. Kaiser Kuo, "The United States' China-Centered Existential Crisis," The China Project, March 9, 2023, https://thechinaproject.com/2023/03/09/the-united-states-china-centered-existential-crisis/.

Industrial Policy and Uncertainties in US-ROK Cooperation in Semiconductors: The US Chips & Science Act Subsidy Conditions and Guardrails

June Park, PhD

Does the US Chips and Science Act promise cooperation on semiconductors between the US and South Korea? The US-ROK cooperation on semiconductors has come at a crossroads of uncertainties. What began as a quest to revitalize US industries in manufacturing due to global chip shortage has now become a domestic industrial policy drive – one that puts allies in a very difficult position given the pressures compounded by the lack of incentives from the business perspective.[55] The US reigns as the inventor of semiconductors and the key player in design and fabless business, and also has the lead in logic chips that are fit for AI. But the US has outsourced manufacturing of chips for several decades and has lost leadership in memory chips and miniaturization in chip production technology, with Intel (aiming for 7nm processing technology) trailing behind TSMC (2nm processing technology) and Samsung (3nm processing technology). The Biden administration's response to the global chip shortage at the onset of the

pandemic, facing discontent from the auto industries that were crunched by unmet deliveries of automotive chips, has led to efforts to entice allies to invest in chip manufacturing in the US Uncertainties have arisen due to lack of incentives stated in the latest US Commerce announcement of thresholds for chip subsidy applications, which requires of the chipmakers that apply for and receive the US subsidies ($38.22 billion and up to $75 billion in direct loan or guaranteed principal amounts) to allow for monitoring of facilities and balance sheets by the US government, as well as upside sharing up to 75% of the subsidy amount received in case of excess returns earned. [56] Chip manufacturers are in a dilemma, as they seek benefits from the US subsidy, but the net revenue projected may not come as originally expected.

The eligibility criteria and guidelines for chip subsidies were announced on February 28, 2023, via the 'Notice of Funding opportunity (NOFO) CHIPS Incentive Program – Commercial Fabrication Facilities' by the National Institute of Science and Technology (NIST) under US Commerce.[57] The announcement has made the landscape of allied industrial cooperation with the US profoundly difficult, as it chips away possible incentives that were expected by the ROK chip manufacturers. The unprecedented NOFO came at a time when South Korean chip producers are already dwelling on their next steps in response to the newly added license requirements by the Bureau of International Security (BIS) at Commerce on October 7, 2022,[58] under which items destined to a chip fabrication facility in China were blocked based on the following thresholds: logic chips 16nm or 14nm or below, DRAM memory chips of 18nm half-pitch or less, and NAND flash memory chips with 128 layers or more.[59]

The national security guardrails for CHIPS for America Incentives Program which ensued the NOFO by the NIST further complicated the issue.[60] By banning material expansion at 5% of existing semiconductor manufacturing capacity for advanced nodes and 10% of that of legacy chips in China for a 10-year period, readjustments for business planning for those operating chip fabs in China become inevitable. But such concerns go beyond operational restrictions in China. Firms expecting to benefit from the subsidies are subjected to US demands for trade secrets. This include financial revenue projections as well as costs and other metrics such as number of wafers to be sold from the facility each month at peak capacity, expected unit price sold during first year of production, and expected annual price fluctuations are also required in excel form.[61]

It is debatable whether the US seeks in earnest cooperation with allies or simply a gradual absorption of industrial capacity of allies through the allocation of subsidies under the Chips & Science Act. While the US is touting national security in its endeavors to block advanced chip

technology to China, its actions make it less of a security issue and more of a commercial problem. A far more compelling argument based on the observation of recent developments would be that the US seeks to complete the semiconductor ecosystem within its borders by enticing allies to move production to the US at their own expense.

The current measures are ramping up immense pressures upon South Korean chip manufacturers that consequently impacts South Korea's overall economy which relies heavily on semiconductor manufacturing, which accounts for almost 20 percent of its exports.[62] The main companies that are on the frontlines are South Korea's Samsung and SK Hynix due to their operations in China. In the US, TSMC has a $40 billion plant under construction in Arizona, and Samsung and SK Hynix are at odds because they pledged investment in the US[63] The Chips & Science Act NOFO and national security guardrails restrict their operational expansion in China, and pose further challenges to Samsung and SK Hynix, as Samsung's NAND flash plant in Xian accounted for 16% of global NAND flash memory production and SK Hynix's Wuxi plant accounted for about 12% of global DRAM memory production, in addition to the NAND flash plant acquired from Intel in 2020.[64] This stands in sharp contrast with TSMC's Shanghai and Nanjing plants which only have a combined yield of 6% as far as the company's total contract chip-making capacity is concerned.

The ROK-US summit at the end of April 2023 in commemorating the 70th anniversary of the Mutual Defense Treaty did not focus on semiconductor issues, but instead covered up the issues regarding the mismatch of interests in the US chip subsidy scheme instead with buzzwords such as 'technological alliance' or 'tech alliance'. It may be the decisive moment for the two South Korean companies - if the companies fail to negotiate for a better condition for the subsidy eligibility criteria and conditions, they may be left with no other choice than to opt out. Under such a circumstance, the US pressures based on unilateral measures would do more harm than good for the alliance due to unmet economic expectations in the relationship.

Both Samsung and SK Hynix are reconsidering their plans to apply for the US subsidies given the conditions for eligibility and guardrails, as the restriction details are beyond what they expected and they might incur losses in the US if they receive them. The current bilateral negotiations on chip subsidy conditions would need to consider that tech cooperation should be a two-way street, and to bring about full-fledged cooperation chip subsidy conditions should be revised to incentivize further for a healthy relationship. Otherwise, disillusions of expected synergy effect with the US and distrust may cloud the relationship. Recognizing that 'strategic

trade' may be a good tool for domestic politics but may override principles for 'free and fair trade' is essential, as it continues to weaken US leadership and credibility if not supported by persuasive logic and actions that what the US is vouching for is for national security rather than commercial interests.

55. "Korean Semiconductor Industry Calls US Demands 'Hardly Acceptable'", Business Korea, March 29, 2023. http://www.businesskorea.co.kr/news/articleView.html?idxno=111736.

56. NOTICE OF FUNDING OPPORTUNITY (NOFO) CHIPS Incentives Program – Commercial Fabrication Facilities, U.S. Department of Commerce, February 28, 2023. It is noted under 'UPSIDE SHARING' on page 22 that "Recipients receiving more than $150 million in CHIPS Direct Funding will be required to share with the U.S. government a portion of any cash flows or returns that exceed the applicant's projections (above an agreed-upon threshold specified in the award). The Department expects that upside sharing will only be material in instances where the project significantly exceeds its projected cash flows or returns and will not exceed 75% of the recipient's direct funding award. Because successful projects will differ considerably in their key attributes, upside sharing arrangements may vary by project, and, in exceptional circumstances, may be waived." https://www.nist. gov/system/files/documents/2023/02/28/CHIPS-Commercial_Fabrication_Facilities_NOFO_0.pdf.

57. U.S. Congress, House, CHIPS and Science Act (CHIPS Act) Act of 2023, HR 4346, 117th Cong., 2nd sess., introduced in House 07/01/2021, https://www.congress.gov/bill/117th-congress/house-bill/4346.

58. "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," Bureau of International Security, U.S. Department of Commerce. October 7, 2022. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computingand-semiconductor-manufacturing-controls-final/file.

59. June Park, "The United States doubles down on its tech war with export and IP controls that target China but also hit

Taiwan and South Korea," East Asia Forum. November 30, 2022. https://www.eastasiaforum.org/2022/11/30/the-united-states-doubles-downon-its-tech-war-with-export-and-ip-controls-that-target-china-but-also-hit-taiwan-and-south-korea/.
60. "Preventing the Improper Use of CHIPS Act Funding," Federal Register, National Institute of Standards and Technology (NIST), March 23, 2023. https://www.federalregister.gov/documents/2023/03/23/2023-05869/preventing-the-improper-use-of-chips-actfunding.
61. "Semiconductor Firms Asked to Submit Financial Projections to Get Chips Act Funds," The Wall Street Journal, March 27, 2023. https://www.wsj.com/articles/semiconductor-firms-asked-to-submit-financial-projections-to-get-chips-act-funds-aafeba1a.
62. "Semiconductor Industry Driving Korea's Economic Growth," Industry Focus, Invest Korea, September 8, 2021. https://www.investkorea.org/ik-en/bbs/i-308/detail.do?ntt_sn=490760.
63. Samsung pledged $17 billion for a second fab in Taylor, Texas adjacent to the first fab in Austin; SK Hynix contemplating a testing and packaging plant site in the U.S.
64. "For Chip Makers, a Choice Between the U.S. and China," Wall Street Journal, March 28, 2023. https://www.wsj.com/articles/for-chip-makers-a-choice-between-the-u-s-and-china-looms-5450df30?fbclid=IwAR3vCQuXiqoDdDuYlZ0JUDIzdY57DGMSXCGsZL4gpG4BjWoXkU2QYUDz_Q.

5G/6G, Cybersecurity and US–South Korea Cooperation

Lami Kim, PhD

With its rapid speed and very low latency, the 5th generation (5G) technology will allow us to collect a huge amoint of data from sensors, and Internet of Things (IoT), and analyze them to make optimal decisions, and transmit them to end users. It enables new civilian and military applications such as self-driving vehicles, smart cities, telemedicine, precision agriculture systems, and autonomous weapons. The upcoming 6th generation (6G) of mobile technology, which is expected to be rolled out in the late 2020s, will provide internet services based on low earth orbit satellites. It will extend coverage from two dimensions to three dimensions, enabling internet of everything (IOE), and providing services such as autonomous flying vehicles and flying robots, and even the detection and tracking of hypersonic missiles.

Given the importance of mobile technology as the bedrock of the Fourth Industrial Revolution and future warfighting capabilities, countries are in fierce competition in this area. In the so-called 5G race, China seems to be leading the pack, particularly in the 5G infrastructure market. China's 5G dominance will enhance its surveillance capability as well as its coercive power. The United States and South Korea, two democratic allies that uphold the rule-based international order and have complementary digital technological advantages, are perfect partners that could offer an alternative for the secure and reliable utilization of these new mobile technologies.

China's 5G dominance

China is the forerunner in the 5G race. Huawei is leading the 5G equipment market, holding about 30% market share followed by Ericson and Nokia.[65] In terms of 5G roll out, China has deployed the largest number of base stations—close to 2 million.[66] The European 5G Observatory reported that China has built one base station for every 1,531 people. The United States is far behind with one base station for as many as 6,690 people. The gap between China and the United States is widening, with China aggressively adding new cell sites. Graham Allison and Eric Schmidt assessed that

"America is far behind China in almost every dimension of 5G."[67] Of course, the equipment is only part of the picture, the 5G ecosystem also includes mobile devices, operating systems, and microchips. China is behind the United States in terms of microchip design, and behind South Korea and Taiwan in terms of microchip foundries. But China is striving to catch up in other areas, as well, by putting far greater investment into 5G than the United States.

Why does this matter?

China's dominance in 5G matters greatly from national/international security and geopolitical perspectives. The most obvious and most direct security concern is the possibility that China uses its equipment for espionage and surveillance purposes. Experts have warned that Chinese manufacturers have built "backdoors" to access sensitive data in network equipment.[68] There is evidence to back this claim. One is the data theft that occurred in the African Union's headquarters, the construction of which was financed by Beijing, and for which Huawei supplied servers from 2012 to 2017.In addition, U.K.-based carrier Vodafone found and fixed backdoors on Huawei equipment used in its Italian business. An employee of Huawei was arrested in Poland in 2019 on charges of spying. [69] In the United States, Huawei has built 5G equipment in the middle of nowhere near American military bases and missile silos, allegedly to gather intelligence about military drills, readiness, and personnel. While Huawei is a private company, the company has strong ties with the Chinese Communist Party. It has received a huge amount of government funding, and the head of Huawei previously served as an engineer in the People's Liberation Army.[70] Like other Chinese entities, Huawei is required to support China's national intelligence activities under the 2017 National Intelligence Law.[71]

Cyberattack is another grave concern. Unlike 3G and 4G that were built primarily on hardware, 5G depends on cloud and greater software components. This implies that 5G has a larger attack surface that requires added security measures to ensure protection. Moreover, with digital infrastructure increasingly encroaching upon daily life, the sheer number of devices, users, and apps connected to the 5G network expands the attack surface. Thus, the stakes are very high. Hackers may hack into self-driving cars to assassinate people, disrupt traffic light control systems, and even manipulate military command and control systems. Given the high stakes, countries like China could threaten network shutdowns to achieve political objectives. China has not been shy about weaponizing its economic clout for political purposes. Dependence on China's 5G equipment will make countries vulnerable to China's bullying.

Washington's Efforts to Thwart China's 5G Dominance

To counter China's relative dominace in the 5G race, Washington has made efforts to address these security concerns. It has imposed restrictions on chipmakers using American technology, such as Taiwan Semiconductor Manufacturing Company and Samsung, from supplying chips to Huawei. Washington has also ordered US carriers to remove Chinese equipment from their networks and pressured other countries to avoid 5G equipment made by Huawei and ZTE, which all Five Eyes countries and others such as Denmark, Finland, India, Japan, Poland, and Sweden, have implemented.[72]

However, a vast number of developing countries in Southeast Asia and South America are already using or planning to use Chinese 5G equipment. Huawei provides quality technology at a fraction of the price that other providers offer, thanks to Beijing's enormous amount of subsidies. Cost is an important factor, as 5G is very expensive—far more than 4G, because it needs more cell sites due to its lower wavelength. Moreover, China offers package deals, inclusive of 5G equipment with surveillance technology and cloud systems at very low prices. The deal attracts low-income countries, particularly authoritarian regimes, from which China can collect data that can contribute to its espionage and surveillance activities, as well as its further technical development.

As efforts to simply persuade other countries not to use Chinese 5G equipment seem ineffective, Washington is pushing for an Open Radio Access Network (RAN) system, which would create standardized and interoperable (i.e. open) interfaces between systems in the RAN. With their possible adoption of OPEN RAN, telecom companies would no longer need to buy one vendor's integrated, propriety system, and could instead purchase different hardware and software components separately. Open RAN is still in its infancy, but it has the potential to decrease the influence of 5G equipment providers such as Huawei. The Chips Act also provides funding to invest in Open RAN technology.[73]

Opportunities for US–South Korea Cooperation

Contrary to the US, countering China's 5G dominance has not been a priority for Seoul. South Korea has avoided irking China for obvious reasons. China is South Korea's largest trade partner, as well as an important actor in North Korea issues. Despite this, South Korea considers the security and reliability of 5G/6G paramount to its role as a tech innovator.

This creates an ample room for cooperation with the US. In fact, the two countries are ideal partners that can compensate for each other's weaknesses. The United States has a comparative advantage in microchip designs and operating systems, but does not build 5G equipment or manufacture microchips, both of which are South Korea's forte. In particular, the two countries can collaborate in developing an Open RAN system that combines South Korea's 5G hardware and the US' 5G software.[74] On the hardware side, Samsung is one of the leaders in Open RAN, with increasing market share. For example, Samsung supplied Open RAN hardware for Vodaphone in the United Kingdom, filling the gap left by Huawei's equipment, that needs to be eliminated by 2027.[75] Samsung is the perfect partner for the United States, as Ericsson and Nokia are reluctant to pursue Open RAN due to their oligopoly in the proprietary 5G equipment market. Another advantage of Samsung as a US partner in the 5G market is that its equipment is more secure than Ericsson and Nokia, which have significant manufacturing operations in China. Some say Ericsson and Nokia are just as vulnerable to Chinese spying as Huawei. After Australia decided to ban Huawei equipment in its network services and go with Ericsson instead, it discovered Ericsson uses parts produced by its joint venture with a Chinese company named Panda, which has been designated as one of 20 Chinese military-linked companies by the Pentagon.[76] In contrast, Samsung's plants are located in South Korea and India, which makes Samsung's products more secure. It has already won Pentagon clearance for government use of its devices equipped with its proprietary Knox security software, trusted by the US military.[77]

In addition, South Korea and the United States should combine their technological expertise to make advances in mobile technology innovation. China is striving for leadership in next-gen mobile technology, to seize the huge first-comer advantage. This includes not only economic benefits but opportunities to set standards. The United States and South Korea have a great number of talented scientists, engineers, and researchers, and their collaboration will generate synergistic effects. They have already agreed to cooperate in developing 6G[78], with Samsung joining the Next G alliance, a group of companies in like-minded countries that collaborate for 6G innovation[79]. To counter China's potential dominance in the next frontier of mobile technology, it is critically important for these two countries that possess advanced technology to collaborate to reap a first-comer advantage.

Actively pursuing such lines of effort pose a relatively low risk for South Korea and presents desirable options, especially from a commercial perspective. Therefore, South Korea can justify its actions as economically motivated, rather than just purely geopolitical. The timing for the two countries' collaboration in the area of mobile technology is ripe. The two leaders in Seoul and Washington are eager to tighten their alliance and cooperate in emerging technologies. Together, the two countries can reap both economic and geopolitical benefits, while maintaining the rule-based international order.

65. "Telecom Equipment Growth is Slowing,"Dell'oro Group, October 5, 2022, https://www.delloro.com/key-takeaways-1h22-total-telecom-equipment-market.
66. "5G Scoreboard," European 5G Observatory, last accessed on March 31, 2023, https://5gobservatory.eu/observatory-overview/5g-scoreboards.
67. Graham Allison and Eric Schmidt, "China's 5G Soars Over America's", Wall Street Journal, February 16, 2022, https://www.wsj.com/articles/chinas-5g-america-streaming-speed-midband-investment-innovation-competition-act-semiconductor-biotech-ai-11645046867?st=hmjpsnr5e7nmxni&reflink=article_copyURL_share.
68. Bruce Schneier, "China Isn't the Only Problem With 5G," Foreign Policy, January 10, 2020, https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/.
69. "Poland Arrests Huawei Worker on Allegations of Spying for China," Guardian, January 11, 2019, https://www.theguardian.com/technology/2019/jan/11/huawei-employee-arrested-in-poland-over-chinese-spy-allegations.
70. Sherisse Pham, "Who is Huawei founder Ren Zhengfei?" CNN, March 13, 2019,
71. Yi-Zheng Lian, "Where Spying is the Law," New York Times, March 13, 2019, https://www.nytimes.com/2019/03/13/opinion/chinacanada-huawei-spying-espionage-5g.html.
72. "Canada bans China's Huawei Technologies from 5G networks," National Public Radio, May 20, 2022, https://www.npr.org/2022/05/20/1100324929/canada-bans-chinas-huawei-technologies-from-5g-networks.
73. "FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China," The White House, August 09, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.
74. Jung Suk-yee, "United States to Keep China in Check by Working with South Korea," Business Korea, May 25, 2021, http://www.businesskorea.co.kr/news/articleView.html?idxno=67856.
75. Joyce Lee and Supantha Mukherjee, "Samsung enters Europe with Vodafone 5G network deal in Britain," Reuters, June 14, 2021, https://www.reuters.com/article/ctech-us-vodafone-group-samsung-elec-bri-idCAKCN2DQ0FN-OCATC.
76. Richard Baker, "Chinese Military Has Links to Supplier of 5G Equipment in Australia," Sydney Morning Herald, July 2, 2020, https://www.smh.com.au/national/chinese-military-has-links-to-supplier-of-5g-equipment-in-australia-20200702-p558g2.html.
77. "Samsung Devices Achieve Approval from the U.S. Department of Defense," Samsung Newsroom, June 26, 2018, https://news.samsung.com/us/samsung-devices-achieve-approval-u-s-department-defense.
78. Jung Suk-yee, "United States to Keep China in Check by Working with South Korea," Business Korea, May 25, 2021, http://www.businesskorea.co.kr/news/articleView.html?idxno=67856.
79. "New Founding Members Strengthen ATIS Next G Alliance as It Sets the Course to Advance North American 6G Leadership," Business Wire, November 12, 2020, https://www.businesswire.com/news/home/20201112005290/en/New-Founding-Members-Strengthen-ATIS-Next-G-Alliance-as-It-Sets-the-Course-to-Advance-North-American-6G-Leadership.

US–South Korea AI Cooperation: Opportunities, Challenges, and Prospects

Alexandra Seymour

The United States and South Korea are uniquely positioned to champion the democratic model for artificial intelligence (AI) development, use, and cooperation. Unlike the semiconductor industry, where the United States has pursued strong export controls and South Korean firms cannot easily decouple from countries like China, because Beijing represents 41 percent of its semiconductor exports, both countries have approached AI in a complementary fashion.[80] For example, the United States and South Korea prioritize federal investment in AI capabilities, as well as share concerns how AI furthers China's military objectives.

However, despite mutually held perspectives, American and South Korean government investments in AI have taken different forms, therefore cultivating different strengths. Specifically, whereas South Korea prioritized commercial applications, the United States has focused on the military space. For example, last year, South Korea committed more than $16.4 billion over three years in data, AI, and networks, and its 2019 National Strategy for AI has three pillars designed to ensure competitiveness and prosperity in the midst of technological change[81]: AI ecosystem, AI utilization, and a focus on a people-centered approach. Furthermore, South Korea's Fourth Industrial Revolution improved data privacy laws and created an Innovation Academy to train individuals and connect them with jobs—two areas where the United States significantly lags.[82]

By contrast, the US Department of Defense (DoD) has requested over $3 billion for AI and joint all domain command and control (JADC2) programs in its fiscal year 2024 budget alone.[83] Although US AI investment is meant to be government-wide, DoD receives the majority of funds for AI projects, serving as an example for other agencies. The US was also the first country in the world

to issue military ethics principles for AI, which it reinforced through the Political Declaration on Responsible Use of Artificial Intelligence and Autonomy.[84] South Korea only recently embraced this topic when it co-hosted the Responsible AI in the Military Domain (REAIM) summit in February 2023.

Given the two countries' desire for closer cooperation, as evidenced by the US-South Korea high-level dialogue on defense technology, the United States and South Korea can leverage the 70th Anniversary of the US-Korea Mutual Defense Treaty to highlight how they can learn from and leverage each other's strengths.[85] At the same time, while their ultimate objectives for AI development align, the United States and South Korea will face several challenges to full cooperation, such as technical barriers to technological development as well as differing public sentiment toward AI systems. Consequently, this piece examines the opportunities, challenges, and prospects for US-South Korea AI cooperation.

Opportunities

Growing interest globally in commercial and military applications of AI technologies, such as robotics and predictive analytics for military logistics, creates several opportunities within the US-South Korea relationship. To ensure the two countries can effectively further their momentum for heightened AI collaboration, they must focus on two aspects of long-term progress for the AI ecosystem: building a robust, skilled talent pool and furthering research goals for trustworthy AI, meaning AI technologies are accurate, explainable, reliable, robust, safe, and secure, among other characteristics.[86] Both countries bring unique strengths that will fill critical gaps.

As Presidents Biden and Yoon noted in their 2022 Joint Leader's Statement, they "fully recogni[ze] that scientists, researchers, and engineers of the ROK and the US are among the most innovative in the world."[87] For South Korea, this can be attributed to its education ecosystem. The United States, by contrast, can attribute its success to its innovation ecosystem, which boasts a flexible, regulatory system for emerging technologies and world-leading levels of investment.[88]

While AI specialization across the United States is growing, the country's approach to growing its AI talent pipeline has not been as intentional as that of South Korea.[89] In 2022, South Korea designated ten local universities as AI engineering schools and four national universities as AI research centers. Moreover, South Korea continues its commitment to cultivating its talent pool. In addition to endorsing and implementing an AI curriculum for high schoolers, South Korea

recently pledged to train 52,000 individuals in areas including AI.[90] Seoul has bolstered its digital education system for elementary and middle schoolers, and has created resources such as the Digital Talent Bridge to connect individuals to jobs. As a result, Stanford HAI's vibrancy tool ranks South Korea as third for AI talent concentration.[91] The United States, on the other hand, is number 13.

However, when assessing areas related to research and development—such as newly funded AI companies, total private investment, AI patents grants, and conference citations—the United States far outpaces South Korea.[92] While South Korea's innovation ecosystem is growing, with about 400 AI startups in the country, its regulatory regime holds it back from progressing.[93] Hence, the Korean government called for a "negative" regulatory system that can "approve first, regulate later," in its 2019 National Strategy for AI.[94] By bolstering confidence in the AI ecosystem through simultaneous cooperation on research for trustworthy AI, the United States can help South Korea transition to this system in a way that accounts for its concerns about AI safety, ethics, and privacy.

Both countries share an interest in advancing trustworthy AI. South Korea, for example, introduced the first explainable AI standard in 2020, which formed the basis of the working group at ISO/IEC JTC/SC 42.[95] According to the Center for AI and Digital Policy, South Korea also consistently ranks highly for its commitment to democratic values in AI.[96] Likewise, through actions such as Executive Order 13960: Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, the United States has broadened its focus beyond national security-related AI concerns that spurred the DoD's AI Ethics Principles to societal regulation, guidance, and standards. For example, the United States created an AI Bill of Rights and the National Institute of Standards and Technology (NIST) AI Risk Management Framework.

By combining South Korea and the United States' innovation capacity and talent pools, coupled with their demonstrated commitment to advancing global AI norms, standards, and democratic governance frameworks, the two countries are well-suited to further research for trustworthy AI if they coordinate their resources accordingly. This could include aligning investments for under-developed methods for AI trustworthiness, such as AI explainability and testing and evaluation methods for AI models, particularly those that use multiple data types, or for the creation of additional test-beds.

Challenges

Despite the opportunities the US-South Korea partnership presents, there are two primary challenges to achieving them. First, although the United States and South Korea are committed to AI trustworthiness, the rapidly evolving nature of these technologies make upholding accountability difficult. A timely example of this challenge is the European Union, which stalled a vote on its proposed AI Act to include distinct requirements for foundation models due to unforeseen risks emanating from ChatGPT.[97]

Additionally, while many prominent names in the business and research community have responded to ChatGPT developments with a call for a "six month pause" to establish safety protocols, a pause would not be effective.[98] Specifically, a pause would not slow down the AI development of authoritarian nations, which would create more risk. Additionally, accountability metrics are not stagnant; they must constantly be monitored and updated to suit new scenarios that AI models may face. AI trustworthiness is also a broad term that encompasses complex issues such as safety, ethics, security, bias, and fairness, all of which have implications for individual users and broader society. Therefore, tackling AI trustworthiness and making technical progress will require strategic alignment of resources, particularly as the two countries further their AI cooperation in the military domain.

Second, public perceptions of AI's potential differ greatly between the United States and South Korea, which makes it challenging to rally societal support for investment in technological development. According to Stanford HAI's 2023 AI Index, only 35 percent of Americans viewed the benefits of products and services that use AI as outweighing the drawbacks.[99] For South Korea, this number was 62 percent, demonstrating that South Koreans are much more optimistic about the potential of AI than Americans. Convincing the public about the benefits of AI—particularly given most American workers believe AI will have a negative impact on the workplace—will be key to harnessing the potential of AI technologies in both American and South Korean societies.[100]

Prospects

Drawing on the strengths and recognizing the weaknesses of both countries, South Korea and the United States can take the following steps to advance AI cooperation, which will reinforce the importance of the US-Korea Mutual Defense Treaty:

- **South Korea should endorse the United States' Political Declaration on Responsible Use of Artificial Intelligence and Autonomy.** At the REAIM summit in February 2023, the US Department of State announced its approach to responsible use for AI in military settings and beyond, and invited other countries to join. South Korea's endorsement of this political declaration would be an important step for setting a global precedent for trustworthy AI in military settings and would establish the two countries as leaders in this space.

- **South Korea and the United States should organize an educational summit comprised of university and private sector stakeholders.** Although the US trails South Korea in terms of talent initiatives, both countries recognize the importance of bolstering their AI talent pipelines. Given rapidly evolving technological changes and talent shortfalls, the US and South Korean governments should organize an educational summit to increase knowledge sharing and exchange best practices for building a sustained talent pipeline. This forum would enable the two countries to exchange ideas about curriculum development for all ages (i.e., K-12, undergraduate, and postgraduate education), as well as would provide a platform to discuss skills needed to address emerging AI challenges across applications ranging from the workflows to the battlefield. An outcome of this summit should be the creation of an AI talent exchange program to ensure the two countries implement their takeaways from the convening. The countries may also consider leveraging resources for this exchange from the educational initiative announced at the Biden-Yoon summit in April.[101]

- **South Korea and the United States should create a joint research and development (R&D) funding pool to advance specific capabilities that promote trustworthy AI.** Creating a joint R&D funding pool could have implications for both military and commercial applications. Some areas that South Korea and the United States may choose to explore are adversarial attacks, methods to curb misuse of AI-enabled autonomous weapons systems, which are becoming a growing concern for both countries, or cooperation on AI capabilities that can be misused by authoritarian actors, such as surveillance technologies.

- **South Korea and the United States should use the 70th Anniversary of the US-Korea Mutual Defense Treaty to signal a new era of military cooperation with a data sharing agreement.** As South Korea and the United States celebrate the milestone of their 70-year partnership, they should acknowledge how a new era defined by strategic competition necessitates a new approach to military cooperation. Both countries have put AI at the center of their technology strategies, and Presidents Biden and Yoon reinforced the importance

of AI cooperation at their summit in April.[102] Access to data, however, is what will enable both countries to progress their capabilities for this new era of warfare. Building on the momentum from the Biden-Yoon summit, a data sharing agreement would bolster Foreign Minister Park Jin's claim that AI is "all the more important, especially for Korea, which is facing a real threat from North Korea in terms of escalating weapons of mass destruction program, including nuclear and missile threats."[103] It would also support the goals of the DoD, which identified AI as the leading capability for global supply chain security and a key technology area that will continue advancing the two countries' partnership.[104]

Conclusion

Today's uncertain geopolitical environment marked by an intensifying strategic competition makes public assurance on the development and deployment of trustworthy or ethical AI vital. Indeed, it is concerning how authoritarian nations such as China infringe on human rights and threaten national security by disregarding safety, ethics, and stability in technological development, all for the sake of achieving their own technological, military, and economic aims. With the 70th Anniversary of the US-Korea Mutual Defense Treaty, South Korea and the United States have an opportunity to use their complementary strengths to advance AI responsibly and productively.

80. Jacob Stokes, Alexander Sullivan, and Joshua Fitt, "Digital Allies: Deepening US-South Korea Cooperation on Technology and Innovation," Center for a New American Security, March 22, 2022, https://www.cnas.org/publications/reports/digital-allies.

81. Yonhap, "S. Korea to invest over 20tr won in data, network, AI sectors," The Korea Herald, March 25, 2022, https://www.koreaherald.com/view.php?ud=20220325000326; "National Strategy for Artificial Intelligence," The Government of the Republic of Korea, December 17, 2019, https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9.

82. "About the Academy," Innovation Academy, accessed June 4, 2023, https://innovationacademy.kr/en/innovation_academy/academy_info/info.html.

83. Jon Harper, "Pentagon requesting more than $3B for AI, JADC2," DefenseScoop, March 13, 2023, https://defensescoop.com/2023/03/13/pentagon-requesting-more-than-3b-for-ai-jadc2/.

84. Gregory S. Dawson, Kevin C. Desouza, and James S. Denford, "Understanding artificial intelligence spending by the US federal government," The Brookings Institution, September 22, 2022, https://www.brookings.edu/blog/techtank/2022/09/22/understanding-artificial-intelligence-spending-by-the-u-s-federal-government/; "Political Declaration on Responsible Military Use

of Artificial Intelligence and Autonomy," US Department of State, February 16, 2023, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/.

85. Ji Da-gyum, "S. Korea, US agree to launch high-level dialogue channel on defense tech cooperation," The Korea Herald, September 15, 2022, https://www.koreaherald.com/view.php?ud=20220915000627.

86. "Advancing Trustworthy AI," National Artificial Intelligence Initiative Office, accessed June 4, 2023, https://www.ai.gov/strategic-pillars/advancing-trustworthy-ai/.

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

88. Chaeri Park, "Q&A: South Korea Weighs Its Strengths Amidst US-China Tech Competition," DigiChina, Stanford University, April 11, 2022, https://digichina.stanford.edu/work/qa-south-korea-weighs-its-strengths-amidst-us-china-tech-competition/.

89. Nestor Maslej, Loredana Fattorini, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Vanessa Parli, Yoav Shoham, Russell Wald, Jack Clark, and Raymond Perrault, "The AI Index 2023 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2023, https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

90. Ibid.; Han-Gyeol Seon, "Korea to invest $367 million to nurture AI, metaverse, digital talent," The Korea Economic Daily, January 19, 2023, https://www.kedglobal.com/artificial-intelligence/newsView/ked202301190018.

91. "Global AI Vibrancy Tool," Institute for Human-Centered AI, Stanford University, Stanford, CA, accessed June 4, 2023, https://aiindex.stanford.edu/vibrancy/.

92. Ibid.

93. "South Korea - Country Commercial Guide," International Trade Administration, August 2, 2022, https://www.trade.gov/country-commercial-guides/south-korea-information-and-communication-technology.

94. "National Strategy for Artificial Intelligence," The Government of the Republic of Korea.

95. Jaesik Choi, "South Korea's Response to Surging AI Use in the US and China," Vol 17, No. 4, Seoul, Korea: Global Asia, December 2022, https://www.globalasia.org/v17no4/cover/south-koreas-response-to-surging-ai-use-in-the-us-and-china_jaesik-choi.

96. "AI Index - 2022 v. 2021 v. 2020," The Center for AI and Digital Policy, April 10, 2023, https://www.caidp.org/reports/aidv-2022/.

97. Suphantha Mukherjee and Martin Coulter, "As AI booms, EU lawmakers wrangle over new rules," Reuters, March 22, 2023, https://www.reuters.com/technology/ai-booms-eu-lawmakers-wrangle-over-new-rules-2023-03-22/; Luca Burtuzzi, "AI Act: MEPs close in on rules for general purpose AI, foundation models," EURACTIV, April 20, 2023, https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-close-in-on-rules-for-general-purpose-ai-foundation-models/.

98. "Pause Giant AI Experiments: An Open Letter," Future of Life Institute, March 22, 2023, https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

99. Maslej, Fattorini, Brynjolfsson, Etchemendy, Ligett, Lyons, Manyika, Ngo, Niebles, Parli, Shoham, Wald, Clark, and Perrault, "The AI Index 2023 Annual Report".

100. Lee Rainie, Monica Anderson, Colleen McClain, Emily A. Vogels, and Risa Gelles-Watnick, "AI in Hiring and Evaluating Workers: What Americans Think," Pew Research Center, April 20, 2023, https://www.pewresearch.org/internet/2023/04/20/ai-in-hiring-and-evaluating-workers-what-americans-think/.

101. "Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea," The White House, Statements and Releases, April 26, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/leaders-joint-statement-in-commemoration-of-the-70th-anniversary-of-the-alliance-between-the-united-states-of-america-and-the-republic-of-korea/.

102. Ibid.

103. Kang Seung-woo, "Foreign minister stresses need for responsible use of AI in military domain," The Korea Times, February 17, 2023, https://www.koreatimes.co.kr/www/nation/2023/02/356_345655.html.

104. C. Todd Lopez, "DOD Looks at US-South Korea Technology Cooperation," DOD News, June 9, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3058558/dod-looks-at-us-south-korea-technology-collaboration/

From creating trustworthy robotic partners to establishing trustworthy US–ROK partnerships in robotics

Boyoung Kim, PhD

Promoting effective and sustainable partnership in robotics between the United States and South Korea is an important but challenging task. Leveraging psychological theories of trust in human-robot interaction, this paper proposes potential frameworks to explore strategic collaborations across private, academic, and government sectors both within and between the two countries.

The history of robotics in the US and the ROK

The US has played a major role in developing industrial robots and military robots. In 1954, the US invented Unimate, the first industrial robot. The robotic arm was placed on a General Motors assembly line in New Jersey and helped automate metalworking and welding. In 2002, military robots were used in ground combat for the first time by the US in the Afghanistan war. Military robot Hermes was deployed ahead of US troops to inspect a series of caves in Qiqay, Afghanistan that were suspected to be a possible hiding place for enemy personnel and weapons.

Contrary to the US, South Korea has focused more on developing and implementing service robots, entertainment robots, and humanoid robots. In 2005, ROK created Albert HUBO, the world's first bipedal humanoid robot with an expressive human face. Increasing demand for service robots are driven in large part due to low birth rate and rising life expectancy that can assist older adults in healthcare settings and children in educational settings.[105]

Over the past decades, questions surrounding the potential roles of robots have started to converge in the US-ROK relations. Rather than viewing robots merely as a tool for dull, dirty, dangerous tasks, a dominant trend started to emerge: robots as collaborators that operate alongside or in cooperation with humans. The crux of this trend is rooted from the growing recognition on the importance of promoting a balanced partnership between humans and robots.[106] For example, in 2011, the US National Science Foundation (NSF) launched the National Robotics Initiative (NRI) program in pursuit of facilitating the advancement and utilization of "corobots," or collaborative robots.[107] Conversely, South Korea's Ministry of Trade, Industry and Energy established the Korea Institute for Robot Industry Advancement (KIRIA) in 2008 imbued with the mission of developing the robot industry to support business and policy in the country. Since its foundation, KIRIA has sought to build "good robots" that are beneficial to humans. It has also supported the development and production of industrial robots and service robots, as well as the robots' main parts such as sensors and manipulators.

Opportunities for building strategic collaborations in robotics between the US and the ROK

Given the current momentum of robotics development in the two countries, there are opportunities that the US and South Korea can pursue to strengthen collaboration. First, establishing the two countries' shared goals with a narrow focus on identifying specific domains that would produce and maximize collective benefits. A key element to consider in making these decisions would be identifying a common ground on each country's unique historical, geopolitical, economic, and cultural backgrounds. Another factor would be maximizing each country's comparative advantages in the research and development or in the supply chain of robots.

Based on recent developments, the healthcare and defense sector stand to be the most promising domains of robotics collaboration for South Korea and the US. In the defense domain, the two allies can work together to develop and deploy robots like drones and agile mobile robots. These robots can serve as collaborators, assisting personnel to detect potential intrusions in the airspace or navigate terrains that are difficult for humans to access. Relatedly, the US and ROK could combine their scientific and technological expertise for the physical rehabilitation and administering mental health care of robots. South Korea is anticipating an increasing demand for caring for older adults, while the US is grappling with rising healthcare costs. Each country could also harness the role of robots to address their distinct societal challenges. Thus, such prospects for collaborations can lead to fruitful outcomes for both countries.

Frameworks for promoting trustworthy US–ROK partnerships in robotics

On May 21st 2022, President Yoon and President Biden issued a joint statement in which they recognized autonomous robots as a field of emerging technology planned for fostering bilateral alliance. The two leaders' commitment to this tech cooperation is reaffirmed in the joint statement released on April 26th 2023 in commemoration of the 70th anniversary of the US-ROK alliance.

To foster effective and sustainable US-ROK collaborations in the field of robotics, it is important that researchers from diverse disciplines—including but not limited to psychology, philosophy, computer science, and robotics engineering, across industry and academic sectors and policy makers—should first establish communication channels to achieve cross-cutting collaboration grounded on open communications. These communication channels among diverse stakeholders at the domestic level should be complementary at the international level to assist productive collaborations between South Korea and the United States. Establishing such network of experts and practitioners can assist policy makers specify and rank fundamental emerging technologies, such as AI and semiconductors, critical for designing and manufacturing both hardware and software of robots and establish strategies for cooperating on developing those technologies. Furthermore, through the proposed communication channels, experts and practitioners can help in accurately identifying societal and ethical issues that may arise as more and more advanced robots are created and deployed in societies. Such channels can conduct deeper evaluation to understand the underlying cause of potential issues, and swiftly implement the knowledge obtained from research in policy making.

The need for creating systems for open communications is fundamentally grounded in the issue of trust, and thus, the existing research on the trust in human-robot interaction can offer insights into building trustworthy US-ROK partnerships in robotics. Trust is defined as a multi-faceted latent construct that emerges in an uncertain and vulnerable situation. It mediates the relationship between the events an agent experienced in the past and the agent's subsequent act of reliance upon another agent.[108] In studying trust in human-robot interaction, researchers have found the importance of a well-calibrated trust.[109] Allocating either too much or too little trust to a robot beyond the merits of its design and capabilities can lead to dire consequences. For instance, if the human user excessively trusts an anti-missile system, it may lead to possible misidentification of an ally's jet as a foe.[110] Likewise, if human users doubt an autonomous navigation system,[111] they may not recognize the value of the information provided, leading to potential accidents.

These problems of miscalibrated trust in human-robot interaction should provide critical lessons as South Korea and the United States explore possible opportunities to work together

as partners in the field of robotics. Monitoring systems are integral in creating and maintaining open communication channels and preventing the occurrences of over trust and under trust among different stakeholders and countries. To realize effective and sustainable collaborations between the two countries, it is important to navigate with caution when, where, and how to trust respective partners.

In preparing these systems for communications, it would be conducive to take into consideration the extant investigations on psychological factors that affect trust in human-robot interaction. For instance, researchers in human-robot interaction proposed human-, robot-, and environment-related factors that influence the process of trust development in human-robot interaction.[112] Among these three factors, it is critical to emphasize the environmental factor, which consists of team collaboration and tasking, to foster systems of open communication channels within and between the US and South Korea. Team collaboration is especially useful as it specifies in-group membership, culture, communication, and shared mental models as key factors affecting trust. These factors help narrow the focus on projects that necessitate the pursuit of common goals, based on historical, geopolitical, economic, and cultural backgrounds of the two countries, and to maintain systems to facilitate active and open communications. Incorporating environmental factors would contribute to maximizing mutual benefits and reducing costs in the long term because it would enable trust-building among public and private sectors.

Towards building effective and sustainable US–ROK partnership in robotics

Communication and trust are the key components in the robotics partnership between the US and South Korea. The open communication channels between the two allies should be established as the fundamental first step of the R&D collaboration. Trust must be the guiding principle for such channels to expand and fortify robotics collaboration. Research on human-robot interaction can help draft the guidelines for creating and maintaining such communication channels centered around mutual trust. People's trust in robots evolves over time and the level of their trust can fluctuate depending on the past behavior of robots. Further, as a multidimensional construct, trust in human-robot interaction can be determined not only by a robot's performance dimension that manifests its competence and reliability in accomplishing tasks but also by a robot's moral dimension to manifest its ethicality and sincerity in serving as a member of society.[113] In exploring trust in human-robot interaction, South Korea and the US must recognize trust-building is a dynamic process of incrementally accumulating acts of trust by demonstrating each country's technological competence as well as ethical values constituting the foundation of technologies.

105. G. Bekey, & J. Yuh, "Reviewing the issues of robotic self-X," IEEE Robotics & Automation Magazine 14, no. 4 (2007), 6-7; G. Bekey, & J. Yuh, "The status of robotics," IEEE Robotics & Automation Magazine 15, no. 1 (2008), 80-86; F. C. Park, "Robotics in Korea [Regional]," IEEE Robotics & Automation Magazine 20, no. 1 (2013), 99-100.
106. C. Breazeal, J. Gray, G. Hoffman, & M. Berlin, "Social robots: Beyond tools to partners," In RO-MAN 2004. 13th IEEE International Workshop on Robot and Human Interactive Communication (IEEE Catalog No. 04TH8759), 551-556. IEEE; T. Fong, J. Scholtz, J. A. Shah, L. Fluckiger, C. Kunz, D. Lees, ... & J. G. Trafton, "A preliminary study of peer-to-peer human-robot interaction," In 2006 IEEE International Conference on Systems, Man and Cybernetics 4, (2006), 3198- 3203).
107. D. J. Hicks, & R. Simmons, "The national robotics initiative: a five-year retrospective," IEEE Robotics & Automation Magazine 26 no. 3 (2019), 70-77.
108. B. C. Kok, & H. Soh, "Trust in robots: Challenges and opportunities," Current Robotics Reports 1, (2020), 297-309.
109. K. E. Schaefer, J. Y. Chen, J. L. Szalma, & P. A. Hancock, "A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems," Human Factors 58, no. 3 (2016), 377-400.
110. J. Kirkpatrick, E. N. Hahn, & A. J. Haufler, "10 Trust and Human–Robot Interactions," in Patrick Lin, Keith Abney, and Ryan Jenkins (eds), Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence (New York, 2017; Oxford Academic, 19 Oct. 2017), 91.
111. L. Laursen, "Robot to human: Trust me," IEEE Spectrum 50, no. 3 (2013), 18-18.
112. P. A. Hancock, D. R. Billings, K. E. Schaefer, J. Y. Chen, E. J. De Visser, & R. Parasuraman, "A meta-analysis of factors affecting trust in human-robot interaction," Human factors 53, no. 5 (2011), 517-527.
113. B. F. Malle, & D. Ullman, "A multi-dimensional conception and measure of human-robot trust," In C. S. Nam and J. B. Lyons (eds.), Trust in human-robot interaction: research and applications, (Elsevier: 2021), 3-25.

Choke, Collaborate, and Coordinate: Countering North Korea's Cybercrime Threats

Mark Bryan Manantan

Despite the imposition of international sanctions, North Korea has made progressive leaps to advance its nuclear weapons program. The costs of such coercive measures have not effectively deterred North Korea to capitulate, or course correct its behavior. As a prominent instrument of economic statecraft—often at the large disposal of great powers like the US and China—sanctions have yielded mixed results. With its pixelated track record, scholars and policymakers are divided regarding its continuing efficacy to influence policy preferences or achieve tangible results as in the case of North Korea.[114]

Driven in large part by either innovation or desperation, Pyongyang has found creative ways to evade the economic sanction payload that meant relying on cost-effective and asymmetric capability like cyber operations. Referred to North Korea's "all-purpose sword," cyber operations provide Pyongyang untethered access to the rest of the world amid the veneer illusion of its exclusion or being "off the grid" from the internet and the global financial and trading system.[115]

Although attribution—at the technical, legal, and political level—has been frequently used to name and shame or hold North Korea accountable for its malicious cyber activities, the opaque nature of cyber operations still afford it a cloak of anonymity which allows plausible deniability. With the advent of cryptocurrencies combined with its deployment of ransomware attacks, North Korea will continue to advance its nuclear weapons program. Such malicious activities can undercut the current momentum of the US and the ROK's technological competitiveness. Consequently, it continues to erode international security and stability.

This article examines the implications of North Korean-linked cybercrime operations in undercutting the prospects of technological innovation spanning critical technologies like Artificial Intelligence (AI) and semiconductors in the context of US-ROK relations. Conversely, it will also assess the far-reaching impact of Pyongyang's cyber operations in undermining international regimes like non-proliferation and state sovereignty under international law governing cyberspace. It contends that if unaddressed over time, North Korea's cyber-enabled crimes could lead to the weakening and potential breakdown of such norms and standards which underline international security and stability. To counter this, three policy recommendations are enumerated to forge a stronger US-South Korea cyber cooperation: Choke, Coordinate, and Collaborate.

Unpacking the Double Helix Threat: Ransomware and Cryptocurrencies

Initially, North Korea's cyber operations were designed to inflict social disruption—as exemplified by high-profile attacks against Sony Pictures in 2014 and the WannaCry ransomware in 2017—and purloin classified data from governments. But as North Korea grapples with tightening sanctions from the United Nations (UN) and the US and its allies, the Kim Jong-un regime faced immense pressure to find other means to support the country's struggling economic condition.[116] Relying on its cyber capabilities, North Korea's hacking units shifted their attention towards cybercrime to achieve two objectives: keep the economy afloat and sustain its military, and nuclear weapons program.[117]

To date, the most notable act of North Korea's cybercrime was the 2016 Bangladesh Bank heist linked to the Lazarus Group that wiped out $81 million through fraudulent bank transfers.[118] In 2020, the UN Security Council's Democratic People's Republic of Korea Sanctions Committee's Panel of Experts found that North Korea's cyberattacks netted a whooping revenue of $2 billion that supported its weapons of mass destruction programs (WMD).[119] The COVID-19 pandemic further highlighted North Korea's evolving cyber tactics to further raise funds for its WMD programs amid the country's looming food shortages and health crisis.[120] Despite being poor, isolated, and heavily sanctioned, North Korea even conducted more missile tests, leaving policymakers, scholars, and cybersecurity experts to ask: Where did the money come? —Cryptocurrency.

Cryptocurrencies are digital currencies not supported by central banks, meaning they operate outside the remit of the international banking system. Rather than relying on financial intermediaries, cryptocurrencies utilize a decentralized network of users for verification using

alphanumeric aliases.[121] Because they are deregulated and decentralized, cryptocurrencies are effective tools for sanction evasion. Financial transfers are not processed through conventional payment systems, which complicates the tracking and calculation of cryptocurrencies. This scheme creates barriers to financial and regulatory bodies and law enforcement agencies. For instance, North Korea's Lazarus Group has utilized Tornado Cash, a platform that uses different types of cryptocurrencies to obscure the origins of funds. So far, the traceability of transactions of such virtual assets were instrumental for the Kim Jong-un regime to recover lost revenues due to sanctions, launder proceeds from its cybercrime activities, and even pay for its imports.

As a low-cost and low-risk means of cybercrime, and with very little chance of international and legal retribution, ransomware attacks were found to be highly lucrative tools for North Korea compared to its traditional illicit activities like counterfeiting or smuggling.[122] Like Iran and Russia, North Korean hacking groups extort ransomware payments through cryptocurrencies from their victims in exchange for a decryption key. Bitcoin is the cryptocurrency of choice for ransomware as they are easily available and does not require personal identifiable information.[123] This allows adversaries to extract payments from victims while maintaining anonymity.

Recently, the US Government has publicly attributed two ransomware families—Maui and H0lyGhOst—to North Korea which targeted healthcare and public health sectors.[124] High profile North Korean cyber hacking groups like Lazarus, APT38, BlueNoroff and Stardust Chollima are becoming increasingly active in cryptocurrency thefts. In April 2022 the US Department of Treasury identified the Lazarus Group and DPRK cyber group APT38 responsible for the $620 million cryptocurrency heist from the video game Axie Infinity.[125] Recognizing the growing "two-headed" cyber threats that cryptocurrencies and ransomware attacks pose, the US Treasury has sanctioned a cryptocurrency exchange for facilitating ransomware payments by a criminal cyber group.[126]

Exact figures are difficult to quantify, but the 2021 UN Security Council estimated that North Korea has generated a revenue income of approximately $316.4 million in virtual currency between January 2019 and November 2020.[127] Prior to that, cyber criminals also extorted mainstream cryptocurrencies Bitcoin and Ethereum following an attack on Bithumb, a South Korean digital asset trading platform. These earnings suggest that North Korea's ransomware attacks aided by cryptocurrency operations have become significant revenue-generating streams.

As international efforts to regulate the cryptocurrency environment gain further momentum, North Korea will continue to rely on the vast web of cybercrime networks spread throughout

Russia, Iran, and India to support its illicit crypto activities.[128] Aside from partnerships, North Korea is also capitalizing on the fragmented digital currency landscape and using it to its advantage. The rise of decentralized finance—that removes third party institutions and processes like brokerages, exchanges, and banks—has allowed North Korean hackers to launder stolen funds.[129] Additionally, Over the Counter (OTC) brokers continue to be vital assets in converting digital currencies into actual funds. In 2018, the US Treasury's Office of Foreign Assets Control indicted two Chinese nationals, Tian Yinyin and Li Jiadong, after laundering money from a 2018 cyber intrusion of a cryptocurrency exchange conducted by the Lazarus Group.[130] Tian and Li transferred the stolen money from DPRK-controlled accounts to Chinese bank addresses to withdraw the funds and obfuscate its origins.[131]

Assessing the Implications of North Korea's cybercrime on technological innovation, nonproliferation, and international law in cyberspace

Amid increasing sophistication of cyber capabilities, North Korea remains more circumspect in engaging in a full-blown cyberwarfare that rises above the threshold of armed conflict.[132] However, North Korea's cyber-enabled crimes will only continue to pose daunting economic, security and strategic challenges one cyber intrusion at a time. In response to the alarming impact of North Korea's ransomware attacks, the US and South Korea issued joint-advisory, noting how profits generated from its cyber-related crimes were critical in enhancing the tools, tactics, and procedures of its cyber units.[133]

The increasing sophistication of North Korea's cyber capabilities threatens the deepening collaboration of the US and South Korea in critical and emerging technologies. But North Korea's cyber operations do not only prey on American and South Korean tech companies. Its cyber operations have ripple effects which could undermine the entire innovation ecosystem that depends on the complex web of research and development collaboration and partnerships, intellectual property rights arrangements, exchange of data, and talent, and global supply chain.

On the eve of the US-ROK's Mutual Defense Treaty's 70th anniversary, US President Joe Biden and South Korean President Yoon underscored the urgency to develop new technologies like quantum technology, AI, and biotechnology and address the global shortage of semiconductor chips.[134] On cybersecurity, Seoul and Washington pledged to develop a Strategic Cybersecurity Cooperation Framework to deter cyber adversaries, secure critical national infrastructure, combat cybercrime, and secure cryptocurrency and blockchain applications. Both Presidents

agreed on the integral role of North Korea's cyber operations as the culprit behind its continuing development of WMD and ballistic missiles.[135]

North Korea is staying ahead of the curve, exhibiting strong prospects of integrating AI to amplify its offensive cyber operations.[136] The regime is exploring the role of AI to enhance its cyber capabilities to conduct stealthy operations through neural networks and genetic algorithms.[137] North Korea's AI-enabled cyberattacks can fast-track the identification of zero-day vulnerabilities present in US and South Korean computer systems. This may compromise nuclear command, control, and communications systems and degrade the alliance's extended deterrence. As the US and South Korea potentially explore the establishment of data-sharing mechanisms to advance the military and commercial applications of AI, North Korea may use adversarial AI to manipulate the data, invert training models, and/or use malware against AI systems.[138]

Taking cues from similar largescale cyberattacks like the SolarWinds, and the Colonial pipeline incidents, North Korea's supply chain compromise is gaining traction. Hackers associated with the Lazarus Group were found to have breached 3CX, a software firm that provides voice and video calls to large swathes of multinational firms.[139] Forensic analysis show that North Korean hackers installed malware and backdoors to steal credentials and information to target cryptocurrency companies.[140] The latest incident demonstrates North Korea's growing supply chain attack capabilities that uses legitimate security software to deploy malicious payloads.[141]

At the recent Biden-Yoon summit, the two countries repeatedly mentioned supply chain resilience as key to rapid technological advancement under the CHIPS act umbrella.[142] In recent years, the US and South Korea have established a working group that deals with manufacturing resilience and dual-use export controls, specifically on semiconductors.[143] But to achieve resilience, chip security should be at the core. Semiconductor companies will surely be at the frontlines of North Korean supply chain cyberattacks, and therefore, hardware and software assurances are critical to mitigate potential threats at the very onset of the research and development down to the manufacturing process.[144]

As pointed out, North Korea will continue to wreak havoc on computer systems and networks of critical infrastructure, and in worst-case scenario, even destabilize the global financial system. But equally concerning are the cumulative effects of North Korea's cybercrime spree. The Biden-Yoon summit has recognized North Korea's illicit cyber activities as the highly-lucrative revenue-generating mechanism funding the regime's nuclear programs that ultimately threatens international stability. But the UN Panel of Experts went even further stating that North Korea's cyber-enabled

theft has serious ramifications toward international norms and standards of nonproliferation and demonstrates a clear transgression of state sovereignty under international law.

Since 2019, the UN Panel of Experts have identified North Korean hackers engaged extensively in cyberattacks to evade sanctions, including spear-phishing attempts against UN representatives of Member States of the Security Council. The UN Panel estimates that North Korea has generated a total revenue of $2 billion, with increasing contribution from cryptocurrency heist which is critical to North Korea's WMD programs. Like the WannaCry ransomware, North Korea's increasing wave of crypto heist mainly through crypto jacking and cryptocurrency mining impinge on state sovereignty.[145]

Although digital forensic investigations and technical attribution of cybersecurity firms Kaspersky and Symantec point to the Lazarus Group as the penetrator of WannaCry due to identical malware used in the 2014 Sony hack and the 2016 Bangladesh heist, determining North Korea's legal liability remains a daunting task.[146] Given the borderless nature of conducting cybercrime, pressing criminal culpability will still depend heavily on national crime investigations and mutual legal assistance among authorities that have jurisdictions in countries where North Korean hackers and their affiliates operate. And given the current patchwork of cybercrime legislation in countries where North Korean hackers are located, prosecuting them will still be difficult.

Recommendations

The evolving scale, speed, and reach of North Korea's cyber operations have demonstrated its capability and intent to disrupt, collect intelligence, generate illegal revenues, and undermine technological collaboration.[147] The borderless nature of cyberspace, and the fragmented regulatory landscape of cryptocurrencies adds complexity in prosecuting North Korean hacking groups and their affiliate networks and partners. North Korea's nuclear arsenal remains the ultimate guarantor of regime survival, yet without its cyber capabilities its WMD programs will not prosper.

North Korea's proven success of exploiting vulnerabilities to launch ransomware attacks and subsequently use cryptocurrency to launder stolen funds provide other malicious state and non-state actors a viable business model they can emulate. With the advent of AI-enabled cyber capabilities, and the rapid integration of global supply chain through the adoption of the Internet of Things, nefarious entities are afforded with an expanding threat surface, greater resources,

and financial incentives to pursue cybercrime activities. Over time, the cumulative impact of such malign activities that transgresses international agreements on non-proliferation, cyber norms, and international law on responsible state behavior in cyberspace will weaken international peace and stability.

The US and South Korea should therefore ramp up their cyber cooperation in a strategic fashion. To be more productive and impactful, Seoul and Washington D.C. should address the fundamental root cause of the problem which is the funding source that supports and sustains North Korea's cyber operations and consequently its WMD programs. Three policy recommendations are outlined to achieve this:

Choke. The US and South Korea should go beyond "following the money" to see the bigger picture of the ransomware payment ecosystem to trace and stop the movement of paid ransom.[148] Using blockchain technology, US investigators were able to track the movement of illicit funds—a breakthrough in the growing market of ransomware attacks and rising liquidity of cryptocurrency markets.[149] Building on this, the US and South Korea should act more proactively to identify potential choke points of the ransomware payment process. To achieve this, acquiring full visibility of the ransomware payment ecosystem is vital. And this will only be feasible by piecing often disparate information from concerned stakeholders—cyber insurance companies, web host providers, operating system vendors, cryptocurrency platforms cybersecurity vendors, security researchers and law enforcement officers—to identify the blockchain addresses of malign actors, and trace movement of illicit funds. Targeting the source of its revenues can dent North Korea's ability to further develop its cyber capabilities.

Coordinate. The US and South Korea should improve their alignment towards cryptocurrency regulations to achieve greater information-sharing. Seoul and Washington D.C.'s varying regulatory and legal approaches on virtual currencies present a gaping vulnerability.[150] If left unattended, the two countries will continue to struggle to materialize efforts that help track and recover crypto payments. Establishing a common definition and standards under the US and South Korea joint cyber working group should be a good starting point to mitigate any frictions and accomplish regulatory convergence. This will allow US and South Korean regulatory, intelligence, and law enforcement agencies enhance coordination to target cyber-enabled financial activities, while adopting a balanced approach towards innovation and regulation of digital assets.

Collaborate. Finally, fighting cyber-enabled crime requires coalition and partnership-building. North Korean cyber hackers rely on their web of networks and partners spread mostly in Southeast Asia, and Central Asia. Therefore, the US and South Korea should continue to collaborate with financial and law enforcement agencies in those jurisdictions through cyber capacity-building initiatives to improve legal and technical skills to fast-track mutual assistance on investigation. As North Korea remains a key member of the ASEAN Regional Forum, the US and South Korea should reinforce their existing cyber consultations with greater attention among ASEAN member states where crypto engagement is rapidly gaining much traction.[151]

114. Jiawen Chen, "Why Economic Sanctions on North Korea Fail to Work?," China Quarterly of International Strategic Studies 03, no. 04 (January 2017): 513–34, https://doi.org/10.1142/S2377740017500300; Mikael Weissmann and Linus Hagström, "Sanctions Reconsidered: The Path Forward with North Korea," The Washington Quarterly 39, no. 3 (July 2, 2016): 61–76, https://doi.org/10.1080/0163660X.2016.1232635.

115. Jeong Yoon Yang, So Jeong Kim, and Il Seok Oh (Luke), "Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities," in Information Security Applications, ed. Dooho Choi and Sylvain Guilley, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2017), 102–11, https://doi.org/10.1007/978-3-319-56549-1_9

116. "Note by the President of the Security Council," United Nations Security Council, March 4, 2021, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf; "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," US Department of the Treasury, June 9, 2023, https://home.treasury.gov/news/press-releases/sm774.

117. Choe Sang-Hun, "North Korea Tries to Make Hacking a Profit Center," The New York Times, accessed June 13, 2023, https://www.nytimes.com/2017/07/27/world/asia/north-korea-hacking-cybersecurity.html.

118. "The Lazarus Heist: How North Korea Almost Pulled off a Billion-Dollar Hack," BBC News, accessed June 13, 2023, https://www.bbc.com/news/stories-57520169.
119. "Note by the President of the Security Council," United Nations Security Council, August 30, 2-2019, https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/S_2019_691.pdf.
120. Ethan Jewell, "North Korean Hackers Weaponize COVID Outbreak in Latest Cyber Attack," NK News, May 19, 2022, https://www. nknews.org/2022/05/north-korean-hackers-weaponize-covid-outbreak-in-latest-cyber-attack/; Edith M. Lederer, "UN Experts: North Korea Using Cyber Attacks to Update Nukes," AP News, accessed June 13, 2023, https://apnews.com/article/technologyglobal-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33.122 William Alan Reinsch and Andrea L. Palazzi, "Cryptocurrencies and US Sanctions Evasion: Implications for Russia," December 20, 2022, https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia.
121. William Alan Reinsch and Andrea L. Palazzi, "Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia," December 20, 2022, https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia.
122. Bruce Klingner, "North Korea Cybercrimes Undermine Sanctions and Threaten America," The Heritage Foundation, Accessed June 13, 2023, https://www.heritage.org/cybersecurity/commentary/north-korea-cybercrimes-undermine-sanctions-and-threaten-america.
123. Bart Lenaerts-Bergmans, "Follow the Money: How Cybercriminals Monetize Ransomware," Ransomware.org, December 19, 2022, https://www.crowdstrike.com/blog/how-ecriminals-monetize-ransomware/.
124. Ionut Arghire, "US, South Korea: Ransomware Attacks Fund North Korea's Cyber Operations," SecurityWeek, February 10, 2023, https://www.securityweek.com/us-south-korea-ransomware-attacks-fund-north-koreas-cyber-operations/.
125. "North Korea Cyber Threat Overview and Advisories," CISA, June 13, 2023, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.
126. Heeu Millie Kim, June Lee, and Rachel Paik, "North Korean Cryptocurrency Operations: An Alternative Revenue Stream," Harvard Belfer Center, May 2022, https://www.belfercenter.org/sites/default/files/files/publication/North%20Korean%20Cryptocurrency%20Operations%20-%20An%20Alternative%20Revenue%20Stream.pdf.
127. Ibid.
128. Ibid.
129. Ibid.
130. "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," US Department of the Treasury, June 9, 2023, https://home.treasury.gov/news/press-releases/sm924.
131. Ibid.
132. 133. Min-hyung Kim, "North Korea's Cyber Capabilities and Their Implications for International Security," Sustainability 14, no. 3 (January 2022): 1744, https://doi.org/10.3390/su14031744.
133. Ionut Arghire, "US, South Korea: Ransomware Attacks Fund North Korea's Cyber Operations," SecurityWeek, February 10, 2023, https://www.securityweek.com/us-south-korea-ransomware-attacks-fund-north-koreas-cyber-operations/.
134. Chang Jae Sun, "Full Text of Joint Summit Statement between Yoon, Biden," Yonhap News Agency, April 27, 2023, https://en.yna.co.kr/view/AEN20230427001900315.
135. Ibid.
136. Scott Harold, Nathan Beauchamp-Mustafaga, Jenny Jun, "Will Artificial Intelligence Hone North Korea's Cyber 'All-Purpose Sword'?," Korea Economic Institute of America , Accessed June 13, 2023, https://keia.org/publication/will-artificial-intelligence-hone-north-koreas-cyber-all-purpose-sword/.
137. 138. Su Fei, "Military Developments in Artificial Intelligence and Their Impact on the Korean Peninsula," in The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, ed. Lora Saalman, Stockholm International Peace Research Institute, 2019, https://www.jstor.org/stable/resrep24532.12.
138. 139. Mark Bryan Manantan, "The Cyber-AI Nexus: Implications for the US-Japan Cybersecurity Alliance," in US-Japan Cybersecurity Cooperation: Beyond the Tokyo 2020 Olympics, ed. Mark Bryan Manantan and Crystal Pryor, Pacific Forum, 2021, https://pacforum. org/wp-content/uploads/2021/11/PacForum_Report_Final_Single_Page.pdf

139. A. J. Vicens, "Supply Chain Cyberattack with Possible Links to North Korea Could Have Thousands of Victims Globally," CyberScoop, March 29, 2023, https://cyberscoop.com/3cx-hack-supply-chain-north-korea/; Sean Lyngaas, "North Korean Hackers Breach Software Firm in Significant Cyberattack," CNN Politics," June 13, 2023, https://www.cnn.com/2023/04/20/politics/north-korea-hacking-supply-chain-3cx-mandiant/index.html.

140. Carly Page, "3CX Blames North Korea for Supply Chain Mass-Hack," TechCrunch," April 11, 2023, https://techcrunch.com/2023/04/11/3cx-north-korea-cryptocurrency-hack/.

141. Sergiu Gatlan, "North Korean State Hackers Start Targeting the IT Supply Chain," Bleeping Computer, October 26, 2021, https://www.bleepingcomputer.com/news/security/north-korean-state-hackers-start-targeting-the-it-supply-chain/.

142. "Leaders' Joint Statement in Commemoration of the 70th Anniversary of the Alliance between the United States of America and the Republic of Korea," The White House, April 26, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/04/26/leaders-joint-statement-in-commemoration-of-the-70th-anniversary-of-the-alliance-between-the-united-states-of-america-and-the-republic-of-korea/.

143. "United States - Korea Supply Chain and Commercial Dialogue Ministerial Joint Statement," US Department of Commerce, April 27, 2023, https://www.commerce.gov/news/press-releases/2023/04/united-states-korea-supply-chain-and-commercial-dialogue-ministerial.

144. "NSA Publishes Guidance on Characterizing Threats, Risks to DoD Microelectronics," National Security Agency/Central Security Service, accessed June 13, 2023, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3092566/nsa-publishes-guidance-on-characterizing-threats-risks-to-dod-microelectronics/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3092566%2Fnsa-publishes-guidance-on-characterizing-threats-risks-to-dod-microelectronics%2F.

145. North Korea employs three methods for its cryptocurrency activities: crypto mining, crypto jacking, and fraudulent initial coin offerings (ICOs). Crypto mining entails solving cryptographic equations to win rewards in the form of cryptocurrency. This means the miner will solve a cryptographic function to successfully verify a cryptocurrency transaction which is then added to a blockchain or a public record of all cryptocurrency transactions. Since 2017, North Korea has begun mining bitcoin but due to its energy-intensive and high computational power it prefers Monero over other mainstream bitcoin platforms like Ethereum due to lover technical requirements. In crypto jacking, hackers use malware through phishing and spear-phishing attacks, or inserting mining scripts that runs on browsers. Infected computer systems and networks bear the costs of crypto mining that include electricity as well as the wear and tear of a users' device or equipment while tokens are deposited in the account of the hacker. Crypto jacking allows cyber criminals to conceal operations while capitalizing the network bandwidth to engage in crypto mining to overcome limited computation requirements. ICOs involves raising capital to launch new tokens, apps, goods, or services. Ethereum is the most popular utility tokens. Another type is called security tokens which act as a digital contract that is represents a fraction of an asset with tangible value in the form of real estate, cars, or ships. Marine Chain is North Korea's most prominent fraudulent ICO that is an asset-backed security token for tokenized shipping vessels. Through Marine Chain, North Korea was able to purchase and trade the fractional ownership of marine assets, while securing illicit funds from investors and even interests in maritime shipping vessels. It also aided North Korea's illegal ship to ship transfers. More information: Heeu Millie Kim, June Lee, and Rachel Paik, "North Korean Cryptocurrency Operations: An Alternative Revenue Stream," Harvard Belfer Center, May 2022, https://www.belfercenter.org/sites/default/files/files/publication/North%20Korean%20Cryptocurrency%20Operations%20-%20An%20Alternative%20Revenue%20Stream.pdf

146. "WannaCry Campaign: Potential State Involvement Could Have Serious Consequences," CCDCOE" accessed June 13, 2023, https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/; Alex Hern, "Swift Network Bank Thefts 'linked' to Sony Pictures Hack," The Guardian, May 27, 2016, sec. Technology, https://www.theguardian.com/technology/2016/may/27/swift-network-bank-theft-sony-pictures-hack-lazarus-symantec.

147. Quentin Hodgson et al., Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace (RAND Corporation, 2019), https://doi.org/10.7249/RR2961.

148. Gordon Archibald Chopra Paul Black,Priyank Baveja,Saahil, "Using Blockchain to 'follow the Money' in Ransomware -

KPMG Australia," KPMG, June 5, 2023, https://kpmg.com/au/en/home/insights/2021/08/blockchain-analytics-tools-follow-money-in-ransomware-cases.html.

149. Ibid.

150. Jason Bartlett, "How to Strengthen South Korea-US Cooperation on Combatting Cyber-Enabled Financial Crime," The Diplomat, March 25, 2022, https://thediplomat.com/2022/03/how-to-strengthen-south-korea-us-cooperation-on-combatting-cyber-enabled-financial-crime/.

151. Office of the Spokesperson, "The 6th US-Republic of Korea Cyber Policy Consultations," United States Department of State, accessed December 15, 2022, https://www.state.gov/the-6th-u-s-republic-of-korea-cyber-policy-consultations/; "Growing Crypto Engagements Carries Risks for SE Asian Banks," January 27, 2022 https://www.fitchratings.com/research/banks/growing-crypto-engagement-carries-risks-for-se-asian-banks-27-01-2022.

Concluding Remarks

Mark Bryan Manantan

If President Yoon's surprise performance was the barometer of the current state of the US-ROK relations, the answer is obvious. It is easy to just sit back and sing along as President Biden did. But not everybody seems to approve of Yoon's performance as he faced mounting criticism at home for his anti-feminist legislation and rapprochement with Japan. Like Yoon, President Biden is also wrestling with inflation, immigration, and a potential rematch with Donald Trump in the 2024 US Presidential elections. It thus takes more than just a catchy melodramatic pop song to solve the barrage of challenges animating the US-ROK alliance.

With the release of South Korea's National Security Strategy (NSS), the Yoon administration outlines a more ambitious defense and security policy outlook. While North Korea remains a key defense and security priority for Seoul, the latest iteration of the NSS steps out of the box, echoing a more global South Korea keen to tackle non-traditional security threats like supply chain resilience and critical technologies that are covered in-depth in our publication. Our hope is that our edited volume extends the celebratory high of Washington and Seoul beyond the commemorative summit of the MDT. Ideally, the policy recommendations pitched here jumpstart interventions that are fit for purpose yet flexible to cement a path forward towards an enduring US-ROK alliance.

PACIFIC FORUM
INTERNATIONAL

pacforum.org | pacificforum@pacforum.org