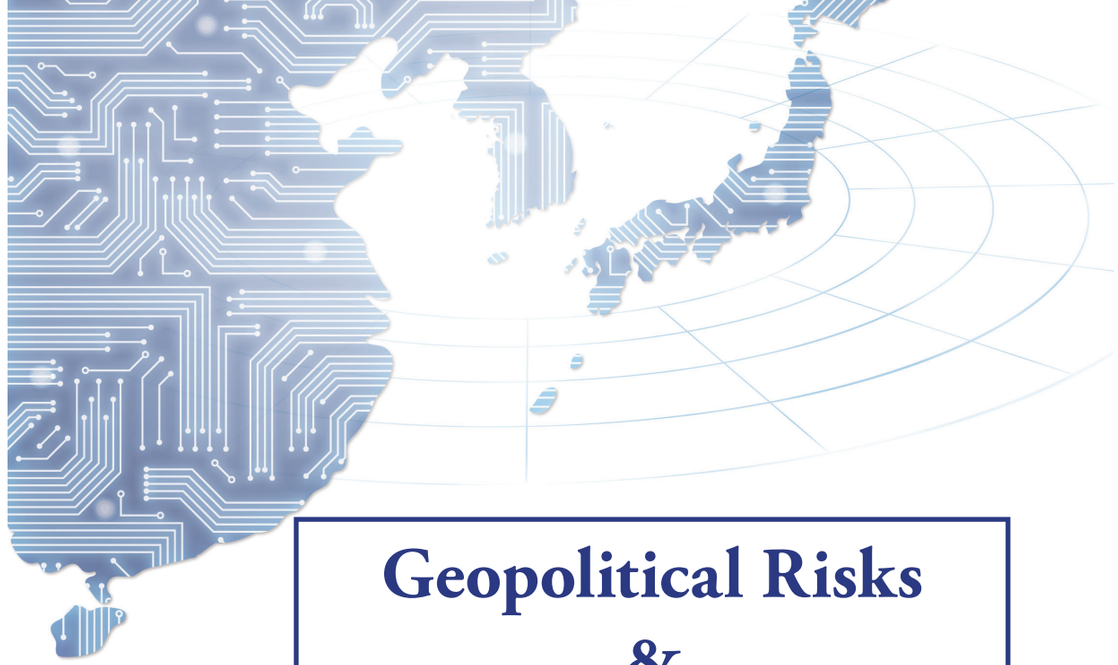
Conference Proceeding

Geopolitical Risks & Scientific Innovation

January 30-31, 2020

CHEY | CHEY INSTITUTE FOR ADVANCED STUDIES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES



Geopolitical Risks & Scientific Innovation

Conference Proceeding

Chey Institute for Advanced Studies
&
Center for Strategic and International Studies (CSIS)

January 30-31, 2020

DISCLAIMER

The views expressed herein are solely those of the conference participants and do not reflect those of the Chey Institute for Advanced Studies and/or CSIS.

Table of Content

Conference Program

Day 1: January 30, 2020

Session	Time	Speakers
Welcoming Speech	9:00 AM–9:30 AM	PARK In-kook, Chey Institute for Advanced Studies Kathleen HICKS, CSIS
Opening Speech	9:30 AM–9:45 AM	SUH Wook, Chief of Staff, ROK Army
Session 1: Artificial Intelligence and Machine Learning	9:45 AM–11:30 AM	**Moderator** AHN Jung Ho (Seoul National University) **Speakers** Lindsey SHEPPARD (CSIS) Jason BROWN (U.S. Air Force) KIM Yoon (SK Telecom) PARK Byung Jin (Advanced Defense Technology Research Institute, Agency for Defense Development)
Session 2: Advanced Materials Science and Supply Chain Implications	11:45 AM–1:15 PM	**Moderator** Kathleen HICKS (CSIS) **Speakers** Andrew HUNTER (CSIS) Brett LAMBERT (The Densmore Group, LLC.) JUNG Hee-Tae (Korea Advanced Institute of Science and Technology)
Session 3: Unmanned Systems and Robotics	2:15 PM–4:15 PM	**Moderator** LEE Geunwook (Sogang University) **Speakers** Kathleen HICKS (CSIS) Morgan DWYER (CSIS) LIM KiHoon (ROK Army)

Conference Program

Day 2: January 31, 2020

Session	Time	Speakers
Opening Speech	9:30 AM-9:45 AM	WON In-choul, Chief of Staff, ROK Air Force
Session 4: Cyber Security and Blockchain	9:45 AM-11:15 AM	**Moderator** Andrew HUNTER (CSIS) **Speakers** R. David EDELMAN (Massachusetts Institute of Technology) KIM Hyoung Joong (Korea University) LIM Jong-in (Korea University)
Session 5: Space Technologies	11:30 AM-1:15 PM	**Moderator** HONG Kyu-Dok (Sookmyung Women's University) **Speakers** Michael HAMEL (Ret., U.S. Air Force) JU Gwang-Hyeok (Korea Aerospace Research Institute) KIM Kwang-Jin (ROK Air Force) REU Taekyu (Defense Science & Technology Academy, Agency for Defense Development)

Welcoming Speech

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

Good Morning.

Chief of Staff of the ROK Army, General SUH Wook.
Senior Vice President of CSIS, Dr. Kathleen HICKS.
Ladies and gentlemen.

It is my great pleasure to welcome everyone to today's conference on "Geopolitical Risks and Scientific Innovation." It is the first harvest in the collaboration between the Chey Institute for Advanced Studies and CSIS. I trust that today's conference will serve as a platform for consolidated exploration between the two institutions.

As the title of today's conference suggests, we are gathered here today to examine the impact of scientific innovation on geopolitical risks. I am confident that over the course of the next two days, we will engage in an enriched discussion involving topics that will greatly influence the future of peace and security on the Korean Peninsula and in Northeast Asia.

As many of you are already aware, the Chey Institute for Advanced Studies was established to commemorate the 20th year of the passing of Chairman CHEY Jong-hyon, the founding father of the Korea Foundation for Advanced Studies (KFAS). During his lifetime, he had an unswerving dedication to modernize Korea by investing in human capital and by sending promising young Koreans to study abroad to earn their Ph.D.s, many in the United States. As a result, for more than 50 years, we have successfully produced a pool of 1,000 Ph.D.s, mainly from leading universities in the world. That is why, we named our Institute in honor of the late Chairman Chey.

With this solid intellectual base, the Chey Institute for Advanced Studies was launched to expand the international academic network, and to focus exclusively on the following:

First, to identify geopolitical risks in Northeast Asia and beyond, and to shape global strategies in response to such risks;
Second, to explore the limits of scientific innovation and its impact on the entire spectrum of our society;
Third, to explore the impact of scientific innovation on geopolitical and geoeconomic risks.

As part of our mandate, the Chey Institute launched the *Scientific Innovation Conference Series* last summer, focusing on the potential and limits of science and technology. The inaugural conference covered various fields including AI, nanotechnology, bioengineering, neuroscience, and quantum technology. We were very fortunate to have 16 distinguished speakers from Harvard University, Stanford University, Massachusetts Institute of Technology, University of California-Berkeley, Yale University, Columbia University, University of Chicago, Carnegie Mellon University, Johns Hopkins University, Seoul National University, and Korea Advanced Institute of Science and Technology (KAIST). The second conference, which was held just three weeks ago, focused on the keywords *battery* and *semiconductor,* and how these two technology areas develop with the advancement of AI.

Today's event is the manifestation of our third mission and we want to analyze how geopolitics and scientific innovation influence and affect each other.

During yesterday's lunch, EU Ambassador to Korea Michael REITERER asked me whether a science attaché or a political attaché should attend today's conference. Given the unprecedented delicacy of the issues, I recommended that both attachés attend! I welcome members from more than 50 diplomatic corps.

Through today's conference, we aim to build a foundation for the consolidated base of interdisciplinary discourses that crisscross science and geopolitics. In 5-6 months, we will hold our next round of workshop in Washington, D.C. and jointly publish a final report. It is our ultimate goal for this project to contribute to promoting peace and stability, as well as co-prosperity, in the Northeast Asian region and beyond.

Last but not least, I'd like to extend my heartfelt appreciation to President John HAMRE of CSIS and Dr. Kathleen HICKS, Senior Vice President and Henry Kissinger Chair at CSIS, for their special dedication to this project. Dr. Hicks graciously agreed to act as a locomotive to get this

project off the ground. In fact, this project was in large part drawn up during our meeting in Washington, D.C. last year. She took the trouble of coming to Reagan National Airport to have an urgent meeting at the airport coffee shop. That moment in the café set the tone for this conference.

Taking this opportunity, I'd also like to thank the CSIS delegation for traveling all the way from the United States. I extend my special thanks to General SUH Wook, Chief of Staff of the ROK Army, for his attendance and special message today.

We are indeed navigating an uncharted path. I hope this conference will point the right way and serve as an impetus for a better and safer future for our generation as well as future generations.

Thank you.

Welcoming Speech

Dr. Kathleen HICKS
Senior Vice President; Henry A. Kissinger Chair; Director of the International Security Program (ISP), CSIS

Good morning everyone.

Thank you so much for joining us today. As President Park described it, this is the beginning of what we hope to be an enduring relationship between our institutions, the Center for Strategic and International Studies and the Chey Institute. We embarked on this endeavor together in part because we believe in the importance of the issues we are going to talk about today particularly with regard to emerging technologies and their implications for the economy, national security, and US-ROK relations—the last of which CSIS firmly believes is central to how we think about peace and prosperity in Northeast Asia and beyond.

If you don't know about CSIS, we live by three basic principles. The first is that we are politically bipartisan in the context of U.S. politics. The second is that we work from an analytic basis on all our efforts. We believe in finding truth, being focused on facts, and seeing where they lead us. The third is that we are independent. Each of our scholars comes to represent his or her own views. Both the CSIS scholars who are here today and those we have invited from the United States outside of CSIS are here representing their own viewpoints on the issues that they will speak about.

We have brought a stellar group of people who are first in class in their fields. I hope you will see how much opportunity there is for collaboration between the United States and Korea in many of these areas. As President Park said, the purpose of this conference is to look at how emerging technology is shaping both peace and prosperity in the region and beyond. This has been true in every age but no more so than in the age that we are in, where there is an incredible diffusion of technology across multiple different disciplines. Over the course of this conference, we will focus on several of those areas. Our goal is to scope down to the major issues that come out of both our research and this conference, and work together in a final report that comes out later this year.

The report will hone in on the key issues that we should be working on together and the key considerations or findings for the region.

This very much reflects the state of the conversation on these issues in Washington, where the national defense strategy and national security strategy of the Trump Administration have prioritized both the competition with China and U.S. innovation in order to find out how the United States could best innovate in order to compete in a positive direction. To do that, 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.

There are specific dynamics around each technology that we will talk about in the next two days. But the broader issue set of governance partnership and the role of government does transcend various different areas of technologies. We hope that in the next two days, we will bring together the right combination of understanding at the broad-level, specifically how we think about scientific innovation and security in the region and what specific findings and recommendations we might want to pursue in each of these technology areas.

As I said, we brought a world class group from the United States and you also have an incredible group of scholars from Korea. I want to thank General SUH Wook for coming and giving opening remarks today. We are really looking forward to the dialogue and, as I mentioned, this is the beginning of our dialogue. We hope it will continue and endure going forward. Thank you all very much and I look forward to the discussion.

Opening Speech

General SUH Wook
Chief of Staff, ROK Army
January 30, 2020

Hello, I am General SUH Wook, Chief of Staff of the Republic of Korea Army. I would like to thank the Chey Institute for Advanced Studies for the invitation and the opportunity to deliver my congratulatory remarks for this conference.

In 1532, Pizarro led his soldiers against an army of the Incan Empire at Cajamarca, located in modern day Peru. The battle was fought by 168 Spanish men against 80,000 Incans. Despite the numerical advantage, the eighty thousand strong Incans were defeated, leaving seven thousand Incans dead on the battlefield. Jared DIAMOND, in his book *Guns, Germs, and Steel,* describes this battle as the Massacre of Cajamarca, where the Spanish conquistadors armed with cold steel, gunpowder, and horses annihilated Atahualpa's army of stone hatchets and clubs. The technological gap evident between these two nations have incurred same results in battles fought by European powers against other Native Americans. At the time, European kingdoms were involved in constant competition, which accelerated development for the purposes of survival. Historically, geopolitical environment has shaped development and created differences in advancements between civilizations.

International relations and politics are, and will always be, complicated. A few weeks ago, the United States used its drone assets to eliminate the commander of the Quds Force of Iran's Islamic Revolutionary Guard Corps. This led to a spike in crude oil prices and an attack on a Ukrainian airliner, resulting in many innocent deaths. No country is free from the influence of others. Historically, this has rung true for Korea, where depending on our perceived military strengths, we have been heavily influenced by our neighboring countries. During the Imjin War of 1592, when we had a weaker military, Japanese invading forces, armed with muskets, ravaged our lands for seven years. A century ago, great powers have competed to bolster their influence over the Korean Peninsula, with the Qing Dynasty and Imperial Japan fighting their war atop the soils

of our Peninsula. However, when we commanded a stronger force during the Three Kingdoms period, the northern Kingdom of Goguryeo collapsed China's Sui Dynasty and threatened the Tang Dynasty as Goguryeo expanded into Tang territory.

History has a habit of repeating itself. In this time of heightened competition between our neighboring nations, I believe this conference, with its focus on "Geopolitical Risks and Scientific Innovation," is timely. Today's conference would not have been possible without Chairman CHEY Tae-won's deep interest in, and commitment to, the future of Korea. Although he is not present here today, I'd like to extend my deep gratitude to Chairman Chey for enabling this conference. Furthermore, thank you to Ambassador PARK In-Kook, President of the Chey Institute, and all the staff who put this event together. Thank you, Dr. Kathleen HICKS of CSIS and other researchers who traveled a long way to attend this conference today.

While Korea's geopolitical environment today may seem tumultuous, unstable, and dangerous, we must use this period of challenge to our own advantage, like a surfer gaining speed and energy as waves become steeper. Especially for Korea, a country with comparatively few natural resources and a small population, scientific and technological progress is imperative. For the ROK Army as well, we see technological innovation as an essential factor for victory on the battlefield and protection of our soldiers' lives.

In 1993, U.S. forces in Somalia incurred great damage during an operation to recover pilots of a downed helicopter in Mogadishu. Soldiers lost their sense of direction in the busy alleys, identification of the location of friendly and foe was unclear, and low-level of troop protection aggravated the casualties. This famous battle was later published into a book and produced into a movie titled "Black Hawk Down." Fast forward twelve years to 2004, when yet another helicopter was downed in the urban sprawl of Tall'Afar, Iraq. This time, soldiers utilizing C4 and ISR systems correctly identified the location of the helicopter, while a UAV 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.

Last January, during my visit to the United States, I visited the Army Futures Command and the U.S. Army Space and Missile Defense Command, and saw with my own eyes that the United States has not taken a break from innovation, and that its wheels of change continue to roll forward. For example, the U.S. Army has been coordinating with Uber's Flying Car Project and has been acquiring the technologies necessary to develop future generations of drones, and is even preparing to use artificial intelligence for equipment maintenance and check.

I believe that opportunities are cloaked behind crises, especially if we are able to respond promptly to the changing tides and prepare for the future. The Asia Paradox refers to the phenomenon where globalization increases the economic cooperation of Asian countries and, at the same time, widens their political and security rifts. Countries of Northeast Asia share history steeped in conflict, whilst the region also serves as an arena where great powers like the United States, China, Japan, and Russia inject massive amount of their defense budgets to improve their cutting-edge technologies.

Technologies of the 4th Industrial Revolution—drones, robots, artificial intelligence, and autonomous driving to name a few—are closely connected to military technology, and neighboring countries are pursuing technology-based military innovations. Military innovation through technological advances will play a key role in altering the balance of national influence and military power. The future, by definition, cannot be guaranteed, for in its purest essence, it is uncertain, complex, and plagued by vagaries.

Despite this, the ROK Army, as the central force behind Korea's national defense, needs to answer the nation's call to maintain peace through strength. This is why the ROK Army devised "Vision 2030: Hyper Elite Army Beyond Limits" and is aiming for transformative advances in order to become a state-of-the-art technological army. The ROK Army is developing capabilities based on five game changers in order to realize Vision 2030. Through the Warrior Platform Project, we will increase our soldiers' lethality and survivability via wearable devices and smart weapon systems, increase combined arms interoperability, and maximize combat efficiency. Also, the Dronebot Combat Systems will implement artificial intelligence and Internet of Things (IoT) technologies to visualize the battlefield, minimize combat damage, and conduct various missions outside the scope of direct action such as detonating explosives and clearing obstacles.

The hyper-connected and super-intelligent Army Tiger Project will not only increase the maneuverability of infantry units through its wheeled APCs, but utilize automatic position reporting equipment that can create networks among soldiers, vehicles, and units, so as to ultimately create smart-units that can automatically identify and analyze targets. Even though the ROK Army will decrease in size and personnel, we will expand our scope of operations,

and acquire faster and stronger combat capabilities through these efforts. Furthermore, through preemptive and predictive measures of the future, we will prepare ten next-generation game changers as well.

The advancement of technology will bring future warfare into different dimensions, and the ROK Army, in order to support the security and prosperity of the Republic of Korea through strength, will continue our endeavors to modernize our Army. However, this transformation cannot be attained alone. It can only be fulfilled by cooperating with the private sector, other government agencies, military services, industry, academic institutions, and research organizations. The ROK Army will provide a testbed for innovative technologies, while the private sector will support our transformation with new advancements and creative ideas.

I am sure that today's conference, organized by the Chey Institute, is yet another opportunity for us to be inspired and, in the process, verify the direction of the ROK Army's transformation. During World War II, the U.S. Department of Defense invented the world's first electronic computer, ENIAC, intended to compute ballistic trajectories. The development of the atomic bomb opened up a new era of nuclear energy. ARPANET, a data exchange network test supported by the U.S. Department of Defense, was the father of today's Internet. Regardless of country, times of crisis have brought forth more innovations compared to those of peace.

Transformation is catalyzed by necessity, which is why crises and opportunities coexist. The impetus provided by our geopolitical risks will surely provide us with opportunities for new endeavors and new innovations. While it is near impossible to predict the future, we can set directions and objectives for the future by analyzing the past and the present.

We march not into the past, but towards the future. And these are times when we need a compass that will guide us to the True North of transformation. I hope this conference provides the Republic of Korea and the ROK Army valuable insights that may assist us in shaping the future.

Thank you.

Opening Speech

General WON In-choul
Chief of Staff, ROK Air Force
January 31, 2020

Good morning everyone.

This is the Chief of Staff of the Republic of Korea Air Force (ROKAF), General WON In-choul.

It is a great honor for me to present the "Future Development and Aerospace Power of the ROKAF" in front of world-renowned scholars during today's CHEY-CSIS Conference. Considering the security environment of today, I believe it is highly meaningful that the Chey Institute for Advanced Studies, a leading institute in educating talents across the world as well as hosting international academic exchange programs, has decided to jointly host a conference on "Geopolitical Risks and Scientific Innovation" with CSIS, the world's top national security think tank.

Furthermore, the keyword of this conference, *scientific innovation,* is an important keyword that cannot be left out when discussing today's national security environment. In particular, today's sessions involve topics pertaining to space and cyber domains, all of which are areas of priority for the ROKAF. I hope today's discussions will be fruitful and in-depth as we have world-class scholars and experts from a variety of fields.

With the advancement of cutting-edge science technologies, we are now able to utilize space and cyber domains for military purposes. These domains are critical means for us to gain an edge over adversaries in terms of minimizing decision-making time and human casualties in modern warfare that involves synchronized network-based warfighting. The development and innovation of science and technology are gradually expanding the battlespace from the traditional air, land, and sea domains to include non-traditional space and cyber domains.

Furthermore, we are witnessing an advent of an era when technology will influence everything from decision-making speed to cognitive ability and psychology of major policy and decision-makers. In particular, a new arms race for dominance in space is already starting to surface among major powers around the world. Space is no longer a battlespace of the future, but a major factor that should be prioritized to maintain today's security situation. From the military perspective, information collection through unimpeded and extensive space surveillance and reconnaissance systems is the key to today's battlespace awareness. Positioning, navigation, and timing information from space are core factors for successful operations of precision strike weapons systems. Long-range communications satellite systems and early warning satellites are also important space assets for missile defense. As such, space power is a vital component in modern warfare. Battlespace awareness, protection, precision strike capabilities, command and control, and other key functions all heavily rely on space capabilities. For this reason, damage to space assets could lead to fatal results in modern warfare.

Despite the critical role space assets play, their inherent vulnerabilities such as lack of protection, concealment, and mobility render them susceptible to attacks. It is, therefore, anticipated 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.

Based on these understandings of space, the ROKAF has been striving to improve its space capabilities for a number of years. The ROKAF is the first military branch to have established an independent space unit in 1998 and has been building its space power by nurturing space professionals and developing space operation doctrines. Moreover, the ROKAF established the Korea Space Operations Center within its headquarters in 2015, supporting stable operations of national space assets and safeguarding citizens' lives by collecting information on falling and collision of space objects on a real-time basis and disseminating such information. We are also enhancing our space awareness by maintaining close information-sharing with the U.S. Space Force.

Along the same lines, the ROK and U.S. personnel in the Space Integration Team at Air Force Operations Command collaborate during combined training exercises to develop and familiarize joint response procedures against space threats. In addition, we are currently in pursuit of fielding an electro-optical satellite surveillance system, which is one of our top priorities for space operations capabilities development. The fielding of such system will be the foundation for the Air Force to introduce laser-based satellite tracking system and radar space surveillance system.

The ROKAF is currently devising a three-phased Future Space Capabilities Development Plan based on the efforts it has made so far, with the goal of enhancing its space power by 2050—the 100th anniversary of the founding of the ROKAF. First, phase 1 of the plan involves building a system that allows centralized control over space assets on the Korean Peninsula by interfacing missile defense and space surveillance systems based on big data technology and networks. In phase 2, air-space integrated operations capability will be developed through interoperability between airborne and space assets. If reconnaissance, communication, and navigation satellites sustain damage or malfunction during this period, airborne assets will be rapidly deployed to replace them. In addition, aircraft will be used for rapid air-launch-to-orbit, which will allow us to meet urgent demands for satellites and, thereby, build resiliency in space. In phase 3, the ROKAF will apply the concept of air superiority in the space domain to develop space operations capabilities that will allow the ROK-US Combined Forces to establish both air and space superiority.

However, the ROKAF alone will not be enough to develop such level of future space power. Building a competent space power requires the conjunction of national and military space development plans, in addition to cooperation among the government, research institutes, and the industry as well as with partner nations since space domain demands a synthesis of technology from multiple fields. Therefore, technology cooperation between multiple sectors based on close ROK-US cooperation is more important than ever.

The Future Space Capabilities Development Plan presented here will be materialized through the ROKAF's plan called Air Force Quantum 5.0. The ROKAF has named the plan for its future aerospace power to prepare for the 4th Industrial Revolution and to account for the diversifying security environment. The title is the embodiment of our commitment to taking a big leap to space in the future. It consists of five space development projects and serves as the vision of the ROKAF for the next 30 years.

Air Force Quantum 5.0 consists of five specialized areas: space, cyber and electromagnetic wave, command and control, force integration and fusion, and future professional development and

organizational restructuring. These are areas that the ROKAF will further develop based on the technologies that will be available in the near future to make our vision a reality. This five-part future plan is sub-divided into five flagship projects such as the Space Development Plan and the Space Odyssey Project.

The ROKAF's five flagship projects fully reflect the importance of multi-domains, including air, land, sea, space, and cyber domains as well as cognitive, psychological, and time factors, all of which are battlespaces of future warfare. As the ROKAF celebrated its 70th birthday last year, this plan was developed for us to take a new leap forward in building aerospace power with the next 30 years in mind, by the end of which we will celebrate our 100th birthday. All service members will give their best to achieve these goals and I ask for your warm support and encouragement.

I hope that in-depth discussions on space and cutting-edge technologies that will take place here today will play a meaningful role in further developing the ROK Air Force and its space power. Last but not least, I would like give my most sincere thank you to the Chey Institute for Advanced Studies and the Center for Strategic and International Studies for hosting this conference, and all the distinguished guests for honoring today's event with their presence. I hope today's conference will be a great success.

Thank you very much.

Key Takeaways

Session 1: Artificial Intelligence and Machine Learning

On AI and Geopolitics

- Global trends in data and software show a transition towards an increasingly digital society and economy driven by the adoption of data-driven technologies and software intensive systems. This trend can also be found in national security and defense, with a growing number of security actors having access to advanced technologies.
- Governments adopting these technologies need to build up the necessary infrastructure and think about how to leverage these technologies from a policy and strategy standpoint.
- Governments must think about sharing the processes by which the outcomes and performance of artificial intelligence (AI) systems are tested, verified, and validated. This will lead to assurances that the systems are working as intended, which could eventually lead to trust among nations.
- All users, security actors, and nations must be mindful of the potential misunderstandings or misapplications of relatively immature technologies that could exacerbate geopolitical tensions.

On Challenges and Opportunities of AI for the U.S. Department of Defense

- In its effort to better develop and implement AI, the United States Department of Defense (DoD) is seeking ways to engage with start-ups to expand the defense industrial base, while trying to leverage cutting-edge resources by partnering with academia and allies.

On the Application of AI in the Private Sector

- AI introduces new risks such as poor decision-making based on biased data, and increased risks of cyber hacking.
- Inference technology used in deep learning, especially when combined with other types of AI technologies, may trigger a global AI arms race.
- Private sectors and governments need to focus more on human-centered AI to help address global social problems such as health, education, environmental issues, and elderly care.

Session 2: Advanced Materials Science and Supply Chain Implications

On the Implications of Global Supply Chains for Security and Geopolitics in Northeast Asia

- The global strategic competition for control of supply chains is at its peak in Northeast Asia. Scientific innovation and technologies show their true potential when incorporated into the supply chains, which then feed into the broader systems or networks of systems. This provide nations with opportunities to gain strategic advantages. This dynamic is currently visible in the struggle over 5G and mobile networking.
- Northeast Asian countries and the United States are developing supply chains for microelectronics and microelectronics-based technologies, starting from the basic components at the chip-level, that can provide a trusted foundation for national security systems. Secure technologies include innovations such as blockchain, at the software-level, that can also help secure supply chains in terms of validating the authenticity of parts and transactions in the supply chain.
- Governments could play a greater role in evaluating the performance of advanced technologies and in driving commercial and military progress in supply chains by setting appropriate standards and procuring from secure supply chains. Governments and the private sector need to work together on supply chain issues to ensure that critical national security functions are protected.
- Bifurcation in the supply chains is starting to show between a bloc led by China and a bloc led by a coalition of free market economies. This bifurcation is pushing other nations and companies to choose sides. Bifurcation is a suboptimal outcome, but it can be done as demonstrated by many defense supply chains that focus on secure sources. Notwithstanding the real costs it imposes on societies, bifurcation may be the path chosen.

On the Evolution of the Industrial Base and Policies Toward Supply Chain

- Today's systems have become so complex and dependent on a wide variety of commercial base technologies that they cannot possibly all be engineered, constructed, and delivered by a single company.
- The amount of data created in the industrial base that must be protected is so immense that it likely requires new technology such as AI to manage a large volume amid proliferating attacks. In addition, the sophisticated nature of supply chains and interdependency of networks complicates efforts to come up with policy prescriptions to protect and develop the industrial base due to the risk of unintended side effects. We need new tools to help us manage supply chains to mitigate these challenges.
- There are five potential ways to deal with the growing complexities of supply chains and the materials within those supply chains: 1) rely on a completely open architecture and system; 2) protect the infrastructure and supply chains from the bottom to the top; 3) control and verify supply chains which comply with procedures designed to guarantee safety; 4) stratify protection by applying tight restrictions on the most sensitive categories of capabilities; and 5) assume that all systems are compromised and operate under zero-trust environments.

On the Implications of Nanotechnology and Nanomaterials for Defense

- Nanotechnologies have great implications for national defense in that they can create nanoscale devices and systems that have fundamentally different properties than similar systems that operate at a larger scale. These technologies utilize well-known and sometimes low-cost material inputs to deliver capabilities such as high-strength and lightweight materials, and intelligent nanobots.
- Technologists can leverage this property of nanotechnologies to support a wide-range of national security missions including: 1) improving human performance; 2) creating lighter, efficient, and more effective military components, such as gears; 3) miniaturizing existing systems by creating nanorobots and other intelligent systems; 4) creating biologically-based systems of great complexity; 5) creating smart weapons, intelligent ammunitions, trackers, and other adaptive systems; and 6) creating light-absorbing and deflecting materials for low-observable coverings.
- Making these new capabilities a reality, however, requires incorporating nanomaterials into military and commercial supply chains. While some "easy" nanomaterials have already entered the commercial supply chains, many others are still a long way from being ready for practical use.

Session 3: Unmanned Systems and Robotics

On Unmanned Systems and Robotics

- Despite being the oldest technology being discussed, the current understanding of unmanned systems is heavily focused on the kinetic effect—the physical use of the system in warfare. There is a lack of understanding on how these systems impact escalation and deterrence dynamics.

- There is surprising underinvestment in the field of unmanned systems. This is driven in part by cultural resistance, especially in the United States, to the expansion of unmanned systems due to the perception that unmanned systems threaten the traditional role of service members. Nonetheless, there's potential for greater usage on the back-end of military operations and for increased international R&D collaboration between the United States and its major allies.

On the Technical Architecture of Unmanned Systems and Structure of the Industry

- How we implement unmanned systems is becoming increasingly critical. Instead of a single and monolithic system that carries out the entire mission with the help of mission modules, the mission itself can be disaggregated into roles for separate discrete systems. Militaries must consider the use of unmanned autonomous systems (UAS) to partner with manned systems and collectively carry out those missions.

On the Future of ROK Army's Use of Unmanned Systems and Robotics

- A combination of intelligence, surveillance, and reconnaissance (ISR), precision-guided munitions (PGM), hyper-intelligence, hyper-connectivity, and cyber-electronic warfare will revolutionize future warfare. Future ground forces must expand their areas of operation to additional domains, such as air and sea, in order to operate in all fields of war.

Session 4: Cyber Security and Blockchain

On the Nature of Cyber Technologies and Their Impact on National Security

- Over the past fifteen years, we have learned a great deal about the nature of cyber technologies. First, attribution is possible. Second, concerns over proliferation of cyber weapons have been over-exaggerated. Third, asymmetric risks may be more important than anticipated. Fourth, norms and regulations may not be enough to restrain states from engaging in cyber attacks. Lastly, the involvement and participation of private companies in the cyber environment complicates the statecraft of cyber security.
- In terms of security implications, cyber technologies provide revisionist states with opportunities to cause political and diplomatic disruptions. They also provide states as well as militaries the means to advance their military, foreign policy, and strategic goals.
- At the same time, cyber technologies provide opportunities for stabilization. Unilaterally, states can utilize cyber technologies to counter threats to their democracies. Bilaterally, states have begun to identify areas of cooperation and confidence-building related to cyber security. Multilaterally, core military alliances such as NATO have begun to enhance their cyber security capabilities to better defend one another.

On the Impact of Blockchain on Military Operations

- Blockchain technologies have three distinct characteristics that have major implications for military operations: de-centralization, transparency, and integrity.
- Blockchain has found limited application thus far, but building on its ability to track data manipulation could leave militaries better equipped to deal with cyber attacks. First, it can help protect critical military weaponry. Second, it can help manage drone operations. Third, it can help verify command and control with accuracy. Lastly, it can help manage logistics and supply chains.
- Since blockchain is a decentralized technology by nature and military operations have traditionally relied on centralized systems, implementing the former will be difficult and time-consuming in the military context. Therefore, militaries should utilize blockchain on a partial basis to test its applicability.

On Cyber Threats to Korea

- To better deal with growing cyber threats, the Korean government must be more pro-active in improving its cyber defenses. It can do so by committing to capacity-building. trust-building, and cyber diplomacy.
- There needs to be a clearer line of what cyber-attacks are and are not acceptable. For example, the United Nations should take a greater role in implementing sanctions and establish an international court for cyber crimes.

Session 5: Space Technologies

On the Current Trend of Space Systems and the Emerging Concept of "New Space"

- The private sector is witnessing frequent disruptions of its communication operations. There is growing evidence to suggest that space has become an inviting target for adversaries. Further, given that most of these technologies are dual-use and their applications often transcend borders, managing proliferation has proven to be a challenge.
- With the growth of the commercial space industry, labeled as "New Space," fundamental

changes are beginning to take place. Technologies relevant to this change include the use of small satellites, usually weighing less than 100kg. Sustainability of space systems is also a part of these changes. New technologies are being researched such as “refueling” older satellites in space, thereby extending their lifespan.

On the Use of Space Systems in the Military

- The current era of space systems may be defined by anti-satellite tests and introduction of offensive and defensive capabilities in space. Thus, “space deterrence,” will become a critical concept which involves the protection and maintenance of space assets. Key elements of this space deterrence will involve securing retaliatory capability, effective command and control mechanisms, and defense capability sufficient to deny attacks.
- In terms of the geopolitical risks in Asia, technological advancements in space systems may allow Korea to combat North Korea’s missile and nuclear threats. However, prior to acquiring the resources necessary, it is imperative to persuade the Korean public that space is truly important for counter-operations against North Korea.

Session 1

Artificial Intelligence and Machine Learning

Moderator

AHN Jung Ho (Seoul National University)

Speakers

Lindsey SHEPPARD (CSIS)

Jason BROWN (U.S. Air Force)

KIM Yoon (SK Telecom)

PARK Byung Jin (Advanced Defense Technology Research Institute, Agency for Defense Development)

Rapporteur

Ashley PARK (Chey Institute for Advanced Studies)

Session 1 titled “Artificial Intelligence and Machine Learning: Data-Driven Techniques and Software Intensive Technologies” was moderated by Professor AHN Jung Ho of Seoul National University.

The first speaker, Ms. Lindsey SHEPPARD, Fellow in the International Security Program (ISP) at CSIS, introduced artificial intelligence (AI) as a technology that is part of a broader trend of data-driven technologies and software intensive systems. Ms. Sheppard observed that many countries are currently transitioning towards an increasingly digital society and economy. This trend can also be found in national security and defense, where a growing number of actors are getting better access to advanced technologies.

Ms. Sheppard described artificial intelligence/machine learning (AI/ML) as an umbrella term that is often used interchangeably to reference a variety of computer science disciplines. Specifically, machine learning is a process in which intelligence functions, including natural

language processing and computer vision, are implemented via a machine. We also use the term AI to include its applications, such as facial recognition or autonomous vehicles. Ms. Sheppard argued that in the context of national security and defense, we need honest technical discussions given that we are still using relatively immature technologies.

Ms. Sheppard also explained that many states are now thinking about ways to use AI to meet national goals and needs, but pointed out that the ways in which they leverage the technologies differ since they have different priorities. For example, the U.S. focuses heavily on the concept of human-machine cooperation, while Korea's strategy on AI emphasizes the 4th Industrial Revolution and digital transformations such as Internet of Things (IoT), cloud computing, and mobile telecommunications.

Furthermore, she stressed that all users, security-relevant actors, and governments must focus on the ecosystem surrounding these modern technologies. They must consider the workforce, including people developing the technologies, people using them, and senior leaders and middle managers making decisions on where best to use them. There is also the need to build up the IT infrastructure that supports these technologies and to think about how to leverage them from a policy and strategy standpoint.

The presentation concluded with the identification of some of the risks associated with AI/ML, including misunderstandings or misapplications of relatively immature technologies that could exacerbate geopolitical tensions. These technologies have the potential to introduce new vulnerabilities in our defense systems. In response, the defense industry must verify that the systems are behaving as intended when technologies are being procured from the private sector. This is critical given that many military applications are of high consequence and can result in the loss of life. Ms. Sheppard also stressed the importance of people and education—expanding the knowledge base for young programmers as well as senior leaders who make decisions on how to best leverage these capabilities.

The second speaker of the session was Colonel Jason BROWN, Director of the Chief of Staff of the U.S. Air Force Strategic Studies Group. Colonel Brown focused on what the U.S. Department of Defense (DoD) is doing, including how AI is being implemented within the DoD and how it is dealing with the challenges posed by AI. According to Colonel Brown, DoD's thinking over AI can be traced back to the first research at MIT in the 1950s. More recently, the establishment of the Defense Innovation Unit (DIU) and the Defense Innovation Board, the latter consisting of members from academia as well as the private sector, have heavily influenced DoD's approach to AI.

Many of DoD's mega projects have tried to learn and understand how AI can be useful. In particular, these projects aimed to improve the speed and quality of decisions at the tactical-, operational-, and strategic-level. They also tested AI's influence on different phases of capabilities (e.g., providing better analysis, making predictions, and optimizing the decision-making process to better conduct operations). Stemming from these efforts, Colonel Brown introduced six critical strategies to effectively develop and implement AI for DoD:

- Engage with start-ups to expand the defense industrial base;
- Leverage cutting-edge research by partnering with academia and allies;
- Organically develop and deploy software at scale;
- Cultivate digital skills (hard skills and soft skills) and enhance digital literacy;
- Develop new investment strategies to bridge the gap between procurement of new technologies and implementation by working with start-ups and venture capitalists;
- Inspire, support, and scale innovation at the edge.

As a final note, he identified some of the challenges facing IT infrastructure. First, some DoD programs are not given enough funding to achieve IT modernization, including logistics, maintenance, and human resources. He added that fundamental work is needed to modernize IT, especially with regard to data architecture and platform architecture, when adopting AI.

The third speaker of the session, Dr. KIM Yoon, currently serving as CTO, Executive Vice President, and Head of the AIX Center at SK Telecom (SKT), presented the private sector's views on AI and 5G. He stated that SKT's vision is to use the data collected from network mobile infrastructures such as 5G and mobile services to help its customers via a variety of applications. In the process, SKT aims to become the world leader in hyper-connected intelligence technologies and products. Referring to today's 5G network as an "*intelligence* super highway," he observed that we now rely on the connections among devices, users, companies, and countries. He argued that everything will have intelligence, from small sensors at home to super computers. From the commercial standpoint, this development will lead to hyper-connected experiences for consumers.

Furthermore, advancements in 5G connectivity and hardware/software innovations in mixed

reality (including virtual reality, augmented reality, and diminutive reality) will blur the boundaries between the physical and virtual worlds from a user's point of view. The most obvious advancement in user experience involving hyper-connected intelligence can be seen in the mass consumption of media. In gaming or concerts, for example, streams of data could flow from the content distribution network to mobile devices and provide users with enhanced experiences.

As an example of AI application in the industry, Dr. Kim described smart factories, which combine 5G with hyper-connected intelligence. In smart factories, advanced factory machines could detect defects in the manufacturing process, which is important for cost-saving and yield. Such technology is extendable to smart hospitals, schools, and offices to make services safer, faster, and more reliable. He added that these technologies have implications for security and defense since they include the use of robots and machines to carry out mission critical tasks utilizing network hyper connectivity and intelligence.

Nevertheless, Dr. Kim pointed out that AI brings new risks such as the potential to make poor decisions based on biased data. There are also security risks associated with hyper-connected intelligence given the potential for hackers to penetrate and compromise these systems. He expressed concerns that inference technologies used in deep learning such as image and speech recognition functions and other machine learning technologies may trigger a global AI arms race. At the same time, he played down concerns surrounding *artificial general intelligence*—AI that can self-learn without human assistance and, in the long-run, exceed human intellectual and physical capabilities—pointing to technological limitations. He stressed that while we should be concerned about the ramifications of artificial general intelligence, we still have a long way to go before fully understanding its capabilities and applications.

From the private sector's point of view, he stressed the need to focus more on human-centered AI in order to better deal with global and social problems such as health, education, environment, and elderly care. Dr. Kim argued that people developing AI, using AI, and those creating policies both in government and the private sector must understand that AI must be safe, equitable, trustworthy, and augmentative.

The presentations were followed by a Q&A session. The first issue raised by the moderator was about the sharing of AI data, algorithm, and hardware. Ms. Sheppard noted that one area we need to think about sharing is the processes by which we verify and validate the performance of AI systems. This will lead to assurances that the systems are working as intended, which will eventually lead to trust among nations. Colonel Brown agreed with Ms. Sheppard regarding the importance of testing, validating, and verifying the outcomes of AI applications. Furthermore, he stressed the importance of locating potential biases embedded within the data, the AI model, or the user interface to assure reliability.

On deep learning, Dr. Kim said that experts in many cases do not understand why deep learning works well in certain contexts. This draws sharp contrast to shallow learning, where we have a robust understanding of the mathematical techniques. As such, he described a recent trend that tries to simplify a complex problem using deep learning so that shallow learning systems can better understand it. According to Dr. Kim, this is one way to come up with a detailed and fundamental analysis of quantitative data.

Ms. Sheppard said that there have been movements at the national-, regional-, and UN-level to prevent AI from being misused, even though coming up with a set of universal definitions and parameters to using AI has proven to be a challenge. Colonel Brown added that there are two opposing ethical frameworks to the issue: a consequence-based framework and a duty-based framework. The former focuses on the dangers of using modern technologies such as AI while the latter addresses the need to possess these technologies to gain a comparative advantage over adversaries. In response, Dr. Kim argued that we are still at an early stage of understanding machine learning and its potential uses against adversaries. Therefore, a number of technical issues must be resolved before these systems can be deployed.

Another question asked how to overcome unpredictability when AI is used in the battlefield. Colonel Brown stressed the importance of making the distinction between what AI can and cannot do on the battlefield. Dr. Kim replied that it is crucial that the system is fault-tolerant and robust, especially in extreme situations where system performance is hampered (e.g., hyper-connection failure). He also stated that humans and AI technologies need to work together in an effective manner.

A question from the audience asked about the potential for a third AI winter. Dr. Kim pointed out that even though AI and deep learning are currently overhyped, it will not cause another AI winter. If the third AI winter does come, he argued that it will not be caused by technical factors, but rather by social and human factors. He speculated that the biggest winter may come in the

form of a cold war or an AI arms race.

The last question of the session asked whether the relationship among the military, academia, and the private sector surrounding IT and new technological developments will change in response to the quickly evolving atmosphere. Colonel Brown reiterated that governments can no longer compete with the private sector in terms of investments. As such, he emphasized the importance of finding innovative ways to leverage money from the private and commercial sectors. Dr. Kim drew from his personal experience to emphasize the importance of making venture capitalists cooperate with governments and, by doing so, coming up with solutions to important social and security problems so that all of humanity can benefit.

Session 2

Advanced Materials Science and Supply Chain Implications

Moderator

Kathleen HICKS (CSIS)

Speakers

Andrew HUNTER (CSIS)

Brett LAMBERT (The Densmore Group, LLC.)

JUNG Hee-Tae (Korea Advanced Institute of Science and Technology)

Rapporteur

Ashley PARK (Chey Institute for Advanced Studies)

Session 2 titled “Advanced Materials Science and Supply Chain Implications” was moderated by Dr. Kathleen HICKS, Senior Vice President, Henry A. Kissinger Chair, and Director of the International Security Program (ISP) at CSIS.

Mr. Andrew HUNTER, Senior Fellow in the International Security Program (ISP) and Director of the Defense-Industrial Initiatives Group at CSIS, focused on the global strategic competition for control of supply chains. He stated that this competition is at its peak in Northeast Asia and that players in this region are the largest, most dominant, and most advanced countries currently engaged in this global competition.

Mr. Hunter indicated that scientific innovations and technologies show their true potential when incorporated into the supply chains, which then feed into the broader systems or network of systems. It is for this reason that nations look to dominate parts of supply chains that they consider key sources of strategic advantage. He added that advanced materials frequently re-shape supply

chains and, therefore, can dramatically change the potential for advantage in the supply chain competition. This is the underlining reason why nations seek to control advanced materials and to put themselves in positions of advantage within the global supply chains.

While recognizing that government investments in supply chains create tremendous opportunities, Mr. Hunter warned that there are also security risks to consider. For example, there is an ongoing debate on how to operate highly sensitive national security systems embedded with many software and hardware vulnerabilities. He mentioned that the Defense Advanced Research Projects Agency (DARPA) is now developing methods to operate under a zero-trust environment. A zero-trust environment assumes that a network is already compromised and possesses vulnerabilities. This allows information within the network to be carried out in a way so that critical information is protected.

Further, Mr. Hunter talked about the military providing a testbed for new military applications and the challenges that come with doing so without fully understanding how to test, evaluate, and understand these technologies. He emphasized that the government has a tremendous role to play in evaluating the performance of these technologies and driving commercial and military progress. Urging the need for the government and the private sector to work together on supply chain issues, Mr. Hunter asserted that this cooperation would allow everyone engaged in the international competition to gain an advantage while ensuring that critical national security functions are protected.

On the idea of a bifurcated global supply chain, Mr. Hunter stated that there was emerging potential for a bifurcation into a Chinese-led bloc and a bloc led by the coalition of free market economies. The dangers associated with this bifurcation are that nations and companies will be forced to choose sides and that it would create inefficiencies. Lastly, Mr. Hunter highlighted the growing importance of software to global supply chains since so much of the functionality in many critical supply chains comes in software rather than hardware. However, many of the systems for managing supply chains have traditionally focused on the hardware. Since software production is very different from traditional manufacturing, the control mechanisms developed for hardware are poorly suited to managing software.

He concluded his presentation by examining whether the growing importance of software will increase the potential for bifurcation between blocs in the global supply chains. On the one hand, software is extremely difficult to manage and control, and can easily leak out to or be copied by the rival bloc. On the other hand, global trade statistics suggest that there is significantly less trade with regard to software and services than manufacturing. Overall, Mr. Hunter remained unsure how the growing importance of software will impact the bifurcation of supply chains between blocs.

Mr. Hunter was followed by Mr. Brett LAMBERT, Managing Director at the Densmore Group. Mr. Lambert began his talk by raising three questions. First, how has the national security industrial base, or the millennial industrial base, changed over the last two decades and how does it impact the supply chains? Second, what are the policy prescriptions on how can we understand, control, and optimize the supply chains? Third, how is the ROK and U.S. military approaching the supply chain issue and what dangers do they face?

First, he analyzed the revolution in the national security industrial base during the past 20 years. He pointed out that systems have now become so complex and dependent on a wide variety of commercial base technologies that they cannot possibly all be engineered, constructed, and delivered by a single company. This exemplifies the revolution from steel to sand (silicon) industrial base. According to Mr. Lambert, we have transitioned from a procurement system that focuses on acquisition of steel-based products to one that relies much more on complex microelectronics and advanced materials, including bio-materials.

Mr. Lambert further discussed how the supply base has become much more global and commercial. He warned that it has become dangerous to rely on vertical supply chains, especially for governments, because they fail to take advantage of all the innovation and creativity that the commercial sector has to offer. Another change can be found in the vast amount of data that is being created that need to be protected in the industrial base today. Moreover, increasing sophistication of the supply chains and the interdependency of networks complicate any effort to come up with policy prescriptions to protect and develop the industrial base.

According to Mr. Lambert, there are policy ramifications resulting from choices we make to manage the growing complexities of the supply chains and the materials within those supply chains. First, we could rely on a completely open architecture and system and, therefore, have less stringent protection and standards. Second, we could protect the infrastructure and the supply chains from the bottom to the top. Third, we could control and verify supply chains compliance

with certain procedures to guarantee security. Fourth, we could stratify protection by applying restriction on certain categories of capabilities. Lastly, we could assume that no system is trustworthy and operate under zero-trust environments.

He concluded by stating that governments tend to approach this problem with only a single solution in mind. In that sense, he reinforced the important roles that academia and industry must play because they understand supply chains better. When the industry and academia do not get involved in supply chain issues early on, governments will be forced come up with prescriptions, which could have negative implications for the long-term interests of the industry and national security. Furthermore, this could result in unnecessary bifurcated supply chains, which would damage the national security industrial base.

The last speaker of the session, Professor JUNG Hee-Tae, Chair Professor at the Korea Advanced Institute of Science and Technology (KAIST), addressed the subject of defense nanotechnology. He began by questioning why advanced materials and nanomaterials are so important for global issues. He explained that development of new materials often leads to revolutions in human society. Nanomaterials are bringing about new breakthroughs in today's world. Professor Jung highlighted two important qualities of nanomaterials: increase in surface area and changes in property. Utilizing these qualities, nanotechnologies can impact issues such as aging societies, artificial intelligence, climate change, and defense.

According to Professor Jung, defense nanotechnologies require new fabric and materials that are durable, lightweight, and multi-functional. These materials, in turn, would help the military in the following ways:

- Improve human performance;
- Create lighter, efficient, and effective military gears;
- Create nanoscale devices and systems such as nanorobots and microrobots;
- Create novel biological systems, ranging from nanobombs and nano-engineered self-multiplying agents to bombs that use nanometals and next generation biomaterials;
- Create smart weapons such as miniaturized robotics;
- Create intelligent ammunition such as intelligent nanobugs;
- Create metamaterials-based invisibility suits;
- Create adaptive sensors and microsensors;

- Create virtual tracking systems.

Unfortunately, many past investments in Korea and the U.S. were not successful. However, Dr. Jung argued that many applications are currently in the process of being developed, with some being "easier" than the others to develop. He observed that easy technologies such as nanocomposites, high-performance gas/health sensors, nanopatch, and stealth materials are already being commercialized. At the same time, it appears that technologies such as 3D printing, cyber security-related applications, nanofilters, nanorobotics, and artificial muscles will require much more time before being fully commercialized.

During the Q&A session, speakers shared their views on advanced materials and their supply chain implications. On the question of how to respond to instances of scarcity in supply chains that are critical to national security, Mr. Hunter responded that this scarcity serves as the basis for global strategic competition for control of supply chains. He noted that nations will try to identify the scarcity, gain an advantage, and leverage that advantage. For example, China has actively worked to become the world's dominant supplier of rare earth elements, and has leveraged that comparative advantage to move up the value chain. Limited supply chain presents a challenge for any nation trying to leverage that scarcity for advantage and causes other nations to get into the game. At the same time, it can reinforce bifurcation because a monopoly of scarcity can force other countries to engage in bifurcation strategies such as making major investments to develop domestic sources.

A question raised by the moderator was whether there will be a growing push for bifurcation during this era of great power competition. Dr. Hicks questioned how likely it is that we will see a new export control regime formed by a coalition of likeminded democracies, similar to the Coordinating Committee (CoCom) of the Cold War. Mr. Lambert said that this would be ideal, but predicted that it would be politically difficult since states have different interests. Mr. Hunter added that he is skeptical that a CoCom-like arrangement is going to be an optimized structure, particularly since it was built around the idea that a piece of supply chain could be restricted and certain kind of materials could be controlled. However, export controls are part of a larger system of control. Referring to the new strategic battlefield of standard-setting bodies, he argued that winning the competition on standard-setting may ultimately be more significant than the way we would have thought about CoCom as a key part of maintaining U.S. technological advantage during the Cold War.

The last question of the session asked about the importance of joint R&D projects among countries to develop supply chains. Mr. Hunter argued that different industries and nations are capable of developing good networks to acquire technologies that effectively address their specific requirements. Since different countries have unique comparative advantages in certain areas, he urged the importance of sharing these technologies among partners and allies for the benefit of all.

Session 3

Unmanned Systems and Robotics

Moderator

LEE Geunwook (Sogang University)

Speakers

Kathleen HICKS (CSIS)

Morgan DWYER (CSIS)

LIM KiHoon (ROK Army)

Rapporteur

KIM Sunghyun (Chey Institute for Advanced Studies)

Session 3 titled “Unmanned Systems and Robotics” was moderated by Professor LEE Geunwook of Sogang University. Professor Lee began the session by outlining the emergence of unmanned systems in the modern age. He argued that the issue for states is not about whether they should embrace unmanned systems or not. Rather it is about how to maximize the strategic values of those systems.

The first speaker of the session was Senior Vice President of CSIS and former Deputy Under Secretary in the U.S. Department of Defense, Dr. Kathleen HICKS. Her presentation focused on the geopolitical and strategic considerations involving unmanned systems. Dr. Hicks labeled unmanned systems as “the oldest of the new technologies being discussed.” She appraised that while the United State has had unmanned systems since the Vietnam War, the field is surprisingly under-invested.

Another imperative point put forward by Dr. Hicks was that the primary focus of unmanned

systems to date has centered on how they might be used in a kinetic manner—the physical usage of the system for active military operations. How escalation dynamics work or should work remains unanswered.

Further, Dr. Hicks analyzed that the potential for additional uses of unmanned systems are for the back-end of military operations such as:

- Domain awareness or intelligence, surveillance, reconnaissance (ISR), where unmanned systems are already well-employed;
- Maritime realms, where long duration and range have significance;
- Areas including lift and logistics.

Dr. Hicks also mentioned that there is resistance within the U.S. due to the perception that unmanned systems threaten the traditional role of service members. Thus, it is very difficult to find significant investments in unmanned systems. A breakthrough, she argued, will come as a result of economic and demographic pressures. Further, she saw unmanned system as an area where R&D collaborations between the U.S., ROK, and major allies can be quite beneficial, especially in the following fields:

- HALE (High Altitude Long Endurance systems);
- Countering electronic warfare;
- Survivability of unmanned systems;
- Ground-based autonomous vehicles;
- Underwater unmanned vehicles.

Next, Dr. Morgan DWYER, Deputy Director for Policy Analysis in the Defense-Industrial Initiatives Group at CSIS, discussed how an unmanned system's technical architecture reflects the larger structure of the industry and its organizations. She explained that system architecture is about high-level functions, key systems, and their allocations. Dr. Dwyer argued that the structure of technical systems may not necessarily be conducive to collaboration. A good example she put forward was the F-35 fighter. The F-35 is a multi-mission, highly integrated, and monolithic system and its architecture aggregates many capabilities into a single platform. This means that it is hard and costly to break into small modules that can be developed independently by separate organizations. Dr. Dwyer asserted that this complex architecture increases the cost and lengthens the schedule of development. Although high cost implies there is potential economic benefit for manufacturers, longer schedules for technological development also make collaboration more difficult as state priorities may shift.

Dr. Dwyer also touched upon the changing operational environment in the military context. These changes are raising questions about the utility of large, multi-mission, and monolithic platforms, especially manned systems such as the F-35. Instead of breaking a manned system into smaller modules, she urged the use of unmanned autonomous systems (UAS). For example, the U.S. is considering the use of drones to serve as a wingman to the F-35. Drones would team with manned aircrafts, fly ahead of manned fighters, and collect intelligence. Drones would be cheaper than the F-35 and, more importantly, would not involve the loss of human lives. Another example introduced by Dr. Dwyer was the U.S. Navy's experiment with Sea Hunter, an unmanned autonomous surface vessel that primarily serves as a sensor to detect enemy submarines.

Dr. Dwyer analyzed the common engineering characteristics of these attempts to adopt unmanned systems. First, instead of adopting a monolithic system that carries out the entire mission, the mission itself is disaggregated into separate systems. Second, manned systems are paired with unmanned systems. By doing so, the manned platform can make effective decisions based on the intelligence collected by UAS. The UAS would also ensure human safety by giving unmanned systems more dangerous roles. Third, software and network have become very important in UAS particularly because systems consist of multiple disaggregated systems. Data protection and standardization have become increasingly important and, thus, have increased the demand for companies to improve cyber security and come up with data standards. As a final note, Dr. Dwyer pointed out that the transition towards UAS creates more opportunities for international collaboration among governments, not just in R&D, but involving acquisitions of systems.

Brigadier General LIM KiHoon of the ROK Army began by giving an example of a technology revolution in warfare. During World War II, it took the British Air Force two years to hit 145 German targets. During the Gulf War, one day was sufficient to hit 198 targets. Today, the ROK-US alliance has the capability to hit 1,500 targets within an hour. In addition, Brigadier General Lim identified trends that are currently accelerating military science and the technology revolution:

- Emphasis on intelligence, surveillance, and reconnaissance (ISR) across all domains;

- Precision-guided munitions (PGM) revolution that will allow militaries to hit any target on Earth within an hour;
- Emphasis on hyper-intelligence, hyper-connectivity, and convergence;
- Growing cyber-electronic capabilities.

He explained that these trends will bring further changes to the military system. In future warfare, AI-based systems will be a critical component of combat power. He argued that future ground forces must expand their area of operations in order to engage in all fields of war. This includes the ability to attack an opponent's air force and navy, as well as control cyber space and electromagnetic components of the battlefield. Their new strike weapons system must also diversify the means of attack, improve ISR capabilities, and ensure that all combatants are connected. In responding to these challenges, Brigadier General Lim introduced the future roadmap of the ROK Army:

- By mid-2020s: implement Defense Reform 2.0, which focuses on missiles, warrior platforms, and mobilized units;
- By 2025: implement Army Tiger System 4.0, which transforms the current infantry into well-connected mobilized units, and connects armed vehicles with all platforms to share military information. AI is also used to support the command and control process;
- By 2030: introduce the next game-changers, such as laser weapons, super long-range firing system, quantum technologies, and strengthen asymmetric capabilities.

He added that efforts to utilize advanced science and technology for force requirements within the ROK Army, called the Himalaya Project, are already underway. This project aims to create a large pool of scientists and utilize the collective intelligence of the military, industry, academia, and research institutes for military applications.

During the discussion session, Dr. Hicks touched on a number of critical issues. First, she addressed the nature of resistance concerning unmanned systems. She argued that this resistance is a cultural issue, rather than an interest issue. If the resistance existed because unmanned systems went against the interests of military institutions or national security, we should have seen attempts to maximize the effectiveness and efficiency of unmanned systems specifically to address these concerns. Similarly, the resistance to unmanned systems cannot be explained as coming only from a certain military branch such as the Army or Air Force, because each military branch could benefit from the use of these systems.

Another key point raised by Dr. Hicks was on the issue of testbed—the idea that the military must act as a test platform for new technologies. The problem with the testbed approach is again cultural in nature. Also, regulatory limitations challenge the efficiency and risk tolerance of military institutions. For example, she explained that the U.S. government simply cannot accept the risks associated with commercial projects such as SpaceX since the cost of failure is much higher.

Dr. Hicks also discussed the impact of newly emerging technologies on escalation and war. She argued that the most constructive way to prepare for the future is to have a normative approach and an understanding about how these new technologies should be used. While the best way to create such norms is a multilateral approach, Dr. Hicks asserted that this may be difficult, suggesting that the U.S. may have to pave the way during the initial stage.

In response to questions about the tradeoffs between monolithic systems and disaggregated systems, Dr. Dwyer stated that in disaggregated systems, individual systems might be less costly, but one may have to purchase more to guarantee overall performance. On the issue of international collaboration, she argued that both openness and security are critical to forming viable partnerships with allies. Professor Lee asked Dr. Dwyer about the issue of power source, a field that has been less developed. Dr. Dwyer argued that progress is usually driven by market forces, which explains why storage space has increased exponentially while power capacities have not.

Brigadier General Lim concluded the session by identifying the potential obstacles in moving toward a technology-intensive Army. The first challenge involves technologies themselves. In order to develop a technology-intensive Army, relevant technologies have to be developed successfully, which is itself a difficult task. Second, even if such systems are developed, it is equally important to assimilate service members into their new roles. This situation has been exacerbated by the fact that mandatory military service for Korean nationals has shortened. Lastly, he pointed to the difficulty of incorporating civilian technologies into the military sector with greater efficiency.

Session 4

Cyber Security and Blockchain

Moderator

Andrew HUNTER (CSIS)

Speakers

R. David EDELMAN (Massachusetts Institute of Technology)

KIM Hyoung Joong (Korea University)

LIM Jong-in (Korea University)

Rapporteur

John J. LEE (Chey Institute for Advanced Studies)

Session 4 titled "Cyber Security and Blockchain" was moderated by Mr. Andrew HUNTER, Senior Fellow in the International Security Program (ISP) at CSIS. Mr. Hunter began the session by observing that all technology clusters being discussed during the conference are closely inter-related. He added that cyber security may be the one with the most impact on all other technologies.

As the first panelist to speak, Dr. R. David EDELMAN, Director of the Project on Technology, and the Economy, and National Security (TENS) at Massachusetts Institute of Technology (MIT), described how our perceptions of cyber security have changed over the past fifteen years. According to Dr. Edelman, initially there was a great deal of uncertainty surrounding cyber technologies and their impact on national security. Much of this had to do with the fact that cyber security was a relatively new subject at the time. Perceptions began to change when states started to understand the potential risks associated with cyber technologies. For example, cyber security was the first agenda that U.S. President Barack OBAMA discussed with Chinese President XI Jinping when they met for the first time. For President Obama, it had become clear that Chinese theft of strategic and critical U.S. intellectual properties posed a growing threat to American security. A few years later, the United States government indicted several Chinese actors for cyber espionage, which ended up driving a wedge between the two countries' diplomatic relations. In recognition of the growing importance of cyber security, the United States also began to incorporate cyber security scenarios into its bilateral military defense exercises with its allies, including Korea.

Dr. Edelman stated that the world now has a better understanding of cyber security and its security implications. First, cyber technologies provide unconstrained states with opportunities to cause disruptions. Second, states as well as militaries can utilize cyber technologies to advance their military goals. Third, states can use cyber technologies to disrupt any political or diplomatic process that they consider unfavorable. At the same time, he argued that there are clear opportunities associated with cyber technologies. Unilaterally, states have begun to use cyber technologies to push back against threats to their democracies, as showcased in French President Emmanuel MACRON's presidential campaign in 2017. Bilaterally, states have begun to find areas of stability, confidence-building, and de-escalation measures related to cyber security. Multilaterally, military alliances such as NATO and others have begun to enhance cyber security capabilities in order to better defend one another. Most importantly, states have figured out what large-scale cyber attacks could look like. For example, Russian cyber attacks against Estonia in 2007 led to the shutdown of Estonian banks, media outlets, and government bodies. In 2015, Russian hackers also succeeded in shutting down the Ukranian power grid. Another example can be found in the form of North Korea, whose cyber warfare has disrupted joint ROK-US military exercises in the past. The North is also responsible for hacking Sony Entertainment, which became a target for filming a comedy about the assassination of its leader KIM Jong-un.

Dr. Edelman outlined several lessons regarding the nature of cyber security. First, we have learned that attribution is possible. Second, concerns over proliferation of cyber weapons, especially to non-state actors, have been exaggerated. Third, asymmetric risks may be more important than previously anticipated. Fourth, coming up with norms and regulations for dealing with cyber activities is important but not enough to restrain states from engaging in cyber attacks. Lastly, the involvement and participation of private companies in cyber space complicates the statecraft of cyber security. In conclusion, Dr. Edelman made the following observations:

- The grey zone between armed conflict and verbal insults is growing;
- Due to this grey zone, low probability-high impact cyber attacks cannot be completely ignored;
- New thresholds are being crossed, as witnessed in the 2016 U.S. Presidential Election;
- Artificial intelligence has yet to become a perfect system which can greatly impact cyber security;
- The international community must come up with mechanisms to restrain cyber attacks from taking place.

Professor KIM Hyoung Joong, Professor in the Graduate School of Information Security at Korea University, followed Dr. Edelman by describing blockchain technology and its advantages. Professor Kim identified blockchain as having three distinct advantages over other security systems: 1) de-centralization, 2) transparency, and 3) integrity. These qualities allowed Bitcoin to become blockchain's most successful application and opened the era of decentralized finance (De-Fi). Bitcoin's success inevitably led to a strong sense of hope surrounding blockchain's potential applications.

However, Professor Kim emphasized that cryptocurrency remains the only successful application of blockchain so far. This is because only a small portion of blockchain technology is currently being utilized. According to Professor Kim, blockchain's most important quality, the hash-stamp functionality, has been severely under-utilized. The hash-stamp functionality is the ability to locate data manipulation when it occurs, which makes blockchain better equipped to deal with cyber hacking. He argued that this functionality must be used more readily. In particular, blockchain can improve security in four areas of military operations: 1) protecting critical military weaponry, 2) managing drone operations (automated swarm systems), 3) verifying command and control with accuracy, and 4) managing logistics and supply chains.

At the same time, he argued that while blockchain system can provide the optimal solution to military operations, it is more expensive than previous military security systems. Also, blockchain is not completely immune to hacking, especially since hackers can target weaknesses in smart contracts, a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract without the involvement of third parties. In response, he stressed the importance of making appropriate adjustments to deal with threats to blockchain. For example, smart contract *audits* can enhance the security of smart contracts and, therefore, guarantee the overall security of blockchain application.

Professor LIM Jong-in, Professor in the Graduate School of Information Security at Korea University, spoke in detail about the various threats to Korea's national cyber security, especially from North Korea, China and Russia. North Korea's capabilities to deliver cyber attacks have already been proven. In 2017, the North surprised the world with its ransomware, WannaCry, which infected 230,000 computers and servers in 150 countries overnight. Given that the North's cyber capacities are more offensive and goal-oriented, Professor Lim argued that threats to Korea's cyber security are particularly acute. Further, he cited Moore's Law, adding that computing power will only increase over time. Therefore, the scope and frequency of cyber threats from the likes of North Korea, China, and Russia will likely increase as well.

Cyber attacks can be particularly dangerous to Korea for a number of reasons. Korea hosts not only the largest American foreign military base but two of the world's largest semiconductor manufacturers, SK Hynix and Samsung Electronics. Cyber attacks against the latter two companies will not only debilitate Korea's economy, but impact the global supply chain for semiconductors. Therefore, Professor Lim argued that Korea must be more pro-active in improving its cyber defenses. Specifically, Korea must improve in terms of capacity-building, cyber deterrence, cyber diplomacy, and collaboration with allies to combat cyber breaches. Professor Lim added that capacity-building requires strong public support, similar to how the U.S. public showed strong support for cyber capacity-building following the Edward SNOWDEN incident. Moreover, Professor Lim stated that there has been a lack of support at the government-level in terms of investments, infrastructure, and resources.

According to Professor Lim, one way to improve Korea's cyber capabilities is to increase its collaboration with the United States, a country that is significantly more experienced and has better access to information. This was why General Paul NAKASONE, Commander of the U.S. Cyber Command, urged greater bilateral cooperation on cyber security issues when he visited Korea in December 2019. Overall, Professor Lim urged the Korean government to improve in the following areas:

- Capacity-building;
- Trust-building (targeting the Korean public as well as its allies);
- Cyber diplomacy.

To achieve this, Professor Lim urged the Korean government to start participating in international projects on cyber security. In particular, he remained convinced that Korea should join "Five Eyes," an intelligence alliance comprising of the United States, United Kingdom, Australia, Canada, and New Zealand.

The Q&A session centered around three major questions. First, can cyber security provide a pathway for the public and private sectors to work together on key issues related to scientific innovation? Second, do cyber security issues show that we have embarked on a new era of state-civil sector violence? Third, do cyber security challenges include deterring non-state actors?

Dr. Edelman stated that there has to be a fundamental understanding of what is on- and off-limits. In the case of China, this distinction has been non-existent, which is why the United States has been trying to convince China that there is a fundamental difference between stealing intellectual rights for commercial gain and for strategic gain. Dr. Edelman added that while there is a general agreement that international law applies to cyber security, if and when states will begin to observe these laws remains difficult to predict. In terms of cyber deterrence, Dr. Edelman argued that there is a lack of discussion on where countries, including Korea and the United States, draw the line as unacceptable.

One question from the audience asked about the implications of China entering the cryptocurrency market. In response, Professor Kim described the cryptocurrency market as a place without norms and regulations, which makes China's entry that much more significant. Professor Lim added to the discussion by saying that the United Nations should take a larger role in implementing sanctions and establishing an international court for cyber crimes. The last question of the session asked how cyber security can be applied to the military sector. Professor Lim stated that modern weapons rely on software, making them the targets of cyber hackers. Moreover, he warned that cyber weapons can become a poor country's nuclear weapon. In terms of blockchain's applicability to the military, Professor Kim admitted that implementing blockchain, a decentralized technology, to military command and control, which has traditionally relied on centralized systems, will be difficult and time-consuming. As such, Professor Kim urged the military to utilize blockchain on a partial basis, testing the waters before implementing the system in full. Dr. Edelman concluded the session by stating that offensive cyber activities—targeting states as well as civilians and private actors—will continue to be a part of military conflicts in the future.

Session 5

Space Technologies

Moderator

HONG Kyu-Dok (Sookmyung Women's University)

Speakers

Michael HAMEL (Ret., U.S. Air Force)

JU Gwang-Hyeok (Korea Aerospace Research Institute)

KIM Kwang-Jin (ROK Air Force)

REU Taekyu (Defense Science & Technology Academy, Agency for Defense Development)

Rapporteur

KIM Sunghyun (Chey Institute for Advanced Studies)

During Session 5 titled "Space Technologies," four distinguished speakers gave their views on the future of space technologies. The session was moderated by Professor HONG Kyu-Dok of Sookmyung Women's University.

The first speaker of the session was former Lieutenant General of the U.S. Air Force and former Vice President of Lockheed Space Systems Company, Lt. Gen. Michael HAMEL. He started the session by asking three questions on space technologies. First, how did we get to where we are? Second, what specific technologies contributed to today's advanced capabilities? Third, what is the current security environment concerning space systems?

Lt. Gen. Hamel explained that the space age began in 1957 when the Soviet Union (USSR) successfully launched the *Sputnik*. Subsequently, the hegemonic competition between the United States and USSR fueled the two countries' race for superiority in space. Space was also the basis on which their deterrence strategies were formulated. By the end of the Cold War, people began to see the tactical benefits of space technologies as more than just nuclear deterrence.

This understanding accelerated the use of space technologies for non-strategic national security purposes. The tactical value of space was firmly established by the beginning of this century and space technologies became necessary for all kinds of operations. One key development, Lt. Gen. Hamel pointed out, has been the growth of the commercial sector.

In response to his second question, Lt. Gen. Hamel identified a number of technologies that have transformed the space system, including advanced computing and larger storage, gigabit communication, optics, sensors, power, propulsion, and new materials. A major contributor to these advancements has been the private space sector. Not only is the private sector leading the space domain today, it is doing so by introducing innovative technologies while bringing prices down. Concerning how we understand today's technologies, Lt. Gen. Hamel explained that they consist of ground, satellite, and link components. Further, he elaborated that different states utilized similar approaches to space in the past and there existed a standard to satellites and launch vehicles. Today, however, there is a myriad of different approaches to space, from small innovative launchers and small cubesats to conventional large satellites. Also the number of actors operating in the space realm has grown and diversified.

On the current security environment involving space technologies, he observed that we have already begun to witness sinister applications of space technologies. For example, the commercial sector has seen frequent disruptions of its communications operations. Given that most space technologies are dual-use and applications often transcend borders, proliferation of space threats has proven to be a challenge. At the same time, Lt. Gen. Hamel mentioned that there are now growing opportunities for allies to cooperate on civil, scientific, and industrial issues as well as national defense. He concluded by mentioning that space power will be a critical determinant of national power and a major point of collaboration with other countries in the 21st century.

Dr. JU Gwang-Hyeok, Executive Director at the Korea Aerospace Research Institute, gave a presentation on innovations in the aerospace sector and on the concept of "new space." His presentation was centered on five smaller topics, including Korea's national space development program, "old space vs. new space," small satellites (SmallSat), AI in aerospace, and the new moon rush.

According to Dr. Ju, Korea's space program began with KITSAT-1, the first satellite built and launched by Korea in 1992. Recently, Korea has developed a moon exploration vehicle while next-generation satellites are currently being developed. Korea is also working on numerous technologies

such as the capacity to discern space waste, and to make infrared and high-definition observations.

Dr. Ju explained that there are transformations taking place within the field of space systems. With the growth of the commercial space industry labeled as "New Space," fundamental changes are beginning to take place. Technologies relevant to this change include the use of small satellites, usually weighing less than 100kg. These technologies have been labeled a game changer.

Dr. Ju noted that the sustainability of space systems has also become important. In the past, satellites and launch systems were only single-use. However, new ideas such as refueling older satellites and, therefore, extending their lifespans are being explored. For example, SpaceX has developed launch vehicles that may be used up to 100 times. Further, new developments in AI, deep learning, drones, and 3D printing are all being applied to space technologies, making space technologies cheaper and more accessible.

Lastly, Dr. Ju touched on the re-emergence of the moon rush. In this regard, Korea plans to send an unmanned vehicle into the moon's orbit. As for other states such as the United States, the objective is to make space habitable. The U.S. announced the Artemis Program last year, with the goal of sending manned missions to the moon by 2024 and achieving extended periods of stay on the moon by 2028.

Brigadier General KIM Kwang-Jin of the ROK Air Force followed by explicating the three elements of space system: the space segment (e.g., satellites), the link segment (e.g., communication systems), and the ground segment (e.g., mission control centers). Furthermore, he categorized the military space system into four distinct eras.

- 1st era (beginning of the Cold War): Space system consisted of the launch segment (e.g., ballistic missile), and space-based and ground-based missile warning systems. Nuclear ballistic missiles were the most critical part of the space system in this era.
- 2nd era (Strategic Defense Initiative proposed by the Reagan Administration): Transformed space systems into a command and control battle management system as well as space-based and ground-based missile defense.
- 3rd era (characterized by the Revolution in Military Affairs, or RMA): Space systems were used for rapid command and control, information analysis, and precision strikes.
- 4th era (brought upon by anti-satellite tests, and the growing capability to attack space objects): Offensive and defensive capabilities in space were introduced.

According to Brigadier General Kim, changes brought by the different eras could be explained by convergence theory. Convergence theory states that as states move toward industrialization, they begin to converge and resemble one another. Utilizing this theory, he argued that since relevant technologies and space strategic concepts result in certain types of space systems, different states tend to converge in terms of their space programs, especially for states within the same era.

Following his explanation of the space system, Brigadier General Kim provided a number of key predictions and policy recommendations. He predicted the advent of "space deterrence," a concept involving the protection and maintenance of space assets. Key elements of this space deterrence will be securing retaliatory capabilities, effective command and control mechanisms, and defense capabilities sufficient to deny attacks. Therefore, he emphasized the importance of forming partnerships with other countries and the private sector as well as securing inter-operability and investments in small satellite technologies.

During the discussion session, Professor Hong raised the possibility of a "space Pearl Harbor." Lt. Gen. Hamel argued that there is growing evidence to suggest that space has become an inviting target for adversaries. Space systems are composed of numerous parts that must all come together for the system to function effectively. He added that a "space Pearl Harbor" is a possibility and that all of us must remain vigilant to avoid such a disaster.

Professor Hong asked Dr. Ju whether technical difficulties in developing space system force engineers to accept trade-offs between performance and costs, schedule, and risks of mission failure. Dr. Ju responded that because space programs in Korea are fully funded by the government, it is not easy for programs to allow for the possibility of failure especially during the design phase. Thus, the integrity and reliability of systems have to be stressed from the very beginning.

Brigadier General Kim discussed the idea that technological advancements will allow Korea to combat North Korea's missile and nuclear forces. He stated that it is imperative for the Korean government to persuade its public of the importance of space in countering North Korea's missile threats. In response to the question about Air Force priorities given its budget constraints, he stressed that while it is difficult to prioritize different items on the Air Force wish-list, it is important to pay special attention to high-end technologies, which allow weapons to have multiple functions.

Participants

In alphabetical order

AHN Jung Ho
Professor, Seoul National University

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

Morgan DWYER
Fellow; Deputy Director for Policy Analysis of the Defense-Industrial Initiatives Group, CSIS

R. David EDELMAN
Director of the Project on Technology, the Economy, and National Security (TENS), Massachusetts Institute of Technology (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

HONG Kyu-Dok
Professor, Sookmyung Women's University

Andrew HUNTER
Senior Fellow; Director of the Defense-Industrial Initiatives Group, CSIS

JU Gwang-Hyeok
Executive Director, Korea Aerospace Research Institute

JUNG Hee-Tae
Chair Professor, Korea Advanced Institute of Science and Technology (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

Brett LAMBERT
Managing Director, The Densmore Group, LLC.

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

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

REU Taekyu
Vice President, Defense Science & Technology Academy, Agency for Defense Development

Lindsey SHEPPARD
Fellow, CSIS

SUH Wook
Chief of Staff, ROK Army

WON In-choul
Chief of Staff, ROK Air Force

Rapporteurs

In alphabetical order

KIM Sunghyun
Assistant Manager, Chey Institute for Advanced Studies

John J. LEE
Team Manager, Chey Institute for Advanced Studies

Ashley PARK
Program Manager, Chey Institute for Advanced Studies

Editor

John J. LEE
Team Manager, Chey Institute for Advanced Studies

About the Chey Institute for Advanced Studies

The Chey Institute for Advanced Studies is a non-partisan 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.

Chey Institute for Advanced Studies
17F, 211 Teheran-ro, Gangnam-gu
Seoul 06141, Republic of Korea
www.chey.org

About the Center for Strategic and International Studies (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, crossdisciplinary 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 is ranked the number one think tank in the United States as well as the defense and national security center of excellence for 2016-2018 by the University of Pennsylvania's "Global Go To Think Tank Index."

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 and International Studies (CSIS)
1616 Rhode Island Avenue, NW
Washington, DC 20036, USA
www.csis.org


CHEY
CHEY INSTITUTE FOR
ADVANCED STUDIES


CSIS
CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES