A Joint Report of the
CSIS INTERNATIONAL SECURITY PROGRAM
AND THE CHEY INSTITUTE

JUNE 2021

Geopolitical Implications of Scientific Innovation Trends in Northeast Asia

CO-CHAIRS
Seth G. Jones
Park In-kook

PROJECT DIRECTORS
Andrew P. Hunter
Hong Kyu-Dok

CHEY | CHEY INSTITUTE FOR ADVANCED STUDIES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Joint Report of the
CSIS INTERNATIONAL SECURITY PROGRAM
AND THE CHEY INSTITUTE

JUNE 2021

Geopolitical Implications of Scientific Innovation Trends in Northeast Asia

CO-CHAIRS
Seth G. Jones
Park In-kook

PROJECT DIRECTORS
Andrew P. Hunter
Hong Kyu-Dok

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

CHEY | CHEY INSTITUTE FOR ADVANCED STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

About the Chey Institute for Advanced Studies

The Chey Institute for Advanced Studies is a nonpartisan think tank with the mandate to explore the geopolitical dynamics and avenues of scientific innovations in Northeast Asia and beyond. It was established in October 2018 to honor the 20th anniversary of the passing of CHEY Jong-hyon, the former chairman of SK Group.

Today's world faces a wide range of risks and opportunities caused by a rapidly transforming world. The Chey Institute is committed to identifying and analyzing these risks and opportunities, and offering practical ways to manage them so that the world can better prepare for the future.

In doing so, the Chey Institute partners with leading academic institutions, research organizations, and think tanks around the world to establish a global network consisting of leading thinkers committed to solving the challenges that humanity faces today.

Acknowledgments

This collaborative project was made possible by the generous support of the Chey Institute for Advanced Studies. The editors are grateful for the participants at the Seoul conference and Washington workshop who contributed their time and ideas and the teams at both organizations that made these cohosted events a success and enabled this report. The editors would like to specifically thank Asya Akca for her work in organizing the Washington workshop and support for the paper; Wes Rumbaugh for his insights on missile advances; Ashley Park and Astrid Price for their support and for coordinating the project's conclusion; as well as Emma Bates, Phil Meylan, Jeeah Lee, Elizabeth Richardson, and the CSIS iDeas lab for their editorial assistance. Finally, the authors wish to thank John J. Lee for his contributions and invaluable role in coordinating with the Chey Institute team.

CHEY-CSIS Conference on Geopolitical Risks & Scientific Innovation Participants

(by alphabetical order, positions as of January 2020)

U.S. Participants

Jason Brown, Director of the Chief of Staff, U.S. Air Force

Morgan Dwyer, Fellow; Deputy Director for Policy Analysis, Defense-Industrial Initiatives Group, CSIS

R. David Edelman, Director of Project on Technology, the Economy, and National Security (TENS), MIT

Michael Hamel, (Ret.) Lieutenant General, U.S. Air Force; (Ret.) Vice President and General Manager of Commercial Space, Lockheed Martin Space Systems

Kathleen Hicks, Senior Vice President; Henry A Kissinger Chair; and Director of the International Security Program, CSIS

Andrew P. Hunter, Senior Fellow; Director of the Defense-Industrial Initiatives Group, CSIS

Brett Lambert, Managing Director, The Densmore Group, LLC

Lindsey R. Sheppard, Fellow, CSIS

ROK Participants

Ahn Jung Ho, Professor, Seoul National University

Hong Kyu-Dok, Professor, Sookmyung Women's University

Ju Gwang-Hyeok, Executive Director, Korea Aerospace Research Institute

Jung Hee-Tae, Chair Professor, KAIST

Kim Hyoung Joong, Professor, Korea University

Kim Kwang-Jin, Brigadier General, ROK Air Force

Kim Yoon, Chief Technology Officer; Executive Vice President; and Head of the AIX Center, SK Telecom

Lee Geunwook, Professor, Sogang University

Lim Jong-in, Professor, Korea University

Lim KiHoon, Brigadier General, ROK Army

Park Byung Jin, Vice President, Advanced Defense Technology Research Institute, Agency for Defense Development (ADD)

Park In-kook, President, Chey Institute for Advanced Studies; President, Korea Foundation for Advanced Studies

Reu Taekyu, Vice President, Defense Science & Technology Academy, ADD

Final Report Editors

Gregory Sanders, Fellow; Deputy Director for Research, Defense-Industrial Initiatives Group, CSIS

Lindsey R. Sheppard, Fellow, CSIS

Kim Jina, Research Fellow, Korea Institute for Defense Analyses

Lee Geunwook, Professor, Sogang University

Contents

1

Executive Summary

This report examines the implications of scientific innovations and emerging technologies on geopolitics in Northeast Asia. It focuses on five areas: (1) data-driven techniques and software-intensive technologies, (2) advanced materials and supply chains, (3) cybersecurity, (4) uncrewed systems and robotics, and (5) space technologies, including satellites and missiles. In doing so, this report assesses their implications for national security and identifies the opportunities they present for bilateral and regional cooperation. The findings are a reflection of expert perspectives and analyses, including from leading experts within the security and foreign policy communities in both the United States and the Republic of Korea (hereafter, Korea or ROK).

As a collaborative effort between the Center for Strategic and International Studies (CSIS) and the Chey Institute for Advanced Studies (CHEY), the project identifies several findings. The main takeaways are as follows:

- The applications of today's emerging technologies are exacerbating regional tensions, bringing new considerations to longstanding security challenges, and propelling new non-state and commercial actors onto the global stage.
- Effective engagement with the private sector—the driving force in scientific innovation and technology development—must be made a priority effort by countries and government agencies to effectively address modern challenges to the geopolitical order in Northeast Asia.

- Establishment of appropriate norms and standards relating to the application of emerging technologies, such as artificial intelligence (AI) and space systems, is needed to govern the interconnectedness of technologies and national security.
- A "high-tech" alliance, including cooperation in cybersecurity, space, and information communications technology (ICT) infrastructure, provides the U.S.-ROK alliance with the most promising opportunity to strengthen technological and defense cooperation and to form a common front to shape the strategic impact of scientific innovation on geopolitics.

Successful extension of the alliance will be most likely if it is built on a "sturdy foundation" of diplomatic efforts that find common ground between both countries' concerns about external threats from potential adversaries and that address the potentially uneven economic costs of closer technology cooperation.

Key Elements of Scientific Innovation Trends in Northeast Asia

This section briefly highlights the current status of burgeoning technologies in five key areas and explores new challenges and difficulties in managing these technological innovations in terms of security concerns in Northeast Asia.

- **Data-driven techniques and software-intensive technologies**, including AI, machine learning, and cloud computing, are driving scientific innovations in this era. Both the public and private sectors of Northeast Asian countries are racing to attain dominance in employing AI technologies over a wide area of applied fields, including for commercial and military purposes. However, potentially problematic transfers of software-based technologies such as AI cannot be managed smoothly through existing hardware-based control regimes, on which most countries continue to rely. Abusive uses of AI could introduce unrecognized or unfamiliar risks in the form of flawed data processing and cyberattacks.
- **Advanced materials and their supply chain implications** are emerging as a major source of strategic advantage. U.S.-China competition is particularly fierce in critical areas such as advanced microelectronics, including in semiconductors and other microchips. As the global supply chain is becoming increasingly integrated, a debate regarding the need for greater control over supply chains is growing. Specifically, there are growing concerns that this competition may result in a bifurcation between two blocs, one led by China and the other led by a group of nations espousing free markets.
- **Cybersecurity** is another domain in which countries are vying for greater technological advantage in Northeast Asia. Ever expanding connectivity and private networks, coupled with the difficulty of attribution in the cyber realm, are complicating how governments and state services respond to cyber threats. While software-based approaches hold promise for enhancing cybersecurity in managing supply chains, their potential vulnerabilities still demonstrate the importance of maintaining good cybersecurity practices.
- **Uncrewed systems and robotics** have been recognized as transformative technologies. All major actors in Northeast Asia, including those in the private sector, are currently engaged in intense competition over prototyping and fielding various uncrewed systems and robotics, such as drones

and vehicles designed for aerial as well as undersea surveillance. However, the continued fielding of uncrewed systems, especially smaller systems, has revealed challenges and vulnerabilities in counter-uncrewed system capabilities.

- **Space technologies, including satellites and missiles,** have become more widespread and capable in recent years. The "new space" sector has generated a variety of commercial concerns that manage small satellite systems and commercial launch services. Whereas the ROK—following the example of the United States and Japan—has displayed little hesitancy in advancing its space ambitions and missile defense systems, the Democratic People's Republic of Korea (DPRK) has provided the biggest surprise and threat in missile technology development during the past decade. Despite the limitations of its industrial base, the DPRK has unexpectedly made substantial progress in space, satellite, and long-range missile capabilities, which led to Kim Jong-un's declaration during the 8th Congress of the Ruling Workers' Party in January 8, 2021 that North Korea will continue to advance its land- and submarine-launched ICBMs. As a result, changes in newly available technologies—combined with the DPRK's continued investment, lower risk aversion, and willingness to break the mold on how nations previously achieved ballistic missile technology—have the potential to trigger changes in the security environment in Northeast Asia.

Emerging Technologies with Implications for Northeast Asian Security

As mentioned above, emerging technologies have had destabilizing effects in key sectors.

- **Key technological advances by China and the DPRK have shifted** practices and norms across multiple technology domains and have caused a noticeable racing behavior in terms of fielding new technologies. This trend has also revealed the uncomfortable availability of new options for relatively low-cost malicious activities against military or civilian infrastructure—asymmetric attacks that are difficult to rapidly detect and attribute.
- The current technology cooperation among the United States, ROK, and other democracies has contributed significantly to creating a stable environment for technological advances to revamp security dynamics in Northeast Asia. However, **existing cooperation remains vulnerable to adversarial efforts to divide allies** over contentious issues, such as bifurcation of global supply chains.
- This project identified **Northeast Asia's microelectronics supply chain** as a key asset; participants urged the ROK and the United States to place a high priority on protecting vital nodes of this supply chain present in democratic countries.

Norms and Standards of Innovative Technologies

- Given the divisive nature of regional technology collaboration and cooperation, **setting up an appropriate norms and standards regime for emerging technologies is critical** to addressing various security issues in the region. The United States and Korea should play a leading role in laying the groundwork for developing a framework on what behavior is in and out of bounds.
- Upholding norms and standards does not just require detecting and attributing violations, it also means observing and responding when current regimes may be outpaced by changes in technology. **Space, including missiles and satellites,** stands out as an area where established

norms and standards may require revision and should be bolstered by better sensing technology as a result of the small satellite revolution and breakdowns in traditional technology controls. The rapid advancements in satellite development and missile programs, especially by the DPRK and PRC over the past decade, highlight the need for regional actors to engage in robust discussions on emerging norms and standards. A number of participants also raised concerns about North Korea's growing indigenous nuclear capabilities, which stunned the global community in 2017.[1]

- **Developing norms and standards for technologies such as AI, cybersecurity, and uncrewed systems is even more challenging,** in part because these technologies have been advancing at breakneck speed, much faster than national or multilateral regulatory systems can expand capacity to deal with them. In this vein, participants agreed that developing norms and standards in this area will require not just multilateral cooperation but also engaging civil society, academia, and private sector actors who see the benefit in building trust and transparency.
- In those cases where different countries in Northeast Asia have very different ideas about acceptable and unacceptable behaviors, **individual countries cannot just collaborate on multilateral efforts but must also work to improve detection and reduce vulnerabilities.**

Collaboration in Technology Innovation Among Allies in Northeast Asia

While dealing with key emerging technologies and their impact on geopolitics requires broad partnerships across academia, industry, and government, questions about the best venues and practices for international collaboration and cooperation remain unanswered.

- Given the growing share of scientific innovation taking place in the commercial sector, **finding effective ways to engage the private sector in strategic cooperation** should be made a priority issue in security-related U.S.-ROK dialogues. Greater effort is needed to expand collaboration between the private sector, governments, and universities in the field of emerging technologies. Only regular engagements and frequent exchanges based on trust and transparency among relevant stakeholders can address the obstacles standing in the way of the private sector's active involvement. These obstacles include hesitancy within the private sector to work with various branches of governments due to concerns over transferring intellectual property rights or becoming involved with controlled exports. Fears of literal weaponization or weak norms and standards can also undermine private sector partnerships.
- The U.S.-ROK alliance could evolve further if more **members of industry and research communities are involved in broader policy initiatives,** particularly on matters pertaining to national security and strategy. There is still an important role for discussions led by defense agencies, which can be exclusive by necessity, but these should be supplemented by alternate venues, especially in those emerging technology domains where governments are not the primary customer.
- **Cybersecurity, space, and the ICT infrastructure related to data-driven techniques,** such as semiconductors, 5G, AI, and cloud computing, would be natural areas for U.S.-ROK collaboration. Key areas that could be addressed by this collaboration are risks to civil and private infrastructure as well as infrastructure that shares sensitive information for improved interoperability in mutual defense.

- The United States and ROK should expand their bilateral cooperation in emerging technologies; in particular, the United States and Korea have critical opportunities to expand their efforts to advance collaboration in space, uncrewed vehicles, and cyber activity. Greater U.S.-ROK and U.S.-ROK-Japan cooperation may reinforce one another. Increased rapidity and agility in incorporating scientific innovations would be a key marker of success for these efforts.
- Some experts pointed out **the necessity of targeted exercises** that would allow alliance partners to test capabilities, share lessons, and adapt operations to new technologies.
- Efforts to strengthen the U.S.-ROK alliance's deterrence posture should be cognizant of concerns and possible reactions by regional actors. Korea will disproportionately bear the damage of any retaliation by potential adversaries, and understanding one another's perspective must accompany any deepening of cooperation. China's boycott of ROK goods following the ROK decision to deploy Terminal High Altitude Area Defense (THAAD) systems serves as a prime example of a negative reaction by a regional actor hindering efforts to improve ROK's deterrence posture.
- Emerging technologies do pose substantial risks for enabling adversaries to destabilize the security environment in Northeast Asia. The ROK and United States will have to work together to achieve an effective response that fosters democratic values and leverages scientific innovation. Moreover, U.S. experts emphasized the critical role that commercial sectors must play in this process. Success will take a lot of work, dedication, mutual trust, and multi-level cooperation between and within allied countries. CSIS and the CHEY Institute present this report in the hope that the priorities outlined above can inform and support scholars, government practitioners, and those in the private sector working to advance U.S.-ROK security and economic interests.

2

Introduction

Scientific advances and emerging technologies are reshaping the geopolitical environment. Perhaps no region of the world is as central to this shift, and as affected by it, as Northeast Asia. The region is both militarily and economically pivotal, home to a large share of the world's population, many of its biggest ports, and approximately 30 percent of its military forces.[2] While Northeast Asia has been relatively peaceful for the last several decades, its security dynamics are remarkably complex, from the Korean Peninsula to the South and East China Sea areas. Key tech industries dot the region, including the vast majority of the world's semiconductor production, which powers the electronics that underpin major economic sectors and advanced military systems. These tech industries are being shaped by an overarching struggle between nations for strategic advantage and enduring control, which also involves private actors.

An essential feature of the struggle is the interconnectedness of emerging technologies and national security. Nations clearly understand that the technologies that provide economic advantage also convey national security advantage. This linkage between technologies and national security is not new. Technologies such as nuclear energy and rocketry have long been understood as dual-use—having discrete and significant military and commercial applications and demanding careful separation and control between the two. To be effective, these control efforts have required international cooperation. Today's emerging dual-use technologies are responsible for an increasing proportion of militarily relevant innovation, and so national efforts to establish leadership in these technologies are even more intense.

There are new elements, however, that are reshaping how technology affects strategic competition. The private sector now dominates these technologies, challenging the ability for governments and militaries to access, control, and leverage new capabilities and increasing the need for international cooperation. More than two decades of globalization have increased private sector interconnections between Northeast Asian nations and the United States, particularly in the realm of supply chains.

This holds significance for strategic competition. Increased use of commercial components in military supply chains means that it is harder to separate and control the military application of many dual-use technologies. Economic powers can weaponize interdependence, using technology leadership and networks to collect intelligence and even threatening to cut off access to key supplies on which nations' militaries depend.[3] And, unfortunately, military and intelligence uses of technology can have huge commercial implications, for example, when a nation-state actor hacks a commercial enterprise. As a critical engine of the global economy, these dynamics are becoming increasingly important for security in Northeast Asia.

The Center for Strategic and International Studies (CSIS) and the Chey Institute for Advanced Studies (CHEY) set out to foster an in-depth dialogue on the implications of scientific innovation and emerging technology on geopolitics in Northeast Asia. As President Park In-kook addressed during the public conference, the study team "invited the best experts from the United States and Korea to shed light on the impact of cutting-edge science and technology on the geopolitical risks in Northeast Asia and beyond."[4] Specifically, the goal was to explore which emerging technologies have military implications, how these dynamics are likely to progress, what their geopolitical impact is, which mechanisms for international coordination and cooperation are especially promising, and what near-term actions are most essential. Over the course of the project, the Chey Institute and CSIS hosted a widely attended public conference in Seoul, Republic of Korea (hereafter, Korea or ROK), and an off-the-record senior workshop carried out online between U.S. and Korean experts. Perspectives on key technologies came from a wide range of viewpoints from both nations. Notably, key leaders of each of the Korean military services spoke at these events. Likewise, senior leaders from the defense and diplomatic establishment in the United States participated.

As President Park In-kook addressed during the public conference, the study team "invited the best experts from the United States and Korea to shed light on the impact of cutting-edge science and technology on the geopolitical risks in Northeast Asia and beyond."

This report captures the state of key scientific innovations affecting Northeast Asian geopolitics and the most promising opportunities for U.S.-ROK and broader collaboration to shape relevant security implications. The key technology areas examined are:

- Data-driven techniques and software-intensive technologies, such as artificial intelligence (AI) and machine learning;
- Advanced materials and supply chain implications;
- Cybersecurity, including blockchain;
- Uncrewed systems and robotics; and
- Space technologies, including satellites and missiles.

The report goes on to briefly describe the status and importance of these emerging technologies. It then examines three key aspects of their geopolitical impact: (1) the threats and challenges these technologies pose for the existing geopolitical order in Northeast Asia and the military and alliance structures that underpin it; (2) the extent to which norms and standards relating to these technologies are in place or in development and the role that they can play in reshaping or reaffirming the geopolitical order; and (3) the most promising opportunities for cooperation and collaboration among allies in Northeast Asia to ensure that scientific innovation's impact on geopolitics is a net benefit to free societies.

3

Key Elements of Scientific Innovation Trends in Northeast Asia

Data-Driven Techniques and Software-Intensive Technologies

Data and software, including AI, machine learning, and cloud computing, are driving scientific innovation. AI is an umbrella term often used in reference to a variety of computer science disciplines (e.g., machine learning, natural language processing, computer vision), applications (e.g., facial recognition surveillance, targeted advertisements and messaging, intelligent robotic assistants), and theoretical capabilities (e.g., artificial general intelligence). The field of AI is dedicated to the building of intelligent programs and machines to creatively solve problems. Machine learning, which is a subset of AI, provides these systems with the capability to recognize patterns and improve from experience. Globally, the private sector leads in the research, development, and application of AI. Since 2012, machine learning has been successfully applied in a variety of industries, from advertising to healthcare to financial services. Current world leaders in AI and other data-driven technologies are located in the United States, Korea, and across Northeast Asia.

The U.S. Department of Defense (DoD) has prioritized an approach to AI that augments human talent through a focus on intelligence, surveillance, and reconnaissance (ISR), humanitarian assistance and disaster relief, cybersecurity, maintenance and logistics, intelligent business automation, service member healthcare, and command and control. While the U.S. technology sector continues to dominate AI, many nations seek to leverage AI capabilities for their own national interests. The ROK

has articulated the importance of AI to industrial success, particularly in the chip fabrication industry, and its position relative to digital revolution developments such as the Internet of Things (IoT), mobile telecommunications, big data, and cloud computing.[5] Elsewhere in the region, China has declared its intention to be a world leader in AI by 2030 through massive government investment in both commercial and military AI applications.[6] Multiple experts at the workshop observed that China had collected an immense amount of data, a necessary precursor to exploiting associated technology. As a result, "China leads the pack in the world when it comes to vision AI," in the view of one Korean industry expert.

Militarily, Chinese leadership views the application of AI and related techniques as a transformation to "intelligentized" warfare, with AI integrated across the defense enterprise, from weaponry to analytics.[7] The U.S. and Korean militaries are also working to leverage data-driven technologies in military operations across all military domains: land, air, sea, cyber, and space. At the closed workshop, two U.S. technology experts offered similar ideas of what AI would mean on the battlefield: "faster intelligence and situational awareness" and "next-generation command and control networks that connect sensors and decisionmakers at machine speed."

The significance of AI reflects an overarching innovation trend in the twenty-first century: many of the critical technologies are fundamentally software-based, sometimes challenging traditional hardware frameworks and existing practices. Software-based technologies change rapidly through software updates to hardware platforms or by using software to achieve high performance on generic or commercial hardware. The democratization of software results in lower barriers to entry, though it does place a premium on human talent over industrial resources. Managing the transfer of AI is not easily accomplished through hardware-based control regimes, with many open-source algorithms being widely accessible. Despite these shifts, there are still limits on the range of government and private actors that can effectively employ AI. Many AI applications are computationally intensive, requiring significant quantities of data to train algorithms and access to cloud computing capability and modern computer infrastructure, thus demanding significant investment before the benefits of AI can be realized.

Ahn Jung Ho, Lindsey R. Sheppard, Jason Brown, Kim Yoon, and Park Byung Jin (left to right) discuss artificial intelligence and machine learning at the Seoul conference.

AI both behaves and fails in unrecognized or unfamiliar ways; it is vulnerable to a variety of new exploits through both data and models.[8] Many nations have high expectations for deploying AI, which introduces the risk of potential misuse and misunderstanding that may undermine stability, intensify crisis escalation, or exacerbate existing regional dynamics. At the conference, Dr. Kim Yoon noted that AI was vulnerable to bias stemming from flaws in the data used for training the AI models, a concern echoed by Colonel Jason Brown, who pointed out that AI models and user interfaces could also be sources of bias. Finally, risks can stem from the combination of different technology areas. For example, many AI systems rely on cloud-stored data and widely shared connectivity and thus are more vulnerable to cyberattacks.

Together with AI, synthetic biology was identified by one U.S. technologist as one of "the two most important technologies for the next few decades," an assessment echoed by a closing speaker. Synthetic biology research is enabled by the same data-driven techniques that have exponentially decreased the costs of sequencing and synthesizing DNA. These advances have broad implications ranging from vaccine development and personalized medicine to new crops and materials.[9] While synthetic biology holds great promise, it also has risks. For example, an experiment in 2017 found that recreating the smallpox virus would only take "a small scientific team with little specialized knowledge half a year and cost about $100,000."[10] These innovations mean that a wider variety of actors could maliciously introduce a pathogen or, more likely, lead to an accidental release. While not focused on synthetic biology, the United States and ROK have a history of collaboration in this area, including biodefense exercises in the Able Response exercises, which ran through 2016.[11]

Many nations have high expectations for deploying AI, which introduces the risk of potential misuse and misunderstanding that may undermine stability, intensify crisis escalation, or exacerbate existing regional dynamics.

Advanced Materials and Supply Chain Implications

Supply chains for key technology components and materials are emerging as a major source of strategic advantage and competition. Understanding and managing supply chains supporting national defense is particularly important to national governments. However, the struggle for influence over commercial supply chains is an increasingly critical issue for policymakers as well due to the significant economic and security implications.

A key example of this competition is found in advanced microelectronics, including semiconductors and other microchips critical to mobile networking, as well as the materials and equipment used to produce them, which form the basis for advanced technologies such as 5G.[12] The current disputes over 5G equipment provider Huawei as well as efforts by national governments throughout the region

to assert greater control over semiconductor supply chains illustrate the trend. Further, in 2019, semiconductor supply chains were disrupted by a larger diplomatic conflict between the ROK and Japan, with perhaps longer-lasting economic consequences, when Japan restricted exports of core materials used for microchips.[13]

While these technologies have been part of an integrated global supply chain since at least the 1970s, the potential is emerging for a bifurcation in this supply chain between a bloc led by China and another led by a group of free-market nations. The challenge is that China is deeply embedded in the global supply chain and could potentially attract key players in the current supply chain to its side. Such a bifurcation, if it takes hold, would force nations and even individual firms in many cases to choose a side, possibly irrevocably. Bifurcation may have seemed like a far-fetched possibility a few years ago, but the United States, to a great extent, operates bifurcated supply chains for some of its key defense systems already, paying a premium to use specialized domestically produced microelectronics, especially where radiation hardening is a key component. The existence of this U.S.-only supply chain illustrates that bifurcation is possible, but also that it has significant ramifications for cost and innovation.

Software-based technologies, however, may challenge this bifurcation. Software-driven technology can often be easily replicated once it has been demonstrated, assuming intellectual property protections are ignored, and people with critical knowledge of the technology can be recruited and moved easily between nations. On the other hand, trade in software and services is much less internationally integrated today than trade in manufacturing, suggesting that there may be other structural and market factors, such as language and culture, that enable continuing bifurcation in software and services.

Significant investments in microelectronics supply chains are being made by allied governments, in cooperation with industry, to shape the outcome of this strategic competition. With security concerns in mind, the ROK, Taiwan, Japan, and the United States are independently developing supply chains for microelectronics and microelectronics-based technologies. Recent innovation trends are directed at delivering more secure approaches to building and operating such networks, both because commercial entities have begun to place a high priority on securing their networks and information and because industry has developed new concepts for security at the sub-chip and chip levels. While these efforts can be complicated by international trade rules, there is a wide range of potential policy approaches, both carrots and sticks, for national governments to shape the use of these technologies. Disincentives may take the form of policy mandates and oversight and compliance regimes, including specifications, standards, and the imposition of contractor liability, while incentives may incorporate competition and revenue inducements and shared cost/investment approaches.

Cybersecurity

Cyberspace is an arena where geopolitical competition in Northeast Asia plays out daily. The United States, ROK, and Japan have all been at the receiving end of cyberattacks from the Democratic People's Republic of Korea (hereafter, DPRK or North Korea) or China.[14] Ransomware is used to hold cities and municipalities hostage, and financial, banking, and utility infrastructure are frequent targets of denial or shutdown attacks. For governments monitoring cyber activity within their borders, it is often difficult to immediately distinguish between state-sponsored attacks and non-state criminals. In the case of the DPRK, both are often seeking financial gain from their cyber exploits.[15] At the closed workshop, a Korean regional expert estimated that North Korea could draw on a force of 7,000

hackers and has sought to bolster their technological capacities with AI research in partnership with Chinese companies.[16] Cyberattacks can also have geopolitical implications, such as to further military objectives. More broadly, the cyber domain offers many chances to sabotage adversaries, including their foreign and domestic affairs.

Governments continue to grapple with how and when to become involved in cyber activities against private entities. Furthermore, as the number of internet-connected devices grows, cybersecurity is required to ensure the integrity and functionality of the resultant networks. IoT brings network connectivity to everything from daily-use items, such as refrigerators, to critical infrastructure and utilities, such as water and power. However, with connectivity comes vulnerability to cyberattacks and disruption. States continue to work toward establishing norms in cyberspace, such as building international agreements against the targeting of critical infrastructure and utilities. The difficult task of attribution complicates the response options for governments and state services. In the United States and Korea, cybersecurity is carried out by an interconnected web of private sector and government actors who must work together to defend against, attribute, and defeat attacks from state and private actors alike. Increasingly, these efforts can only succeed when coordinated effectively across international borders.

In addition to the defense of networks, software-based approaches can serve to enhance security in real-world supply chains. Blockchain approaches hold promise for supply chain security and transparency, including producing and validating the underlying supply networks, ensuring that not only the design but also the production of these networks are secure. Companies and investors, such as the U.S.-based IBM and Standard Chartered's strategic investment in China-based Linklogis, continue to explore the applicability of trusted-ledgers and smart contracts to banking, finance, shipping, and manufacturing.[17] However, the scalability of such an approach has yet to be demonstrated. Further, while appealing in low-trust or opaque environments, blockchain ledgers are not fool-proof. Security vulnerabilities should be considered before nations integrate the technology in sensitive or critical areas, as demonstrated through the theft of cryptocurrencies and rewritten transaction histories.[18]

Given the limitations of new approaches, it is critical that nations maintain and encourage good cybersecurity practices. Old cyber concerns are still valid as the risk profile is not yet changing drastically. Current threats, such as phishing and outdated operating systems, remain core cyber vulnerabilities and favored exploits for malicious actors.

Uncrewed Systems and Robotics

In Seoul, General Suh Wook, then-chief of staff of the ROK Army, provided a vivid example of uncrewed systems' transformational nature and associated advances in command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) systems.[19] He contrasted the confusion, vulnerability, and casualties that accompanied the rescue attempt of a U.S. helicopter downed in urban Mogadishu, popularized in the film *Black Hawk Down*, to a 2004 helicopter downing in Tal Afar, Iraq. "This time," Suh noted, "soldiers utilizing C4 and ISR systems correctly identified the location of the helicopter, while a [uncrewed aerial vehicle] provided identification and positions of friendly and enemy forces. Kevlar vests and Stryker vehicles protected soldiers from incoming enemy attacks. No books or movies were made about this battle."[20]

All major security actors in Northeast Asia, including the DPRK, are currently employing uncrewed systems. China's People's Liberation Army (PLA) fields a range of uncrewed systems, from the Yilong-2 (GJ-2), a platform comparable to the U.S. MQ-9 Reaper drone, to small quad-copter-style systems. All key security actors are also prototyping and fielding uncrewed systems designed for the undersea, surface maritime, and ground domains. The PLA is particularly notable for its continued prioritization of research and development in uncrewed systems across all domains, emphasizing the incorporation of AI to achieve autonomy and intelligent functionality in these robotic platforms.[21]

Uncrewed systems in the U.S. arsenal go back to the Vietnam war, but Dr. Kathleen Hicks argued that fear of displacing the past and present role of troops had inhibited support for spending.[22] From the U.S. and Korean perspective, uncrewed systems provide a primary means of gathering information on significant military movements and the DPRK's nuclear and missile programs developments, especially given limitations on other sources of information due to the closed nature of the North Korean regime. As with its approach to AI, the United States focuses its research and development efforts on intelligent support to human operators through human-machine teaming. The U.S. Air Force's Loyal Wingman uncrewed aerial system program and the U.S. Navy's Sea Hunter uncrewed surface vehicle program both seek to provide autonomous uncrewed system support to crewed systems. Small drones with swarming capabilities are emphasized for urban warfare environments where these maneuverable systems with limited payloads can provide enhanced situational awareness to personnel in a network-enabled system of systems. Japan's Ministry of Defense (MOD) highlights undersea warfare in future conflict and strategic competition. The MOD's 2019 *R&D Vision* calls for investment in uncrewed undersea systems as well as support for undersea communications infrastructure and intelligent decisionmaking, ostensibly implanted with AI.[23] The ROK's Smart Navy policy includes a greater emphasis on incorporating uncrewed systems and automation enabled by a command and control system that connects various platforms.[24] The ROK Army's 2030 vision strategy seeks new technologies such as drones and IoT systems "to visualize the battlefield, minimize combat damage, and conduct various missions outside the scope of direct action such as detonating explosives and clearing obstacles."[25]

Many of the technology trends in other software-intensive technologies apply to the development of uncrewed systems, particularly those that leverage off-the-shelf commercial equipment such as small drones. These systems employ software-centric design, which often utilizes open-source code and requires competing for talent from a limited pool of researchers. Significant private sector investment is focused on small drone and swarming technology development that will be used for both commercial and military purposes. These trends will only accelerate as technology further diffuses, AI improves, and demographic pressures increase.

The continued fielding of uncrewed systems, particularly smaller systems, is drawing attention to a gap in counter-uncrewed system capability. In instances where drone employment involves potential kinetic use, many unanswered questions arise around risk calculus and potential escalation dynamics. The risk of retaliation or escalation is more ambiguous for the downing of a uncrewed system than a piloted one. It is also unclear how states will respond to the use of kinetic force from a drone, particularly in times of crisis. However, the proliferation of uncrewed systems for security will be driven mostly by their potential to create efficiencies in non-kinetic areas, such as domain awareness and logistics and lift. There will still be implications for signaling and escalation, but overall, the promise of robotics for non-kinetic uses should be embraced by the United States and its allies in the region.

Space Technologies including Satellites and Missiles

While satellite technology saw widespread use in the late twentieth century, scientific innovation and changing economics have contributed to the emergence of a "new space" sector. Commercial access to space is increasing with the advent of small satellite constellations and commercial launch services. While China, Japan, and the United States have historically maintained access to space through launch infrastructure, smallsats, CubeSats, and agreements for launch services provide access to space for a wider variety of nations and commercial entities.[26] Private companies are not only building their own launch infrastructure, but low-cost satellite technologies result in lower barriers to entry for space-based technologies.

In 2018, China carried out 39 orbital launches, whereas the United States conducted 34 launches.[27] In a headline civil space advancement, China's *Chang'e-4* become the first spacecraft to land on the moon's far side. China also has ambitious future civil space plans to include a new orbital space lab and space telescope. This investment consists of both direct spending, $11 billion in 2017, and investment in private Chinese space companies, $336 million in 2018.[28] North Korea also made significant strides in the past decade with its first two successful orbital launches. However, Todd Harrison et al. note that "there is little indication that North Korea is making substantial efforts to build or sustain a space industrial base."[29]

The response of other Northeast Asian nations to these investments and technological security measures is key to understanding the second-order implications of U.S. and Chinese choices. Japan demonstrated advanced satellite technology capabilities in 1998, including a test of satellite docking and robotic arm capabilities. Since passing the Basic Space Law in 2008, Japan has prioritized developing space technologies, and in 2019, it expressed the intention to form a "space defense unit to protect itself from potential threats."[30] The ROK was a later entrant into the space race, putting its first rocket into space in 2013, with reporter Choe Sang-Hun noting that "Korea's space ambitions have languished under the constraints of agreements with the United States" due to U.S. fears of a regional missile arms race.[31] The ROK Air Force has invested in indigenous capacities, including establishing a space unit in 1997 and a Korea Space Operations Center in 2015 to support ROK space assets and track possible space debris sources. This space situational awareness goal is also shared by ROK civil space initiatives now monitoring deep space by telescope for risks from asteroids to space assets as part of a larger mission. The ROK presently seeks to build up its ground station capacity following the example of the United States and Japan, integrating satellite surveillance into missile defense systems and fielding space systems with electro-optical sensors, with the goal of developing satellites employing lasers and radar. In 2018, further launches demonstrated the ROK's satellite and indigenous rocket engine manufacture technology.[32] Defense against space-based technologies, including investments in GPS jamming and spoofing, is a focus of research and development for the major security actors in the region.

The DPRK provided the biggest surprise in missile technology development in the past decade. While the general direction of its research efforts was well anticipated, its rapid pace shocked many analysts due to technological challenges shown in failures of Musudan tests in 2016, the limitations of the DPRK's industrial base, and historical limits on investments.[33] The DPRK has made substantial investments in space, satellite, and long-range missile capability. The DPRK has also arguably become less dependent on the international black market and is believed to have developed some of its capability through the Unha (Taepo-Dong 2) space launch program.[34] Recovery of the first stages of the Taepo-Dong 2 rockets

after the 2012 and 2016 launches provided evidence of indigenous rocket production when "the only foreign-made components in the [four small steering] engines were salvaged ball bearings from Soviet missiles."[35] Further, satellite imagery shows continued work on manufacturing facilities near Pyongyang during missile tests and an industrial base for solid-fuel rocket motor development, although the details of facility capabilities and usage are largely speculative.[36]

Changes in available technology may combine well with the DPRK's continued investment, lower risk aversion, and willingness to break the mold on how earlier nations achieved ballistic missile technology. Foreign assistance also plays a role, but there is significant controversy over the extent. Whatever the combination of traditional investments, new approaches, and external assistance, the DPRK has changed Northeast Asia's strategic calculus through its demonstration of missile capability. Competing explanations as to the nature of these advances point to the even greater difficulty of understanding the origin and extent of emerging technology capabilities, where extensive records of past developments are not available as a guide.

The DPRK provided the biggest surprise in missile technology development in the past decade.

Chinese advances—starting from a far more developed position than North Korea—worry key observers in other nations. These concerns range from proliferated ballistic missiles, to cruise missiles, to direct-descent anti-satellite systems combined with advances in ballistic missiles and nuclear capacity.[37] In general, anti-satellite capabilities are spreading. China possesses a range of options beyond the anti-satellite missile it demonstrated in 2007.[38] Moreover, a growing number of powers have publicly displayed their anti-satellite capacity, including India in 2019. The future of space and satellite technology will continue to be influenced by adjacent military applications, notably ballistic missiles and anti-satellite weaponry.

4

Emerging Technologies with Implications for Northeast Asian Security

Key Technological Advances by China and the DPRK

In all the discussions held as part of this project, some common themes emerged on potentially destabilizing advances across multiple fields of emerging technology. First, practices and norms are shifting across multiple domains, and racing behavior is emerging. One leading U.S. government official highlighted the acceleration of fielding new technologies, in particular by China but also observable in the DPRK's series of advances in missile technology. For example, the Chinese Chengdu J-20 aircraft went from first flight to fielding from 2011 to 2017, compared to the U.S. joint strike fighter, which went from a 2006 flight to a 2015 initial operating capacity. Whether or not the successful application of these technologies to battlefield innovations is accelerating, the widely seen military potential for AI was repeatedly cited as risking prompting an arms race. In addition to the direct benefits of AI in the domain of C4ISR, a U.S. technologist speaker at the workshop forecast that it would lead to "more advanced cyber weapons and autonomous physical weapons that are cheap and abundant. Small weaponized drones that are enabled by AI could become the twenty-first century's version of the AK-47."

Workshop participants saw the domain of space as experiencing a major shift in norms, driven by the current reliance on space systems and the vulnerability of these systems to anti-satellite threats and countermeasures. Both China and the DPRK have shown capabilities in this area. The changing

economics of launch, combined with a desire for risk mitigation, is prompting the increasing growth of the microsatellite sector, which lacks many of the norms established for larger satellites.

A second common thread is that emerging technology has created new options for relatively low-cost and often difficult to attribute actions against military or civilian infrastructure and information. As a Korean opening speaker at the workshop noted, "the world has become increasingly susceptible to cyberattacks and disruptions." In particular, the cyber domain is conducive to asymmetric attacks, although the growth of non-state actors' capabilities may be overstated.[39] Korean participants noted the DPRK's history of employing aggressive asymmetric attacks, including cyberattacks against commercial activity as well as military exercises and GPS.[40] While the DPRK is believed to employ drones primarily in a reconnaissance capacity, that potential attack vector is considered to be a threat.

Meanwhile, a U.S. government speaker emphasized longstanding U.S. accusations of the Chinese theft of intellectual property from other nations to accelerate weapons development.[41] As one U.S. technology security expert highlighted, the risks go beyond threats to military targets: "We face growing dangers to the privacy and integrity of information belonging to the citizens of both our countries and belonging to the commercial, industrial, and financial entities throughout our societies and economies."

Achieving information security requires the protection of both on-premises servers and the larger cloud infrastructure, as well as the services and software that feed into it. Workshop participants identified internet data centers and microelectronic manufacturing facilities as a possible area of vulnerability.[42] The threats raised for one or both categories of these highly interconnected sites included fire, microdrones capable of carrying a small but effectively targeted explosive payloads, and attacks on the power grid. The scope of challenges for this backbone infrastructure goes beyond the range of threats that the private sector is typically asked to defend against.

Korean participants noted the DPRK's history of employing aggressive asymmetric attacks, including cyberattacks against commercial activity as well as military exercises and GPS.

Adversarial Efforts to Divide Allies on Science and Technology Cooperation

The United States, Korea, and other democracies are significant contributors to the technological advances shaping security dynamics in Northeast Asia. Moreover, science and technology cooperation among these allies will be critical to generating geopolitical trends favorable to democracies. Yet there are tensions in relationships throughout the region that can serve to undermine cooperation. The U.S.-

China trade dispute is currently driving potential for a fundamental disruption of the global technology supply chain. As a bifurcation of global supply chains deepens and results in the development of separate China- and U.S.-led models, regional actors face pressure to align with one or the other at the expense of increased costs and exclusion from developments in the other sphere.

This pressure to make stark economic choices could potentially prompt a shift in focus for the U.S.-ROK relationship. As one Korean geostrategic expert observed, part of the challenge is that the "[the ROK has] been dealing with the North Korean threat, but we are being requested to deal with China at the same time." The DPRK's nuclear, missile, and cyberattack advances in recent years have contributed to the threat, meaning it may remain the top priority for the ROK. Moreover, China can respond harshly to moves it sees as threatening: the move of Terminal High Altitude Area Defense (THAAD) missile batteries and their radars to the Korean Peninsula resulted in months of economic retaliation against ROK goods and companies, effecting areas from cars to entertainment to supermarkets.[43] A top U.S. regional expert noted at the private workshop that while "these very interesting discussions about expanding and broadening the horizons of the alliance are important and relevant, it is difficult to imagine this [expansion] outside the context of a broader [alliance] reset."

This dynamic has particularly put private sector firms in Korea in a challenging situation. One Korean academic at the workshop noted the magnitude of this challenge. The expert pointed out that 30 percent of the ROK's trade is with China or Hong Kong, which exceeds the total sum of the ROK's trade with the United States and Japan. The region's economics suggest that access to the Chinese market is essential to business success, potentially pitting national security concerns against economic ones. These economic tensions are subject to debate within the ROK and are at risk of being exacerbated by adversaries employing information warfare to leverage the open society of democratic nations to create wedges in alliances. As a U.S. expert noted, the United States and ROK have close defense cooperation, including deliveries of the F-35 fighter and Global Hawk uncrewed system.[44] Nonetheless, a Korean speaker asserted that even successful transfers can be lengthy and that the United States' refusal to export advanced weapon systems in 2013 and 2015 "lowered the trust between the two allies."[45] That speaker thought the absence of further progress on space and cyber cooperation could be attributed to "political consideration, not only in the United States but also in Korea. I think China and the trust issue is in the center of this problem."

The flip side of the trust issue is the U.S. government's accusations of China achieving technological advances by a range of illegitimate means: direct theft of intellectual property; employing technology militarily that was only authorized for commercial use; or accessing technology that was shared with third countries under the provision that it not be made available to China. Growing cyber capabilities have created more opportunities for adversaries to raise the cost of cooperation and deplete trust. Several high-profile technology losses have damaged trust in the past and have led the ROK to substantially upgrade its technology control laws and institutions.[46] The ROK's emergence as a top 10 global arms exporter from 2015 to 2019 can be a double-edged sword.[47] The ROK's advanced capabilities can be a boon to the partnership; as a U.S. official at the workshop noted, the ROK has developed its own fighter aircraft that "not only enhances the combat capabilities of the ROK air force, but also the combined operational capabilities of the U.S.-ROK alliance to address emerging threats in the region." At the same time, the United States "urge[s] caution when identifying potential export markets."

Protecting Microelectronics Supply Chains in Northeast Asia

Given the scale of challenges to Northeast Asian regional security resulting from emerging technology and the complications that arise even among closely allied national actors, it is necessary to establish some prioritization for near-term cooperation. Multilateral efforts aimed at China can raise fears that the ROK would be pulled into a conflict that may not be relevant to Korean interests and one where Korea may disproportionately bear the burden of any retaliation. One U.S. expert cautioned to carefully choose areas of cooperation, looking to whether "China is weaponizing in this area," and for the United States to weigh "relative assets versus liabilities" when choosing where to push greater collaboration.

For example, a Korean academic cybersecurity expert detailed the industrial choke points at the workshop: "When you think about memory and non-memory in semiconductors, the largest memory factories in Korea are Samsung and SK Hynix. On the non-memory side, TSMC is located in Hsinchu, Taiwan. And Nvidia, the most popular GPU company these days, is an American company, but its factory is in Taiwan. These factories are trying to be 'smarter,' utilizing AI, 5G, and IoT technologies."

In this particular area, a U.S. speaker expressed a clear priority: "The Republic of Korea has one of the most important resources in the world, which is advanced semiconductor manufacturing. Please protect it. Please nurture it. It is more important to the future than any single weapon system." The present ROK administration has placed emerging technology at the center of its economic strategy. This summer the ROK announced a "digital new deal" that includes investments in 5G and AI and calls for "spending 1 trillion won ($820 million) over ten years to support the development of the AI semiconductor industry."[48] While the economic and national security objectives for this sector are sometimes in tension, the workshop identified areas where cooperation is a good match for both countries' expressed interests.[49]

> ***"The Republic of Korea has one of the most important resources in the world, which is advanced semiconductor manufacturing. Please protect it. Please nurture it. It is more important to the future than any single weapon system."***
>
> *U.S. speaker at the conference*

Experts underlined the priority that the United States and ROK put on cybersecurity and cyber defense at the workshop.[50] Here, the interests of both governments and private actors are closely aligned. While commercial actors can often work around or within frameworks that China has advocated as a means of extending its national security agenda, and thus do not pose the same threat to commercial

actors as they do to national security officials, cyberattacks pose a substantial threat to all actors in the region. Here, states have shown a willingness to surveil, steal intellectual property, and potentially even target critical civilian infrastructure, which means not only that interests are aligned, but that commercial actors must depend on sophisticated state capabilities for support in their defense.

5

Norms and Standards of Innovative Technologies

Importance of Norms and Standards

Dynamics in Northeast Asia illustrate why norms and standards are particularly important in the international approach to scientific innovation and emerging technology. The region's complex relationships and highly competitive economic and national security structures mean that international dialogue and international cooperation can easily fracture. Such a fracturing could undermine the civil and commercial coordination that is often necessary to achieve the positive potential of emerging technology. Norms and standards allow states to reach common ground on what counts as, in the words of a workshop moderator, "aggressive" or "threatening" behaviors. These new norms cannot always be derived based on what was out of bounds with older technologies. Working out what is in and out of bounds works best via a multilateral process, but in those cases where this is particularly challenging, Dr. Hicks suggested that the United States can play a useful early role in laying the groundwork.[51]

Private sector behaviors and norms are also important and influence norms governing nation-state behavior, but these are rarely addressed effectively in government-to-government discussions. The nature of today's emerging technologies is that private sector actors are the largest investors, developers, and deployers of these technologies. The Chinese Communist Party directs its commercial sector's engagement through civil-military fusion, working aggressively to shape regional and global

norms and standards for emerging technologies to the government's liking, especially for AI. For others, a return to Cold War era regulation of technologies would be difficult. Influencing technical standards might be the more pertinent struggle for maintaining technological advantage.[52] Norms and standards that affect significant commercial interests in turn impact private citizens' interests on issues such as safety and privacy, increasing their importance to democratic governments.

The pace of technology development challenges governments to keep up with effective, relevant norms and standards. As one expert pointed out, 25 years passed between the first use of a nuclear weapon and the establishment of the Nuclear Nonproliferation Treaty (NPT). Such a lengthy timeline to establish controls on today's technologies would clearly be ineffective. As a result, governments must prioritize critical areas for focused effort. Northeast Asia provides several venues for these discussions, including bilateral dialogues between the United States and Korea, as well as broader regional and multinational discussions. The United Nations is a useful forum for norms and standards discussions, and the UN strategy for new technology presents five principles that make a helpful starting point.[53] However, as an experienced diplomat observed, while the United Nations and its staff have important roles as conveners and agenda-setters, they are unlikely to effectively lead these discussions and implement processes. That expert instead thought the United States should "constitute some kind of like-minded group to implement that process in detail."

On the one hand, norms and standards are an area of potential cooperation between sometimes rival nations when addressing the risk of misuse of emerging technology by non-state actors or the potential to apply technology to common challenges such as cross-national commercial infrastructure, disease, or climate change. On the other hand, these discussions can simply become another venue for countries to engage in technology "racing" behavior, seeking to set norms and standards advantageous to them, as China has done on 5G. As the 5G example illustrates, technological advantage can allow nations with effective market power in relevant areas to have a greater ability to set the terms of norms and standards discussions. In the microelectronics sector, as a U.S. speaker noted, Japan, the United States, and the Netherlands are the major producers of the manufacturing tools used for high-end semiconductors, and the Republic of Korea, Taiwan, and Japan are the key producers of the semiconductors themselves. Meanwhile, China remains dependent on its external supply chains, importing over $300 billion in semiconductors in 2019 and $350 billion in 2020.[54] Thus, the microelectronics sector could present a major opportunity for Korea and allied nations to set the norms and standards for a broad array of related technology issues.

Norms and Standards in Space

The role of space is changing for major powers, as General Won In-choul, then-chief of staff of the ROK Air Force, observed at the conference; there are signs of "a new arms race for dominance in space" making that domain "no longer a battlefield of the future," but a priority for today.[55] Conflict has not been limited to the military realm; Lieutenant General Michael Hamel (ret.) observed that commercial communications satellites have suffered from regular interference.[56] This competition is driven by space's importance for a range of military functions, from intelligence gathering and communications to navigation and targeting. General Won observed that this central role, combined with space systems' vulnerability to attack, leads him to expect "that future crises and conflicts will be triggered from space as nations compete to preemptively establish dominance in space using various means. As

such, the ability to immediately identify initial signs of provocation and to recover space power from damage will become increasingly important."[57]

Hong Kyu-Dok, Michael Hamel, and Ju Gwang-Hyeok (left to right) discuss space technologies at the Seoul conference.

In the civil, commercial, and military space domains, the use of microsatellites has been dramatically expanding, enabled by lower launch costs and spurred by fears of space denial attacks. This change prompted one U.S. policy expert to inquire whether policymakers should "look at this sort of rapid expansion of redundancy of capability as a positive racing quality that should be allowed to build resilience into the system or a negative form of racing, to which we might want to seek to apply some international controls in order to incentive states not to pursue such extensive redundancy?" The correct answer may not yet be known, with one expert arguing that "the reliability of smallsats is still questionable" and that some military users of large satellites may be overly hesitant to adopt new methods. That said, even if the international community chooses to embrace this shift, new norms and standards may be necessary to manage the heightened risk of collisions and space debris.

A prerequisite to applying norms and standards is knowing what is happening so that violations can be mitigated and countered. This knowledge is hard to come by in many emerging tech realms, such as space and cyber. One U.S. general observed that this phenomenon was previously dealt with for Nuclear Test Ban Treaties, where "the technologists developed and established the means to do that verification" and suggested that expanded space activity could bring more verification opportunities. Many countries, including the ROK, have limited space sensing, which means that attacks on their space assets may go undetected. The DPRK has sometimes leveraged this lack of transparency to threaten ROK civilian infrastructure, circumventing norms and sometimes UN sanctions with assistance from Chinese commercial technology.

Space and satellites stand out as an area where norms and standards are likely to become more important as a means of governing state behavior as technology reduces the effectiveness of more formal mechanisms such as export controls. The United States loosened satellite technology controls as the Cold War ended, only to tighten them again after an investigation into the failed launch of a U.S. satellite which may have contributed to greatly increasing China's launch reliability.[58] The U.S. Congress's highly restrictive classification of satellites as a regulated munition was subsequently eased somewhat in 2013 to focus on stopping satellite cooperation with or launch by China or the DPRK and any related entities. Other rules, such as the annually renewed 2011 Wolf Amendment, constrain civil space cooperation between the United States and China.[59] However, the marginal effect of these restrictions on China and North Korea is difficult to judge, as both nations have made significant strides in space capabilities and missile programs.

Multiple nations are making major pushes on missile programs and may be collaborating, leading Ian Williams of CSIS to state that "we believe we're entering a missile renaissance."[60] The pertinent technologies are informally regulated by the Missile Technology Control Regime (MTCR) and, for nuclear-capable missiles, the more broadly based Hague Code of Conduct Against Ballistic Missile Proliferation. However, despite past successes, Jeffrey Lewis notes the maturity of the technology is now a challenge for control regimes: "the prospects for controlling proliferation of missiles are fading rapidly as the technology to build them becomes more prosaic."[61]

This challenge is also shown in the DPRK's first satellite, the *Eunha-3*, launched in 2012 and subsequently salvaged by the ROK Navy. An analyst laid out the ROK's findings: "With the exception of one item, the components of Eunha-3 were assembled using semiconductor chips from commercial products such as TVs and DVDs. The reason North Korea succeeded in launching Eunha-3 was that it was able to procure commercial materials and parts that were not subject to international export controls."

The region will need to engage robustly in discussion about emerging norms and standards regarding the use of space and space-related systems. As a U.S. expert noted, "the U.S. Department of Commerce imposes the appropriate controls on export, re-export, and transfer of emerging and foundational technologies." Simultaneously, the U.S. Department of State works to make sure those controls do not undermine U.S. innovation or collaboration with nations such as the ROK. Nonetheless, the widespread availability of technology that was once difficult to access will impede any export control efforts. That said, as was noted by a Korean expert, there is undoubtedly room for multilateral efforts, such as the UN Sanctions Committee on North Korea, to be more robust and transparent.

Establishment and Enforcement of Norms

Developing norms and standards regarding AI and related technologies is a significant challenge in part because scientific innovation has been moving at a faster pace than national or multilateral regulatory systems have been able to respond. The theoretical problems go even deeper. CSIS technology expert Lindsey Sheppard observed at the conference that efforts to prevent inappropriate use of AI were taking place at a range of levels in the international system, but also that there was little agreement on the terminology and scope of the issue.[62] The Seoul conference and the closed Washington workshop identified a range of priorities for AI norms and standards: developing approaches for verifying and validating the output of AI systems; increasing the resilience, robustness, and ideally anti-fragility of machine learning systems; ensuring transparency, especially as the United States and China compete

in this domain; and addressing human rights concerns. Last year, the DoD announced a set of five ethical principles regarding AI and an AI partnership for DoD with delegations from 13 partner nations covering a range of high-tech democracies, including the ROK.[63] Addressing ethical questions has not been a priority for some countries. There has been a growing bifurcation of AI talent when academic and commercial cooperation once was common.

Beyond government-to-government approaches, a speaker with a background in both government and the tech industry added that the process of building regulation and policies often begins with civil society conferences and workshops such as the ones in this project and in the academic sphere. Moreover, as a private sector technologist commented, businesses have a motive to establish norms and standards: "if you aren't building systems that are transparent and understood, especially as consumers try to understand the issues of trust and data transparency, you simply are not going to succeed."

Addressing intellectual property theft, whether by means of a cyberattack or any other approach, is another area of potential collaboration to establish norms and standards. Participants observed that certain countries in Northeast Asia do not acknowledge boundaries between legitimate and illegitimate targets, despite U.S. efforts to differentiate commercial and national security targets. A U.S. government speaker called for moving from bilateral to multilateral efforts to "international standards of protection of intellectual property." In the past year, one such multilateral fight took place over the new head of the World Intellectual Property Organization, culminating in the defeat of China's nominee.[64] The United States has championed a framework for responsibility in cyberspace that seeks to apply the UN Charter and international humanitarian law, including a 2015 Group of Governmental Experts report with non-binding norms against attacking critical infrastructure.[65] That said, Dr. David Edelman argued that the debate on which cyberattacks are unacceptable is underdeveloped and that United States and ROK could do more to establish boundaries.[66] Some workshop participants also supported alliance efforts to reduce vulnerabilities to cyberattacks; for example, the NATO alliance has long worked to build mutual cyber defense capabilities. A Korean cybersecurity expert raised the 2018 U.S. Cloud Act as an approach to collecting forensic information regarding cyber issues.[67] The Cloud Act does raise national sovereignty concerns and would require executive agreements to develop mutually agreeable ways to enable rapid collaboration on discovering the origin of attacks.

Regulations on uncrewed systems, on both the national and international level, are still evolving. Larger uncrewed aerial systems, those "capable of carrying a 500-kilogram payload at least 300 kilometers," are also covered by the Missile Technology Control Regime, the United States has proposed narrowing that definition on the basis of speed and taken unilateral steps last year in that direction, but much of the discussion at the workshop focused on smaller drones, possibly in large numbers.[68] Even commercial drones are now being employed in conflict. One workshop participant called for stronger national-level regulations, highlighting that commercially available systems too light to be subject to registration requirements could nonetheless be easily modified to become remotely piloted grenades.

6

Collaboration in Technology Innovation between Allies in Northeast Asia

The importance of collaboration between nations in Northeast Asia to deal with emerging technology issues is profound because these technologies are not contained by international borders and the vital interests of every country are at stake. As Dr. Hicks noted in Seoul, the current U.S. national security strategy and national defense strategy have prioritized both competition with China and building up U.S. innovation to ensure competitiveness. "To do that," she stated, "it will require working together with allies and partners around the world, and partnering across academia, industry, and government. Each of us do that in our domestic context differently, but by working together, we can surface the major issues that help us define where governments can play an important role and where we need to develop stronger partnerships across all those domestic and international actors."[69]

This emphasis on partnerships raises questions about what the best venues might be for international cooperation and what the best practices might be for engaging on these issues. The United States and ROK have a strong foundation for collaboration on emerging technology issues, with existing strategic dialogues and related alliance frameworks. In addition, the U.S.-Korea Free Trade Agreement (KORUS FTA) provides a framework for cooperation in the commercial technology arena. Other areas are not as well served by existing agreements. Space is an area where there have been significant limits on U.S.-ROK cooperation despite existing bilateral agreement and dialogue, such as the 2016 Framework Agreement for Cooperation in Aeronautics and the Exploration and Use of Airspace and Outer Space

for Civil and Peaceful Purposes and the U.S.-ROK dialogue on space cooperation which began in 2014. Engaging in further dialogue, including coming up with concrete implementation mechanisms for space as well as in other technology areas, is much needed.

Engagement of the Private Sector in Strategic Dialogues

It is also clear that the private sector must be a part of the dialogue, a topic that has not necessarily been a high priority in the security-related U.S.-ROK dialogues of the past. Greater private sector involvement is a potential source of strategic advantage for the United States and the ROK as they can try to outcompete the civil-military fusion approach by potential adversaries with countervailing activity led by the dynamic U.S. and Korean private sectors. The private sector has been able to achieve speed and, in the words of one technologist at the workshop, "does a remarkable job of bringing together researchers and developers into markets, quite frankly, as an economic driver." In particular, the ROK has spent more than a decade in the top five proportional global spenders on R&D.[70] In the view of a U.S. expert on research, this makes the U.S.-ROK research and development relationship "one of [the United States'] most critical partnerships to get right," noting "it really behooves us to listen and understand what the top-level strategic constraints are, what [the private sector's] needs are, and what a real collaboration looks like."

One known obstacle is that key parts of the private sector may be wary about collaboration. A workshop participant from industry observed that semiconductor companies have been skeptical about working with DoD because of concerns about transferring intellectual property rights or becoming involved with controlled exports. Fears of literal weaponization or weak norms and standards can also undermine private sector partnerships, for example, the withdrawal of Google from an AI project processing drone imagery because of employee concerns that their work would lead to drone strikes.[71] On the other hand, such objections may also drive skepticism in the corporate sector and academia about collaborations with China.[72] As a U.S. practitioner noted, "there is a strategic advantage in the nations that employ dual-use technology in a responsible, ethical way. But it requires that we build trust and transparency with our constituents, our allies, and our partners, as well as the companies that develop the technology."

In particular, the ROK has spent more than a decade in the top five proportional global spenders on R&D.

Starting a dialogue may necessitate changes in framing. As one U.S. strategic expert noted, "the U.S. tends to do many things through the DoD that the rest of the world does through other instruments of government and industrial power." Likewise, other workshop speakers cautioned that there are some security discussions, especially regarding sensitive technology, where there are practical limits on the extent of private sector inclusion. Better venues may be needed for "empowering conversations around where our industries compete and where they can collaborate effectively." These conversations are

crucial in sectors where governments are not the main, or even necessarily a significant, customer for the technology. At the same time, another expert noted that government leadership is necessary. For example, in some domains AI is "being weaponized" in ways that impact the public and may require government action to address. Especially with regard to network technologies, there is a clear national interest in the geopolitical and security implications of private sector decisionmaking.

At the conference, both Korean and U.S. speakers discussed private sector outreach, notably including both nations playing the role of a "testbed" for applying emerging technologies in a military context.[73] General Suh added that he was impressed by the way the U.S. Army Futures Command and Army Space and Missile Defense Command innovated, including via cooperation with private sector companies such as Uber that are not part of the traditional defense industry.[74] CSIS's Andrew Hunter emphasized that the government has a "tremendous" evaluative role but faces "challenges that come with doing so without fully understanding how to test, evaluate, and understand these technologies."[75] Dr. Hicks also discussed the cultural and regulatory challenges for the military to act as a testbed, as "the cost of failure is much higher" for military projects than for experimental commercial ones.[76] At the workshop, an expert on government research went further to suggest posing challenges that might inspire the private sector in ways that the government's traditional role as an investor does not.[77] This competition could then enable a binational dialogue to identify barriers to U.S. and ROK collaboration at both the company and individual level. Outreach is necessary because of the complexity of global supply chains and their constraints and the limitations of expertise in the foreign policy community regarding supply chains that are not part of that nation's defense industrial base.[78] The expert also suggested that these dialogues may work best if not led by governments.[79]

The markets for semiconductors and other information technology products are enormous, approximately several trillion dollars, and governments' direct leverage as an investor and purchaser is relatively small. On the other hand, as multiple workshop participants noted, the vulnerabilities faced by pivotal private sector facilities go well beyond the risks the commercial sector traditionally can manage.[80] The U.S. and ROK governments and societies have common interests in cyber resiliency that reduces cyber fragility and vulnerability to asymmetric attacks on commercial infrastructure.

One critical success story in multinational private and public sector collaboration has been Korea's response to the Covid-19 pandemic. One expert speaker from the Korean private sector described how ICT providers worked with one another and the Korean government, including the Korea Disease Control and Prevention Agency, to better understand the pandemic's rising threat. That cooperation was primed by the hard experience of the SARS and MERS outbreaks, which underlined the importance of building connections to manage present crises and prepare for future ones.

Bilateral and Regional Partnerships in Northeast Asia

INFRASTRUCTURE FOR INFORMATION SHARING

Multiple participants emphasized the need to cultivate the physical and personnel infrastructure of technology innovation between allies. Enhancing the ability for the United States and ROK to share sensor data and allow platforms on the same operation to communicate is a marker of success. At the same time, growing reliance on networks, including those from multiple nations, and adversary investments in cyberattack and electronic warfare capabilities mean that cybersecurity will remain a contested environment.[81] A U.S. speaker recommended that "we need to collectively implement

procedures and protocols" that will make it more difficult for potential adversaries "to exploit other nations' intellectual property and data." Current U.S. thinking in cybersecurity is that attempting a secure perimeter around allied networks is not sufficient and that adopting "zero trust" protocols easing information sharing across compromised systems is necessary.[82] Boosting security is not a substitute for developing truly international norms and standards but could serve as a stopgap and reduce the benefits of defecting from existing standards. However, technological solutions are necessary but not sufficient. As a Korean alliance expert laid out, a key question is: "do we, the United States and allies, have enough trust to share all these technologies and the sensitive information?"

One way to measure this infrastructure's success is if the allies can work together to innovate in an agile and timely manner. Extended timeframes are typical in joint development, but choosing forms of cooperation that can be executed in shorter time frames and minimizing coordination delays matters. As Dr. Morgan Dwyer notes, a longer time window makes it harder to align priorities between states.[83] Both U.S. and Korean speakers discussed collaboration in acquisition as an overall goal, although the U.S. keynote speaker emphasized multinational cooperation over bilateral efforts. Regarding multinational cooperation, a Korean speaker suggested that trilateral talks among the United States, Korea, and Japan on security as well as AI and other emerging technologies would be possible by bringing together officials at the assistant secretary-level through the existing Defense Trilateral Talks mechanism.

Information sharing involves technological and regulatory challenges, as steps to reduce risk can inadvertently increase the transaction costs of cooperation. Whether jointly developing or procuring a capability or exporting a U.S. system, technology security issues are easier to address at the front end of projects with transparency about the handling of intellectual property. Regardless of the mechanism, success will require a foundation of technology security that can build future trust and alignment between the allied acquisition systems.[84]

As a Korean alliance expert laid out, a key question is: "do we, the United States and allies, have enough trust to share all these technologies and the sensitive information?"

SECTORS AND PROJECTS FOR COLLABORATION

Workshop participants raised combinations of cybersecurity, space, and ICT infrastructure related to data-driven techniques (e.g., semiconductors, 5G, AI, and cloud computing) as natural areas for collaboration.[85] Across multiple domains, proposals focused on shared intelligence and warning, command and control, and responding to cyber vulnerabilities, such as outright hacking and disinformation. For uncrewed systems, the Seoul proceedings include a list of promising areas for cooperative research suggested by Dr. Hicks: "high-altitude long-endurance systems, countering electronic warfare, survivability of [uncrewed] systems, ground-based autonomous vehicles, and underwater [uncrewed] vehicles."[86] The ROK and the United States have an existing foundation for cooperation in space, including information sharing between the U.S. Space Force and the ROK

Air Force and joint training exercises with personnel from both nations at the Air Force Operation Command's Space Integration Team. As General Won argued, the ROK Air Force's progress in space requires a multitude of factors to come together, and "technology cooperation between multiple sectors based on close ROK-US cooperation is more important than ever."[87] A Korean speaker raised an aspirational model of U.S. and Japanese cooperation on space and cyber that "has leveled up the U.S.-Japan alliance in the region."

Existing venues could help identify possible collaborative projects through the Technology and Industrial Cooperation Committee and Technological Cooperation Subcommittee mechanisms.[88] Past CSIS workshops have suggested that the ROK may need to bring a shortlist of potential projects to these forums and that the United States may need to be more willing to commit when common research efforts bear fruit. One Korean speaker suggested these subcommittees may need to report to the higher-level meetings what they have done and their tasks for the next year. These tasks might include finding ways to better adapt private sector technology in the model of the U.S. Defense Innovation Unit. A senior diplomat at the workshop suggested that universities may be able to bring together private and public interests without facing some of the same constraints as the government, and multiple Korean speakers emphasized the importance of integrating not just industry but also academia and the wider research community.

ECONOMIC SECURITY

Engaging the private sector in dialogue, particularly on matters of great economic significance but also on matters of security and national strategy, does not overcome differences in interests but allows blazing better paths forward. One sign of success would be the extent to which the broader industrial and research communities are interested in supporting national and economic security objectives. Another sign of success will be appreciating and incorporating one another's perspectives regarding expanding the scope of the U.S.-ROK alliance to include more high-tech or multilateral aspects. Achievement of these goals will be complicated by the fact that Korea will disproportionately bear the cost of any Chinese economic retaliation. Reducing this dependence is also part of the effort to foster a closer relationship.

INNOVATING VIA EXERCISES

At the workshop, the Korean military opening speaker raised the example of innovation in the Pacific theater in World War II. Japan had developed the directional antenna before the United States, but the United States was nonetheless better able to innovate in the use of the radar technology writ large, which, combined with cryptology breakthroughs, directly contributed to the Allied victory against a larger force at the Battle of Midway. Raw technology leadership is desirable, but accepting and adapting to new technologies and integrating them into operations is more relevant to deterrence and success on the battlefield. The ROK is well positioned to innovate thanks to its investments in military and civilian Fourth Industrial Revolution technologies and its experience in challenging operating environments and facing concrete risks from the DPRK. Success will involve alliance partners learning from one another, furthering their abilities to act in concert, and experimenting together.

Experts from both countries expressed an interest in targeted exercises that would allow participants to test capabilities, learn from one another, and adapt operations to new technology. A U.S. practitioner praised the existing foundation for this work: "I've seen Korean and U.S. analysts and operators sitting side by side at watch centers or operations centers, and there's an excellent

opportunity to experiment and have those folks exercise some of these capabilities together." Areas for possible collaboration include cyber red-teaming—preparing defenses against both cheap and lightweight drones as well as the higher-tech challenge of AI-enabled drone swarms. Another would be finding opportunities for the United States to learn from the ROK's successful application of both established and information technology-oriented methods in its Covid-19 response. Some workshop participants suggested that resuming the Adaptive Shield exercises and other work in the context of the multilateral Global Health Security Agenda could further cooperation on "the bio surveillance portal, which uses big data for response and prediction."[89]

7

Conclusion

This project reveals notable commonalities in U.S. and Korean expert views on how emerging technologies are shaping strategic competition, suggesting a strong foundation for cooperation. Topping that list is the extent to which these technologies are catalyzing the variable of time. While these often software-oriented innovations are rapidly advancing, prior regulatory regimes, typically more focused on hardware, advance on a slower time scale. Technological change is reshaping key elements of military advantage rapidly, putting a heavy burden on allies to work closely together to mitigate emerging threats and capitalize on new opportunities. A vital enabler of that cooperation will be extensive information sharing in real-time.

As Dr. Hicks stated, "the broader issue set of governance partnership and the role of government does transcend various different areas of technologies."[90] The application (existing and potential) of today's emerging technologies and associated regional dynamics are exacerbating regional tensions, bringing new considerations to longstanding security challenges, and propelling new non-state and commercial actors onto the global stage. The emerging technologies discussed in this paper have substantial commercial and military consequences, areas that will both prove strategically important. Especially in ICT, the commercial sector often leads the way. Therefore, it is imperative to link commercial and military activities; allies in the region must be able to protect their critical infrastructure and key commercial information. The United States and ROK will need to find ways to attract the private sector to support their technical goals. At the same time, these advances

come with dangers such as cyberattacks on the networks that enable data-driven techniques and software-driven technologies.

When it comes to scientific innovation, regional security dynamics are complicated. Lines between economic security and national security blur and intertwine as the digital era brings 5G telecommunications, IoT, and commercial space access to the region. Both the United States and Korea have China as a major trading partner, including in high-tech supply chains, with the ROK especially close economically. From a military perspective, Northeast Asia is faced with a series of security challenges and risks, with the ROK having a particular interest in North Korean technological advances and U.S. strategy focusing primarily on China. Meanwhile, the DPRK is eager to exploit the possibilities presented by growing competition between the United States and China. Moreover, in its response to THAAD missile deployments to the ROK, China showed its willingness to retaliate economically against the ROK when it disapproves of strategic moves.

The emerging technologies discussed in this paper have substantial commercial and military consequences, areas that will both prove strategically important.

One possible way of responding to the strategic implications of emerging technology would be to pursue a "high-tech alliance." This approach would seek to strengthen economic and defense cooperation in emerging technology to form a common front that could promote and defend norms on intellectual property, data, or cybersecurity. However, some experts on the U.S.-ROK relationship noted that putting together such an alliance would demand significant hard work to reconcile competing priorities. A top U.S. expert similarly called for "a sturdy platform from which to launch a big initiative on something like the U.S.-ROK Alliance in the context of multilateral cooperation on AI and 5G." Expanding the alliance's focus on economic issues and potential great power competition in East Asia will need to be grounded in the diplomatic work of building a robust common strategic outlook and finding concessions when the cooperation's costs are unevenly distributed.

Nonetheless, many of the technological issues of common interest are pressing today and already align with the ROK's concerns with the DPRK. On the private sector side, the ROK has a strong interest in defending its infrastructure, particularly facilities involved with microelectronic production, against cyberattacks and deniable physical attacks that could be enabled by uncrewed systems. Both countries and their respective industries would also benefit from enhanced abilities to detect and trace violations of norms related to emerging technology. While there is likely to be limited near-term progress on any multilateral agreements that include China, better U.S.-ROK commercial collaboration on detection can help develop and enforce norms. In addition, multilateral cooperation with regards to the DPRK remains a key ROK priority. That said, Korean calls for not losing focus on the DPRK are not synonymous with seeking a hard line; the closing

Korean speaker called for "a more pragmatic and realistic approach" that is more in line with ROK diplomatic efforts.

In these discussions, experts from both countries agreed that developing technology in and of itself does not confer security advantages. Rather, the technology must be adapted and integrated into operations to prove useful. In terms of government-to-government cooperation, both the United States and ROK would benefit from the resumption of targeted exercises, particularly those focused on defense against cyber and uncrewed system attacks. The United States and ROK have also participated in contagious disease response exercises that have helped the ROK strengthen its response after previous pandemics. These exercises could now be an opportunity for the United States to learn from the ROK's recent success in responding to Covid-19. In the medium term, existing coordination methods could facilitate closer progress in finding ways to share data with robust cybersecurity protection. Continued improvement in this area includes joint development work on improved cross-platform and cross-alliance C4ISR capabilities of the sort enabled by data-driven techniques and software-intensive systems. The multilateral aspects of this cooperation could contribute over time to developing norms and institutions that aid in regulating these emerging technologies, just as prior generations responded to their eras' technological challenges.

Emerging technologies do pose risks for enabling adversaries to destabilize the security environment in Northeast Asia. The United States and its allies will have to work together to achieve an effective response that is informed by democratic values, fosters and utilizes scientific innovation, and gets the best from commercial sectors. Success will take a lot of work and require broad-based cooperation between and within allied countries. The priorities outlined above are promising areas where interests can align for common efforts. While the United States is the larger partner in the alliance, semiconductors are an example that shows that in some emerging technologies the ROK is better positioned. This example also serves as a reminder of how vital the ROK can be to achieving ethically grounded norms and standards. The authors hope this first-of-its-kind CHEY-CSIS endeavor can be used by scholars, government practitioners, and those in the private sector to advance U.S.-ROK security and economic interests.

Endnotes

1 In 2017, Kim Jong-un announced that North Korea had "entered the final stage of preparation for the test launch of intercontinental ballistic missile." After the testing of the Hwasong-15 that year, Kim declared that North Korea had "completed" its nuclear force.

2 "Armed forces personnel, total," World Bank, accessed November 3, 2020, https://data.worldbank.org/indicator/MS.MIL.TOTL.P1.

3 Titli Basu, "Securing Japan from Chinese 'Predatory Economics'," *Japan Times*, July 20, 2020, https://www.japantimes.co.jp/opinion/2020/07/20/commentary/japan-commentary/securing-japan-chinese-predatory-economics/; and Genevieve Feely and Rhys De Wilde, "It's Time to Take an Alliance-based Approach to Securing Rare-earths Supplies," Australian Strategic Policy Institute, *The Strategist*, August 6, 2020, https://www.aspistrategist.org.au/its-time-to-take-an-alliance-based-approach-to-securing-rare-earths-supplies/.

4 "Welcoming Speech by Park In-kook," in Chey Institute for Advanced Studies (CHEY) and the Center for Strategic and International Studies (CSIS), *Geopolitical Risks & Scientific Innovation* (Seoul and Washington, DC: January 2020), 7, https://www.chey.org/UploadData/IssuesContents/cb241585-11ae-4975-9635-5f3ed7a0a8bd.pdf.

5 Government of the Republic of Korea Interdepartmental Exercise, "Mid- to Long-Term Master Plan in Preparation for the Intelligent Information Society," Korea-EU Research Center, 2016, https://k-erc.eu/uncategorized/master-plan-for-the-intelligent-information-society/.

6 Department of International Cooperation Ministry of Science and Technology of the People's Republic of China, "Next Generation Artificial Intelligence Development Plan," China Science & Technology Newsletter, No. 17, September 15, 2017, http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf; Rogier Creemers, Elsa Kania, Paul Triolo, and Graham Webster, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan'," New America, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

7 Elsa Kania, "Chinese Military Innovation in Artificial Intelligence," Center for a New American Security, June 7, 2019, https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence.

8 Kendra Albert, David O'Brien, Ram Shankar, Siva Kumar, Jeffrey Snover, and Salome Viljoen, "Failure Modes in Machine Learning," Microsoft, November 10, 2019, https://docs.microsoft.com/en-us/security/failure-modes-in-machine-learning.

9 For more on synthetic biology, see Morgan Dwyer, Andrew Philip Hunter, and Tara O'Toole, "Synthetic Biology and National Security: Risks and Opportunities (Part 1 of 2)," (public event, Center for Strategic and International Studies, Washington, DC, April 14, 2020), https://www.csis.org/events/online-event-synthetic-biology-and-national-security-risks-and-opportunities-

part-1-2.

10 Kai Kupferschmidt, "How Canadian Researchers Reconstituted an Extinct Poxvirus for $100,000 Using Mail-order DNA," *Science*, updated July 6, 2017, https://www.sciencemag.org/news/2017/07/how-canadian-researchers-reconstituted-extinct-poxvirus-100000-using-mail-order-dna.

11 The Adaptive Shield exercises replaced the Able Response exercises in 2016.

12 The computing power employed in the highest-profile AI training runs has been doubling every three and a half months since 2012, suggesting that demand for microelectronics will continue to expand. Dario Amodei and Danny Hernandez, "AI and Compute," OpenAI, May 16, 2018, https://openai.com/blog/ai-and-compute/.

13 Samuel M. Goodman, Dan Kim, and John VerWey, "The South Korea-Japan Trade Dispute in Context: Semiconductor Manufacturing, Chemicals, and Concentrated Supply Chains," U.S. International Trade Commission Office of Industries, working paper ID-062, October 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470271.

14 "The U.S. National Security Strategy announced in August 2017 by the Trump Administration has designated China as a threat to the U.S. national security innovation base by unfairly obtaining the innovative achievements of liberal societies through infringement of U.S. patented technologies and pre-commercial ideas. Cyberattacks on U.S. companies and experts with proprietary knowledge are perceived as threats to U.S. long-term competitiveness, and access to U.S. innovative economy as having been unfairly used to pursue China's economic development and military modernization efforts. China's non-market economy system has been recognized as the main culprit behind its weak regime for adequate protection of intellectual property and innovation efforts." Hyo-young Lee, "U.S. Trade Policy Against China: U.S. Perspectives and Implications," *IFANS Focus*, IF 2019-31E, December 12, 2019, 2, http://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?clCode=P11&pblctDtaSn=13494&koreanEngSe=ENG.

15 A confidential UN report accused the DPRK of raising up to $2 billion through cybercrime and cryptocurrency. The DPRK denied the accusation. Michelle Nichols, "North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: U.N. Report," Reuters, August 5, 2019 https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

16 Timothy W. Martin, "North Korea, While Professing Peace, Escalated Cyberattacks on South," *Wall Street Journal*, May 25, 2018, https://www.wsj.com/articles/north-korea-while-professing-peace-escalated-cyberattacks-on-south-1527239057.

17 IBM Blockchain, "Transform Supply Chain Transparency with IBM Blockchain," IBM, accessed November 28, 2020, https://www.ibm.com/downloads/cas/1VBZEPYL; and "Standard Chartered Invests in Chinese Supply Chain Finance Blockchain Linklogis," Ledger Insights, January 21, 2020, https://www.ledgerinsights.com/standard-chartered-blockchain-supply-chain-finance-linklogis-2/.

18 Mike Orcutt, "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked," *MIT Technology Review*, May 2, 2019, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

19 General Suh Wook has served as ROK defense sinister since September 2020.

20 "Opening Speech by Wook Suh," in *Geopolitical Risks & Scientific Innovation*, 12.

21 Elsa Kania, *The PLA's Unmanned Aerial Systems* (Montgomery, AL: China Aerospace Studies Institute, 2018), https://www.airuniversity.af.edu/Portals/10/CASI/Books/PLAs_Unmanned_Aerial_Systems.pdf.

22 Dr. Kathleen Hicks spoke at the Seoul conference as director of CSIS's International Security Program. She has subsequently served as U.S. deputy secretary of defense since February 2021. "Unmanned Systems and Robotics," in *Geopolitical Risks & Scientific Innovation*, 37–38.

23 Acquisition Technology & Logistics Agency, *R&D Vision: Toward Realization of Multi-domain Defence Force and Beyond* (Tokyo: Japan Ministry of Defense, August 2019), https://www.mod.go.jp/atla/en/policy/policy_vision.html.

24 Sukjoon Yoon, "Make Way for South Korea's Underwater Drones," *The Diplomat*, February 19, 2020. https://thediplomat.com/2020/02/make-way-for-south-koreas-underwater-drones/; and Xavier Vavasseur, "South Korea Starts Bidding Process for ROK Navy's KDDX Future Destroyer," Naval News, June 4, 2020, https://www.navalnews.com/naval-news/2020/06/south-korea-starts-bidding-process-for-rok-navys-kddx-future-destroyer/.

25 "Opening Speech by Suh Wook," in *Geopolitical Risks & Scientific Innovation*, 13.

26 Adrienne Harebottle, "The Big Power of the Smallsat Revolution," Via Satellite, Asia Edition, 2017, http://interactive.satellitetoday.com/via/asia-edition-2017/the-big-power-of-the-smallsat-revolution/.

27 [33] Yiwei Hu, "Graphics: 2019, a Crucial Year for China's Space Launch Vehicles," CGTN, December 27, 2019, https://news.cgtn.com/news/2019-12-27/Graphics-2019-a-crucial-year-for-China-s-space-launch-vehicles-MLwIKh1lQc/index.html; and Todd Harrison, Kaitlyn Johnson, and Thomas Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, 2019), 8, https://www.csis.org/analysis/space-threat-assessment-2019.

28 Ibid., 9–10.

29 "Satellite imagery suggests that the nation's only active spaceport—the Sohae Satellite Launching Station on the country's western coast—was being actively disassembled in 2018," perhaps part of ongoing negotiations with the United States. However, as of March 2019, this dismantling appeared to be in the process of being reversed. Harrison, Johnson, and Roberts, *2019 Space Threat Assessment*, 30.

30 Mari Yamaguchi, "Japan Reveals Plan for Space Defense Unit," *Defense News*, January 21, 2020, https://www.defensenews.com/space/2020/01/21/japan-reveals-plan-for-space-defense-unit/.

31 Sang-Hun Choe, "On 3rd Try, South Korea Launches Satellite Into Orbit," *New York Times*, January 3, 2013, https://www.nytimes.com/2013/01/31/world/asia/on-3d-try-south-korea-launches-satellite-into-orbit.html.

32 Han-joo Kim, "S. Korea's Space Program Opens New Chapter with Rocket Engine

Launch, Satellites," Yonhap News Agency, December 5, 2018, https://en.yna.co.kr/view/AEN20181205007000320.

33 William J. Broad and David E. Sanger, "North Korea's Missile Success Is Linked to Ukrainian Plant, Investigators Say," *New York Times*, August 14, 2017, https://www.nytimes.com/2017/08/14/world/asia/north-korea-missiles-ukraine-factory.html.

34 Krishnadev Calamur, "How Did North Korea's Weapons Tech Get So Good So Fast?," *The Atlantic*, September 6, 2017, https://www.theatlantic.com/international/archive/2017/09/north-korea-tech/538959/; and Missile Defense Project, "Taepodong-2 (Unha-3)," *Missile Threat*, Center for Strategic and International Studies, modified June 15, 2018, https://missilethreat.csis.org/missile/taepodong-2/.

35 Joshua H. Pollack, "How North Korea Makes Its Missiles," NK News, August 18, 2017, https://www.nknews.org/2017/08/how-north-korea-makes-its-missiles/.

36 Joseph S. Bermudez.and Dan Dueweke, "Expansion of North Korea's Solid Fuel Ballistic Missile Program: The Eight-Year-Old Case of the Chemical Materials Institute," 38 North, July 25, 2018, https://www.38north.org/2018/07/cmi072518/; and Jonathan Cheng, "North Korea Expands Key Missile-Manufacturing Plant," *Wall Street Journal*, July 1, 2018, https://www.wsj.com/articles/north-korea-expands-key-missile-manufacturing-plant-1530486907.

37 Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, D: DoD, C, September 2020), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

38 Defense Intelligence Agency, *Challenges to Space Security* (Washington, DC: January 2019), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

39 Rachel A. Gabriel and Barnett S. Koven, *Malicious Non-state Actors and Contested Space Operations* (College Park, MD: START, 2018), https://nsiteam.com/social/wp-content/uploads/2018/07/START_Malicious-Non-state-Actors-and-Contested-Space-Operations-Final.pdf.

40 Emma Chanlett-Avery et al., *North Korean Cyber Capabilities: In Brief*, CRS Report No. R44912 (Washington, DC: Congressional Research Service, 2017), https://fas.org/sgp/crs/row/R44912.pdf.

41 Hyo-young Lee, "U.S. Trade Policy Against China: U.S. Perspectives and Implications," IFANS Focus, IF 2019-31E, December 12, 2019, http://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?clCode=P11&pblctDtaSn=13494&koreanEngSe=ENG.

42 The risk to internet data centers was highlighted by past incidents in Korea where fires have led to loss of service. See Ji-hye Shin, "Blaze Puts Halt to Samsung's Financial Services," *Korea Herald*, April 21, 2014, http://www.koreaherald.com/view.php?ud=20140421001120; and Ju-young Park, "KT Fire Sparks Chaos in Seoul," *Korea Herald*, November 25, 2018, http://www.koreaherald.com/view.php?ud=20181125000198.

43 Sang-Hun Choe, "South Korea and China End Dispute Over Missile Defense System," *New York Times*, October 30, 2017, https://www.nytimes.com/2017/10/30/world/asia/north-korea-nuclear-

test-radiation.html.

44 The aggregate figures are also striking: "The United States accounts for 80% of Korea's foreign weapons procurements. Since 2013, Korea has acquired over $19 billion in foreign military sales equipment and training, and approximately $18 billion directly from U.S. companies via direct commercial sales."

45 "S. Korea to Buy Bunker Busting Missiles from Europe," Reuters, April 4, 2013, https://web.archive.org/web/20130704011637/http:/www.reuters.com/article/2013/04/04/korea-defense-missiles-idUSL3N0CR1D120130404; Jun Ji-hye, "KF-X Project in Jeopardy on Botched F-35 Deal," *Korea Times*, September 24, 2015, https://www.koreatimes.co.kr/www/news/nation/2015/09/205_187515.html; and Myo-Ja Ser and Yong-Su Jeong, "U.S. Denies Exports of Three More Technologies for KF-X," *Korea Joongang Daily*, November 25, 2015, https://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3012026.

46 Richard Armitage, Victor D. Cha, Kevin Fahey, Andrew Hunter, and Jung-hong Wang, "DAPA Conference 2019: A New Generation of Partnership in the U.S.-ROK Alliance Conference," CSIS, public event transcript, January 2, 2020, https://www.csis.org/analysis/csis-dapa-conference-2019-new-generation-partnership-us-rok-alliance-conference.

47 Aude Fleurant, Alexandra Kuimoya, Diego Lopes Da Silva, Nan Tian, Pieter D. Wezeman, and Simeon T. Wezeman, "SIPRI Fact Sheet: Trends in International Arms Transfers, 2019," Stockholm International Peace Research Institute, March 2019, 5, https://www.sipri.org/publications/2020/sipri-fact-sheets/trends-international-arms-transfers-2019.

48 Ho-Jeong Lee, "Moon's Korean New Deal Detailed," *Korea Joongang Daily,* June 1, 2020, https://koreajoongangdaily.joins.com/2020/06/01/economy/newdeal-digitalnewdeal-greennewdeal/20200601193300201.html.

49 "Economic Policies, H2 2020," Ministry of Economy and Finance of the Republic of Korea, https://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4913.

50 A recent U.S.-ROK intergovernmental agreement included notes on cooperation on space, automation, and artificial intelligence, but placed special emphasis on cyber defense. "Joint Communiqué of the 51st ROK-U.S. Security Consultative Meeting," DoD, November 16, 2019, https://www.defense.gov/Newsroom/Releases/Release/Article/2018651/joint-communiqu-of-the-51st-rok-us-security-consultative-meeting/.

51 "Unmanned Systems and Robotics," in *Geopolitical Risks & Scientific Innovation*, 41.

52 "Advanced Material Science and Supply Chain Implications," in *Geopolitical Risks & Scientific Innovation*, 35.

53 The five principles are "protect and promote global values; foster inclusion and transparency; work in partnership; build on existing capabilities and mandates; and be humble and continue to learn." António Guterres, "Secretary-General's Strategy on New Technologies," United Nations, September 2018, https://www.un.org/en/newtechnologies/index.shtml.

54 Masha Borak, "China Boosts Semiconductor Production in 2020, but Imports Keep Apace,

Frustrating Self-sufficiency Goals," *South China Morning Post*, January 19, 2021, https://www.scmp.com/tech/policy/article/3118327/china-boosts-semiconductor-production-2020-imports-keep-apace; and Eamon Barrett, "China Will Spend $300 Billion on Semiconductor Imports as U.S. Squeezes Chip Supply," Fortune, August 27, 2020, https://fortune.com/2020/08/27/china-semiconductor-chip-imports-us-ban-huawei/.

55 General Won In-Choul has served as chairman of the ROK Joint Chiefs of Staff since September 2020; and "Opening Speech by Won In-Chuol," in *Geopolitical Risks & Scientific Innovation*, 16.

56 "Space Technologies," in *Geopolitical Risks & Scientific Innovation*, 48.

57 "Opening Speech by Won In-Chuol," in *Geopolitical Risks & Scientific Innovation*, 16.

58 House of Representatives, U.S. Congress, "The Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," submitted by Christopher Cox, 105th Congress, 2d sess., Rep. 105-851, Chapters 5 and 6, https://china.usc.edu/cox-report-1999.

59 Makena Young, "Bad Idea: The Wolf Amendment (Limiting Collaboration with China in Space)," CSIS, December 4, 2019, https://defense360.csis.org/bad-idea-the-wolf-amendment-limiting-collaboration-with-china-in-space/.

60 Keith Collins and Sergio Peçanha, "Only 5 Nations Can Hit Any Place on Earth with a Missile. For Now," *New York Times*, February 7, 2018, https://www.nytimes.com/interactive/2018/02/07/world/asia/north-korea-missile-proliferation-range-intercontinental-iran-pakistan-india.html.

61 Ibid.

62 "Artificial Intelligence and Machine Learning," in *Geopolitical Risks & Scientific Innovation*, 28–9.

63 Dana Deasy and Jack Shanahan, "Department of Defense Press Briefing on the Adoption of Ethical Principles for Artificial Intelligence," transcribed February 24, 2020 at the Department of Defense, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2094162/department-of-defense-press-briefing-on-the-adoption-of-ethical-principles-for/; and Patrick Turner, "New Pentagon Initiative Aims to Help Allies, Contractors Work Together on AI," Defense One, September, 9, 2020, https://www.defenseone.com/technology/2020/09/new-pentagon-initiative-aims-help-allies-contractors-work-together-ai/168343/.

64 Emma Farge and Stephanie Nebehay, "Singaporean Defeats Chinese Candidate to Head U.N. Patent Office," Reuters, March 4, 2020, https://www.reuters.com/article/us-un-election-wipo/singaporean-defeats-chinese-candidate-to-head-u-n-patent-office-idUSKBN20R17F.

65 Christopher A. Ford, "Responding to Modern Cyber Threats with Diplomacy and Deterrence," U.S. Department of State, October 19, 2020, https://2017-2021.state.gov/responding-to-modern-cyber-threats-with-diplomacy-and-deterrence/index.html; and Elaine Korzak, "The 2015 GGE Report: What Next for Norms in Cyberspace?," Lawfare, September 23, 2015, https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace.

66 "Cyber Cybersecurity and Blockchain," in *Geopolitical Risks & Scientific Innovation*, 46.

67 For a favorable view of the Cloud Act, see Andrew Keane Woods and Peter Swire, "The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems," Lawfare, February 6, 2018, https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems. For a critical view, see Katitza Rodriguez, "The U.S. CLOUD Act and the EU: A Privacy Race to the Bottom," Electronic Frontier Foundation, April 9, 2018, https://www.eff.org/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection-race-bottom.

68 "The aim of the MTCR is to restrict the proliferation of missiles, complete rocket systems, unmanned air vehicles, and related technology for those systems capable of carrying a 500-kilogram payload at least 300 kilometers, as well as systems intended for the delivery of weapons of mass destruction (WMD)." "Objectives of the MTCR," Missile Technology Control Regime, accessed January 17, 2020, https://mtcr.info/deutsch-ziele/; and Paul K. Kerr, *U.S.-Proposed Missile Technology Control Regime Changes*, CRS Report No. IF11069 (Washington, DC: Congressional Research Service, 2021), https://fas.org/sgp/crs/nuke/IF11069.pdf.

69 "Welcoming Speech by Kathleen Hicks," in *Geopolitical Risks & Scientific Innovation*, 9.

70 In percentage terms, the ROK overtook the United States in 2005, broke into the top five in 2007, and has been in the number two spot to Israel since 2012, averaging 4.1 percent of GDP spent on R&D from 2012 to 2018. "Gross Domestic Spending on R&D (Indicator)," Organization for Economic Cooperation and Development, Main Science and Technology Indicators, 2020, doi:10.1787/d8b068b4-en.

71 Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times,* April 4, 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

72 Caroline O'Donovan, "Google Employees Are Quitting Over The Company's Secretive China Search Project," Buzzfeed, September 13, 2018, https://www.buzzfeednews.com/article/carolineodonovan/google-project-dragonfly-employees-quitting.

73 "During the Cold War, policymakers who worked on nuclear strategy regularly spoke to nuclear scientists who understood the workings of the weapons systems being deployed. Supply chains are nearly as complex as nuclear physics, but those who study them rarely engage with policymakers." Henry Farrell and Abraham Newman, "The Folly of Decoupling from China," *Foreign Affairs,* June 3, 2020, https://www.foreignaffairs.com/articles/china/2020-06-03/folly-decoupling-china. See also, "Advanced Material Science and Supply Chain Implementations," in *Geopolitical Risks & Scientific Innovation*, 33.

74 "Opening Speech by Suh Wook," in *Geopolitical Risks & Scientific Innovation*, 13.

75 "Advance Materials and Supply Chin Implications," in *Geopolitical Risks & Scientific Innovation*, 32.

76 "Unmanned Systems and Robotics," in *Geopolitical Risks & Scientific Innovation*, 41.

77 The U.S. Defense Advanced Research Project Agency (DARPA) is famous for using prize money and the chance at prestige to spur commercial and academic teams for topics including autonomous vehicles, cybersecurity, and space launch. For a brief summary of the logic behind challenges as well as a list of contests, see "Prize Challenges," Defense Advanced Research Project Agency,

accessed November 29, 2020, https://www.darpa.mil/work-with-us/public/prizes.

78 "During the Cold War, policymakers who worked on nuclear strategy regularly spoke to nuclear scientists who understood the workings of the weapons systems being deployed. Supply chains are nearly as complex as nuclear physics, but those who study them rarely engage with policymakers." Farrell and Newman, "The Folly of Decoupling from China." For a proposal to bring greater supply chain knowledge into the Korean defense acquisition system, see Jang Won Joon, "[장원준 칼럼] 방위산업기반 강화 위한 '3가지 조치'에 국가역량 집중해야," news2day, March 8, 2021, https://www.news2day.co.kr/article/20210308500205.

79 "Advanced Material Science and Supply Chain Implications," in *Geopolitical Risks & Scientific Innovation*, 34.

80 "Cybersecurity and Blockchain," in *Geopolitical Risks & Scientific Innovation*, 45.

81 "Unmanned Systems and Robotics," in *Geopolitical Risks & Scientific Innovation*, 39.

82 Jackson Barnett, "Zero Trust Gains Momentum as DOD's New Approach to Manage Microelectronics Acquisition," Fedscoop, May 28, 2020, https://www.fedscoop.com/zero-trust-gains-momentum-dods-tech-acqusistions/.

83 "Unmanned Systems and Robotics," *Geopolitical Risks & Scientific Innovation*, 39.

84 Samantha Cohen and Gregory Sanders, *Designing and Managing Successful International Joint Development Programs* (Washington, DC: CSIS, January 2017), 62, https://www.csis.org/analysis/designing-and-managing-successful-international-joint-development-programs.

85 Both Korean and U.S. participants mentioned the U.S. Third Offset Strategy, first proposed in 2014, as relevant to the common interests of both nations. For more, see Gabriel Coll, Jesse Ellman, and Lisa Samp, *Assessing the Third Offset Strategy* (Washington, DC: CSIS, March 20170, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170302_Ellman_ThirdOffsetStrategySummary_Web.pdf.

86 "Unmanned Systems and Robotics," in *Geopolitical Risks & Scientific Innovation*, 38.

87 "Opening Speech by Won In-Chuol," in *Geopolitical Risks & Scientific Innovation*, 17.

88 These committees are part of the larger dialogue system that includes the civilian-led ROK-U.S. Security Consultative Meeting (SCM) and military-led Military Committee Meetings (MCM).

89 The chance to exercise and consider cooperation on bio surveillance issues was already part of considerations in the Able Defense exercise in 2013. For more see, Chaeshin Chu, Jo Hyun Jeong, Seong Sun Kim, and Dong Whan Oh, "Introduction of the Republic of Korea–the United States of America's Joint Exercise Against Biothreats in 2013: Able Response 13," *Osong Public Health and Research Perspectives* 4, no. 5, (October 2013): 285–290, https://www.sciencedirect.com/science/article/pii/S2210909913001148.

90 "Welcoming Speech by Kathleen Hicks," in *Geopolitical Risks & Scientific Innovation*, 9.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**