Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

beyond leading technology

KIAT

BUILDING A SMART PARTNERSHIP FOR THE FOURTH INDUSTRIAL REVOLUTION

BUILDING A SMART PARTNERSHIP FOR THE FOURTH INDUSTRIAL REVOLUTION

VAUGHAN TUREKIAN | TAEHEE JEONG | GIGI KWIK GRONVALL | ELIZABETH PRESCOTT
GWANHOO LEE | REBEKAH LEWIS | BEAU WOODS

ISBN: 978-1-61977-537-4

April 2018

THE SCOWCROFT CENTER EDITORIAL BOARD

ABOUT THE SCOWCROFT CENTER FOR STRATEGY AND SECURITY

The Scowcroft Center for Strategy and Security aims to produce cutting-edge analyses and to develop strategies for how the United States can best work with like-minded countries to shape the future. The transatlantic partnership remains at the core of the Scowcroft Center's analysis of how global trends and emerging security challenges will impact the United States, its allies, and global partners.

The Scowcroft Center works collaboratively with the Council's other regional and functional programs and centers to produce multi-disciplinary analyses. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of non-partisan commitment to the cause of international security, support for US international leadership in cooperation with allies and partners, and legacy of mentorship to the next generation of leaders.

The Scowcroft Center's mission is to:

- Provide foresight, strategy, and policy solutions to anticipate the most pressing risks, solve unfolding challenges, and take advantage of opportunities for the United States and its allies and partners.
- Be thought leaders on cutting-edge global strategy and security matters, ranging from transatlantic, transpacific, and Mideast security, to cyber and emerging technologies.
- Serve as an incubator of new approaches and capabilities for the Atlantic Council as a whole—from gaming to big data analytics—and a catalyzer for new creative communities.
- Cultivate the next generation of rising strategy and policy professionals.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The convergence of our physical and digital worlds is disrupting everything, resulting in profound implications for governments, the private sector, societies, and individuals around the globe. Emerging technologies of the Fourth Industrial Revolution—artificial intelligence (AI) and machine learning (ML), biotechnology and gene editing, the Internet of Things (IoT) and big data—can no longer be thought of as distant possibilities but are instead a part of today's reality.

On the one hand, these technologies offer unprecedented opportunities to revolutionize and improve human life. In industries ranging from healthcare, transportation, and energy, to agriculture, manufacturing, and commerce, emerging technologies can provide increased efficiencies, greater cost savings, and more convenient tools and services. Self-driving cars promise to decrease traffic accidents; precision medicine offers new possibilities for the treatment of diseases; and 5G connectivity and the IoT could pave the way for energy-efficient smart cities. Together, these technologies have the potential to keep people healthier and safer for longer than ever before.

On the other hand, these new technologies also present challenges to national security and the global financial system. Military adversaries and non-state actors are gaining asymmetric advantages in the national security domain, shifting the strategic calculus of national defense. Companies are rethinking their supply chains and business models, with repercussions for labor. Beyond these security and economic disruptions, there are massive social and political implications as well. The rapid pace of technology-driven disruption continues to tear at the fabric of societies around the world, as people's sense of norms, values, place, and culture is upended by the whiplash of change. This places more stress and pressure on governments, which already lack the resources to act and respond to the needs of their citizens.

To ensure its future security and prosperity, the United States must navigate these disruptions—seizing opportunities, overcoming challenges, managing risks, and always looking ahead to the next technological advancement. To remain at the forefront of the innovation wave, the United States must work with its equally capable and like-minded allies and partners, including the Republic of Korea (hereafter South Korea). Already the United States and South Korea enjoy a rich and well-established collaborative partnership on science, technology, and innovation-related issues, through joint research and development projects, education and training programs, and forums, dialogues, competitions, and other avenues allowing for the exchange of people and ideas. However well-established, this partnership needs to be updated given the emerging technologies of the Fourth Industrial Revolution and their disruptions. To this end, **the United States and South Korea should build a "Smart Partnership," one focused on emerging technologies and the rapid pace of the Fourth Industrial Revolution.**

To design this Smart Partnership, the Atlantic Council's Scowcroft Center for Strategy and Security, in partnership with the Korea Institute for Advancement of Technology, convened multiple roundtable discussions in Washington, DC, with experienced policy practitioners, entrepreneurial business leaders, subject matter experts from academia, and civil society organizations to discuss these emerging trends. These roundtables explored technologies (tech), including artificial intelligence, machine learning, and quantum computing; biotechnology; and the Internet of Things and connected tech devices. Participants discussed new advances and trends in each technology, broke down the policy issues, and considered the strategic implications surrounding each of them. The authors of this report drew upon these discussions to provide detailed recommendations for increased US-South Ko-

rean collaboration around the development and implementation of these advanced technologies.

In chapter 1, "**Navigating an Automated Future**," Dr. Vaughan Turekian, senior director of the Science and Technology for Sustainability Program at the National Academies of Sciences, Engineering, and Medicine, identifies the major political, economic, technical, and legal issues caused by the deployment of artificial intelligence and machine learning. He lays out several recommendations for increasing cooperation, including reestablishing high-level, joint committees on science and technology; developing research programs on artificial intelligence's applicability to smart grids; and establishing jurist exchange programs to develop a cadre of lawyers capable of handling issues related to ethics, international trade, and the economy. In addition, Dr. Turekian touches upon a separate but related area of technology, quantum computing, which could have even broader implications for the development of artificial intelligence and machine learning.

In chapter 2, "**Adding Value with Artificial Intelligence**," Dr. Taehee Jeong, a senior data scientist at Xilinx, provides a South Korean perspective on artificial intelligence and how it is changing the manufacturing and healthcare industries in South Korea and around the world. He explores how artificial intelligence, in combination with big data and ubiquitous sensors, can drastically improve production efficiencies and reduce costs in manufacturing. Dr. Jeong posits that similar opportunities also exist in healthcare as developing AI can assist in more accurate, real-time medical diagnoses, though he acknowledges that patient privacy concerns remain an important issue to address. Dr. Jeong also goes into detail about the importance of training data scientists in both the United States and South Korea and offers suggestions for boosting their education and training, including organizing "algorithm competitions" designed to encourage the development of new algorithms.

In chapter 3, "**Ensuring Biosafety and Security**," Dr. Gigi Kwik Gronvall, senior scholar at the Johns Hopkins Center for Health Security and associate professor at the Johns Hopkins Bloomberg School of Public Health, offers an in-depth analysis of the trends driving the development of advanced biotechnologies. She notes that biology is becoming more industrialized and economically powerful, as important industries increasingly rely on biological manufacturing processes. Dr. Gronvall also underlines the importance of examining the safety and security ramifications stemming from biotech's dual-use nature, highlighting the ease with which individuals and small groups can use advances in biotech to inflict deliberate harm. As a result, the United States and South Korea should expand their security cooperation in the areas of global health, gene synthesis, and medical and pharmaceutical research, as well as provide global leadership on safety standards.

In chapter 4, "**Harnessing Convergent Technologies**," Dr. Elizabeth Prescott, professor of the practice and director of curriculum for science, technology, and international affairs at the Walsh School of Foreign Service at Georgetown University, describes a world in which the fields of biology, materials, information, and engineering collide. This convergence has the potential to transform healthcare, though it will have significant legal, social, ethical, and governance implications. To mitigate these issues, Dr. Prescott recommends advancing global norms, standards, codes of conduct, and governance models that prioritize the safe development and use of biotechnologies. In addition, she recommends expanding opportunities for students, scientists, and engineers to work collaboratively on joint projects to bring discoveries to market sooner and to exchange best practices to build a stronger ecosystem of entrepreneurship.

In chapter 5, "**Preparing for a Connected World**," co-authors Dr. Gwanhoo Lee, professor of information technology and analytics at the Kogod School of Business at American University, and Ms. Rebekah Lewis, director of the Kogod Cybersecurity Governance Center at American University, underscore the need for increased international standards for cybersecurity. To achieve this, they suggest promoting a universal framework, such as the US National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. Embracing core components of this framework will allow for more effective and efficient communication and improved research efforts. In addition, the authors point out the importance of relying on market-driven innovation to identify best practices in IoT cybersecurity, allowing governments to focus their efforts on requiring or incentivizing adoption of best practices that are otherwise likely to be resisted.

In chapter 6, "**Preserving Trust with 'Prosperity by Design'**," Mr. Beau Woods, cyber safety innovation fellow at the Atlantic Council, emphasizes the need for *security by design* when developing the Internet of Things and other connected technologies. He recommends that the United States and South Korea work together to develop new models for improved IoT cybersecurity, create platforms for the exchange of information and best practices, and engage not only

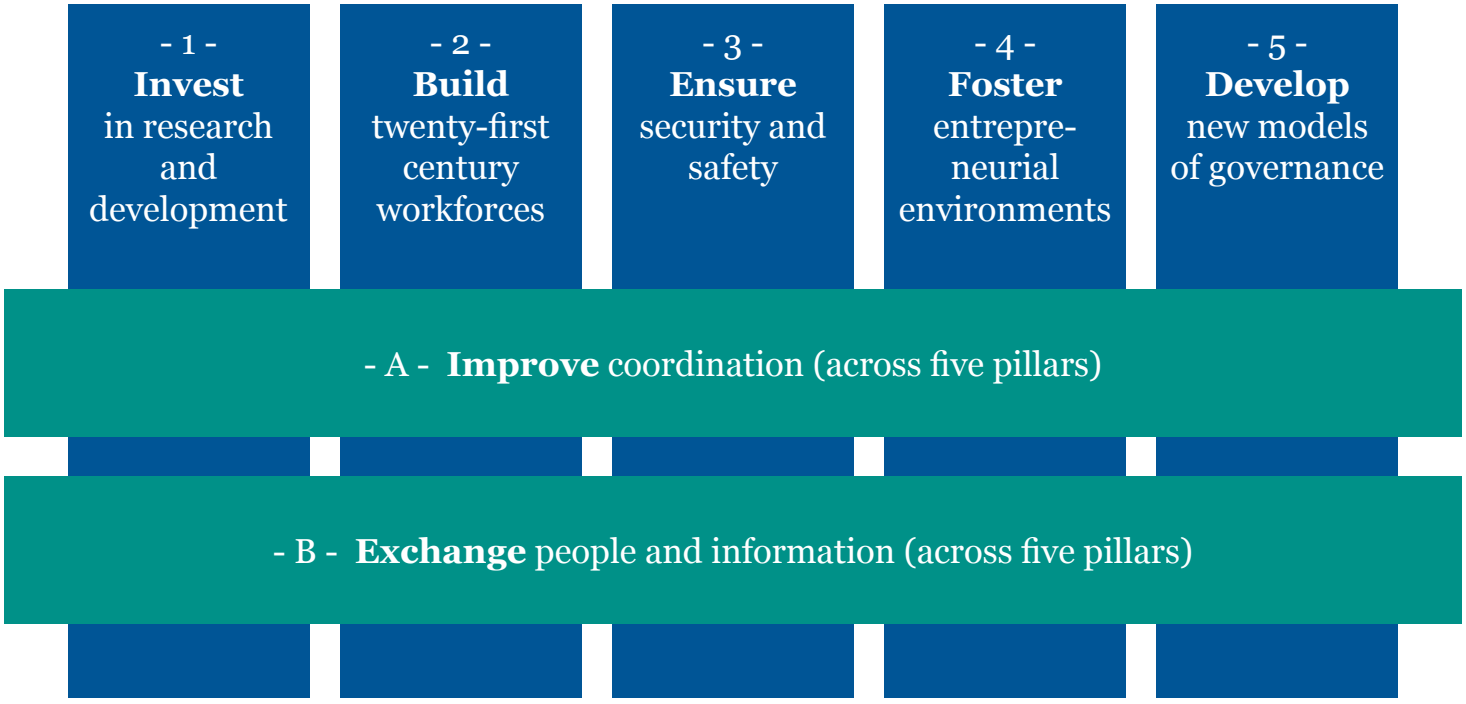
with their respective civil societies but also with one another's private sectors. He advocates for international safeguards that arise from open, frank collaboration between the United States and South Korea. Mr. Woods notes the skill of South Korean security researchers, or white hat hackers, and their untapped potential to help identify cybersecurity vulnerabilities.

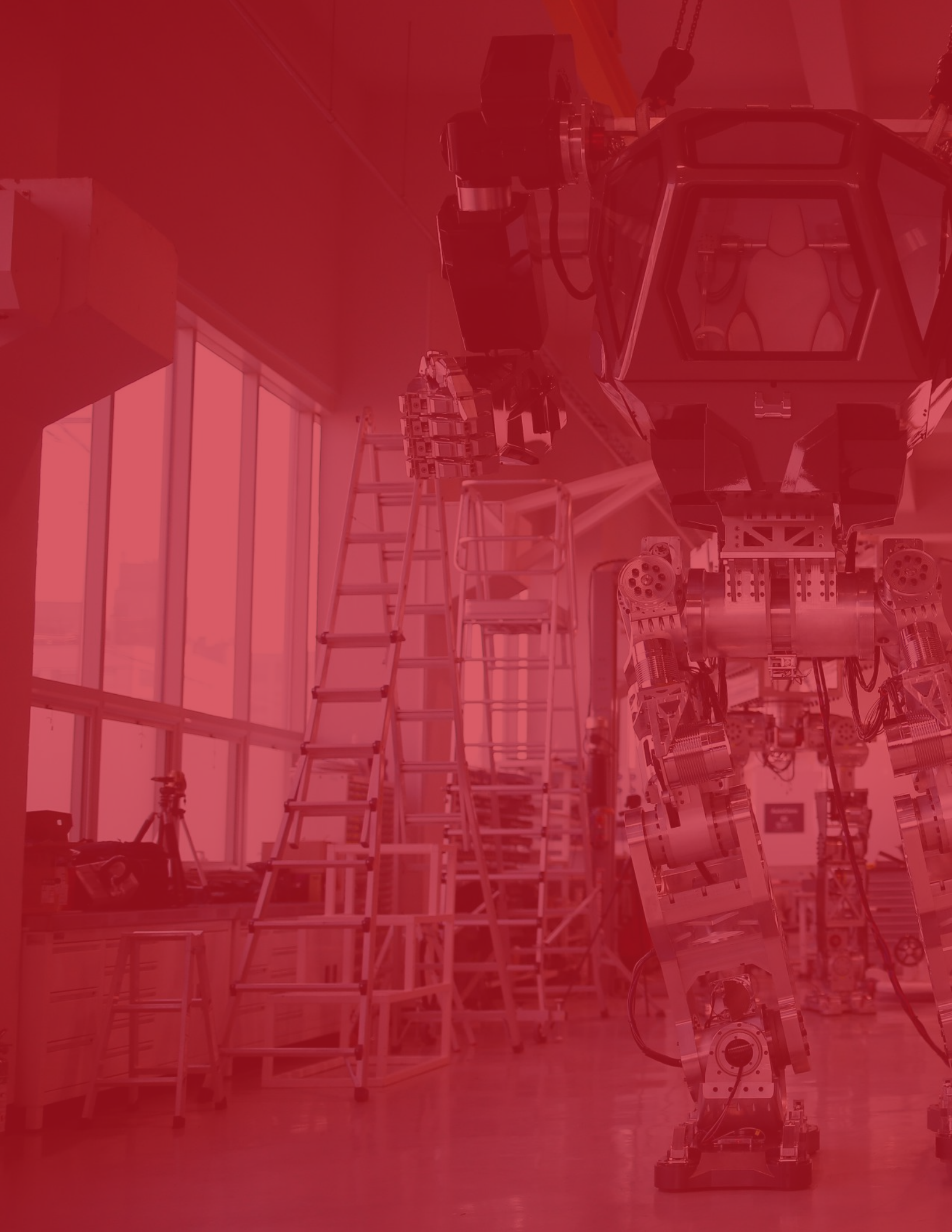
Based on the recommendations in each chapter, a strategic framework for building a Smart Partnership emerges. This framework includes five areas in which the United States and South Korea can focus their collaboration: (1) investing in research and development; (2) building twenty-first-century workforces; (3) ensuring security and safety; (4) fostering entrepreneurial environments; and (5) developing new models of governance. Two building blocks support these five pillars: (A) improving coordination and (B) exchanging people and information. The recommendations included within each pillar are relevant for stakeholders within government, private industry, academia, and civil society. After all, the United States and South Korea will need to work together across disciplines and at multiple levels to implement this proposed framework and navigate the Fourth Industrial Revolution's disruptive changes.

This Smart Partnership comes at a time when the stakes could not be higher. Currently, there is a global competition underway among the world's leading powers to dominate the development and deployment of emerging technologies. The race is on to gain first-mover advantage in everything from artificial intelligence and autonomous vehicles to smart grids, 5G connectivity, and genetic editing. While the United States and South Korea are two of the world's leading innovators, they are by no means the only countries trying to reap the benefits of the Fourth Industrial Revolution. Other countries continue to make significant headway in developing advanced technologies, gaining advantages in some domains and taking the lead in others. In establishing a Smart Partnership, the United States and South Korea can ensure they remain global leaders and reap the very real technological benefits the Fourth Industrial Revolution offers.

Written by:
Samuel Klein, *Assistant Director*, Foresight, Strategy, and Risks Initiative, and Beryl Thomas, *Project Assistant*, Asia Security Initiative.

A Strategic Framework for Building a Smart Partnership





PART I

BUILDING A SMART PARTNERSHIP FOR ARTIFICIAL INTELLIGENCE

CHAPTER 1

NAVIGATING AN AUTOMATED FUTURE

Dr. Vaughan Turekian

Senior Director of Science and Technology for Sustainability Program,
National Academies of Sciences, Engineering, and Medicine

The scene is out of a science-fiction movie. An advanced machine equipped with the latest software faces off against a human in a game of the mind, matching its human competitor in strategy and skill. Ultimately, the computer-powered machine is victorious, leaving experts and political leaders questioning whether the rise of the machines is one step closer to reality. Rather than this being a scene taking place in some future time, the dominance of the machine, the Google-created AlphaGo, over the South Korean grandmaster Lee Sedol in the ancient Chinese game of Go took place in 2016 in the Republic of Korea (hereafter South Korea).

It was not the first time that a computer beat a grand master in a game of skill. When IBM's Deep Blue defeated chess grandmaster Garry Kasparov in 1997, it too had reverberations about the ability of machine learning and algorithms to best the human mind. AlphaGo's victory was in some ways even more impressive given that the game itself is more complicated, with more variables than chess, and thus harder to train a computer for. It also took place almost two decades after Deep Blue's win in a world ever more focused on artificial intelligence (AI) and machine learning as major disruptors in every aspect of the human endeavor. The event marked a watershed moment for South Korean investment in AI, with then-President Park Geun-hye announcing a five-year, nearly $3 billion public-private partnership in AI research and development (R&D).[1]

The rise of the machines and the artificial intelligence/machine learning (AI/ML) software that powers them is rapidly becoming an issue of national and international policy focus. Two of the leading countries in this technological development and deployment, the United States and South Korea, are well placed to steer AI/ML research development and policy. The focus on robotics and AI/ML represents the natural progression in the United States-South Korea research relationship. This cooperation has been built on decades of public and private sector interactions designed to meet both economic and security challenges. With new political leadership in both countries, novel approaches for cooperation in advanced technologies could open trade and employment opportunities.

1 Philip Iglauer, "South Korea Promises $3b for AI R&D after AlphaGo 'Shock,'" ZDNet, March 22, 2016, http://www.zdnet.com/article/south-korea-promises-3b-for-ai-r-d-after-alphago-shock/.

The advent of faster computing and processing speeds and the increased use of cloud-based computing in the 2010s has resulted in a renaissance for artificial intelligence.

To frame the opportunities for cooperation, this chapter starts by presenting a background to AI/ML. Building on this, it identifies some of the major political, economic, technical, and legal issues being created by the rapid pace of innovation and deployment of technologies. The chapter then provides an overview of the context in which US and South Korean science and technology cooperation is taking place, including current areas of priority. Finally, it offers recommendations for mechanisms and themes for enhanced cooperation in this space.

BACKGROUND AND UNFOLDING TRENDS

"I propose to consider the question, 'Can machines think?' This should begin with definitions of the meaning of the terms 'machine' and 'think.' The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous."[2] These opening lines from Alan Turing's 1950 seminal computing paper initiated the field of AI/ML. Building off the question, "Can machines think?" Turing created one of the earliest definitions of artificial intelligence. The Turing test, as it is known, determines that a computer can think if during a series of double-blind interactions and conversations a human interrogator cannot differentiate between the machine and the human being.

The progression of AI/ML through the twentieth century has not been constant. As increasing numbers of computer scientists began developing algorithms and programs that would enable thinking computers, the data requirements for broad-based applications became a limiting condition. Large investments in AI/ML, especially by the Defense Advanced Research Projects Agency and other federal agencies in the United States, yielded a better understanding of the potential applications and uses, but software development far outpaced hardware. As a result, the more rapid advances in AI/ML and investments in the underlying research began to dry up.[3] At the same time, automation through robotics developed as a way to increase productivity, especially in manufacturing. Although these robotic machines were powered by complex software for a task, their ability to learn, and thus be viewed as intelligent, was limited.

The advent of faster computing and processing speeds in the late twentieth century and the increased use of cloud-based computing in the 2010s has resulted in a renaissance for AI/ML, as these systems are now able to perform more complex calculations on larger data sets, at higher speeds, and with greater accuracy than had ever been imagined. Still, the question of what AI/ML actually is and how it can be applied remains an open question. There is no single or widely accepted definition of AI/ML. A key textbook in the field characterizes AI/ML as[4]

1. systems that think like humans;
2. systems that act like humans;
3. systems that think rationally; and
4. systems that act rationally.

This hierarchy of AI/ML imprints the issue of rationality and human-like behavior into the core of the field. The result is that intelligent machines, according to the authors, are presumed to have the capabilities to think and act in ways that allow for them to work with, or even in place of, the humans that created them.

Given the yet-to-be-fully-realized potential of the technology, AI/ML is as much a question of field progression as it is of theoretical existence. Thus, perhaps

2 Alan M. Turing, "Computing Machinery and Intelligence," *Mind* 59, no. 236 (1950): 433-460.

3 Tanya Lewis, "A Brief History of Artificial Intelligence," *Live Science*, December 4, 2014, https://www.livescience.com/49007-history-of-artificial-intelligence.html.

4 Stuart J. Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Pearson Education, Inc., 2010).

the most elegant solution to the definitional question is that "AI can be defined by what AI researchers do."[5] Placing AI into the areas of cutting-edge research and the focus areas where the research community is investigating potential uses makes sense given that it is very much a field (or set of fields) in its infancy, with applications that are not yet completely known. What is better understood is that the range of AI/ML applications varies based upon the distinct types of research and approaches used. These have been described to include:[6]

- large-scale machine learning—algorithms that involve extracting information from extremely large data sets and learning, thus drawing conclusions and predictions from those data;[7]
- deep learning—methods that use developed artificial neural networks to enable unsupervised machine learning from unstructured or unlabeled data (e.g., object recognition in images);[8]
- reinforcement learning—algorithms that seek to enable not only pattern recognition but also experience-driven sequential decision-making, to further allow computers to take action based on those decisions;[9]
- robotics;
- computer vision—a subarea of AI, developed thanks to deep learning, that consists of computers seeing, identifying, and processing images in a way that mimics human vision;[10]
- natural language processing—a method of translation between human and computer languages, which enables the computer to understand human language without being provided with a calculation;[11]
- collaborative systems—development of autonomous systems that can cooperate with other systems and with humans;[12]
- crowdsourcing and human computation—methods that enable automated reference to human expertise to solve problems that are beyond the capabilities of AI alone;[13]
- algorithmic game theory and computational social choice—methods dealing with the economic and social computing dimensions of AI, which consist of systems defining and handling individual and collective preferences of goal-oriented agents;[14]
- the Internet of Things; and
- neuromorphic computing—technologies that seek to mimic biological neural networks by implementing very-large-scale integration systems containing electronic analog circuits, instead of relying on separate modules for input/output, instruction processing, and memory.[15]

POLICY ISSUES AND STRATEGIC IMPLICATIONS

AI development and policy issues have gained major traction in recent years within the public, private, and academic sectors in the United States. A series of activities has served to frame the key concerns to be addressed and opportunities to be better developed. In 2016, Stanford University released the first report from its One Hundred Year Study on Artificial Intelligence (AI100). The project's goal is to understand the advances and potential impacts of AI over a century across a range of fields, including transportation; home/service robotics; healthcare; education;

5 Peter Stone, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyanakrishnan, Ece Kamar, Sarit Kraus, Kevin Leyton-Brown, David Parkes, William Press, AnnaLee Saxenian, Julie Shah, Milind Tambe, and Astro Teller, *Artificial Intelligence and Life in 2030*, One Hundred Year Study on Artificial Intelligence, September 2016, https://ai100.stanford.edu/2016-report.

6 Ibid.

7 Jure Leskovec, Anand Rajaraman, and Jeffrey David Ullman, "Large-Scale Machine Learning" in *Mining of Massive Datasets* (Cambridge: Cambridge University Press, 2014), 415-458, https://doi.org/10.1017/CBO9781139924801.

8 "Deep Learning ou apprentissage profond: définition, qu'est-ce que c'est?" Le Big Data, last updated February 1, 2018, https://www.lebigdata.fr/deep-learning-definition.

9 Stone et al., *Artificial Intelligence and Life in 2030.*

10 "What Is Computer Vision?" The British Machine Vision Association and Society for Pattern Recognition, accessed February 8, 2018, http://www.bmva.org/visionoverview.

11 "Natural Language Processing: What It Is and Why It Matters," SAS Institute Inc., accessed February 8, 2018, https://www.sas.com/en_us/insights/analytics/what-is-natural-language-processing-nlp.html#.

12 Stone et al., *Artificial Intelligence and Life in 2030.*

13 Ibid.

14 Felix Brandt et al., *Handbook of Computational Social Choice* (Cambridge: Cambridge University Press, 2016), chap. 1, http://procaccia.info/papers/comsoc.pdf.

15 Andrew Adamatzky and Leon Chua, *Memristor Networks* (London: Springer International Publishing, 2014), 212.

The TOPIO Dio robot on display at the Automatica exhibition. *Photo credit*: Humanrobo/Wikimedia.

low-resource communities; public safety and security; employment and workplace; and entertainment. The project takes the unique approach of undertaking an assessment of the technology at five-year increments, allowing for a constant evaluation of the potential and actual implications of the technology and its applications as they evolve.

Soon after the release of the AI100 report, and with greater focus on the increased deployment of AI/ML, some of the largest and best-known private sector platform companies developed their own efforts to follow advances and develop policies. The Partnership on Artificial Intelligence to Benefit People and Society (Partnership on AI) was created by Amazon, Apple, DeepMind, Facebook, Google, IBM, and Microsoft with the objective of sharing best practices in AI and educating the public about opportunities in this space. In many ways, it is a consortium developed to respond to increasing concerns in media and in policy circles about the interface between human and machine.

In 2016, then-President Barack Obama's administration released the White House report *Preparing for the Future of Artificial Intelligence*.[16] Drawing on government and academic research, the report presented a US approach to a range of issues where AI will require broader governmental focus, including regulation, research and workforce development, economic impacts, governance, and global engagement. International engagement was one of the key areas of focus for the report, which recommended that "the U.S. Government should develop a government-wide strategy on international engagement related to AI, and develop a list of AI topical areas that need international engagement and monitoring."[17] It also recommended that "the U.S. Government should deepen its engagement with key international stakeholders, including foreign governments, international organizations, industry, academia, and others, to exchange information and facilitate collaboration on AI R&D."[18]

16 US Executive Office of the President, National Science and Technology Council, *Preparing for the Future of Artificial Intelligence*, October 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

17 Ibid, 35.

18 Ibid.

Both the AI100 and the White House report point to many of the potentially beneficial outcomes from AI/ML, but there are also serious concerns that provide an important context for increasing cooperation across the multiple stakeholders. News stories often highlight the potential of self-directed killer robots, as portrayed in the *Terminator* movie franchise. This concern was perhaps most vividly articulated by Russian President Vladimir Putin, who, during a 2017 tour of Yandex, Russia's largest tech firm, asked its chief executive officer when AI "will eat us."[19] Such concerns have been expressed, albeit slightly less colorfully, by scientists and entrepreneurs such as Stephen Hawking and Elon Musk.

Among policy issues that are the more immediate priorities and offer important areas for potential international cooperation is the role of *access to and formatting of data*. AI/ML and robotics are data-intensive activities. For example, autonomous vehicles require large amounts of data and constant integration from multiple data sources to perfect their learning algorithms. Given this, data are becoming much more valuable commodities in the commercial domain of the private sector. At the same time, there is significant public good that can be derived from using large data sets powered by AI/ML analytics. How countries deal with access to and formatting of data, both domestically and internationally, will have major implications for the potential beneficial use of AI/ML and the development and growth of private sector companies.

Legally, there are major issues at the domestic and international level related to liability—with the overriding question of who is responsible for what outcome. Keeping with the example of autonomous vehicle development, in the case of an accident, where does the liability fall? Is it on the owner of the vehicle (who, in the case of autonomy, is not really the operator), or is it on the producer of the algorithm that was responsible for driving the vehicle (similar to the liability of Takata in the airbag malfunctions that led to the recall of millions of cars in 2013)? Given the global trade and manufacture of automobiles (which includes many South Korean and US car companies), legal systems will need significantly enhanced capabilities to deal with such liability issues.

Economically, AI/ML-enhanced automation will lead to major workforce disruptions. The 2016 White House report determined that AI-empowered automation "may also affect particular types of jobs in different ways, reducing demand for certain skills that can be automated while increasing demand for other skills that are complementary to AI."[20] Developing better approaches and practices for minimizing negative impacts of automation will be critical for countries in all regions. As one response in South Korea, President Moon Jae-in's administration announced in mid-2017 that it will reduce the corporate tax deduction for company investment in infrastructure that leads to increased efficiencies. Although this has been dubbed a "robot tax,"[21] in reality this is a modest move compared with other tax policies being discussed in the academic and legal communities. As countries develop fiscal policy responses to workforce replacement, there needs to be greater coordination at the international level.

Scientifically, the numerous paths of research are creating great opportunities for rapid advances in AI/ML and robotics. Given the strong interest by the private sector, much of this research is becoming quickly applied, creating tension between proprietary and precompetitive research. The latter is often the place where robust collaboration is not only possible, but often preferred given the pooling of resources and distribution of risk. At the same time, in the United States, there is increasing concern in universities that the top AI/ML students, from undergraduates to doctoral candidates, are being hired instantly into companies given the potential payouts associated with discoveries in this area. Developing mechanisms for increased fundamental research is critical to ensuring the roaming ecosystem that can lead to higher risk and disruptive discovery.

For each of these areas, there are strong domestic and international drivers for increasing cooperation and coordination with multiple stakeholders. Given the rapid development of AI/ML and the leadership of South Korea and the United States in both the discovery and deployment of automated systems, there is great opportunity for developing and deepening robust areas for engagement.

---

19 Shubham Sharma, "Russian President Vladimir Putin Asks When Will AI 'Eat Us,'" *International Business Times*, September 24, 2017, http://www.ibtimes.co.uk/russian-president-vladimir-putin-asks-how-long-before-ai-eats-us-1640580.

20 US Executive Office of the President, National Science and Technology Council, *Preparing for the Future of Artificial Intelligence*, 2.

21 Yoon Sung-won, "Korea Takes First Step to Introduce 'Robot Tax,'" *Korea Times*, August 7, 2017, http://www.koreatimes.co.kr/www/news/tech/2017/08/133_234312.html.

BOX 1. QUANTUM COMPUTING AND ARTIFICIAL INTELLIGENCE/MACHINE LEARNING

The rise of quantum computing has paralleled AI/ML becoming a deployed technology, leading to increased interest in whether AI/ML can be enhanced with advances in this type of computing.[1] It was only after computing power and speed increased that AI/ML started attracting sustained investments, with ramp up in such investments taking place over the past decade. As increased processing capabilities develop, including through new technologies like quantum computing, it stands to reason that so too should the effectiveness of AI/ML systems.

In recent years, there has been increasing excitement over the potential to use quantum theory to develop quantum computing capabilities. Current computational capabilities (classic computing) are built using binary digital computation. All data and information are stored in two states, zero or one, referred to as bits. Increasing memory involves increasing the number of bits being used at any time. Quantum computing takes advantage of a characteristic of quantum mechanics called superposition—namely that an electron can exist in two states, say zero and one, at the same time or in any position in between. The result is that rather than being based on bits, quantum computers use qubits, which provide potentially infinitely more possible solutions. One of the major advantages of quantum computing is that by making calculations using data in multiple states, quantum computers can factor exceedingly large numbers, making possible certain calculations that are unable to be performed using classical computers. This has major implications for everything from high-speed financial transactions to climate modeling.

In theory, quantum computing should allow for a fundamentally different way to address computation. Rather than looking at quantum computing as being faster computing, it needs to be looked at as a different way of computation. Given the technical architecture and types of computations that these machines perform, taking advantage of the benefits of quantum principles in computing requires new coding and algorithms specifically designed for quantum computing.

The ability to create stable and usable machines that can utilize quantum effects is still more theoretical than actual. Quantum effects are known to take place at atomic scales, but scaling that up to the larger scales required for computing in a stable and useful way is less well established. A lot of research in both the public and private sector has focused on developing not only such capabilities but also the needed algorithms to use with this type of technology.

In terms of quantum computing, only recently has research started to address this issue. Experts are optimistic that quantum computing will improve machine learning by improving reinforcement learning—one of the key areas of machine learning.[2] Peter Diamandis, the co-founder and executive chairman of Singularity University, has stated that one of the key outcomes of quantum computing will be massive increases in AI/ML capabilities. He points to the ability for quantum computing to compute much more data in parallel than classical computing allows as a major advantage of this technology.[3]

The relationship between quantum computing and AI/ML is an area of research with major commercial and security implications. There is great potential for collaborative international work to develop new AI/ML algorithm approaches to take advantage of this powerful technology.

---

1 Eleanor Rieffel and Wolfgang Polak, "An Introduction to Quantum Computing for Non-physicists," *ACM Computing Surveys* 32, no. 3 (2000): 300-335.

2 Vedran Dunjko, Jacob M. Taylor, and Hans J. Briegel, "Quantum-Enhanced Machine Learning," *Physical Review Letters* 117, no. 13 (2016): 130501.

3 Peter Diamandis, "Massive Disruption Is Coming with Quantum Computing," SingularityHub, October 10, 2016, https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/#sm.0000i1jqc3ajecz0sfi1ipf1qpcwl.

The emergence of automation is leading rapid changes in the existing economic, social, political, and legal frameworks.

EXISTING MECHANISMS FOR US-SOUTH KOREAN ENGAGEMENT

In 2015, the US and South Korean governments released a joint statement announcing "new frontiers for cooperation" that articulated a series of top priority science and technology issues.[22] A number of these new frontiers have implications for AI/ML, including "increasing cyber collaboration," "exploring space cooperation," "countering biological threats and advancing the global health security agenda," and "expanding science and technology cooperation."[23] One critical mechanism for accomplishing each of these is through the Joint Committee Meetings (JCM) on Science and Technology Cooperation between the United States and South Korea. Traditionally held at the ministerial level, the 2016 high-level dialogue identified intelligent computing as a priority area for further cooperation.

In addition to the dialogue on science and technology (S&T), South Korea and the United States developed during the Obama administration a robust dialogue on information and communications technology (ICT) through the ICT Policy Forum, which engages government, academic, and industry experts across a range of ICT-related technologies. The third dialogue in late 2016 provided a venue to begin discussing ways to encourage voluntary, industry-led international standards in areas such as the Internet of Things and smart cities, both of which are closely related to AI/ML.

Finally, there has been a series of high-level trilateral meetings held between Japan, South Korea, and the United States at the deputy minister of foreign affairs level. In 2016, these talks led to an agreement by the three foreign ministries to develop a mechanism for further discussion of the foreign policy implications of emerging and disruptive technologies, including AI/ML.[24]

The changes in leadership in the United States and South Korea in 2017 also provide an opportunity to consider ways forward for cooperation across a range of issues. While the bulk of the bilateral and trilateral leader-level discussions are currently focused on security concerns related to North Korea, there is every expectation that these dialogues will expand to a broader issue set. The recommendations below provide a framework for ensuring that AI/ML and robotics continue to play a role within this dialogue.

CONCLUSION

The emergence of automation, including robotics and AI/ML, is leading rapid changes in the existing economic, social, political, and legal frameworks. Rather than these technologies representing an end state, they are means and approaches to altering and disrupting many of the products and processes that exist today. The speed of innovation, distribution of expertise, and tension between public good and commercial development around the world make AI/ML and related technologies central to dealing with a multitude of domestic and international challenges facing governments. As leaders in the AI/ML field, South Korea and the United States have an opportunity to work with each other and others to develop the research and policy environment that can accelerate innovation and impact. At the same time, as democracies with publics that expect their governments to both encourage innovation and protect individual rights, the two countries have added pressure to work together and with other like-minded governments, the private sector, and academics to develop approaches and policies that maximize the positive and minimize the negative impacts of AI/ML and other advances. Such outcomes require dialogues and institutions that are both focused on and adaptable to a technology whose emergence just a half century ago

22 White House, "Joint Fact Sheet, The United States-Republic of Korea Alliance: Shared Values, New Frontiers," October 16, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new; Sean Connell, *New Frontiers of Cooperation in U.S.-Korea Relations: Opportunities for Economic Engagement*, Korea Economic Institute of America, May 17, 2017, http://www.keia.org/publication/new-frontiers-cooperation-us-korea-relations-opportunities-economic-engagement.

23 Ibid.

24 Personal communications based on the author's involvement in this initiative while working at the US Department of State.

changed and challenged the relationship between human and machine.

RECOMMENDATIONS FOR INCREASED COOPERATION

AI/ML and robotics are not ends in and of themselves. Rather, advances and deployment of AI/ML provide a means to enhance or disrupt a range of existing activities. Therefore, the recommendations put forward below are couched in a broader framework of interaction, rather than focused on individual sectors. Finally, while national government–to–national government activities have great potential, the diversity of actors that are affecting and are affected by AI/ML necessitates a broader engagement.

The South Korean Ministry of Trade, Industry, and Energy (MOTIE) and the US Department of Energy (DOE) should develop an AI/ML-in-smart-grids research agenda.

» AI has the potential to increase the efficiency and effectiveness of smart grids, especially in determining and adjusting for peak load energy and supply. MOTIE and DOE should develop a joint committee of experts to develop a research agenda to increase the use and utility of AI in smart grid development and deployment. The joint committee would necessarily engage experts in the relevant ministries, as well as private sector and municipal leaders and academics. The research agenda could both provide a technical road map as well as identify key areas of social science and economics that need to be considered and evaluated before the deployment of any such system.

The United States and South Korea should ensure that the Joint Committee Meetings on Science and Technology Cooperation resume with continued engagement at the highest levels possible.

» The Joint Committee Meetings should dedicate special attention to issues of AI/ML research, including creating better roadmaps for the opportunities to develop more advanced information about the potential roles of AI/ML in health, space, and environmental cooperation. The JCM provides the most efficient way to bring together leaders in the government, science, and funding communities within the two countries. Given the potential for AI/ML in facilitating outcomes in other areas, there is a benefit to ensuring that the appropriate experts from both countries participate in these meetings.

» The JCM should further enhance joint programs in emerging fields of basic research that have potential implications for AI/ML and robotics through the existing bilateral S&T agreement, which provides the most robust and established mechanism to increase joint research in AI/ML-related fields. Two candidates for this enhanced pre-commercialization research include quantum computing (see box) and brain science. Each of these emerging science areas has implications much broader than AI/ML and advances in understanding brain process and function, and increased computing capabilities will impact data analytics and development of neural networks.

The Trump and Moon administrations should commit to activating the existing high-level bilateral ICT Policy Forum and use it to better coordinate on AI/ML-related policy development.

» While the JCM's focus is on science and technology policy, the ICT Policy Forum offers an opportunity to develop a robust science and technology platform for policy engagement on these issues. Of particular value would be further development of coherent policies related to the regulation of AI/ML; taxes and incentives for the creation and deployment of AI/ML-equipped products; ICT policies on AI/ML development and deployment; and liability and regulation of AI/ML-enabled machines and vehicles. These conversations could be critical to helping to develop coherent positions that can be discussed in regional and global forums, including the Group of Twenty and Asia-Pacific Economic Cooperation forums.

The South Korean Ministry of Foreign Affairs should identify a representative to participate in a trilateral emerging-technology and foreign-policy dialogue with the United States and Japan.

» In late 2016, the trilateral dialogue undertaken by the three deputy foreign ministers identified emerging technologies, including AI/ML, as key elements of the economic and security dialogue. As part of this discussion, South Korea was invited to identify a representative to join the science and technology advisers to the foreign ministers of the United States and Japan in a dialogue on emerging science and technology drivers of foreign policy. Although South Korea had not at that time created the position of science adviser, the government started discussions about the potential for doing so. By creating such capacity within the South Korean Ministry of Foreign Affairs, there is an opportunity to develop stronger trilateral connec-

tions on issues like AI/ML that can impact trilateral and multilateral foreign policy engagement.

The Korea Institute for Advancement of Technology (KIAT) and the Korea International Cooperation Agency should work with the US Agency for International Development's Global Development Lab and other appropriate development agencies to help build AI-enhanced infrastructure in select developing countries.

» AI's application across broad segments of the economy will likely create both winners and losers. There are concerns about the consequences of what will happen if developing countries are left behind by advances in this sphere. Increased cooperation between the appropriate South Korean and US agencies with developing country governments will be critical to making sure that developing countries benefit from advances in AI/ML. As part of this effort, it would be useful to develop criteria for such pilot engagements, including such metrics as government investment in computing and existing infrastructure (e.g., access to broadband and digital resources). At the same time, the pilots could focus on sectoral applications (e.g., health, agriculture) or regional priorities.

KIAT and the National Science Foundation should develop a series of exchanges focused on increasing the female workforce in AI/ML R&D.

» Given the priority by KIAT and the Trump administration to increase the participation of women in science, technology, engineering, and mathematics, there is an opportunity to focus on the implications of AI for women and underserved groups in the R&D ecosystem. Such dialogues could include sharing experiences and practices and establishing joint bilateral committees to focus on technical and economic issues associated with AI.

American and South Korean industry leaders should identify ways to bring South Korean companies into the Partnership on AI.

» With the increasing role of the private sector in developing norms and standards for AI, partnerships that bring together the leaders in this area are more relevant to policy development. The Partnership on AI—an industry-launched initiative to bring together the leading companies working on AI development, norms, and applications—is currently leading the effort to develop private sector governance over AI/ML. As of February 2018, no South Korean companies are involved in this partnership. Given the large number of South Korean companies in leadership roles in this space, their participation and expertise would help develop more informed private sector policy discussions.

New public-private partnerships at the municipal and local levels should develop AI/ML training programs in locations where South Korean and US technology companies are operating.

» Given the challenges that AI/ML automation will have on the workforce, it is critical that the private sector work with educational institutions to develop a next-generation workforce capable of providing the needed technical know-how and expertise. There are good examples of this, including the central role that the Intel Corporation has played in working with local Vietnamese institutions in Ho Chi Minh City to locally train engineers as workers in Intel's plants.

South Korean and US schools of law should develop jurist exchange programs focused on AI/ML.

» As more automation and AI/ML advances push the limits of current legal expertise and practice, it will be critical to develop a cadre of jurists capable of dealing with the issues that will arise related to ethics, international trade, and the economy. Through exchange and training programs, such a community can develop and provide an important resource for these issues, both bilaterally and globally.

South Korean and US automobile companies should consider developing a consortium on autonomous vehicles.

» One model that could be useful for this consortium is the California Fuel Cell Partnership, a public-private effort to accelerate the infrastructure and standards for hydrogen fuel-cell vehicles. Such a partnership on autonomous vehicles could be critical for developing common regulations, establishing data-sharing protocols, and standardizing rules of the road for autonomous vehicles at the level of manufacturers with production and sales facilities in both countries and globally.

CHAPTER 2

ADDING VALUE WITH ARTIFICIAL INTELLIGENCE

Dr. Taehee Jeong

Senior Data Scientist, Xilinx

In the last five years, many innovative technologies and business models have emerged, including car-sharing services, house-sharing services, 3-D computing, augmented reality (AR) and virtual reality (VR), improved voice recognition and image recognition, drones, big data, and the Internet of Things (IoT). Around the world, many countries have shown strong interest in these technologies as technological progress has become the main driver for development. Some countries and companies have adapted quickly to the changing environment, navigating these waves of technological advancement and increasing their productivity and economic growth. Today, the world is at the forefront of another wave of innovation, the Fourth Industrial Revolution. Determining how to respond to this wave is a pressing challenge for every country, including the Republic of Korea (hereafter South Korea) and the United States.

UNFOLDING TRENDS

This new wave of innovation includes the rise of artificial intelligence (AI) and machine learning. Artificial intelligence is a very broad term that can be applied to any technique that enables machines to mimic human intelligence, resulting in machines able "to solve problems in ways that at least superficially resemble human thinking."[1] Machine learning, a subset of AI, is a computational statistics method that involves using vast quantities of "training" data to teach an algorithm to find patterns and make predictions. Some applications for these models include voice recognition, language translation, and network intrusion detection.[2]

Artificial intelligence will transform businesses and the job market in the coming decade. It will continue to accelerate productivity and boost economic growth, creating better and more jobs and improving living standards. Accelerating AI capabilities will enable the automation of some tasks that have historically required human intelligence. These transformations will open new opportunities and create different challenges for individuals, industry, and society. While some older-model businesses may close, new jobs and business-

1 The Editors of *TIME*, *Artificial Intelligence: The Fate of Humankind* (2017).

2 Patrick Hall, Wen Phan, and Katie Whitson, *The Evolution of Analytics: Opportunities and Challenges for Machine Learning in Business* (Sebastopol, CA: O'Reilly Media, 2016).

es that rely on AI will be created.[3] Government policy makers in South Korea and the United States should pursue these AI-related opportunities, and not risk falling behind the new wave.

MACHINE LEARNING FOR THE MANUFACTURING INDUSTRY

Manufacturing is the major field to focus on for machine learning applications in South Korea. Traditionally, South Korea has heavily relied on industry, and the economy has continued to expand along with the manufacturing industry. South Korea's manufacturing industry creates semiconductors, mobile phones, display technologies, consumer electronics, automobiles, railroads, power plants, and transportation systems, making the country a competitive producer across the world.

Manufacturing processes are particularly good candidates for **intelligent analytics** (IA) as they are already well-instrumented with sensors and controls. Machine learning in manufacturing "starts with embedding sensors and other advanced instrumentation" into machines.[4] The embedded sensors collect vast quantities of data, which are then used in AI programming to improve machine efficiency and performance and equipment maintenance. To apply machine learning for manufacturing, the first step is to add digital instrumentation to the manufacturing process. Once equipped with digital instrumentation, the data that each device produces can be recorded, saved, and transferred to remote, offsite machines or operators via the internet.[5] Tapping into these connected devices and networks, collected data are stored, analyzed, and later visualized by the machine's internal analytical programming and tools. This feedback loop allows the machine to learn from its data log history and adapt its behavior to work more intelligently by implementing the new machine learning model.

With the advent of the industrial IoT, more than fifty billion devices are expected to be connected to the internet, generating six hundred zettabytes per year, by 2020. These real-time data flows of huge volume will help machine learning programs make predictions in real time. Machine learning can apply data coming from the manufacturing process to optimize the operation of the manufacturing line, reducing downtime and generally maximizing equipment performance. Machine learning is also starting to impact quality control, facilitating visual inspections that reduce defects in products.[6]

Machine learning allows **preventive maintenance** for individual equipment. Machine operations and performance data that are collected and logged allow data scientists to "better understand the condition of critical components."[7] By analyzing the data log, operators can better determine the longevity of a piece of equipment and track how long that particular component has been in use, and under what conditions. Machine learning tools can then compare these findings against the conditions and lifespans of similar components in other machines and equipment, thereby providing "reliable estimates of the likelihood and timing of component failure."[8] This enables operators to avoid outages that take machines offline and to decrease maintenance costs. Embedded sensors and network connections allow machine learning to implement preventive maintenance programs to reduce equipment downtime and maintenance costs. Through the adoption of machine learning technologies, enhanced productivity, lower costs, and reduced waste are achievable.

For example, one of the world's largest adhesive manufacturers used machine learning to tackle a $300 million dollar waste and quality problem. The company worked with an IoT company, and used its machine learning model to identify abnormalities in sensor stream data. Newly discovered sensor operational abnormalities were correlated to quality outcomes. The model learns the typical behavior by processing sensor

3 United States Government, *Artificial Intelligence, Automation, and the Economy*, Executive Office of the President under Barack Obama, December 20, 2016, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF.

4 Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Raffaele Giaffreda, Hanne Grindvoll, Markus Eisenhauer, Martin Serrano, Klaus Moessner, Maurizio Spirito, Lars-Cyril Blystad, and Elias Z. Tragos, "Internet of Things beyond the Hype: Research, Innovation, and Development," in *Building the Hyperconnected Society: Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*, eds. Ovidiu Vermesan and Peter Friess (River Publishers, 2015), 31.

5 "The Next Industrial Revolution," Shaping Tomorrow, April 14, 2015, https://www.shapingtomorrow.com/home/alert/404588-The-next-Industrial-Revolution.

6 Peter C. Evans and Macro Annunziata, *Industrial Internet: Pushing the Boundaries of Minds and Machines*, General Electric, November 26, 2012, https://www.ge.com/docs/chapters/Industrial_Internet.pdf.

7 Ibid.

8 Ben van Lier, "Blockchain and Servitization of Manufacturing," IoT Council, September 5, 2017, https://www.theinternetofthings.eu/ben-van-lier-blockchain-and-servitization-manufacturing.

A manufacturing robot works on aircraft components. *Photo credit*: Tecnalia/Flickr.

data for over a year. Once the model observes a data point that is not in the normal zone, it automatically sends alarm signals.[9]

Predicting product quality is another application of machine learning in manufacturing. While predictive maintenance has already been implemented in both field service and manufacturing, product quality prediction is a new area for machine learning application. Machine learning is capable of recognizing outliers with respect to reliability or performance. Thus, machine learning models can recognize potentially problematic components in advance before the components are packaged or shipped. This predictive quality capability will provide great benefit to the industries that require high standards of reliability, such as the automobile industry.

Today, every automobile is composed of thousands of mechanical and electrical components and devices. It is critical that each component and device work correctly without any malfunctions or errors, even in harsh environments. Because any malfunction or error of the component may result in a loss of life, the automotive industry has expended a lot of energy to prevent any failure of components and improve quality. Predictive quality will provide intelligent quality control on top of conventional quality control.

Even though many people recognize the potential of machine learning in the manufacturing industry, relatively few companies have integrated machine learning into their systems. Across the United States, about 10 percent of packaged goods manufacturers employ machine learning in their plants. Many other companies are evaluating machine learning and starting to implement it in their production lines.[10] Several companies already have big data sets and infrastructure, so they are trying to improve business processes not by developing new workflows, but by developing new capabilities within existing systems, shifting to an intelligent interpretation of data in a way that will yield more productivity and automation while reducing human in-

9 Alan R. Earls, "AI in Manufacturing Beneficial, but Adoption Slow," *Techtarget*, August 2017, http://internetofthingsagenda.techtarget.com/feature/AI-in-manufacturing-beneficial-but-adoption-slow.

10 United States Government, *Artificial Intelligence, Automation, and the Economy*.

volvement. Such implementation has already enjoyed some success, such as using machine learning to detect anomalies and figure out the state of a specific process, because abnormal signals of failure can be detected in advance with machine learning.

The application of machine learning algorithms to the manufacturing sector has several advantages in South Korea. There is no need to develop a new advanced algorithm for manufacturing applications. In most cases, well-established algorithms that are already publicly available can be applied. Furthermore, supercomputers, distributed file systems, and cloud computing platforms are not required to integrate machine learning into the manufacturing sector. Such minimal entry-level requirements will help South Korea apply the benefits of machine learning to its manufacturing sector without hesitation. The opposite case is true for image recognition and medical diagnoses, which require very complicated deep-learning algorithms and tremendous computing power.

Integrating domain knowledge into machine learning algorithms is necessary to develop the application of machine learning for manufacturing, but South Korea will not likely face any obstacles in this regard. There are a lot of domain experts on manufacturing in South Korea as the manufacturing industry underpinned the development of its modern economy. These domain experts, working together with data scientists, can serve as a good resource to deploy machine learning in manufacturing.

In South Korea, the prerequisite information technology (IT) infrastructure for the application of artificial intelligence and machine learning in manufacturing is already well-established, but certain challenges regarding data stream usage and manipulation still exist. To collect data from equipment, sensors must be affixed to such equipment and connected to the internet. To efficiently collect information, new manufacturing equipment should be designed with integrated sensors that log machine data. Sensors should also be installed in existing machines to monitor older manufacturing equipment. For faster data transmission, the application of AI in manufacturing demands IT infrastructure support. Data centers and networks are needed to connect the systems, networks, databases, and machines in different industries around the world, which "will require a combination of inter- and intra- state infrastructure in order to support the significant growth in data flows" pertinent to manufacturing application.[11] In accordance with these requirements, South Korea maintains the fastest internet speed and largest nationwide networks.

MACHINE LEARNING FOR THE HEALTHCARE INDUSTRY

Advances in image recognition can be extended far beyond manufacturing or social applications, and there have been many attempts to bridge the gap between artificial intelligence and medicine by applying deep learning capabilities in the field of medical diagnosis. Throughout their careers, radiologists can view and analyze thousands of images, but a machine can see millions. Soon, it will be possible for machines "to read X-rays, MRIs [magnetic resonance imaging machines], and CT [computed tomography] scans more rapidly and accurately than radiologists, [and] to diagnose cancer earlier and less invasively."[12]

Not only will these advances yield faster analysis and more accurate results, but diagnostic medical services in general will become more reliable across the board. Soon, patients may not need to wait a few days or weeks to get their diagnosis results after MRI or CT scans. With the aid of machine learning, the result will be available immediately.

Another possible application is in internal medicine, whereby machines could make medical diagnoses and prescribe medications to patients. Since machine learning algorithms can search for life-saving medicines based on millions of medical cases, accuracy can be expected to be higher than the opinions of individual medical doctors.

However, there are two big challenges to applying deep learning to making medical diagnoses in South Korea. First, severe competition is expected in this field. Already, many leading AI companies and aggressive startups have been working on medical diagnosis in the United States and other countries. Although making medical diagnoses using image recognition has a lot of promise, effectively doing so will require the development of much more advanced deep learning technology to improve accuracy and advances in supercomputing power.

11 Charles Speicher Jr., "An Emerging Ecosystem," LinkedIn, July 19, 2016, https://www.linkedin.com/pulse/emerging-ecosystem-charles-chuck-speicher-jr-/.

12 Roger Parloff, "Why Deep Learning Is Suddenly Changing Your Life," *Fortune*, September 28, 2016, http://fortune.com/ai-artificial-intelligence-deep-machine-learning/.

A second issue stems from personal privacy issues related to data access and medical regulation. To train an AI model, a lot of medical data—which are directly connected to a patient's other biomedical information—are needed. Ensuring secure accessibility of the medical data could thus be a potential problem given concerns about protecting privacy. A third issue is clarifying who is responsible for the accuracy of the diagnostic predictions made by AI platforms. Since the medical treatment recommended by an AI-based prediction could determine a person's health or survival, a physician must ultimately be responsible for implementing appropriate treatment.

TRAINING DATA SCIENTISTS IN SOUTH KOREA

If South Korea is to become a leader in machine learning, it must immediately cultivate talented data scientists, of which there is currently a shortage. To train the necessary data scientist workforce within a short time frame, South Korea needs access to high-quality data science training programs at top US academic institutions. Through effective coordination between the US and South Korean governments, South Korean students could be trained through data science initiatives (DSIs) or data science master's degree programs. Training thousands of students to become data scientists would help South Korea maintain leadership in using machine learning and understanding the key role machine learning plays in the Fourth Industrial Revolution.

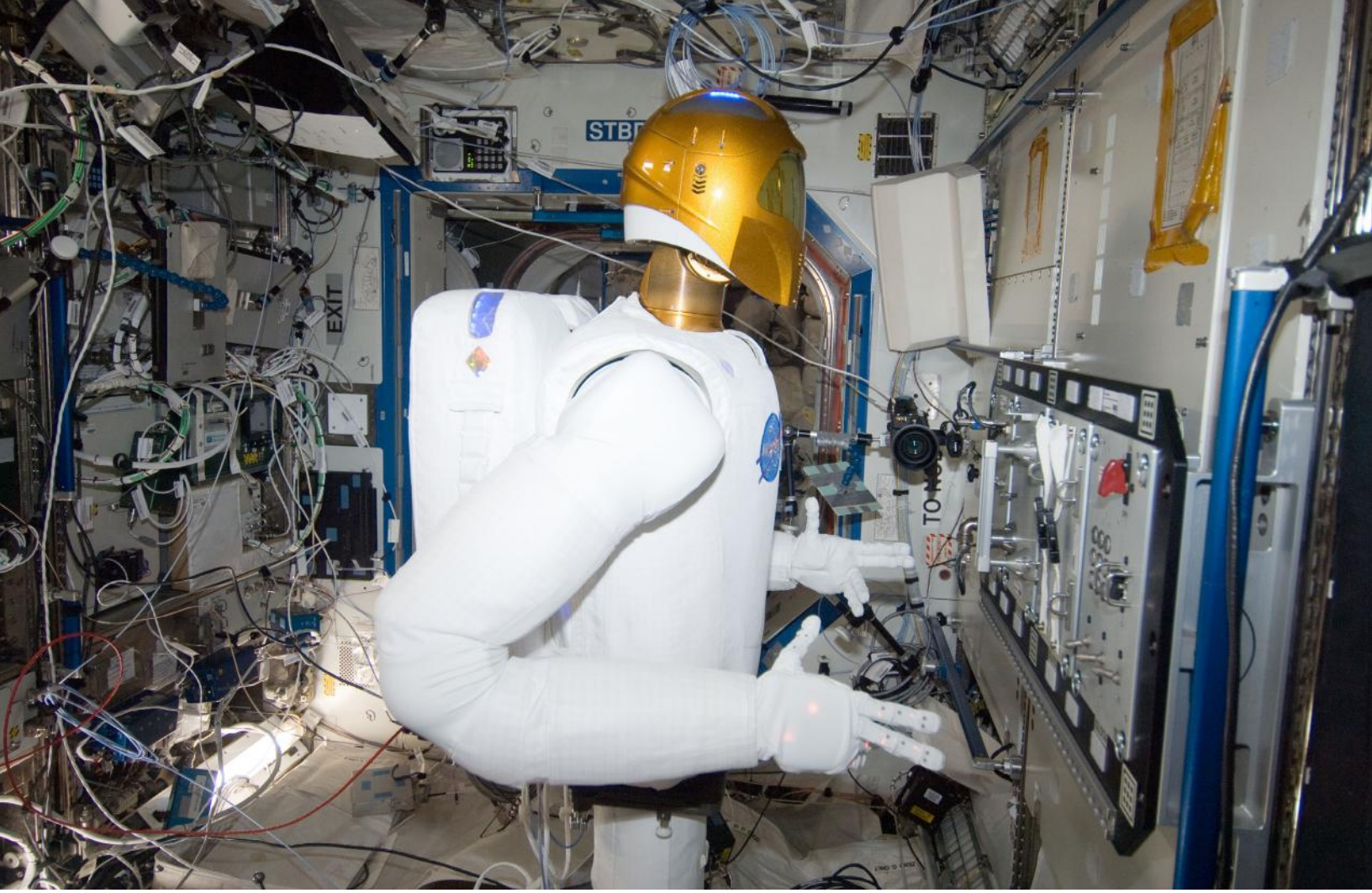
Even though a machine with learning capabilities can learn from its own experiences and does not need any rules-based code programmed by humans, the machine still requires a learning algorithm that instructs it how to treat input data, what kind of statistics-based model it should use, and what kind of output prediction can be expected. These tasks are the purview of data scientists.

Most data scientists have an academic background in computer science, with many of the top computer science schools located in the United States, including Carnegie Mellon University, Stanford University, the University of California at Berkeley, and the Massachusetts Institute of Technology. Companies that are leaders in AI with headquarters or research centers in the United States include Google, Microsoft, Facebook, and Amazon; many academic institutes are also creating machine learning courses to train data scientists.

South Korea needs thousands of data scientists to successfully deploy machine learning throughout its manufacturing industry.

There are currently only a few universities in South Korea that teach machine learning, and it is relatively uncommon to use machine learning at the corporate level or in government offices to improve productivity and performance. Only a few enterprises have started to develop consumer products—which include self-driving cars from Hyundai automotive, voice recognition applications in smartphones from Samsung and LG Electronics, and text translations by Naver—using AI technologies. Even though most people have heard about AI since the "go" game between Google's AlphaGo and Lee Sedol in 2016, South Korea is still in the initial stages of implementing the full capabilities of machine learning.

South Korea needs thousands of data scientists to successfully deploy machine learning throughout its manufacturing industry. Creating data science initiatives or data science master's degree programs would be a first step for the country. As a short-term solution, using online lectures from the United States, such as those from Coursera or Udacity, is one possible solution. Another would be to enable talented South Korean students with backgrounds in computer science, electrical engineering, mathematics, and statistics to attend DSIs in the United States. The US and South Korean governments could coordinate policy to grow the field of data science in the economic interest of both governments.



Robonaut 2, the first humanoid robot in space, performs a series of tests. *Photo credit*: NASA/Flickr.

CONCLUSION

Machine learning will be the main driver of the Fourth Industrial Revolution and will significantly impact and benefit global industry and economy. Applications in manufacturing are a promising area for South Korea to concentrate its resources. South Korea's IT infrastructure and manufacturing-based industries will require further development and involvement of machine learning to successfully integrate artificial intelligence into the manufacturing sector. To apply machine learning into South Korean manufacturing companies, a strong workforce comprised of data scientists is required. To train them, the South Korean government and industry should partner with US academic institutions and develop data science initiative programs to train South Korean students.

RECOMMENDATIONS FOR INCREASED COOPERATION

The South Korean government has the opportunity to boost the application of artificial intelligence technology into a wider range of industries, including the manufacturing sector. The following recommendations are aimed at encouraging cooperation between the United States and South Korea in the next one to two years.

Recommendation 1: The United States and South Korea should collaborate on AI by hosting annual technical forums between US data scientists and South Korean industry leaders and by soliciting support from the South Korean government to engage in cooperative projects with the United States. Inviting actively working data scientists from the United States to South Korea annually or even more frequently would allow data scientists to present their current work to South Korean industry leaders. South Korea would benefit from the lessons learned and knowledge shared by the US scientists. Furthermore, South Korea's government should support cooperative projects that focus on involving US-developed AI in South Korean industry.

Recommendation 2: South Korea's government should provide funding to US research centers specifically to develop AI algorithms for use in South Korean industry. South Korea's government should propose projects to US academic institutions that develop advanced AI algorithms. In getting funding from South Korea, US research centers would then be obligated to

share the research on algorithms with South Korea's industry leaders.

Recommendation 3: South Korea's government should host an AI algorithm competition. A competition based on artificial intelligence is one way South Korea could encourage and develop new AI algorithms. One such example was the Netflix Prize, which is "an open competition for the best collaborative filtering algorithm to predict user ratings for films, based on previous ratings without any other information about the users or films."[13] Another example is the Kaggle competition, in which companies and researchers post data and statisticians and data miners attempt to produce the best models for predicting and analyzing the data. Following these US examples, South Korea's government should host an annual AI algorithm competition. Possible topics could include the application of AI algorithms to the sectors in which South Korea wants to apply AI, or areas in which there are AI needs in South Korean industry. Through the competition, new creative algorithms could be generated for South Korea. Furthermore, this competition would put South Korea on the map within the worldwide data science community.

Recommendation 4: South Korea should invest in strengthening its data scientist workforce by creating data science initiatives modeled after those in the United States. Data scientists are needed to use and deploy AI technology in South Korean industry. Although South Korea's private sector companies want to apply AI in their systems, there are few data scientists working in the country. Sending South Korean students to DSIs in the United States could be a short-term solution while the South Korean government invests in building its own DSIs. Some US lecturers or South Korean data scientists who are currently working in the United States may be invited to South Korea to teach, facilitating cooperation and collaboration between the two countries.

Recommendation 5: The importance of teaching coding skills from an early age has been a tenet in South Korea for several years. South Korea should build a program that allows for promising students to learn basic and introductory-level computer coding concepts. Such programs already exist in the United States and many platforms are available to train students from young ages. By developing this skill set in the next-generation workforce, South Korea could secure its status as a leader in AI technology and as an economic power.

---

13 Reid Johnson, "Advanced Recommendations with Collaborative Filtering," University of Notre Dame, accessed January 18, 2018, https://www3.nd.edu/~rjohns15/cse40647.sp14/www/content/lectures/36%20-%20Recommendation%202.pdf.

PART II

BUILDING A SMART PARTNERSHIP FOR BIOTECHNOLOGY

CHAPTER 3

ENSURING BIOSAFETY AND SECURITY

Dr. Gigi Kwik Gronvall

Senior Scholar, Johns Hopkins Center for Health Security;
Associate Professor, Johns Hopkins Bloomberg School of Public Health

This chapter illuminates areas where cooperation between the Republic of Korea (hereafter South Korea) and the United States may be expanded in the area of advanced biotechnologies. To frame opportunities for future cooperation involving the public and private sectors, this chapter provides an overview of some of the dramatic and rapid changes happening in the biological sciences. These changes open many possible political, economic, technical, and legal issues worthy of continued discussion and collaboration between the United States and South Korea, which are briefly described. Finally, this chapter offers options and recommendations for implementing enhanced cooperation in advanced biotechnologies for policy makers and experts in South Korea and the United States to pursue.

UNFOLDING TRENDS

Biology is becoming industrialized, economically powerful, and diverse. As part of the Fourth Industrial Revolution, "economically and strategically important industries are increasingly relying on biological manufacturing processes for fuel, agriculture, medicines, and products that traditionally have been made using chemistry."[1] Biological processes are already incorporated into commercial products, including tires, adhesives, flavorings, construction materials, and specialized chemicals, in addition to long-standing biological processing applications in medicine (particularly biologics and vaccines) and agriculture.[2]

Just as steam engines and computers heralded the beginning of new technological ages, the industrialization of biology, "has major implications in terms of sources for precursor materials, availability of critical pharmaceutical drugs, global accessibility of powerful technologies," and national and international security.[3] There are, necessarily, additional regulatory con-

1 National Research Council, *Industrialization of Biology: A Roadmap to Accelerate the Advanced Manufacturing of Chemicals* (Washington, DC: The National Academies Press, 2015).

2 ETC Group, *Case Study: Vanilla and Synthetic Biology*, July 3, 2013, http://www.etcgroup.org/sites/www.etcgroup.org/files/Vanilla_SynBio_case_study_Oct2013.pdf.

3 Gigi Kwik Gronvall, Ryan Morhard, Kunal Rambhia, Anita Cicero, and Tom Inglesby, *The Industrialization of Biology and Its Impact on Na-*

trols on medicines and medical therapies compared with nonmedical applications including agriculture, so nonmedical biotechnology applications should proceed at a faster pace, and medical advances may take more time to become accessible. There are also several technical barriers, such as new software developments and an increasing difficulty in managing and organizing large datasets, that could hinder the pace of biotechnology industrialization.[4] Moreover, certain economic factors may limit use of biotechnology applications, particularly biofuels, when the price of oil is low.[5] However, these mitigating issues are likely to diminish the pace, but not the ultimate outcome, of biological industrialization.[6]

As biotechnology continues to mature, it will enable individuals and small groups to develop powerful applications, challenging societal norms. Biological tools and services are more potent and accurate than ever before, and available at rapidly declining costs.[7] The power of biotechnology will be expressed in positive and negative ways, but even in beneficial applications there are likely to be social and ethical challenges associated with their use. For example, some people may use gene editing to make genetic changes that might not be medically necessary; this will be unacceptable to some, who will not be comfortable with "designer babies." Another potential social and ethical problem could occur if a genetic edit is found to be medically beneficial, but not everyone who needs it will have access to that intervention.

One new biotechnology that is raising social and ethical issues is a powerful and relatively recently developed gene-editing tool called CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats).[8] CRISPR/Cas9 allows sections of DNA to be cut and pasted, like how words can be crafted and moved around in a Microsoft Word document. It has been an immensely powerful tool for research discovery, and offers a potential therapy for genetically inherited diseases, such as Huntington's or Beta-thalassemia.[9] Germline modifications (which enable changes to be inherited) through medicinal applications of CRISPR have been demonstrated in the laboratory, and the possibility of a treatment for inherited diseases is likely to spur rapid development regardless of some critics' ethical objections.[10] If the technologies prove to be life-changing and positive, a normative shift is likely to occur so that the technologies will be promulgated and improved upon.

Advanced biotechnology tools could potentially be used to further public health on a grand scale. For example, scientists could theoretically use CRISPR to create a gene drive (which forces the broad inheritance of a specific gene or set of genes) to eliminate malaria-carrying mosquitoes within a geographical region.[11] This advance could have tremendous positive public health consequences, but it also has the potential for accidental and unintended effects beyond its target, necessitating careful planning and research.[12]

The increased power of biological techniques can also be used to inflict deliberate harm, and this power is now more concentrated in the hands of individuals, versus nation states. While advanced biotechnologies are a concern for biodefense, the simple, unfortunate truth is that the development of biological weapons does not require modern biotechnologies. The technologies that were available to large, sophisticated, and now-defunct nation-state biological weapons programs in the 1960s are still available. But the laboratory methods used in those old programs are more accessible, take less time, and are cheaper. The basic starting materials for the weaponization of biology—pathogens that affect humans—are found in nature, laboratories, and sick people all over the world.[13]

---

tional Security, Center for Biosecurity of UPMC, June 8, 2012, http://www.upmchealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2012/2012-06-08-industrialization.pdf.

4 Ibid.

5 Roberta Kwok, "Five Hard Truths for Synthetic Biology: Can Engineering Approaches Tame the Complexity of Living Systems?" *Nature* 463, no. 7279 (2010): 288-90.

6 Kwik Gronvall, Morhard, Rambhia, Cicero, and Inglesby, *The Industrialization of Biology and Its Impact on National Security*.

7 Robert Carlson, "Estimating the Biotech Sector's Contribution to the US Economy," *Nature Biotechnology* 34, no. 3 (2016): 247-55.

8 A. V. Wright, J. K. Nunez, and J. A. Doudna, "Biology and Applications of CRISPR Systems: Harnessing Nature's Toolbox for Genome Engineering," *Cell* 164, no. 1-2 (Jan 14, 2016): 29-44.

9 D. Baltimore, P. Berg, M. Botchan, D. Carroll, R. A. Charo, G. Church, J. E. Corn, et al., "Biotechnology. A Prudent Path forward for Genomic Engineering and Germline Gene Modification," *Science* 348, no. 6230 (April 3, 2015): 36-8.

10 K. S. Bosley, M. Botchan, A. L. Bredenoord, D. Carroll, R. A. Charo, E. Charpentier, R. Cohen, et al., "CRISPR Germline Engineering—the Community Speaks," *Nature Biotechnology* 33, no. 5 (May 2015): 478-86.

11 Elizabeth Pennisi, "Gene Drive Turns Insects into Malaria Fighters," *Science* 350, no. 6264 (November 23, 2015): 1014.

12 National Academies of Sciences, Engineering, and Medicine, *Gene Drives on the Horizon: Advancing Science, Navigating Uncertainty, and Aligning Research with Public Values* (Washington, DC: The National Academies Press, 2016).

13 K. J. Rambhia, A. S. Ribner, and G. K. Gronvall, "Everywhere You Look: Select Agent Pathogens," *Biosecurity and Bioterrorism: Biodefense*

Gene-editing technologies were included in the annual worldwide threat assessment report of the US intelligence community.

The technologies and methods to cultivate and weaponize a variety of pathogens are widely accessible because they overlap considerably with non-bioweapons methods and technologies, which are actively pursued for beneficial purposes. In other words, these are dual-use technologies pursued for important and legitimate purposes. Even though there are many less-sophisticated methods that could be used to make a biological weapon, the possibility that advanced biotechnologies could be used for weapons development should be a concern for several reasons: first, because they could be used to increase the types and accessibility of biological weapons that are not available using more conventional microbiological methods; and second, because the barriers to making biological weapons are lowered as biological tools become more accessible and powerful.

Using gene-synthesis technologies, it would not be necessary to isolate a pathogen from an environmental sample or from a sick patient before developing it as a weapon. The ability to recreate a pathogen without this harvesting step and to make it "from scratch" could also allow the weaponization of eradicated or difficult-to-access pathogens such as smallpox. The accessibility and democratization of biology will require a multipronged approach to prevent, detect, and respond to misuse.

There are other possibilities for misuse besides recreation of a pathogen. Experts have been concerned that gene-editing techniques such as CRISPR could be used to make an already dangerous pathogen worse, by making it more difficult to detect, prevent, or treat. Gene-editing technologies were even included in the annual worldwide threat assessment report of the US intelligence community in 2016 as a potential national security threat.[14] One current attempt to think holistically about the security threats inherent in advances in synthetic biology, and to appropriately evaluate these emerging technologies, is being pursued in an ongoing National Academies study.[15]

POLICY ISSUES AND STRATEGIC IMPLICATIONS

The importance of medicine and public health is a common thread running through the considerations of biotechnology advances, as well as the protection from misuse of advanced biotechnology. Without high standards for public health, the devastation can be immense: the Ebola crisis in West Africa in 2014-15 killed more than eleven thousand people.[16] It devastated the already strained economies of Guinea, Sierra Leone, and Liberia, and cost the US government $5.5 billion in its response.[17]

To try to prevent such a catastrophe from happening again, South Korea and the United States have partnered, along with fifty-seven other nations, on the Global Health Security Agenda (GHSA).[18] Launched in 2014, the GHSA aims "to advance a world safe and secure from infectious disease threats [and] bring together nations from all over the world to make new, concrete commitments" to increasing the standards for public health, elevating global health security to an international platform, and raising health security as a political issue deserving of the attention of government officials, not just health leaders.[19] South Korea has taken a leadership role in the GHSA, serving as the secretariat in 2017, and hosting one of the major meetings of GHSA members. The ability to detect disease, provide

Strategy, Practice, and Science 9, no. 1 (March 2011): 69-71.

14 James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community,* Senate Armed Services Committee, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

15 National Academies of Sciences, Engineering, and Medicine, *A Proposed Framework for Identifying Potential Biodefense Vulnerabilities Posed by Synthetic Biology: Interim Report* (Washington, DC: The National Academies Press, 2017).

16 World Health Organization, "Ebola Situation Report - 16 March 2016," *World Health Organization*, March 16, 2016, http://apps.who.int/ebola/current-situation/ebola-situation-report-16-march-2016.

17 C. Boddie, "Federal Funding in Support of Ebola Medical Countermeasures R&D," *Health Security* 13, no. 1 (January-February 2015): 3-8.

18 Lisa Monaco, "Making the World Safer from Pandemic Threats: A New Agenda for Global Health Security," February 13, 2014, https://obamawhitehouse.archives.gov/blog/2014/02/13/making-world-safer-pandemic-threats-new-agenda-global-health-security.

19 "About," Global Health Security Agenda, accessed January 19, 2018, https://www.ghsagenda.org/about.

medical countermeasures such as vaccines and therapeutics, and give appropriate medical care has been a strength for South Korea and for the United States, and an area where advances in biotechnology can lead to vast improvements.

The development and regulation of pharmaceuticals is another area of intense interest in South Korea and the United States. Advances in biotechnology are changing the pace and progress of introducing new pharmaceutical products—though, in an industry that is understandably heavily regulated, these changes may be slower than are occurring in other sectors. Advances in biotechnology should also improve the regulatory tools that can be applied to assess the efficacy and safety of new products.[20] This is an area where collaboration and standard setting can benefit the actors of the government and private sector, as some concerns may require governmental actions to level regulatory burdens as well as to promote innovation.

Ethical and legal issues also permeate biotechnology, and have for many decades. The most persistent concern about morality and ethics in the biological sciences is whether scientists are "playing God."[21] Such accusations of scientific hubris and overreach may be inevitable, and advances in biotechnology, particularly synthetic biology, seem suited to drawing that concern. In fact, one research objective in the synthetic biology field aims to mimic and better understand the conditions that sparked life on earth—to then ultimately create new life.[22] George Church, a Harvard professor and leading synthetic biology pioneer, wrote "[a]ny technology that can accomplish such feats—taking us back into a primeval era when mammoths and Neanderthals roamed the earth—is one of unprecedented power. Genomic technologies will permit us to replay scenes from our evolutionary past and take evolution to places where it has never gone, and where it would probably never go if left to its own devices."[23] As such, it is a fruitful area for collaboration and discussion for South Korea and the United States to develop agreements about how best to proceed in new, potentially problematic areas of science to determine what can be done to minimize ethical challenges, and to establish common norms.

There are some areas of biotechnology that are controversial due to their potential to be dual use, that is, to be used for both beneficial purposes and biological weapons development. Indeed, "the biological sciences are inherently dual use, so a great deal of the scientific knowledge, materials, and techniques required for legitimate, beneficent biological research could be misused to make a biological weapon. Laboratory research conducted to uncover critical information about how a pathogen manipulates the human immune system to cause disease could be exploited to make a disease harder to treat."[24] Complicating the problem further, the scientific community relies on open access to publications, genetic sequences, and biological materials to advance science and, importantly, to reproduce the results of others to verify gains and build on them.

The United States (through a federal advisory board, the National Science Advisory Board for Biosecurity) has codified dual-use research of concern (known as DURC) as "life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security."[25] However, describing the problem of DURC is easier than lowering the potential risks that may stem from it. Over the past fifteen years, numerous legitimate and informative biological studies have fallen into the DURC category, raising security questions and dividing the opinions of scientists, ethicists, and policy makers on whether the research should have been performed or published.

---

20 Margaret A. Hamburg, "Advancing Regulatory Science," *Science* 331, no. 6020 (2011): 987.

21 Nicolas Dragojlovic and Edna Einsiedel, "Playing God or Just Unnatural? Religious Beliefs and Approval of Synthetic Biology," *Public Understanding of Science* 22, no. 7 (October 1, 2013): 869-85.

22 Fazale Rana, *Creating Life in the Lab: How New Discoveries in Synthetic Biology Make a Case for the Creator* (Grand Rapids, Michigan: Baker Books, 2011).

23 George M. Church and Ed Regis, *Regenesis: How Synthetic Biology Will Reinvent Nature and Ourselves* (New York: Basic Books, April 8, 2014).

24 Gigi Kwik Gronvall, "Chapter 4: Responsible Stewardship of Powerful Biotechnologies," in *Preparing for Bioterrorism: The Alfred P. Sloan Foundation's Leadership in Biosecurity* (Baltimore: Center for Biosecurity of UPMC, December 4, 2012), http://www.upmchealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2012/sloan_book/CH-04_Responsible%20Stewardship_Preparing%20for%20Bioterrorism_Dec2012.pdf.

25 US Government, "United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern," Assistant Secretary for Preparedness and Response, March 2012, https://www.phe.gov/s3/dualuse/Pages/USGOversightPolicy.aspx.

The possibility for negative consequences that result from a biosafety lapse needs to be examined, planned for, and mitigated.

One recent example is research work done to determine if avian influenza (H5N1) could be made more transmissible between humans.[26] This work was performed to determine what genetic changes are required for transmissibility. Once those genetic changes are found experimentally, they would be important to look for when performing public health surveillance of new, emerging influenza strains. Another more recent example is the synthesis of horsepox virus, a close cousin to smallpox, a virus that has been eradicated from the natural world.[27] According to the researchers, the work was performed for a variety of reasons, including to develop a smallpox vaccine with fewer adverse reactions and to develop an oncolytic (cancer) vaccine platform.

Part of the difficulty in overseeing DURC is that control measures would highly depend on how likely the information is to be misused by nefarious actors. It is hard to know, without an unlikely and specific degree of insight into the minds and plans of would-be bioterrorists, just how useful a scientific insight or series of papers is likely to be. The tremendous volume of information that could be considered dual use increases the challenge of acting on this information to benefit security. The conversation about how to control this information and still promote biotechnology advances is ongoing, will likely be tied to the specifics of individual cases of dual-use research of concern, and will require international dialogue. Multiple international efforts in this area, which could be looked to for examples of collaboration between South Korea and the United States, are in progress.[28]

Biotechnology advances also raise concerns about laboratory safety and the safety aspects of the democratization of science. To date, while there have been notable safety failures in research laboratories, advanced biotechnology and synthetic biology have not been directly associated with any accidents. However, the possibility for negative consequences that result from a biosafety lapse with these powerful tools needs to be examined, planned for, and mitigated.

There are several main categories for safety concerns about advanced biotechnologies. The first category involves "outside the laboratory" concerns, which is an issue with synthetic biology, as some applications require synthetic organisms to be deliberately released into the environment. Applications that fall into this category include mosquito control, agriculture, pollution remediation, mining, biofuels, medications, and even the recreation of extinct animals, such as wooly mammoths.[29] These endeavors could yield unintended and accidental consequences, especially if biosafety risks are not addressed and carefully thought through, and if experts from multiple areas (e.g., public health, environmental engineering, and agriculture) are not included in the risk analysis.

The second concern for safety relates to the experience level of scientists and others who work in a laboratory—including amateurs—with biosafety and basic principles of containment. The do-it-yourself Bio (DIY Bio) movement has grown: There are more than 4,400 subscribers to an online forum, where DIY Bio practitioners communicate about their work and arrange to meet up with other "bio-hackers" in their communities.[30] Many of the DIY Bio activities are expressly educational, fun, and proactive about safety for practitioners. In fact, the organization DIYbio.org was created in 2008 to establish a "vibrant, productive and safe

26 Gigi Kwik Gronvall, *H5N1: A Case Study for Dual-Use Research*, Council on Foreign Relations, July 15, 2013, https://www.cfr.org/report/h5n1.

27 Diane DiEuliis, Kavita Berger, and Gigi Kwik Gronvall, "Biosecurity Implications for the Synthesis of Horsepox, an Orthopoxvirus," *Health Security* 15, no. 6 (November-December 2017): 629-37.

28 National Academy of Engineering and National Research Council, *Positioning Synthetic Biology to Meet the Challenges of the 21st Century: Summary Report of a Six Academies Symposium Series* (Washington, DC: The National Academies Press, 2013).

29 Jackson Landers, "Can Scientists Bring Mammoths Back to Life by Cloning?" *Washington Post*, February 9, 2015, https://www.washingtonpost.com/national/health-science/can-scientists-bring-mammoths-back-to-life-by-cloning/2015/02/06/2a825c8c-80ae-11e4-81fd-8c4814dfa9d7_story.html.

30 "An Institution for the Do-It-Yourself Biologist," DIYbio.org, accessed November 29, 2017, https://diybio.org/.

A laboratory at the University of Maryland's BioPark. *Photo credit*: Maryland GovPics/Flickr.

community of DIY biologists."[31] Yet, while most DIY Bio projects are not sophisticated, the tools to do advanced work are accessible: For about $150, an amateur can purchase a gene-editing kit featuring CRISPR—the technology that is revolutionizing the biosciences right now and is only a few years old.[32]

The final category of biosafety concern for advanced biotechnologies is a general worry about the power of biotechnology, and what could go wrong. Because of the increased access to powerful technologies to more laboratories and amateurs in the world, consequential bio-errors may occur more frequently. If an accident occurs with a transmissible pathogen, the damaging effects of an accident could spread well beyond the laboratory. While some technical, policy, and regulatory steps have been taken to address each of these concerns, much more remains to be done to mitigate biosafety risks to minimize harm to people, animals, and the environment.

CONCLUSION

The advent of the biotechnology age underscores the importance of scientific, policy, and diplomatic collaboration between nations. The United States and South Korea are two technology leaders in the biotechnology space, with a substantial number of institutions dedicated to making biotechnology progress within medicine, agriculture, chemical compounds, and basic research; there are numerous private sector institutions that are likewise engaged in collaborations between the United States and South Korea. There have been diplomatic conversations about expanded collaborations in biotechnology, beyond what is currently in place. Given the diversity of technical, ethical, legal, commercial, standards-setting, and safety issues that are brought about due to biotechnology advances, there are many opportunities for the United States and South Korea to collaborate and make progress in safely ushering in the biotechnology age.

31 Ibid.

32 "Trending Now," The Odin, accessed January 19, 2018, http://www.the-odin.com/.

RECOMMENDATIONS FOR INCREASED COOPERATION

The United States and South Korea should expand their security cooperation in biotechnology in the areas of global health, gene synthesis, and medical and pharmaceutical research.

There is an opportunity to expand security cooperation between the United States and South Korea on issues related to biotechnology, to focus on both deliberate and natural biological threats. The United States and South Korea have been demonstrated leaders in taking on the challenges of disease threats. They have participated in biosecurity scenarios (e.g., Able Response, a whole-of government exercise); both countries contributed resources and considerable financial assistance to end the Ebola epidemic in West Africa; and they participate in the Global Health Security Agenda, which aims to reduce global disease risks and supports the International Health Regulations (2005).

Boosting the security quotient of the Global Health Security Agenda. Since its inception in 2014, the GHSA has incorporated a multilateral and multisectoral approach towards strengthening global capacity and nations' abilities to prevent, detect, and adequately respond to infectious diseases.[33] The Ebola epidemic demonstrated how a lack of adequate public health infrastructure could lead to an international crisis, in spite of the International Health Regulations (2005), which call for nations to provide for adequate public health infrastructure. To date, the GHSA has focused on self-assessments (called Joint External Evaluations, or JEE) and there is an opportunity to focus donor country attention where it is most needed.

An unusual aspect of the GHSA—for an initiative that is largely focused on public health—is that from its inception it has included the need to prepare for deliberate threats. Nonetheless, this aspect of the GHSA has not moved forward as much as was initially hoped; while some nations include their departments of defense in GHSA activities, most do not, and in the JEE, biosafety and biosecurity are somewhat mixed together. There is an opportunity for South Korea and the United States to collaborate on efforts that encourage more countries to take a more multisectoral approach through a variety of means, such as holding military-military conferences with other nations from Southeast Asia or developing a JEE supplement with a military focus.

Biosecurity implications of gene synthesis. In the field of biotechnology, DNA synthesis is a valuable research tool for many applications—from medicine to manufacturing—but as with many powerful technologies, it is vulnerable to misuse. One common fear is that DNA synthesis technologies could be used by nefarious actors to procure the genetic material of a variety of pathogens from a commercial supplier, or acquire the capability to do that themselves.[34] Once synthesized, the genetic material could be "booted up" like a computer program, becoming actively infectious. "That many viruses can be made from scratch has been demonstrated repeatedly, including in the construction of poliovirus, 1918 influenza virus, and most recently, the virus that causes horsepox," which is a close cousin to the smallpox virus.[35]

Over the past decade, measures have been taken to reduce the likelihood of misuse.[36] Several gene-synthesis commercial suppliers formed the International Gene Synthesis Consortium to develop protocols designed to allow "individual companies to screen ordered sequences as well as to verify customers."[37] Not all international gene-synthesis companies are members of an industry organization that agrees to either customer screening or sequence screening. There are opportunities for the United States and South Korea to encourage other nations to promote industry-wide screening standards, champion a common code of conduct for suppliers of DNA, and develop mechanisms so that more of the gene-synthesis market performs screening, and has a place to report suspicious orders. There is also the potential for research in this area, as there is no publicly available data about how valuable the sequence screening can be in stopping misuse, or whether screening could be improved.[38]

---

33 "Global Health Security: About Us," Centers for Disease Control and Prevention, May 12, 2017, https://www.cdc.gov/globalhealth/healthprotection/ghs/about.html.

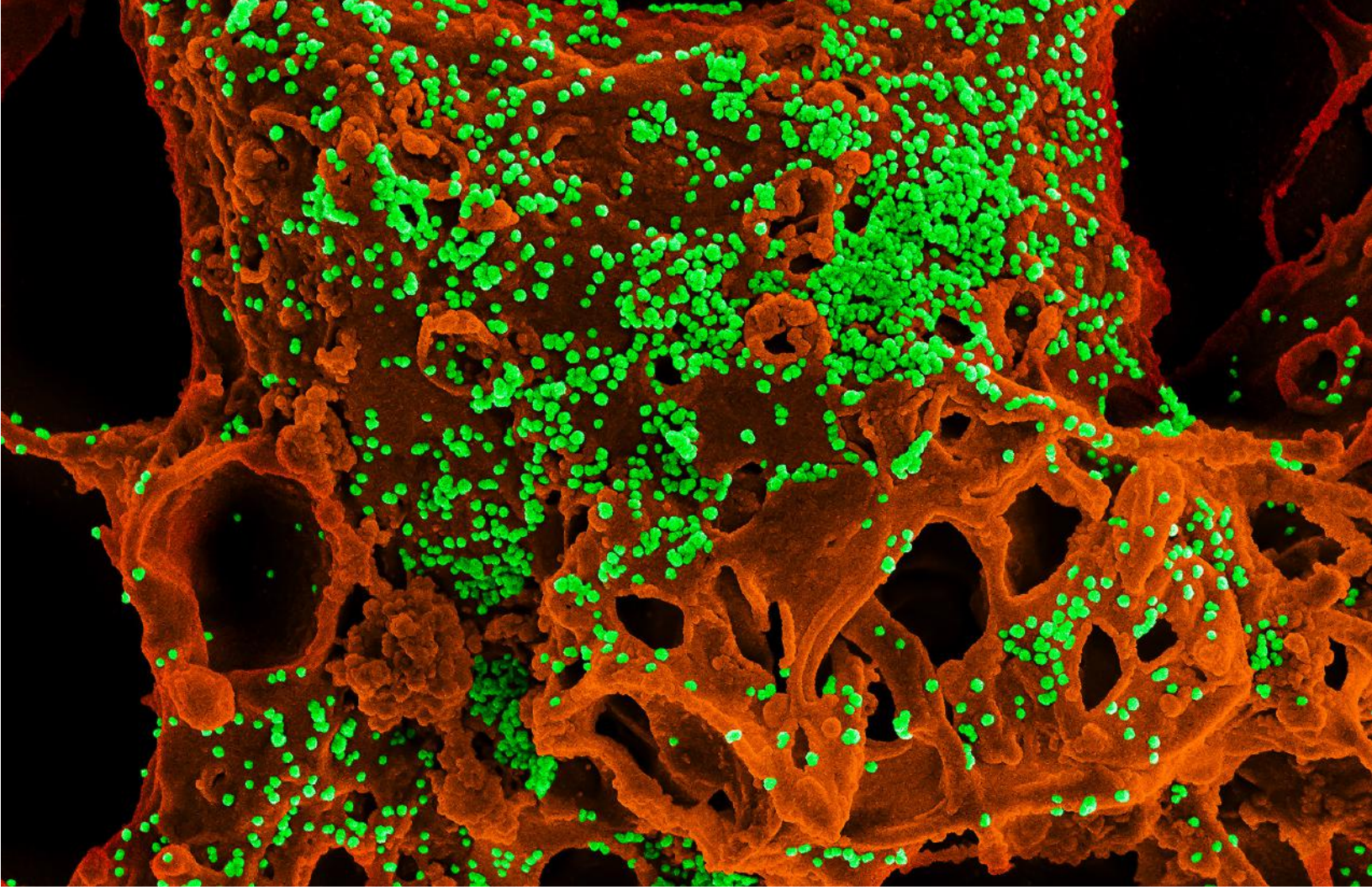
34 Diane DiEuliis, Sarah R. Carter, and Gigi Kwik Gronvall, "Options for Synthetic DNA Order Screening, Revisited," *mSphere* 2, no. 4 (2017), https://doi.org/10.1128/mSphere.00319-17.

35 Ibid.

36 S. R. Carter and R. M. Friedman, *DNA Synthesis and Biosecurity: Lessons Learned and Options for the Future*, J. Craig Venter Institute, October 2015, http://www.jcvi.org/cms/fileadmin/site/research/projects/dna-synthesis-biosecurity-report/report-complete.pdf.

37 DiEuliis, Carter, and Kwik Gronvall, "Options for Synthetic DNA Order Screening, Revisited."

38 Ibid.



The Middle East respiratory syndrome coronavirus (MERS-CoV). *Photo credit*: NIH Image Gallery/Flickr.

Advanced development of pharmaceuticals and other medical countermeasures. There is a memorandum of understanding (MOU) between the US Department of Health and Human Services, US National Institutes of Health, South Korea's Ministry of Health and Welfare, and the Korea National Institute of Health in which all parties "signed a letter of intent (2015) to enhance biomedical research collaboration, personnel exchange and training cooperation in fields of mutual interest."[39] This can be applied towards the development of vaccines and therapies for biosecurity and health security concerns, from early research and development stages through manufacturing.

For example, there could be joint research projects and funding streams to study a virus that is of mutual concern to the United States and South Korea. Middle East respiratory syndrome coronavirus (MERS-CoV), a respiratory virus that caused a serious outbreak in South Korea in 2015, could be a suitable candidate. Under the MOU, multiple vaccine candidates could be tested in a collaborative fashion, or research tools to help advance MERS-CoV research could be developed and jointly shared between the United States and South Korea.

South Korea and the United States should collaborate to advance the safety of biotechnology, provide needed data about how scientific work in the biological sciences can be made as safe as possible, and maintain global leadership in safety.

Products are not used if they are not trusted by consumers, and the biotechnology/biomedical enterprise will not have the broad support it requires for advanced development if safety is not given a high priority.

Safety standards and consensus for specific areas of advanced biotechnology. There are many applications of advanced biotechnology that challenge existing norms and regulations. For example, synthetic organisms could be deliberately released into the environment for specific purposes, such as environmental remediation to clean up waste, for mining, or as an indicator for soil conditions. A mosquito that has a gene drive (i.e., a genetic mechanism that allows all progeny to inherit a specific gene, versus the 50 percent inheri-

39 "Joint Fact Sheet: The United States-Republic of Korea Alliance: Shared Values, New Frontiers," The White House, October 16, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new.

tance that would be typical) could be used to make the mosquito population less able to carry malaria and other diseases. Germline editing could be used to remove the certainty of inheriting a genetic disease. In these cases, there is the potential for tremendous benefits, and there is the possibility for technical collaborations between the United States and South Korea. However, the safety standards for these new applications are still in flux, and should be a focus of collaboration. For example, in what manner should mosquitoes be tested in controlled conditions, and for how long, before there accrues reasonable evidence that the changes to the mosquito population will not spill over to other life forms, once released.

In the agriculture sector, there is a need to apply consensus safety standards as well. Even the perception of a safety lapse could be damaging to an industry that is heavily capitalized and of intrinsic national security importance to both South Korea and the United States. The genetically modified organisms (GMO) debate and controversies over Monsanto—an agriculture-supply company that is the focus of anti-GMO sentiment—should be a cautionary tale.[40] A technology and policy dialogue that focuses on these issues could provide an opportunity for South Korea and the United States to avoid earlier mistakes and promulgate the safe development of agricultural biotechnology.

Collaborative research that increases the safety of advanced biotechnology. One approach to increasing containment of synthetic organisms outside the laboratory is called "intrinsic" biosafety—that is, the biosafety is built into the organism, so that the synthetic organisms cannot escape boundaries that are set for them.[41] Some forms of intrinsic biosafety involve engineering organisms so that they are not able to survive without specific human intervention, such as by supplying a nutrient that is essential for life. If the nutrient is not supplied, the synthetic organism will die, and it will stay "contained" in the area where that essential nutrient is supplied. Early attempts to develop intrinsic biosafety often had a single point of failure, so they often failed, which led to the organism's escape from containment. Newer intrinsic biosafety approaches are subtler and rely on combinatorial complexity to increase containment. Future efforts to increase intrinsic biosafety may involve non-natural coding—called "orthogonal" approaches—which either use artificial genetic languages (no A, C, G, or T) or require nutrients not found in nature.[42]

When it comes to safety, there is unfortunately little commercial imperative to pursue it, unless it is a funding priority for national governments or a regulatory requirement. While the private sector would need to be involved in this effort, a joint initiative between the United States and South Korea could provide the structure, timeline, and political importance to the work that is required to get these safety standards achieved.

South Korea and the United States should collaborate to remove barriers that stand in the way of biotechnology industrialization.

Multiple barriers threaten to impede advances in biotechnology. The first challenge is the requirement for storing massive amounts of biological information; data centers consume an enormous amount of electricity. While the internet giants (e.g., Facebook and Google) have made significant strides in adopting more energy-efficient software, smaller private firms and government research agencies have not typically invested in updates.[43] There is an opportunity to boost the efficiency of these biotechnology-centered research agencies' use of data centers.

A second challenge involves developing software solutions that can effectively manipulate such large amounts of biological data. While the cloud may include an almost infinite amount of data storage and processing potential, the software infrastructure may not be advanced enough to capitalize on processing capability.

Thirdly, "information for bioinformatics analysis needs to be in a computable form, but often it is not."[44] For medical diagnostics, health records, genetic analysis, and environmental monitoring to continue to ad-

40 Ronald J. Herring, "Opposition to Transgenic Technologies: Ideology, Interests and Collective Action Frames," *Nature Reviews Genetics* 9, no. 6 (2008): 458-63.

41 Radha Krishnakumar, "Intrinsic Biocontainment: State of the Science and Future Possibilities" (presented paper, SB 6.0: The Sixth International Meeting on Synthetic Biology, Imperial College, London, England, 2013).

42 Y. Cai, N. Agmon, W. J. Choi, A. Ubide, G. Stracquadanio, K. Caravelli, H. Hao, J. S. Bader, and J. D. Boeke, "Intrinsic Biocontainment: Multiplex Genome Safeguards Combine Transcriptional and Recombinational Control of Essential Yeast Genes," *Proceedings of the National Academy of Sciences of the United States of America* 112, no. 6 (February 10, 2015): 1803-8.

43 Rekha Nachiappan, Bahman Javadi, Rodrigo N. Calheiros, and Kenan M. Matawie, "Cloud Storage Reliability for Big Data Applications: A State of the Art Survey," *Journal of Network and Computer Applications* 97 (2017): 35-47.

44 National Research Council, *Industrialization of Biology: A Roadmap to Accelerate the Advanced Manufacturing of Chemicals* (Washington, DC: The National Academies Press, 2015), 6.

vance and become more medically useful for future patient care, there will also need to be more investment in making the data amenable to processing. The United States and South Korea could collaborate in addressing nonbiotechnology barriers to more productive biotechnology, including developing a list of best practices.

South Korea and the United States should examine their competitiveness in relation to the future of biotechnology, and boost bilateral cooperation in the training of scientific researchers as appropriate.

It will be important to examine whether both nations are well positioned to take advantage of the opportunities that biotechnologies can offer, or if they risk falling behind as new technologies develop. The United States and South Korea are currently leaders in biotechnology, but there will be much more intense competition in the future. Instead of a clear national leader, there will be multiple leaders.[45] Furthering cooperation and collaboration with traditional mechanisms of workforce development, training opportunities, and innovative project development could help both nations boost their competitiveness in the biotechnology arena. For example, the United States and South Korea could develop innovative mechanisms to not only further the training of researchers, but provide "executive education" for researchers in related fields, promote cross-fertilization of fields, and help already trained researchers transition into areas where interest is high, and funding is more plentiful. The United States and South Korea should launch, as part of a high-level political process, a work program to train their workforces in advanced biotechnologies and laboratory management.

While working with the private sectors of both nations is important, the United States and South Korea also need to focus on areas where the private sector is not able to drive progress and where public sector cooperation could increase possibilities of future productivity. For example, in the process of standard setting, implementing safety measures, technical collaboration on the environmental release of synthetic organisms, and the development of new datasets that can be mined for medical advances, both governments have opportunities to shape the future of biotechnology research. The United States and South Korea should look to existing science and technology cooperation agreements as an important framework for accelerating research and development, and as a starting point to spurring collaboration not only between governmental research centers, but with private industry.

Making progress towards and achieving collaboration between the United States and South Korea can be made through a number of forums and mechanisms.

This chapter highlighted issues that require international collaboration and discussion, versus a specific process to make progress. There are a variety of potential forums, established dialogues, and technical exchange mechanisms that the United States and South Korea could use as these issues are considered. Some possibilities include developing a fusion center, which would create regular interactions on topics related to relevant agencies as well as the private sector; developing an advanced biotechnology track in the Group of Twenty; working through the Organisation for Economic Co-operation and Development; or working through the renegotiation of the United States-South Korea free trade agreement. In any event, the 2016 South Korean Biotechnology Strategy and the ongoing investment in this area by the United States provides opportunities and incentives for collaboration within the governmental and private sectors on these issues.

45 Organisation for Economic Co-operation and Development (OECD), *Emerging Policy Issues in Synthetic Biology* (OECD Publishing, 2014), http://www.oecd-ilibrary.org/science-and-technology/emerging-policy-issues-in-synthetic-biology_9789264208421-en.

CHAPTER 4

HARNESSING CONVERGENT TECHNOLOGIES

Dr. Elizabeth Prescott

Professor of the Practice and Director of Curriculum, Science, Technology, and International Affairs, Walsh School of Foreign Service, Georgetown University

The field of biotechnology—"the manipulation . . . of living organisms or their components to produce useful usually commercial products"[1]—has traditionally been shaped by life scientists focused on the healthcare sector. Biotechnologies, however, are now converging with other emerging technologies, allowing health to be achieved in new ways. The Fourth Industrial Revolution is driving rapid change, magnifying the potential applications of the life sciences while creating complexities in how advanced biotechnologies are used and globally governed. When combined with other technological shifts underway—such as artificial intelligence, machine learning, and the Internet of Things (IoT)—profound changes are occurring in industries not traditionally associated with biotechnology. No longer confined to healthcare, advanced biotechnologies have diverse applications across sectors from energy to agriculture with the potential for tremendous economic impact.

The biotechnology revolution has numerous legal, social, ethical, and governance challenges. Many people already connect with biotechnology products through the formal medical system. However, advanced biotechnologies will increase and change the character of consumer interaction with biotechnology as products become more accessible and affordable, and as individuals expand engagement with do-it-yourself citizen science projects. How people perceive themselves as humans may even change. Ultimately, the obstacles to advanced biotechnologies becoming commonly available are less the technology itself, and more the surrounding factors that allow for the technology to be used and effectively governed.

Despite the challenges, these trends also create opportunities for collaboration between citizens and scientists in the United States and the Republic of Korea (hereafter South Korea). The United States and South Korea are both leaders in biotechnology and other technical areas critical to developing advanced biotechnologies, including information-based technologies. Through deepened collaboration at the bilateral, multilateral, and nongovernment levels, both nations can strengthen their technological capacities, advance

1 "Biotechnology," Merriam-Webster's online dictionary, accessed November 26, 2017, https://www.merriam-webster.com/dictionary/biotechnology.

national goals, provide leadership on global challenges, and build stronger bonds between their citizens. Bilateral and multilateral cooperation on global norms formation, standards setting, codes of conduct, and governance for the development and use of convergent biotechnologies could provide more fluidity between products and customers and strengthen the economic position of both nations. Exchanging best practices for building a stronger ecosystem of entrepreneurship and expanding opportunities for students, scientists, and engineers to work collaboratively on joint pilots and efforts to scale applications could more rapidly bring discoveries to market. The democratization of science and technology resulting from convergent biotechnologies could also catalyze greater interaction between US and South Korean citizens.

UNFOLDING TRENDS

Names for technical revolutions are generally confirmed by historians after the fact. Several terms currently in circulation—the Fourth Industrial Revolution,[2] the Second Machine Age,[3] and Exponential Technologies[4]—attempt to describe the broad technical, social, and economic changes underway. As Thomas Philbeck of the World Economic Forum described in 2016, "Building on the backbone of digital technologies and infrastructure, the emerging dynamics of the Fourth Industrial Revolution involve a convergence of technologies and disciplines, nonlinearity, and a re-emergence of digital into material and physical domains." According to Philbeck, "These changes are having a multi-system impact. New technologies—such as 3-D printing, bioprinting, artificial intelligence, blockchain, virtual reality, and augmented reality—are creating pressures and raising questions about how these technologies should be used."[5]

In the life sciences, this integration of technical disciplines has been referred to as *convergence*. The 2016 Massachusetts Institute of Technology report *Convergence: The Future of Health* summed up the potential impact of convergence:

> The Convergence Revolution promises to enhance quality of life worldwide. Convergence comes as a result of the sharing of methods and ideas by chemists, physicists, computer scientists, engineers, mathematicians, and life scientists across multiple fields and industries. It is the integration of insights and approaches from historically distinct scientific and technological disciplines. Convergence is a broad effort across the sciences that will play a crucial role in many fields of endeavor.[6]

The convergence of fields like biology, materials, information, and engineering provides the greatest opportunity for innovation and will likely result in substantial economic growth. Convergence has the potential to transform healthcare from a system focused on treating disease (Sick Care) to one that optimizes health (Healthcare 2.0). However, this transformation will have significant legal, social, ethical, and governance implications, challenging existing social norms, institutions, and governance mechanisms. Other trends currently unfolding, such as individual empowerment and readily available technologies that are accessible without going through highly trained, expensive gatekeepers, will further magnify these implications.

The graphic on the following page depicts the transition from a healthcare system focused on treating disease to one that optimizes for health enabled by more widely available convergent biotechnologies that are less reliant on going through highly trained, high-cost gatekeepers. The left side—a.k.a. Sick Care—represents selected products and services related to disease treatment in the current healthcare system. Going clockwise from the bottom left, the corners represent treatment, aftercare, prevention, and diagnosis, with the emphasis on treatment within the current system. Prevention (yellow) is largely distinct from the Sick Care system (blue) and primarily undertaken by the individual rather than traditional healthcare providers. The concept of health in a Sick Care system is largely defined by the absence of disease rather than good health and vitality.

---

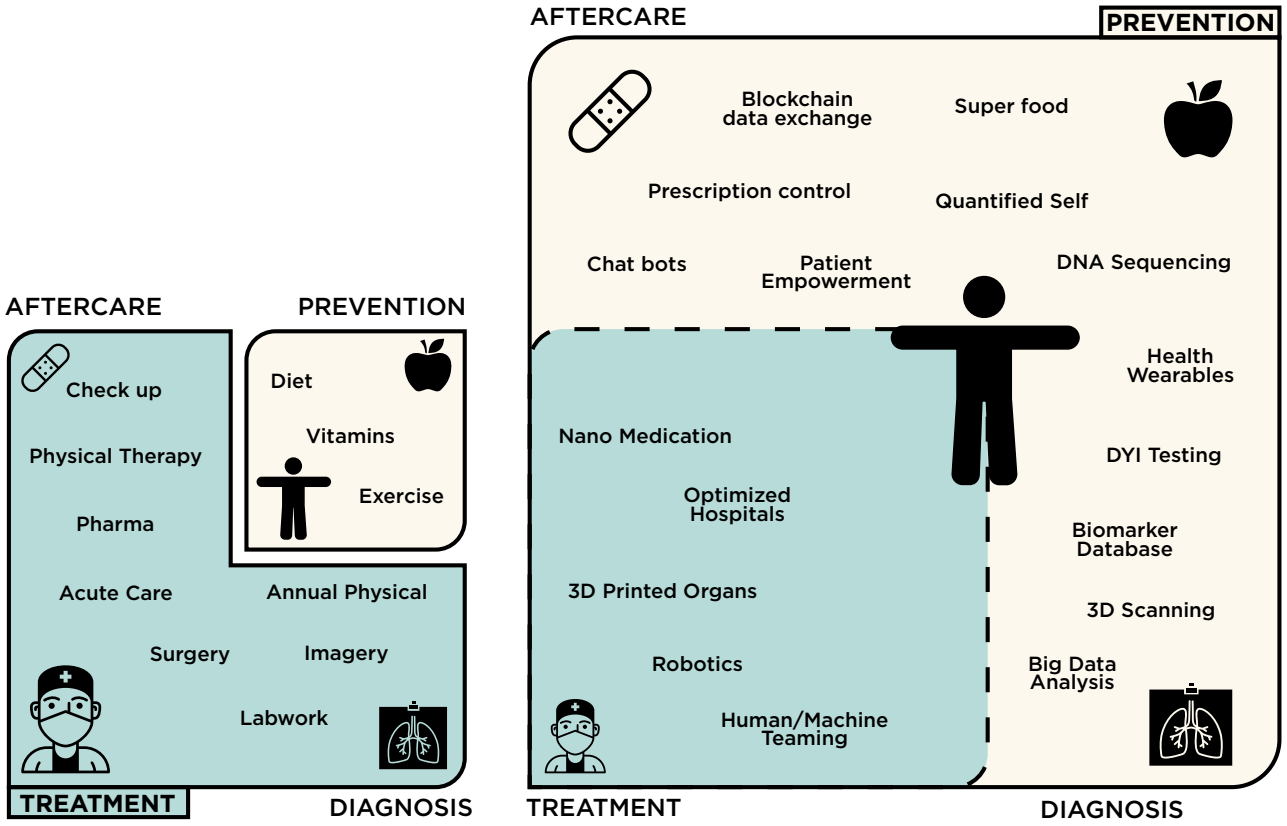
2 Klaus Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond," World Economic Forum, last updated January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

3 Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York: W.W. Norton & Company, 2014), http://secondmachineage.com/.

4 Peter Diamandis and Steven Kotler, *BOLD: How to Go Big, Create Wealth and Impact the World* (New York: Simon & Schuster, 2016), http://www.diamandis.com/bold.

5 National Academies of Sciences, Engineering, and Medicine, *The Fourth Industrial Revolution: Proceedings of a Workshop—in Brief* (Washington, DC: The National Academies Press, 2017), https://www.nap.edu/catalog/24699/the-fourth-industrial-revolution-proceedings-of-a-workshop-in-brief.

6 *Convergence: The Future of Health*, MIT Washington Office, June 2016, http://www.convergencerevolution.net/.



Created by Paul Kumst, Research Assistant. *Image credit*: thenounproject.com.

The right side of the graphic—Healthcare 2.0—depicts a potential future that focuses on improving human health and not just treating disease. Prevention (yellow) is expanded to make for a larger overall system. The boundary with the Sick Care system (blue) becomes more permeable to reflect an increasing number of clinically relevant technologies being made available to the individual. There would still be a need for acute medical care administered by medical practitioners, but their role would change to reflect the increased use of data and analytics, and the ability to intervene prior to the manifestation of disease.

In this convergent future, new healthcare technologies would constantly monitor critical data points and adjust according to an individual's daily routine. In Healthcare 2.0, a technologically empowered individual would be at the center of coordinating their own health optimization, which is more likely to align incentives and encourage actions that better support prevention.

POLICY ISSUES AND STRATEGIC IMPLICATIONS

The snapshot in Box 2 depicts advanced biotechnologies that are technically feasible now or will be in the near future to illustrate their transformational potential on health optimization. Expanded use of convergent biotechnologies could have profound legal, social, and ethical implications that challenge existing institutions and norms but also present unique opportunities for collaboration among individuals and nations, or across sectors of the bioeconomy.

Legal

The heavy reliance on data and analytics in many convergent biotechnologies could undermine existing methods of protecting ownership and regulating the quality of biotechnology products and discoveries. The governance of traditional biomedical products is localized, complex, and heavily influenced by stakeholders

that have substantial interests on the line.[7] In the United States, traditional biomedical products are regulated by the US Food and Drug Administration (FDA) to assure safety and efficacy of the product. Depending on whether the biomedical product is a small-molecule drug,[8] biologic,[9] or device,[10] there are different regulatory criteria. Biomedical product regulation at a global level is mostly derivative of national-level governance, forcing companies to submit approval packages to each market they want to enter. This creates additional costs, delays, and complex business strategies that often involve aggressive intellectual property positions and enforcement.

7 Interests include financial as well as political costs of letting an inferior drug on the market. For example, China executed Zheng Xiaoyu, a former head of the State Food and Drug Administration, in 2007 for accepting bribes to permit drugs on the Chinese market.

8 "Development & Approval Process (Drugs)," US Food and Drug Administration, accessed November 28, 2017, https://www.fda.gov/Drugs/DevelopmentApprovalProcess/default.htm.

9 "Development & Approval Process (CBER)," US Food and Drug Administration, accessed November 28, 2017, https://www.fda.gov/BiologicsBloodVaccines/DevelopmentApprovalProcess/default.htm.

10 "Overview of Device Regulation," US Food and Drug Administration, accessed November 28, 2017, https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm.

BOX 2. A SNAPSHOT OF THE FUTURE: DAILY LIFE IN HEALTHCARE 2.0

Imagine: Your circadian rhythm–linked alarm goes off at a variable time every morning. It is tailored to your body's health needs and your digital assistant's assessment of the time you need to leave for your first meeting. It also factors in the weather, traffic, and likelihood that there will be a line at the coffee shop that has your favorite cheddar scone. Before leaving the house, a small temporary tattoo–like device takes hundreds of health-related measurements of you and automatically analyzes them to provide actionable recommendations.

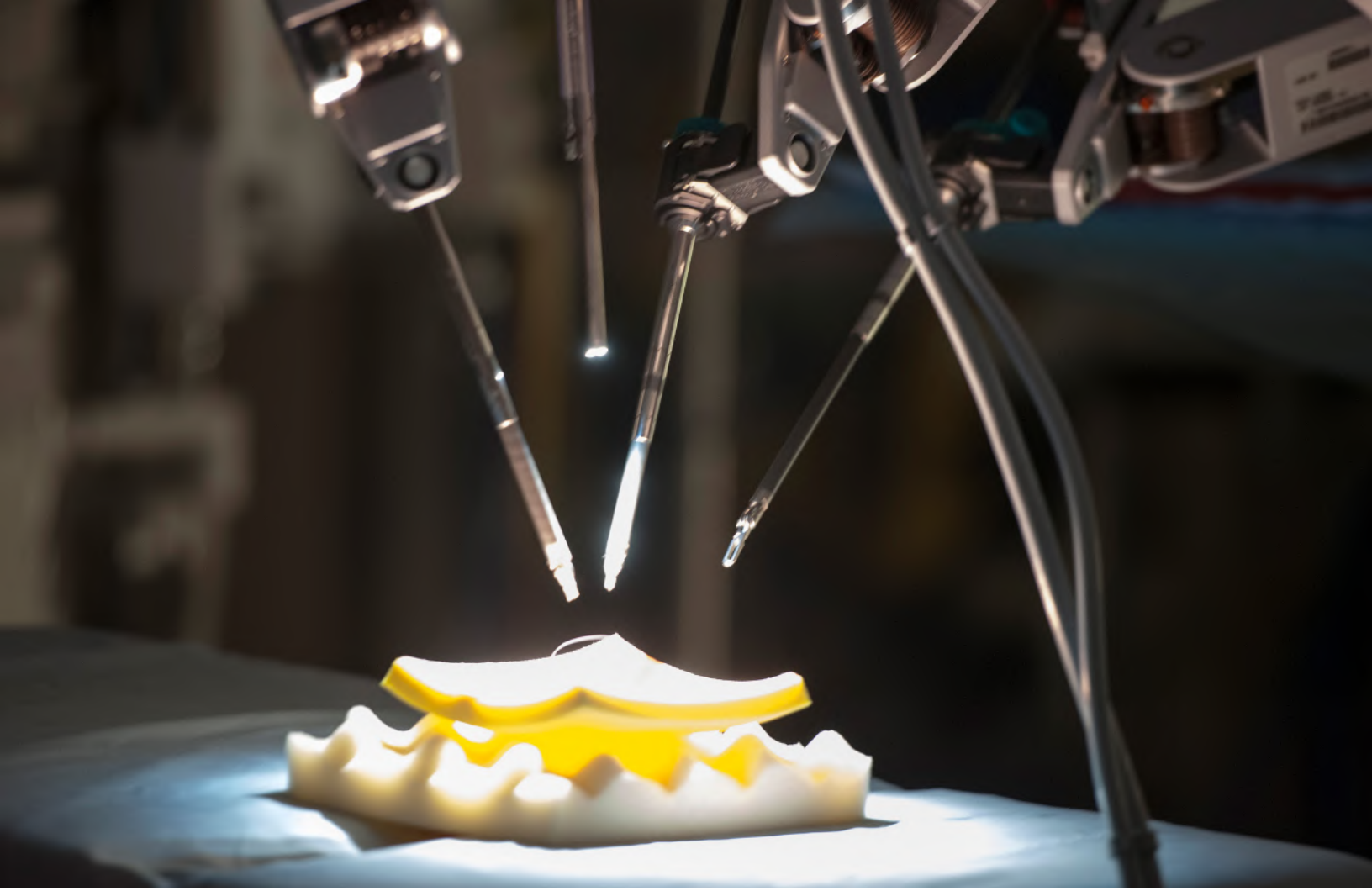
Unlike your old routine of standing on a scale, however, this device works as you sleep, shower, and go about your life, offering near-real-time biochemical measurements.[1] Your digital assistant adds lunch outside to your schedule and suggests putting more milk in your tea; you suspect you are still low on vitamin D. While waiting for the water in your kettle to boil, you make a mental note to check the personal health dashboard when you get to the office. Either way, you are reassured that you are already acting to raise your vitamin D. Your health record was updated during your last overnight data transfer, so the health team would have already sent additional instructions if your vitamin D level was critically low. Plus, your health team will soon send analysis of that cold virus you had last week, which you are pretty sure you got from a coworker who had similar symptoms.

The genetic and epidemiological analysis of the virus may or may not confirm your suspicion, but you are looking forward to the health team's analysis and recommendations for how to avoid future exposure to other viruses known to be in circulation this winter cold season. You expect the report will also rule out the possibility that the virus had a greater impact on your long-term health. Your health team will closely monitor your real-time data[2] over the next few weeks to identify any changes that might need further testing.[3] The kettle dings, you pour the hot water over the tea, and, of course, you remember to add that second dash of milk.

1 Amay J. Bandodkar, Wenzhao Jia, Ceren Yardımcı, Xuan Wang, Julian Ramirez, and Joseph Wang, "Tattoo-Based Noninvasive Glucose Monitoring: A Proof-of-Concept Study," Analytical Chemistry 87 (2015), https://pubs.acs.org/doi/abs/10.1021/ac504300n; Signe Dean, "MIT Has Developed Colour-Changing Tattoo Ink That Monitors Your Health in Real Time," Science Alert, last updated June 13, 2017, https://www.sciencealert.com/mit-is-working-on-colour-changing-tattoo-ink-that-can-monitor-your-health-in-real-time.

2 US Food and Drug Administration, "FDA Approves Pill with Sensor That Digitally Tracks if Patients Have Ingested Their Medication," news release, last updated November 13, 2017, https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm584933.htm.

3 Mark Bowden, "The Measured Man," Atlantic, last updated August 2012, https://www.theatlantic.com/magazine/archive/2012/07/the-measured-man/309018/.



The Da Vinci Surgical System is a robotic surgical system designed to assist in complex, minimally invasive procedures.
Photo credit: Department of Defense/Flickr.

In contrast, governance mechanisms for digital technologies are relatively underdeveloped with few legal hurdles to the global dissemination of a product early in the development cycle. Data and analytics products more closely resemble software development, where the norm is to ship a minimum viable product (MVP) that is subsequently updated with additional functionality based on customer feedback and use. Intellectual property protections require significant upfront legal costs to file and additional resources to enforce. For a technology that can be built by a college student on a laptop, the legal costs to secure intellectual property are a much greater proportion of overall development costs than in the traditional biomedical technology sector. Even the legal tools that are increasingly relevant in the digital world—such as copyright and trade secret—often require actions early in the development cycle at prohibitively high costs. Convergent biotechnologies that are shipped as MVPs, updated frequently, and constantly modified based on new streams of data may require entirely new mechanisms for protecting ownership and regulating safety due to characteristics that are inherent to many convergent biotechnologies.

Social

A healthcare system centered around technologically empowered individuals coordinating their own health optimizations will likely require new societal institutions and infrastructure. Existing institutions and infrastructure treat acute, late-stage diseases at high cost and risk of acquiring lethal infections from just stepping foot inside medical facilities.

Developing the capabilities and services to facilitate data-driven health optimization will likely require the emergence of new institutions able to apply these technologies in novel ways. These new organizations could evolve from mergers of existing consumer-focused companies and traditional healthcare providers, such as the announced merger of CVS and Aetna.[11] Alternatively, the less-regulated wellness industry or community-based institutions could expand to become pro-

11 Michael J. de la Merced and Reed Abelson, "CVS to Buy Aetna for $69 Billion in a Deal That May Reshape the Health Industry," *New York Times*, last updated December 3, 2017, https://www.nytimes.com/2017/12/03/business/dealbook/cvs-is-said-to-agree-to-buy-aetna-reshaping-health-care-industry.html?_r=0.

The gains in human health promised by convergent biotechnologies could exacerbate inequality if not all individuals are able to access the same standard of care.

viders of biomedical data services. Either way, arriving at a system that resembles Healthcare 2.0 will likely require at least as much social and business innovation as it does technological and regulatory innovation.

Additionally, the concept of privacy, which is integral to the current framing of health information, must evolve to enable data fluidity and collective learning. Performing analytics and making recommendations for interventions in real time requires not only tremendous computing power, but also a deeper understanding of the relationship between what is measured and the actions needed to reach the desired outcome. Population-level learning across individual health data would increase the rate at which health in humans can be optimized, but would likely require changes to how an individual's personal health data are viewed, making them more of a public good than the property of an individual. The perception of privacy varies by individual and culture and is constantly evolving in response to emerging technologies, so it will continue to change. However, building more universal norms around privacy to enable species-level management of health-related data will be a significant hurdle to reaching the full potential of advanced biotechnologies.

Ethical

The gains in human health promised by convergent biotechnologies could exacerbate inequality if not all individuals are able to access the same standard of care. A healthcare system predicated on technically empowered individuals proactively engaging in the management of their own health requires these technologies to be accurate, affordable, and understandable by those with minimal training.

A shift in policy or norms around privacy toward individual health data becoming more of a public good may be a prerequisite for realizing many gains from convergent biotechnologies. Personal health data as a public good—through cultural expectations or business models that require sharing health data to gain access to critical health technologies—could create coercive environments that prevent individuals from opting out of sharing personal health data. On the other hand, if individuals choose to opt out of contributing their health data to the public good, the health of other individuals could be negatively impacted because not as much health data would be analyzed. Further, the insights gained from analyzing large quantities of human health data—especially at the intersection of physical health and mental health—could result in the human body being perceived as more of a biological machine with the ability to be fine-tuned, which could have implications on how humans perceive themselves.

Governance

The governance of convergent biotechnologies is currently determined by factors beyond the characteristics of the technologies. If a company accustomed to operating in the highly regulated biomedical product environment decides to pursue a convergent biotechnology, it may choose to follow practices that are the norm for the biomedical sector with the goal of marketing to its usual customer base. However, if software developers create an algorithm-based product with biomedical applications, they would be less likely to consider regulations affecting the product and it may not even be clear to regulators if the product falls outside the standard regulated categories. In 2013, the US FDA issued a warning letter to consumer-focused genetic testing company 23andMe, Inc., appearing to catch many technology evangelists in Silicon Valley off guard.[12] The FDA determined that a website providing health and genealogy information based on an individual's genetic profile was a diagnostic device for regulatory purposes. As a result, 23andMe had to rapidly adapt to its product being considered a medical device and received permission to resume providing limited health information only in 2017 after extensive negotiations with the regulatory agency.[13] Later that year,

12 "Inspections, Compliance, Enforcement, and Criminal Investigations," US Food and Drug Administration, accessed November 28, 2017, https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm376296.htm.

13 On April 6, 2017, the FDA announced approval for 23andMe to market a limited number of genetic tests directly to consumers, indicating that the "FDA intends to exempt additional 23andMe GHR [genetic health risk] tests from the FDA's premarket review, and GHR tests from other

the FDA released its Digital Health Innovation Action Plan and announced nine companies it had selected for a digital health software pilot program. Both actions acknowledge that a new regulatory approach is needed for digital health technologies, with FDA's stated aim being to shift regulation from the product to the firm or developer.[14]

The democratization of affordable, accurate, and real-time sensors and accompanying analytics is changing the dynamic between individuals, medical practitioners, and regulators. Furthermore, the outcomes depicted above would require a profound shift in other heavily regulated areas, including capture, storage, and use of individual health data, which is not a foregone conclusion. Ultimately, the obstacles to advanced biotechnologies becoming commonly available are less the technology itself, and more the surrounding factors that enable the technology to be effectively used and governed.

CONCLUSION

The application of advanced biotechnologies could have profound implications, creating unique opportunities for collaboration among individuals and nations and across industrial sectors. The democratization of science and technology provides opportunities for deepening cooperation between the United States and South Korea at the national, local, and citizen levels.

RECOMMENDATIONS FOR INCREASED COOPERATION

US-South Korean Cooperation in Convergent Biotechnology

The United States and South Korea are well positioned to leverage their existing technical strengths to expand into this rapidly growing segment of the bioeconomy as the market matures, which would align with each nation's economic goals. Proactive engagement on global standards setting and norms formation around the development and use of convergent biotechnologies provides an opportunity to demonstrate responsible leadership in an industry likely to cause legal, social, and ethical tensions. Bilateral and multilateral cooperation also has the potential to diversify and strengthen the bonds between US and South Korean citizens and organizations. The democratization of science and technology resulting from the expanding application of convergent biotechnologies can also catalyze greater interaction between the United States and South Korea at the national, local, and citizen levels.

Bilateral

The United States and South Korea should deepen engagement on convergent biotechnology in existing bilateral fora to explore new models of governance as well as the ethical trade-offs inherent in convergent biotechnologies. Existing mechanisms for bilateral cooperation could include topics related to advanced biotechnologies and be expanded to include broader, interdisciplinary participation from diverse segments of the government in recognition of the multidisciplinary nature of convergent technologies. Discussions should not be limited to technical or economic goals, as the application of advanced biotechnologies could have profound implications for political goals as well. Despite a robust agenda of existing bilateral collaboration, there are avenues for expanding cooperation around convergent biotechnologies through research and development (R&D). Here are some examples to build on:

- The Senior Economic Dialogue between the two countries aims to promote and expand cooperation on economic issues, as well as identify opportunities for collaboration through a joint public-private forum.[15] Given the United States' and South Korea's emphases on science, technology, and innovation, both countries could benefit from further highlighting advanced biotechnologies as an area of cooperation in future dialogues.

- Developing shared legal and ethical norms, principles, codes of conduct, and standards could allow for more fluidity between each nation's products and customers. The US-Republic of Korea Information and Communication Technology (ICT) Policy Forum[16] could be a productive venue

makers may be exempt after submitting their first premarket notification." See US Food and Drug Administration, "FDA Allows Marketing of First Direct-to-Consumer Tests That Provide Genetic Risk Information for Certain Conditions," news release, April 6, 2017, https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm551185.htm.

14 "Digital Health Software Precertification (Pre-cert) Program," US Food and Drug Administration, accessed February 10, 2018, https://www.fda.gov/MedicalDevices/DigitalHealth/UCM567265; "Software Precertification Pilot Program Participants," US Food and Drug Administration, accessed February 10, 2018, https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/ucm577330.htm.

15 US White House, "Joint Statement between the United States and the Republic of Korea," released June 30, 2017, https://www.whitehouse.gov/briefings-statements/joint-statement-united-states-republic-korea/.

16 US Department of State, "Joint Statement on the 3rd US-Republic of Korea ICT Policy Forum," released September 12, 2016,

to discuss bilateral issues related to information technology and data hurdles related to convergent technologies.

» Government-enabled advanced biotechnology projects that aim to more rapidly develop, test, and prototype high-priority areas of convergent biotechnologies in health, agriculture, energy, and industrial application could be a priority area in the US-Republic of Korea Science and Technology Agreement—signed in 1976 and subsequently renewed in 1992, 1999, and 2004.[17] This could include exchanges of information and personnel and joint R&D interagency cooperation, such as increased collaboration on precision medicine—medical approaches that take into account individual variability in genes, environment, and lifestyle—through expanded engagement between the US National Institutes of Health and the Korea Biobank Project.[18]

» Intergovernmental collaboration in the area of research and clinical response to cancer should be established. South Korea is one of the few countries that has government-sponsored cancer screening for citizens, which could provide a competitive advantage in cancer treatment and research data.

Multilateral

The United States and South Korea should endeavor to use existing multilateral venues and develop new fora to deepen technical knowledge and momentum around a shared understanding of legal, social, and ethical issues related to advanced biotechnologies.

» Jointly developed programs can pilot convergent biotechnologies that address global challenges working in partnership with other nations. This could improve the prospect for more rapid economic development in other countries, establish legal and ethical norms, and potentially expand markets for US and South Korean products.

» Expand trilateral engagement with partners such as Japan, Germany, and the European Union (EU) to engage on technical, legal, and ethical norms; principles; codes of conduct; and data and privacy standards that could underpin advanced biotechnologies. South Korea's launch of the Fourth Industrial Revolution Committee and Workshop with Germany in October 2017 could be expanded to include the United States.

» Reinvigorating efforts to collaborate on cancer initiatives between the United States,[19] Japan, and South Korea—including research and data sharing—could result in more rapid innovation in treatments.

» Venues should be created for premier scientists in areas of advanced biotechnology to exchange information and explore opportunities to collaborate with promises of expanded access to government facilities and resources. Sharing information between scientists could cultivate longer-term research collaborations that leverage the comparative advantages of different nations.

» Better multilateral collaboration is needed through fora such as the United Nations and the Organisation for Economic Co-operation and Development (OECD) in the area of neuroscience R&D. The robust domestic efforts underway in the United States' Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative[20] and the Korea Brain Research Institute[21] provide an opportunity to advance research and large-scale brain projects through collaboration on efforts such as the International Brain Initiative.[22]

Nongovernmental Sector

The United States and South Korea should create opportunities to catalyze civil society organizations, companies, and individuals around the responsible development of convergent biotechnologies through

https://2009-2017.state.gov/r/pa/prs/ps/2016/09/261772.htm.

17 "Science and Technology Cooperation," US Department of State, accessed November 28, 2017, https://www.state.gov/e/oes/stc/; "East Asia Region US Science & Technology Agreements," Fogarty International Center, last updated January 2017, https://www.fic.nih.gov/WorldRegions/Pages/EastAsiaPacific-agreements.aspx.

18 "National Institute of Health: Director General's Message," Korea National Institute of Health, accessed November 29, 2017, http://www.nih.go.kr/NIH/eng/contents/NihEngContentView.jsp?cid=17881; "What Is Precision Medicine?" Genetics Home Reference, US National Institutes of Health, last accessed on February 10, 2018, https://ghr.nlm.nih.gov/primer/precisionmedicine/definition.

19 "Home," Biden Cancer Initiative, accessed November 28, 2017, https://bidencancer.org/.

20 "The BRAIN Initiative," US National Institutes of Health, accessed November 28, 2017, https://www.braininitiative.nih.gov/?AspxAutoDetectCookieSupport=1.

21 "The Last Mystery of Humanity, the Brain," Korea Brain Research Institute, accessed November 28, 2017, http://www.kbri.re.kr/new/pages_eng/sub/page.html?mc=2434.

22 "The International Brain Initiative," The Kavli Foundation, accessed November 28, 2017, http://www.kavlifoundation.org/international-brain-initiative.

joint pilots and synergistic efforts to scale applications that address global challenges. Additionally, efforts to engage citizens on topics related to convergent biotechnologies could create a more technically literate workforce and mitigate possible social backlash against the disruptive potential of advanced biotechnology. Collaborations between US and South Korean companies could further the competitiveness of companies in both countries and bolster their positions in overseas markets.

Civil Society

- Stronger collaboration between US and South Korean philanthropies and civil society organizations is needed to develop a more vibrant ecosystem of nongovernmental organizations in South Korea to advance scientific research and explore the legal, social, and ethical issues surrounding advanced biotechnologies.

- Partnerships between US and South Korean hospitals around clinical trials can help leverage South Korea's high-quality and cost-competitive biomedical infrastructure[23] to increase standards and lower financial hurdles to safe and effective products, from both countries, reaching the global market.

- Formal and informal mechanisms for educational exchanges in areas related to convergent biotechnologies should be expanded. South Korea should make a targeted effort to recruit Fulbright scholars in science, technology, and innovation[24] and build a network to connect existing South Korean researchers in the United States, including several hundred doctorate-level scientists based out of the National Institutes of Health and in labs funded by the National Science Foundation.

- Citizen scientists from both countries should be incentivized to expand participation in technical competitions such as those coordinated by the Defense Advanced Research Projects Agency, US Agency for International Development's Global Development Lab, and US National Institute of Standards and Technology's Global City Teams Challenge.[25]

- The United States and South Korea could build a joint bilateral scientific competition in the area of advanced biotechnology similar to the US-China EcoPartnerships initiative,[26] which focused on sustainability.

Private Sector Collaboration

- Samsung's selection in September 2017 by the US FDA to be one of only nine companies to participate in a digital health software pre-certification pilot program[27] should be leveraged to form the basis of synergistic regulations in South Korea. The pilot aims to take a more tailored approach by looking at the software developer or digital health technology provider rather than focusing on the product. This has the potential to revolutionize digital health regulation in the United States and could also inform future regulations in South Korea.

- US and South Korean companies should coordinate and share best practices to ensure compliance with the EU's General Data Protection Regulation, which will apply to all companies processing and holding personal data of subjects residing in the EU, regardless of their jurisdiction. It goes into effect in May 2018 after a two-year post-approval period.[28]

- South Korea's high internet penetration rate could allow it to serve as a test-bed to scale mobile health technologies and integrate them into the existing healthcare system with the country's growing smart city infrastructure. South Korea boasts the highest percentage of households with internet access among OECD countries at 98.8 percent,[29] while also ranking high among OECD countries with 109 mobile subscribers per 100 inhabitants.

---

23 "Review of 2014 Clinical Trial Approvals in Korea," Korea National Enterprise for Clinical Trial, accessed November 28, 2017, http://en.konect.or.kr/whykorea/fns.htm.

24 "The Fulbright Scholar Program: Science, Technology and Innovation," Council for International Exchange of Scholars, accessed November 28, 2017, https://www.cies.org/fulbright-scholar-program-science-technology-and-innovation.

25 Sokwoo Rhee, Martin Burns, and Cuong Nguyen, *Global City Teams Challenge 2016*, National Institute of Standards and Technology, NIST Special Publication 1900-01, June 2017, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-01.pdf.

26 "EcoPartnerships," US-China EcoPartnerships Program, accessed November 28, 2017, https://ecopartnerships.lbl.gov/.

27 US Food and Drug Administration, "FDA Selects Participants for New Digital Health Software Pre-certification Pilot Program," released September 26, 2017, https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm577480.htm.

28 "GDPR Portal: Site Overview," EU General Data Protection Regulation Portal, last accessed February 11, 2018, https://www.eugdpr.org/.

29 "Country Profile of Korea: Innovation and Technology," OECD Data, accessed November 28, 2017, https://data.oecd.org/korea.htm#profile-innovationandtechnology.

Rice plants grow in a biotechnology lab. *Photo credit*: IRRI photos/Flickr.

- The United States and South Korea could exchange information and best practices to build a stronger ecosystem of entrepreneurship. Providing opportunities and a more fluid process for scientists, engineers, researchers, and others to commercialize findings could bring discoveries to market sooner. Learning from the successes of the Johnson & Johnson Innovation Centers—a model of private sector–led efforts to spur innovation by supporting start-ups and small and medium-sized enterprises—could help expand access to existing expertise and facilities.[30]
- Industry leaders from the United States and South Korea could develop partnerships to address emerging issues in technology policy. Intel, Samsung, and industry associations launched an IoT Dialogue[31] in 2017 to address the challenges and opportunities in IoT, which could include policies related to mobile health, wearable technology, and healthcare data protection.

***

The author wishes to thank Georgetown University students Paul Kumst and Julie Yang for research support that was critical to the production of this chapter including literature review, information gathering from policy makers, and constructive feedback on the text.

30 "About Us: Vision, Family, Leadership," Johnson & Johnson Innovation, accessed November 28, 2017, https://www.jnjinnovation.com/about-us.

31 Samsung, "Technology Industry Leaders Release National Strategy to Maximize US Economic and Societal Benefits from the Internet of Things," press release, October 3, 2017.

PART III

BUILDING A SMART PARTNERSHIP FOR THE INTERNET OF THINGS

CHAPTER 5

PREPARING FOR A CONNECTED WORLD

Dr. Gwanhoo Lee and Ms. Rebekah Lewis

Lee is *Professor of Information Technology and Analytics, Kogod School of Business*, American University
Lewis is *Director, Kogod Cybersecurity Governance Center,* American University

The Internet of Things (IoT) is already changing people's daily lives and how businesses are run. Simply put, IoT is a network of "things" equipped with smart sensors and actuators that allow them to communicate and control. The recent uptick in IoT adoption is driven by factors such as lower sensor prices, cheaper bandwidth and data processing, ubiquitous smartphones and wireless connectivity, and advances in big data analytics and artificial intelligence.[1] IoT revenue is estimated to grow to $3 trillion[2] with an economic impact of up to $11.1 trillion by 2025.[3] Although IoT can contribute significantly to economic growth and social welfare, it faces a number of technical, social, legal, and policy challenges, including cybersecurity risks.

Cybersecurity is especially important because it is not only one of the most important reasons that consumers are hesitant to adopt IoT devices,[4] but also an area of significant potential competitive advantage in an already highly competitive market landscape.[5] To mitigate the cybersecurity risks for IoT devices, smart strategies and policies must be developed by collaborating with stakeholders from both the public and private sectors to ensure greater cybersecurity for connected technologies. As leaders in the IoT field,[6] the United States and the Republic of Korea (hereafter South Korea) should closely collaborate to address IoT users' cybersecurity concerns while fostering IoT innovation and deployment.

---

1 Simona Jankowski et al., *The Internet of Things: Making Sense of the Next Mega-Trend*, Goldman Sachs Global Investment Research, September 2014, http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf.

2 Emma Buckland et al., "IoT Global Forecast & Analysis 2015-25," Machina Research, August 2016, https://machinaresearch.com/report/iot-global-forecast-analysis-2015-25/.

3 James Manyika et al., *Unlocking the Potential of the Internet of Things*, McKinsey Global Institute, June 2015, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

4 EY, *Cybersecurity and the Internet of Things*, March 2015, http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf.

5 Harald Bauer et al., *How CEOs Can Tackle the Challenge of Cybersecurity in the Age of the Internet of Things*, McKinsey & Company, June 2017, https://www.mckinsey.it/file/7615/download?token=zTyxQJ1g.

6 "South Korea Leads 2017 IDC Asia Pacific IoT Readiness Index," *Networks Asia*, July 17, 2017, https://www.networksasia.net/article/south-korea-leads-2017-idc-asia-pacific-iot-readiness-index.1500261180.

This chapter discusses unfolding trends and cybersecurity risks for IoT and presents an overview of related US and South Korean policies and regulations. It then proposes several recommendations for cooperation between the US and South Korean governments to increase the security and utility of existing and future IoT technologies. These recommendations include:

- promoting universal adoption of a common cybersecurity framework, such as the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST);
- encouraging development of international standards for increased interoperability of various IoT systems;
- encouraging adoption of Internet Protocol Version 6 (IPv6) for stronger security;
- promoting the principles of *security by design* and *privacy by design* to secure consumer trust in IoT;
- increasing government investment in cybersecurity of IoT by launching various funding programs and establishing cybersecurity centers of excellence;
- educating students and training workforces to supply talents needed for IoT; and
- using a market-driven approach to identify and spread out best practices and cost-effective measures for IoT cybersecurity.

UNFOLDING TRENDS

IoT can transform virtually all industries. IoT technologies can help improve vehicle safety, increase energy efficiency, keep people healthy, and optimize manufacturing operations. The following are a few use cases that demonstrate the potential value of IoT.

Connected Vehicles

The data collected by numerous sensors in connected vehicles can be used to benefit drivers, passengers, carmakers, and many others in terms of enhancing safety and performance. A vehicle will be connected not only to the driver's mobile device, but also to other vehicles and common infrastructure such as roads, traffic lights, and parking garages. All of this data can be transmitted to and processed in the cloud for greater efficiency and innovation. The driver of a connected vehicle can monitor the status of the vehicle and control various functions and features by using a smartphone. People's driving experiences will greatly improve as the vehicle is connected to and seamlessly integrated with various smartphone apps and vehicle infotainment systems.

Smart Energy

IoT can increase energy efficiency by collecting and analyzing energy-related data from various sources. Consumers can monitor and optimize their energy consumption, and energy companies can remotely monitor facilities located in distant areas. The Alta Wind Energy Center in California is one such case. In the center, each wind turbine is equipped with several sensors that monitor wind speed and direction. These data are sent to the server and analyzed to control the direction of the wind turbines to maximize power generation. As a result, wind turbines in the center can adapt to changing weather conditions dynamically and optimally. In another example of IoT-directed energy efficiency, Kansas City, Missouri, has installed 125 smart streetlights in the downtown area that automatically dim when no one is underneath them.[7] Since their installation in 2016, the sensors embedded in the streetlights have collected a large volume of data, including the number of passersby. The city's living lab explores new ways of using such data to optimize resource allocation and development.[8] In yet another example of energy efficiency resulting from advances in IoT, Kingspan, a building materials company based in Ireland, has transformed its headquarters into a net-zero-energy building by implementing a fully automated energy management system that includes an IoT platform, smart meters, and smart lights.[9]

Connected Healthcare

The healthcare systems in many countries are notoriously inefficient. IoT can transform healthcare systems to reduce cost and improve care quality. Two critical areas of IoT application include activity tracking and chronic disease management. Wearable devices such as smartwatches and fitness trackers allow users to monitor and analyze daily activities and other health-related data. The data collected from these wearable devices can be used to help maintain the user's wellness, either

7 Andrew J. Hawkins, "Kansas City Just Installed Free Public Wi-Fi and Dozens of 'Smart' Streetlights," The Verge, May 9, 2016, https://www.theverge.com/2016/5/9/11640558/kansas-city-free-public-wifi-smart-streelights-google-sprint-cisco.

8 "What Is the Kansas City Living Lab?" KC Living Lab, July 15, 2016, http://kclivinglab.com/.

9 Intel, *IoT Enables Smart Energy Management by Kingspan*, accessed February 8, 2018, https://www.intel.com/content/dam/www/public/us/en/documents/case-studies/dk100-quark-soc-kingspan-study.pdf.

by the users themselves or their healthcare providers. Patients with chronic diseases can constantly monitor their health conditions using mobile IoT devices. These data can be shared with doctors and caregivers so that they can detect risky health conditions in real time. Some other use cases include Dexcom's mobile CGM (Continuous Glucose Monitoring) system[10] for people with diabetes, AMC Health's mobile patient monitoring solution for pregnant women,[11] and Vital Smith's "b bless" solution for checking the ovulation schedules of infertile women.[12]

Smart Manufacturing

IoT can transform traditional factories into connected, smart powerhouses that significantly increase productivity, reduce costs, and maintain optimal manufacturing conditions through preventive maintenance based on predictive analytics.[13] For example, Stanley Black & Decker connected all the equipment in its factory in Mexico by using a wireless network and IoT systems. This connectivity helped increase the visibility of manufacturing processes and inventories. As a result, the factory has witnessed substantial improvements in productivity and quality.[14]

POLICY ISSUES, RISKS, AND STRATEGIC IMPLICATIONS

IoT Risks

With the vast quantities of data that IoT devices collect and process, there are numerous opportunities for continued growth and development, but these connected technologies also present a variety of security-related risks. According to a study recently released by HP, "seventy percent of the most commonly used IoT devices contained vulnerabilities ranging from inadequate consumer passwords to more serious [issues]." Furthermore, "the range and number of devices and networks that are being used expand the number of potential targets for cyber threats" and the scope of potential harm resulting from such incidents.[15] Importantly, with IoT applications, cyber risks not only affect information and communications technologies but now also impact physical systems, threatening public safety, economic stability, national security, and even human life.[16] Even now, cyber threats have compromised existing IoT technologies with early models of connected cars and medical devices falling victim to hacking.[17] Despite advances in security for second-generation-and-beyond devices, "low-powered specialized IoT devices may not have the processing power to maintain high levels of security."[18]

The wide range of potential attack vectors, targets, and harms underscores how the cybersecurity of IoT devices is not simply a technological issue but an enterprise-level risk. Therefore, a cybersecurity strategy should take into account the entire connected cyber ecosystem, encompassing customers, suppliers, and third-party partners. Not only is it difficult to ensure adequate consideration of all of these component parts, an additional challenge is that no single player in the IoT ecosystem feels responsible for the security of IoT systems.[19]

In addition to security concerns related to the availability and integrity of data and systems, IoT may present heightened risk to confidentiality, resulting in privacy concerns for users. In particular, IoT devices can and are used to collect, store, and process a wide and growing range of personal and potentially very sensitive data. At the same time, they are by their very nature

10 "Introducing the Dexcom G5 Mobile CGM System," Dexcom, http://www.dexcom.com/g5-mobile-cgm.

11 Verizon, *State of the Market: Internet of Things 2016*, April 2016, https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf.

12 John Yoon, "Korean Startup Vital Smith One of Four Finalists of Grants4Apps Accelerator 2016," Seoul Space, August 24, 2016, http://seoulspace.co.kr/2016/08/24/korean-startup-vital-smith-one-of-four-finalists-of-grants4apps-accelerator-2016/.

13 "Internet of Everything (IoE): Value at Stake in the IoE Economy," Cisco, 2013, https://www.slideshare.net/CiscoIBSG/internet-of-everything-ioe-economy.

14 Cisco, *Leading Tools Manufacturer Transforms Operations with IoT*, 2014, https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/c36-732293-00-stanley-cs.pdf.

15 "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," HP, July 29, 2014, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VrLfonJf2Gk; Gwanhoo Lee, *IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership*, U.S.-Korea Business Council, November 2016, https://www.uschamber.com/sites/default/files/final_accelerating_iot_growth_and_deployment_uskbc.pdf, 5.

16 "IoT Information Security Roadmap," Ministry of Science, ICT, and Future Planning, South Korea, October 2014.

17 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Scott Mace, "For Real: Medical Devices Vulnerable to Hacking," Medpage Today, March 6, 2016, http://www.medpagetoday.com/practicemanagement/informationtechnology/56566.

18 Lee, *IoT Innovation and Deployment*, 5.

19 Bauer et al., *How CEOs Can Tackle the Challenge of Cybersecurity in the Age of the Internet of Things.*

A fleet of self-driving cars. *Photo credit*: Alan/Flickr.

equipped with access and connection points, and are used in a variety of public settings. This combination of factors increases the risk of intrusive monitoring or surveillance, unauthorized access, interception or use of sensitive personal information, and other potential invasions of privacy.

The concern for information vulnerability grows as connected technologies become increasingly common and greater quantities of consumer data are collected, analyzed, and transmitted through platforms and networks that lack adequate security. As IoT devices become normalized in the product market, consumers run the risk of becoming desensitized to their vulnerabilities and may not always realize how their data are being used, or that they are even being collected in the first place. Furthermore, traditional security checks rely on consumer awareness to be successful, and the growing prevalence of "smart" devices can be misleading. The sheer quantity of available devices coupled with a lack of a screen or other direct user interface creates significant privacy issues as consumers become desensitized to information-sharing and the traditional security concepts of "notice and consent."

IoT devices are used by consumers across the globe, often while they are traveling across international boundaries. Accordingly, such devices may be subject to the privacy and security requirements of multiple jurisdictions, which can vary widely and can sometimes conflict. Moreover, due to the rapidly changing nature of innovation and technological change, both among legitimate actors as well as cyber criminals, it is incredibly difficult—if not impossible—to develop a stable and meaningful set of security standards that can be used as a basis for determining legal compliance. All of these factors make addressing the risk of legal noncompliance challenging and resource-intensive, potentially slowing the pace of innovation and growth.

Not only do many of IoT products' defining characteristics (e.g., ubiquity, connectivity, mobility) exacerbate security and privacy concerns, the highly competitive IoT marketplace itself also creates a difficult environment for adequately addressing security and privacy. The combined pressures to innovate, be first to market, and manage limited funding (especially for the large and growing number of IoT startups) encourage a corporate culture that does not naturally prioritize security and privacy, much less give them the extra care and attention they may need in this context.

The South Korean government has been relatively proactive in developing policies to address issues emerging from new IoT technologies.

Current Policies and Regulations Relating to IoT

In response to the increasing risks associated with IoT deployment, governments have introduced policies and revised regulations. Here is a brief review of current cybersecurity policies and regulations for IoT in the United States and South Korea.

The United States

In 2014, the US National Institute of Standards and Technology formed a Public Working Group on Cyber-Physical Systems (CPS) intended to facilitate cross-sector discussions on IoT between public and private stakeholders. The Public Working Group put forth the Framework on Cyber-Physical Systems[20] (CPS Framework) in May 2016. The CPS Framework was designed "to provide a comprehensive tool for the analysis and description of connected devices and systems."[21] The CPS Framework includes extensive discussion of cybersecurity and privacy concerns, including key areas and considerations for further study and recommendations. Separately, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity,[22] (the Cybersecurity Framework or CSF), which serves as a robust model for "multi-stakeholder government-industry efforts to promote cybersecurity in a variety of contexts, including with respect to IoT."[23]

In 2015, the Federal Trade Commission (FTC) initiated a program originally called Start with Security, now known as Stick with Security, to promote the principle of security by design. It also released guidance concerning IoT product design and marketing for private sector development for public consumption use.[24]

That same year, Congress launched the Congressional Caucus on the Internet of Things to facilitate and promote discussion regarding the policy implications of IoT. Caucus members also introduced the Developing Innovation and Growing the Internet of Things Act, which would convene federal stakeholders, advised by nonfederal entities, to provide recommendations related to IoT technologies and deployment. In August 2017, Senators Mark Warner, a Democrat from Virginia, and Cory Gardner, a Republican from Colorado, introduced in Congress the Internet of Things Cybersecurity Improvement Act, a bill that would require companies that sell wearables, sensors, and other web-connected tools to federal agencies to adhere to some new security standards.[25]

South Korea

The South Korean government has been relatively proactive in developing policies to address issues emerging from new IoT technologies. The Ministry of Science and ICT (MSIT) and the Ministry of Trade, Industry, and Energy (MOTIE) spearheaded this endeavor. In 2015, MSIT published a three-year implementation plan to improve IoT cybersecurity.[26] The plan is built upon three pillars: creating a foundation for embedded cybersecurity, developing cutting-edge technology for IoT cybersecurity, and strengthening the competitiveness of the IoT cybersecurity industry. The ministry encourages the adoption of the security by design principle, develops test-beds for IoT security, and builds a global network to address IoT cybersecurity issues. In 2015, the ministry also established the IoT Security

20 Cyber Physical Systems Public Working Group, *Framework on Cyber-Physical Systems Release 1.0*, May 2016, https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf.

21 Lee, *IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership*, 6.

22 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

23 Lee, *IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership*, 12.

24 Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World*, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

25 Tony Romm, "Two U.S. Lawmakers Think the Government Has a New Cybersecurity Problem: The Internet of Things," Recode, August 1, 2017, https://www.recode.net/2017/8/1/16070996/congress-internet-of-things-cybersecurity-laws.

26 Ministry of Science, ICT, and Future Planning, South Korea, *IoT Information Security Roadmap: A Three-Year Implementation Plan*, June 2015.

Alliance to facilitate public-private collaboration.[27] The IoT Security Alliance published the *IoT Common Security Principle* in 2015[28] and subsequently published the *IoT Common Security Guide* in 2016 and the *Smart Home Appliance Security Guide* in 2017.[29] In addition, the ministry launched an IoT-Information Sharing and Analysis Center (IoT-ISAC).

In April 2017, the Ministry of Trade, Industry, and Energy developed a comprehensive plan for the national standardization of emerging technologies through a joint effort with other ministries.[30] According to this plan, MOTIE identified four strategic areas, including:

- standard development for creating global markets;
- expanding the foundation of standardization for supporting companies;
- standardization for improving quality of life; and
- establishing a private sector–driven ecosystem for standardization.

In addition, MOTIE defined twelve core projects for its national standardization initiative and selected twelve emerging industries as top priorities for standardization. These industries include autonomous electric vehicles, smart ships, IoT appliances, robots, drones, new energy, augmented reality/virtual reality, next generation display technology, and bio health.

MSIT will focus its standardization efforts on ten strategic industries including 5G, smart devices, IoT, cloud, big data, and cybersecurity. The Ministry of Food and Drug Safety introduced certification programs for personal wellness/fitness devices and pursues standardization of IoT-based healthcare products. The Ministry of Health and Welfare facilitates the development of standardization of medical and health data. In November 2013, MOTIE released a strategic plan for creating markets for smart healthcare. This strategic plan proposes increasing investments in new healthcare businesses, executing pilot projects, and supporting domestic companies' entrances into the global market.[31]

CONCLUSION

The Internet of Things presents a potentially endless array of opportunities for growth and innovation, as well as an equally broad and evolving range of security and privacy challenges. To emerge from the early years of this new era of explosive growth as effective and responsible global leaders in IoT, the United States and South Korea must take a strategic and collaborative approach to fostering continued progress and protecting security and privacy. Through both domestic policy choices and bilateral coordination, the countries should push for a greater emphasis on cybersecurity while seeking to minimize choices that may impede innovation.

In particular, both governments should proactively collaborate with industry to establish a common framework for thinking about cybersecurity issues and challenges and, within the context of that framework, push for the development of international standards that can help address these issues and challenges while ensuring consistency and interoperability. The principles of security and privacy by design should be pursued and promoted whenever possible, reinforcing the notion that security and privacy are foundational issues that should be reflected in practice from the very beginning of production conception and design, rather than as afterthoughts. Lastly, both governments should increase their own investment in cybersecurity, including by investing in research that will help identify cost-effective cybersecurity measures. By understanding which measures are cost-effective and which are not, both governments can much more strategically choose where to direct their efforts for the greatest impact.

In addition to increasing cybersecurity and privacy protections for consumers of IoT and promoting economic growth in their own regions, the US and South Korean governments, by pursuing these recommendations, can lead the world in modeling effective IoT governance. As IoT continues to expand into every aspect of daily life, establishing leadership in this realm will also position both countries to lead with respect to some of the most important issues of the coming years. Effective information sharing and collaboration will

27 "IoT Security Alliance Launches with 40 Companies Participating," *Yonhap News*, June 18, 2015.

28 Korea Internet & Security Agency, *IoT Common Security Principle v1.0*, March 21, 2016, https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=259&dno=67&fseq=1.

29 Korea Internet & Security Agency, *IoT Common Security Guide*, October 6, 2016, https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=259&dno=80&fseq=1.

30 "Joint Efforts across All Ministries to Support Standardization of Technologies Relating to the Fourth Industrial Revolution," South Korea Ministry of Trade, Industry, and Energy, April 14, 2017.

31 South Korea Ministry of Trade, Industry, and Energy, *Strategy for Creating New Healthcare Markets*, November 12, 2013.

also reinforce indirect but related benefits stemming from robust general bilateral coordination. By demonstrating agility and responsibility in the early stages of IoT, the United States and South Korea will attract even more innovators and investors while providing a template for national, bilateral, and international strategies, thus fostering a global ecosystem that will have broadly applicable benefits.

RECOMMENDATIONS FOR INCREASED COOPERATION

Both domestic and bilateral policy and regulatory decisions should aim to increase the cybersecurity of IoT technologies while fostering innovation and adoption. In particular, government and industry stakeholders should collaborate to identify broadly applicable areas of critical concern related to IoT cybersecurity and to define best practices for addressing them. A coordinated and targeted approach to key areas of concern would help push forward impactful best practices while minimizing the potential for inconsistent and conflicting regulations and requirements, which can impede innovation. The following seven recommendations intend to address such key areas of concern for IoT cybersecurity.

Actively promote universal adoption of a common cybersecurity framework. Both nations should actively encourage the universal adoption of a common, flexible framework created through robust public-private collaboration that promotes best practices for cybersecurity governance and risk management. Specifically, they should embrace the core components of the NIST Framework for Improving Critical Infrastructure Cybersecurity, which not only includes the five critical tenets of Identify, Protect, Detect, Respond, and Recover, but also articulates specific categories, subcategories, and informative references for each.[32] Other countries, including Israel, have already begun to adopt the CSF, either wholesale, in a slightly modified form, or with a modified title but keeping the core components.[33] South Korea should begin using these core components and promote adoption of the framework nationally, and both countries should seek ways to continue encouraging global adoption more broadly, including by making explicit references to adoption in trade and other strategic partnership instruments.

Building this common foundation across organizations and countries will more clearly identify specific, tangible focus areas and opportunities for substantive cooperative engagement between government and industry and between countries. Such public-private cooperation and collaboration is already a proven hallmark of successful international cybersecurity strategy and both countries should also actively embrace it with respect to their specific approaches to IoT security.[34]

In addition, using a common framework broadly across both public and private sectors will promote the following: more effective and efficient communication regarding cybersecurity, resulting from using a common language; the ability to better benchmark across industries; and the ability to more effectively focus discussions and research efforts around commonly recognized topics in the context of the same overarching framework.[35] In the fast-evolving and diverse field of IoT, using a common framework will be particularly helpful in identifying the most broadly applicable and impactful areas of concern, helping government entities determine which areas warrant national and perhaps international engagement and resources.

By encouraging the adoption of a common framework both domestically and internationally, the United States and South Korea can then also use that common framework as a foundation for more robust bilateral coordination, collaboration, and engagement, focused on bolstering the key components of their respective national strategies and the most important cybersecurity issues. For example, the two countries could combine their efforts, through research or information sharing, to identify the most effective forms of public-private collaboration with respect to specific topics within the established common framework. The form of public-private collaboration and the specific government or private sector entities that would be most effective will likely differ depending on the topic (e.g., awareness and training, intrusion detection, prosecution of crimes, incident recovery). Given the vast breadth of potential issues related to cybersecurity, the existence of a common framework will enable both countries to

32 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*.

33 Sara Friedman, "What's Next for NIST Cybersecurity Framework?" GCN, May 16, 2017, https://gcn.com/articles/2017/05/16/nist-cybersecurity-framework.aspx.

34 "The IoT Revolution and Our Digital Security: Principles for IoT Security," U.S. Chamber of Commerce and Wiley Rein, LLP, September 19, 2017, https://www.uschamber.com/IoT-security.

35 Many of these benefits are articulated in the CSF itself.

hone in on specific areas, ensuring that bilateral coordination is most efficient and impactful.

This work of promoting universal adoption of a common framework does not represent an easy, quick win. But, it is also not overly complicated, promises to be very impactful, and most importantly, will provide a *necessary* foundation for effective and efficient follow-on work. Moreover, it should not be surprising that truly effective solutions to some of today's most complex and difficult challenges will require hard work, coordination, and, generally, the investment of time and resources.

Encourage development of international standards. The world is just beginning to witness the early development of international standards for IoT. One example is ISO/IEC CD 30141 (IoT Reference Architecture).[36] In addition to a common framework, which can be used as a high-level conceptual roadmap identifying key topics and areas of discussion and research, both countries should also promote the development of international standards. Such standards could be incorporated into or linked to the framework much like the informative references in the current version of the CSF. In promoting such standards, both countries should aim their efforts at specific issues linked to categories and subcategories of the CSF that industry and government together deem appropriate for standardization. Leveraging existing international bodies or conventions to rename or recast the CSF as a more international framework (rather than a US-based one) may be useful for increasing global adoption. However, such efforts should be careful not to turn the framework itself into a standard, as such a transformation would diminish the benefits of having a flexible and enduring overarching construct that provides the critical universal context for specific standards.

International IoT standards can provide the basis for interoperability of various IoT systems. Without interoperability, companies cannot achieve economies of scale, thus much of the business value of IoT will be lost.[37] Standards that are open and transparent can not only enable integration of various IoT systems but also increase cybersecurity in IoT systems by creating an economy of scale in cybersecurity solutions. Although it is important for governments to support the development of IoT standards, they should focus on promoting and facilitating industry efforts rather than actually making decisions on IoT standards.

Encourage adoption of Internet Protocol Version 6. There is no doubt that IPv6 is superior to IPv4 in terms of its ability to provide a larger number of unique Internet Protocol (IP) addresses.[38] IPv4 will not be able to handle the increasing demand of IoT devices because it will run out of IP addresses very soon. Furthermore, IPv6 is more secure than IPv4 as the former supports more secure host name resolution.[39] Therefore, it is clear that IPv6 will be one of the most important communication protocols for IoT devices. Unfortunately, the adoption of IPv6 has been slower than anticipated. Governments should support the development of IPv6-based technologies and encourage IPv6 adoption in public and private organizations. In addition, governments could educate organizations and individuals about the advantages of IPv6 over IPv4.

Promote security by design and privacy by design. One important barrier to the adoption of IoT systems is users' lack of confidence in data security and privacy. Therefore, it is crucial to build trust with consumers by ensuring that IoT data are well protected from malicious attacks or inappropriate privacy policies and practices. IoT devices are often developed by non-information technology companies such as consumer goods companies, which lack experience with cybersecurity and are not accustomed to prioritizing it. These companies may not be fully aware of their role in securing IoT devices. Consequently, the cybersecurity features of many IoT systems are designed with subpar skills and knowledge.

Efforts to address these security concerns by implementing more managed IoT devices and services—those that are managed by a third-party provider rather than the end user herself—in turn create greater privacy concerns for users with respect to the personal data that such third parties may collect and process. To achieve greater cybersecurity in IoT products while also addressing consumer privacy concerns and demands, government and industry must work together to address the need for this shift in priorities and to effectively cope with the constantly evolving technol-

36 "ISO/IEC CD 30141: Internet of Things Reference Architecture," International Organization for Standardization, https://www.iso.org/standard/65695.html.

37 James Manyika et al., *The Internet of Things: Mapping the Value beyond the Hype*, McKinsey Global Institute, June 2015, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx.

38 IPv5 was never formally adopted as a standard.

39 "Why IPv6 Matters for Your Security," Sophos, accessed February 8, 2018, https://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx.

ogies and risk management challenges arising in the IoT market.

As IoT devices and connected technologies continue to develop quickly and exponentially, corresponding security standards and regulations are at risk of becoming obsolete as rapidly as they are put forth. In this preliminary age of IoT development, highly structured and "top-down" regulations are both premature and more hindering than they are helpful.[40] Regulation would also be premature because of the volatile nature of consumer privacy concerns and the tenuous relationship with budding IoT markets. Instead, the "policy environment should enable cybersecurity solutions to evolve at the pace of the market," as opposed to the pace of the policymaking process.[41] Regulators should "allow IoT to develop within the current policy framework with some possible modifications."[42]

In particular, governments should promote the principles of security and privacy by design to ensure that all IoT devices are designed and produced using best practices in cybersecurity. At their core, these "by design" principles essentially mean that security and privacy issues should be considered and addressed at the earliest stages of product development, alongside basic functionality and design, rather than as add-ons or modifications to a near-final product or as aftermarket solutions. IoT manufacturers should adopt a by design approach to both security and privacy that aims to build safeguards into products upfront.[43]

The CSF's Protect function provides a useful roadmap for security. Regarding privacy, the CSF also explicitly references privacy and civil liberties in the context of the "Identify" function. Within that context, the internationally recognized Fair Information Practice Principles should be leveraged as the foundational principles guiding privacy by design for IoT developers, manufacturers, and distributers. While the limited technological capabilities available to small and low-cost IoT devices can make implementation of the security and privacy by design approach challenging, its early adoption represents a critical underpinning of responsible innovation and development in IoT.

Some of the best by design practices for IoT include the following:[44]

- IoT devices should ship with current software and should have a mechanism for automated, secure software updates
- IoT devices should use strong authentication by default
- IoT devices should use Transport Layer Security or Lightweight Cryptography to ensure secure communications
- IoT companies should look for innovative design features that will promote greater awareness and transparency regarding their data collection and usage
- IoT companies should place greater emphasis on the importance of self-regulation of privacy and encourage consumers to "manage and control their personal data more intuitively and effectively," seeking out technical innovations that would allow the consumer to be the preeminent line of defense in ensuring data privacy[45]

Other best practices that industry should be encouraged or required to pursue include the following:

- IoT developers and manufacturers should increase awareness of vulnerabilities associated with IoT systems as well as their intentions regarding the duration of continued support for the device[46]
- IoT developers and manufacturers should promote transparency regarding the behavior of IoT devices

40 Comments of US Chamber of Commerce, June 2, 2016, before the National Telecommunications and Information Administration, Department of Commerce, Washington, DC 20230, Docket No. 160331306-6306-01, April 2016.

41 Lee, *IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership*, 12.

42 Data privacy also requires cross-border coordination. Neither the United States nor South Korea can act in isolation. They must coordinate with their international partners as different countries have different approaches to protecting data privacy. For example, the European Union takes a horizontal approach to data protection, whereas the US approach is built around specific verticals involving highly sensitive data. An inconsistent patchwork of global regulations relating to data sovereignty would impede IoT innovation.

43 Julie Brill, "The Internet of Things: Building Trust and Maximizing Benefits through Consumer Control," *Fordham Law Review* 89 (2014): 205.

44 Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations*, November 2016, https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

45 Comments of Huawei, June 2, 2016, before the National Telecommunications and Information Administration, Department of Commerce, Washington, DC 20230, Docket No. 160331306-6306-01, April 2016.

46 US Department of Homeland Security, *Strategic Principles for Securing the Internet of Things (IoT)*, November 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

- The IoT device industry should create an industry-wide cybersecurity program such as security certification
- All the players in the IoT supply chain should collaborate to address evolving IoT security and privacy issues[47]

Increase investment in cybersecurity of IoT. The US and South Korean governments should reserve funding for programs designed to encourage the development of secure IoT technologies and applications. In addition, the governments should establish a cybersecurity center of excellence to engage in research and development, applications development, standards development, training, and policy development and implementation.[48] While there could be many ways to operate a center of excellence, one effective way for the United States and South Korea to collaborate is to create a platform through which two to four leading universities from both countries could create a consortium to collaborate on technology development projects funded by the governments where companies validate new technologies through pilot tests or commercialization. In addition, both governments should consider creating or expanding existing efforts to develop ways for actors in the IoT space to demonstrate their investment in and achievements related to cybersecurity, perhaps by leading or collaborating with industry on a certification program like the United Kingdom's Cyber Essentials program.[49] For example, incorporating security as a selection criterion for South Korea's K-Startup Grand Challenge could incentivize competitors to focus more on cybersecurity.[50] Both governments should actively pursue other objective ways that organizations can externally demonstrate their competitive advantage.

Educate students and workforces. If the United States and South Korea want to maintain their lead as IoT technology developers, each government must ensure their future workforce is properly educated and trained in IoT devices and data privacy issues. Both governments must set aside fiscal and human resources for continuing education in cyber and science, technology, education, and mathematics (STEM) disciplines. The demand for workers skilled in cybersecurity and artificial intelligence will be particularly strong for the foreseeable future. The governments should partner with universities to develop curricula on IoT, data science, cybersecurity, and artificial intelligence for high school and higher education; offer training opportunities to businesses; and create scholarship programs focused on STEM education.

Use a market-driven approach. In light of the significant potential benefits arising from IoT innovation and deployment, as well as the particularly competitive landscape in the IoT space, US and South Korean national policies and bilateral and international strategies should incorporate, where possible, market-driven approaches that help develop secure IoT systems while not suppressing innovation. In particular, national policies and initiatives should support research that identifies the most cost-effective IoT cybersecurity measures. Identifying not just the *best* practices but the most *cost-effective* best practices will encourage and facilitate industry's voluntary adoption of cybersecurity measures to the greatest extent possible. Moreover, by identifying best practices that may be critical but are not particularly cost-effective, government actors can more strategically focus their efforts on requiring (e.g., through law or regulation) or incentivizing (e.g., through tax breaks or subsidies) adoption where it is less likely to be voluntary.

Bilateral coordination could be used to make best practices more cost-effective, either through bilateral action aimed at reducing related costs (e.g., cost of material, facilities) or through joint research efforts to improve efficiency or identify more cost-effective alternatives in those areas. Alternatively, bilateral coordination could be used to promote the adoption of best practices that are not cost-effective, perhaps through cross-border trade incentives or regulation. Another important opportunity for bilateral coordination between the United States and South Korea lies in minimizing or eliminating the various requirements and regulations across the border for IoT products and systems. Adoption of the CSF and, therefore, a common language and plan of action could help achieve this goal. This endeavor will result in accelerated innovations and faster time-to-market for IoT companies in both countries.

---

47 Russell L. Jones and Sheryl Coughlin, *Networked Medical Device Cybersecurity and Patient Safety: Perspectives of Health Care Information Cybersecurity Executives*, Deloitte, 2013, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf.

48 Government of India, *National Telecom M2M Roadmap*, Ministry of Communications and Information Technology, May 2015, http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf.

49 "Cyber Essentials," National Cyber Security Center of the United Kingdom, accessed February 8, 2018, https://www.cyberaware.gov.uk/cyberessentials/.

50 "Home," K-Startup Grand Challenge 2017, https://k-startupgc.org/.

CHAPTER 6

PRESERVING TRUST WITH "PROSPERITY BY DESIGN"

Mr. Beau Woods

Cyber Safety Innovation Fellow, Atlantic Council

The Internet of Things (IoT) promises to save millions of lives, contribute trillions to the economies of the United States and Republic of Korea (hereafter South Korea), and transform governance. Yet high-profile cybersecurity failures in any sector would trigger a crisis of confidence to adopt these emerging technologies, delaying or denying benefits much more widely. Therefore, the greatest threat to realizing the promise of IoT is not the speed but the care with which it is deployed. To maximize these societal benefits, policies must preserve the *trust and trustworthiness* of the Internet of Things, and do so with all due haste, particularly in areas impacting human life, public safety, and national security.

Products and components that take a *security by design* approach should be favored. The safety, security, and resilience of products and components are a function of capabilities built into the product, as well as practices in the deployed environment. Automotive components such as brakes, airbags, and adaptive cruise control increase passenger safety and empower drivers. Similarly, in IoT (particularly with regards to autonomous vehicles), security capabilities reduce the cost and improve the reliability of safe, secure, and resilient operation. Policies should incentivize adoption of security by design, favoring capabilities and approaches that reliably work better and avoiding those that reliably fail.

Yet practices for security by design are not well distributed, and age quickly. New research increases the number, quality, and reliability of practices. At the same time, discoveries and effective practices are propagated in proportion to the degree of openness and collaboration in an ecosystem. And improved education and training practices improve initial security postures (e.g., software security, system architecture), increase the number and quality of defenders, and improve responses. Policies should promote openness and collaboration to increase rates of discovery and propagation of cybersecurity capabilities and capacities across the ecosystem.

Incentive alignment and their existing relationship make the United States and South Korea fit for purpose to partner on cybersecurity. These long-standing allies on opposite sides of the globe have common markets, supply chains, threats, and objectives that make collaboration beneficial to both. Strategies and policies in both the United States and South Korea should seek to bolster stability, resilience, and ties of their key regional partners through the Internet of Things.

UNFOLDING TRENDS

The Internet of Things holds great promise for both the United States and South Korea. Several concurrent revolutions are taking place in public health, transportation, energy, smart cities, and other areas. These advances are driven both by new types of computerized, connected devices and the introduction of computers and network technology to existing products. These transformations are the growth engine of both economies, spawning new business models, expanding global trade, and increasingly influencing geopolitics. Benefits accrue to society through not just convenience and economics, but also improved safety, quality of life, and capabilities unimagined in past decades.

- **Healthcare and Public Health.** In the coming decades, new diagnostic and treatment options may not just save but also improve millions of lives. These advances can be delivered more widely and inexpensively, ensuring greater availability of higher-quality care. For instance, centralized telemetry in hospitals allows fewer staff to care for more patients, reducing costs while increasing responsiveness to changes in vital signs. This has become the standard of care in both the United States and South Korea.
- **Transportation.** Smart cars promise to eliminate most road deaths,[1] reduce traffic congestion and pollution, and increase the mobility of underserved populations. In aviation, maritime, and rail, higher traffic volumes, greater fuel and cost efficiency, and improved safety records are expected. Both passenger and product logistics are radically transforming, including through drone deliveries and autonomous trucking. South Korea has built K-City,[2] a test city for autonomous vehicles, and several US states and cities permit autonomous vehicles on their streets.[3]
- **Energy Sector.** The introduction of IoT to the energy sector promises a more reliable electric grid, improved fuel production and efficiency, and greater advances in alternative and renewable energy sources. The energy sector was one of the first to adopt IoT technologies, with smart grids, and plans to rely on IoT and the cloud even more in the future, in both the United States and South Korea.[4]
- **Smart Cities.** Increasing instrumentation unlocks new capabilities for governance of the public good. Public administrators may have access to real-time environmental conditions to manage traffic congestion, air pollution, water quality, and infrastructure, among other issues, enabling more agile decision-making that is better informed with timely evidence. Songdo, near Seoul, is one of the first smart cities, and nearly two-thirds of US cities are investing in IoT capabilities.[5]

Further, billion-dollar investments today are expected to return trillion-dollar dividends over the coming years.[6] Tech goliaths like Dell,[7] IBM,[8] Cisco, and Samsung[9] have each invested over a billion dollars in the

---

1 According to the National Highway Traffic Safety Administration, more than thirty-five thousand deaths each year are attributable to human error. See "Automated Vehicles for Safety," National Highway Traffic Safety Administration, accessed November 30, 2017, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

2 Stacy Liberatore, "South Korea Reveals Plans for Giant Self Driving Car Town Named K-City," *Mail Online*, May 9, 2017, http://www.dailymail.co.uk/~/article-4489398/index.html.

3 Ryan McCauley, "How States Are Legislating Autonomous Vehicles (Interactive Map)," *Future Structure* (blog), July 11, 2017, http://www.govtech.com/fs/How-States-Are-Legislating-Autonomous-Vehicles-Interactive-Map.html; Patrick Caughill, "South Korea Built a 'City' to Test Self-Driving Cars," *Futurism* (blog), November 9, 2017, https://futurism.com/south-korea-built-city-test-self-driving-cars/.

4 GSM Association, *KT MEG: Korea's Smart Energy System*, November 2017, https://www.gsma.com/iot/wp-content/uploads/2017/11/KT-MEG_GSMA_RA.pdf.

5 Ross Arbes and Charles Bethea, "Songdo, South Korea: City of the Future?" *The Atlantic*, September 27, 2014, https://www.theatlantic.com/international/archive/2014/09/songdo-south-korea-the-city-of-the-future/380849/; Teena Maddox, "66% of US Cities Are Investing in Smart City Technology," *TechRepublic*, November 6, 2017, https://www.techrepublic.com/article/66-of-us-cities-are-investing-in-smart-city-technology/.

6 "Roundup of Internet of Things Forecasts and Market Estimates, 2016," *Forbes*, November 27, 2016, https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#40bef0c5292d; "IoT Market | 2018 Forecast Size and Growth Projections by Country, Year, Industry Market Verticals, and Analysts," Postscapes, accessed November 1, 2017, https://www.postscapes.com/internet-of-things-market-size/.

7 Barb Darrow, "Dell Technologies Launches New IoT Division," *Fortune*, October 10, 2017, http://fortune.com/2017/10/10/dell-technologies-new-iot-division/.

8 "IBM Says to Invest $3 Billion in 'Internet of Things' Unit," Reuters, March 31, 2015, https://www.reuters.com/article/us-ibm-investment/ibm-says-to-invest-3-billion-in-internet-of-things-unit-idUSKBN0MR0BS20150331.

9 "Samsung Electronics Says to Invest $1.2 Billion in U.S. for 'Internet of Things,'" Reuters, June 21, 2016, https://www.reuters.com/article/us-samsung-elec-investment-iot/samsung-electronics-says-to-invest-1-2-billion-in-u-s-for-internet-of-things-idUSKCN0Z71PH.

Dallas "Smart District" development project. *Photo credit*: skys the limit2/Flickr.

Internet of Things, and McKinsey estimates the annual market may reach $11.1 trillion per year by 2025.[10] These investments are coming from sources as diverse as federal, state, and local governments; private equity, venture capital, and industry; and nonprofits, individuals, and Kickstarter-sized campaigns. Beyond the hardware and software themselves, the top- and bottom-line benefits will include new business lines, markets, and cost efficiencies for organizations, industries, and society. IoT devices are expected to underpin further trillions of dollars of the global economy by replacing older technologies. South Korea and the United States are expected to be global leaders in the IoT market by 2020.[11]

As our dependence shifts from human capital to IoT, these technologies will increase the speed and scale at which risks manifest, and introduce new vulnerabilities and failure modes. Failures to date have largely been confined to financial costs and privacy breaches, whereas future failures in the Internet of Things will impact public safety, human life, and national security. It is hard to overstate how big a financial and societal bet the world is making on the Internet of Things.

As dependence increases, so must dependability—of systems, supply chains, and partners. Yet an inability to protect credit card numbers, personal information, and IoT devices has routinely been demonstrated. High-profile incidents where cybersecurity impacts human life and public safety may shatter—not erode—public confidence in the market and in government, putting individual investments, national security, and the economy at risk.

Global supply chains, markets, adversaries, and effects call for global approaches. The current administration's first Cyber Executive Order makes its priority clear that "as a highly connected nation, the United States is especially dependent on a globally secure and resilient inter-

10 James Manyika et al., *Unlocking the Potential of the Internet of Things*, McKinsey & Company, June 2015, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx.

11 "South Korea Leads 2017 IDC Asia Pacific IoT Readiness Index," *Networks Asia*, July 17, 2017, https://www.networksasia.net/article/south-korea-leads-2017-idc-asia-pacific-iot-readiness-index.1500261180.

net and must work with allies and other partners."[12] It is critical that the United States and South Korea collaborate to safeguard the promise of IoT and avoid potential peril. This chapter articulates policy objectives and recommendations for how to do so.

POLICY ISSUES AND STRATEGIC IMPLICATIONS

Events of the past eighteen months[13] have demonstrated that the world is neither prepared nor equipped to address defensive lapses in a market segment that independently represents trillions of dollars to the US and South Korean economies, and that increasingly supports the majority of each nation's gross domestic product. Meanwhile, IoT devices in design phases today will be on the road, in the skies, and on the water—powering critical infrastructure—for decades to come. Policy makers weighing alternate approaches must account for both short-term and long-term effects of action—or lack thereof.

Greater consequences, systemic risks

In addition to impacts found in traditional information and communications technology (ICT) equipment, cybersecurity failures in IoT have greater consequences. As Josh Corman, chief security officer at PTC and cyber safety innovation fellow at the Atlantic Council, has said, "through our over dependence on undependable IT [information technology], we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economies, and national security."[14]

The same technologies that can improve and save lives can also harm or take them. As critical infrastructure and public safety systems are increasingly adopting IoT, the benefits—and the downfalls—of globally connected, software-defined capabilities have become more pronounced. Preventable, automated attacks affecting IoT systems have led to a degraded United Kingdom National Health Service, global vaccine shortages, and further consequences that affect human life and public safety—not to mention hundreds of millions of dollars in costs to companies.[15]

National security and prosperity depend on the reliable, safe, secure, and resilient operation of critical infrastructure. Systems across these sectors increasingly rely on connected software for operations and safety. Both software and its connectivity shift risk models toward greater centralization (e.g., failures tend to spread rapidly) from more distributed ones (e.g., failures tend to remain isolated). Exposure to hazardous and hostile conditions through connectivity, therefore, imposes systemic risk across organizations, sectors, and society. At the same time, high-intent adversaries are increasingly acquiring capabilities to threaten national security through cyberattacks.

Additionally, citizens and governments globally have become increasingly concerned about privacy in the Internet of Things. The Federal Bureau of Investigation (FBI) has warned of the privacy risks of toys,[16] researchers have demonstrated remote spying capabilities in cameras,[17] and retailers have pulled smartwatches from shelves over privacy concerns.[18] While privacy concerns have failed to substantially shift buying behavior, changes in sentiment or legislation—particularly from these higher consequences to human life, economies, and national security—could catch manufacturers flat if they are unprepared to adapt their business models and devices to meet changing requirements.

Exotic sources of potential harm, like bioterror or cyberattacks, play an outsized role in shaping consumer confidence in key markets. Too often when a security risk is discovered and reported privately or publicly, companies attempt to cover it up, which preserves the

12 White House, United States Government, Executive Order No. 13800, 3 C.F.R. 32172 (2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

13 Notably, including high-profile incidents such as the Mirai botnet formation and its impact on domain name system infrastructure and the WannaCry and NotPetya attacks.

14 Statement by Joshua Corman, "Cybersecurity of the Internet of Things," Hearing, Before the Subcommittee on Information Technology, 115th Congress, 1st session, 2017, https://oversight.house.gov/wp-content/uploads/2017/10/Corman_Testimony_IOT_10032017.pdf.

15 Fred O'Connor, "NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue," cybereason, November 9, 2017, https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue.

16 Alyssa Newcomb, "FBI Warns Parents of Privacy Risks with Internet-Connected Toys," NBC News, July 18, 2017, https://www.nbcnews.com/tech/security/fbi-warns-parents-privacy-risks-internet-connected-toys-n784126.

17 Danny Palmer, "Security Vulnerability in IoT Cameras Could Allow Remote Control by Hackers," *ZDNet*, November 14, 2017, http://www.zdnet.com/article/security-vulnerability-in-iot-cameras-could-allow-remote-control-by-hackers/.

18 Joseph Venable, "Child Safety Smartwatches 'Easy' to Hack, Watchdog Says," BBC, October 18, 2017, http://www.bbc.com/news/technology-41652742#share-tools.

risk while undermining public confidence.[19] A crisis of confidence in the public to trust IoT will delay, deny, or degrade societal and economic benefits.

Adversary types, capabilities, and willingness

The total number of adversaries is growing, high-intent adversaries are increasingly capable, and high-capability adversaries are ever more willing to use cyberattacks to advance their interests. Tools, tactics, and processes tend to propagate from highest-capability adversaries to the lowest within months to years; meanwhile, critical cyber systems have lifespans of decades. And while some adversaries may be chastened by potential harm from safety-impacting systems, others may seek these systems out. For instance, ideological actors may wish to inflict harm, and criminal groups may suspect owners will pay higher ransoms. It seems only a matter of time before these criminal groups deliberately monetize vulnerable IoT devices. Indeed, the Mirai botnet, WannaCry, and NotPetya incidents may have provided a blueprint to do just that.

Global supply chains, markets, and economics

Cyber safety issues impact both developed and developing states, largely through global supply chains and markets. Where incentives and objectives align, states are likely to cooperate, even if they disagree on other policies. At the same time, changes to quality, reliability, cost, and speed to market tend to propagate throughout the supply chain, benefiting or harming all parties. A more diverse supply chain gives final goods assemblers more choices for delivering the product they want, assuming they can tell a difference in suppliers and can factor in all of their costs.

Forces in a free and fair market tend to be self-correcting, if consumers can distinguish among market alternatives and understand costs, responsibilities, and risks. IoT buyers frequently complain that they cannot tell the difference between the security posture of one IoT device and another. For some, this means they guess at securing them; for others, this means they overinvest. In either case, risk and cost are suboptimal. The Mayo Clinic, one of the world's most prestigious healthcare providers, found after extensive security testing that most medical IoT devices are "just another crappy computer."[20] Yet they are not just another computer, which further obscures distinctions between devices and accounting for costs.

To address these issues, aftermarket IoT security systems have developed that may compete with or erode markets for secure IoT devices. On the one hand, the burgeoning market for IoT security can give manufacturers and buyers more options. On the other hand, operators often feel compelled to add cost to compensate for shortcomings in design. Or worse, operators or others may be harmed through misalignment of incentives or failure to understand cyber safety and security responsibilities. The proliferation of low-cost, low-hygiene devices alongside high-value, highly dependent systems creates a hazard for resilience of societies, markets, and national security.

POLICY OBJECTIVES

Technology and trade strategy tends to seek increased market availability and competitiveness of businesses and products domestically and globally. One of the largest threats to this strategy in the Internet of Things is trust. Yet unfounded trust is quickly shattered in the presence of ever more capable and willing adversaries, or the random accidents that can have similar effects. Where this loss of trust halts or delays adoption, the societal, economic, and national security benefits that the Internet of Things could bring are also lost.

Therefore, this paper argues for an IoT cyber safety and security strategy *that assures trust through trustworthiness in IoT technology, especially that with an ability to directly impact human life and public safety.*

Favor more secure IoT components, products, and practices

Public and financial interests benefit from encouraging those practices that experience shows reliably work, and avoiding those that reliably fail. Capabilities built into the product from the design phase tend to improve effectiveness, lower costs, and give operators more capabilities, as compared with those that are bolted on later. These capabilities defend, dissuade, and deter adversaries, often at a lower overall cost than alternative measures. Where device capabilities extend to the cloud, mobile applications, or device app stores, the same principle applies. Further, built-in capabilities can improve the effectiveness of security measures

19 Michael Herh, "Hacking of Home IoT: Home IoT Hackings on Rise with Manufacturers Engrossed in Hushing Them Up Only," *BusinessKorea*, November 2, 2017, http://www.businesskorea.co.kr/english/news/industry/19694-hacking-home-iot-home-iot-hackings-rise-manufacturers-engrossed-hushing-them.

20 Food and Drug Administration, *Moving Forward: Collaborative Medical Device Cybersecurity*, 2016, https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM489250.pdf.

within a deployed environment, increasing the value of other IT and security products. This idea, sometimes called security by design, is key to both US[21] and South Korean[22] IoT and cybersecurity strategies and policies.

Promote openness and collaboration toward greater cybersecurity capabilities and capacities

"The future has arrived, it's just not evenly distributed yet." - William Gibson, 1992[23]

Improved openness and collaboration between South Korea and the United States bolsters American economic and social benefit by improving the quality and diversity of supply chain components, finished goods, and expertise. This is one reason why both US and South Korean strategies and policies for cyberspace and for IoT favor openness and collaboration, in addition to strengthening cybersecurity. Stable public platforms and services, threat information sharing, coordinated vulnerability disclosure, procurement transparency, as well as common commercial and open-source software components speed innovation, increase reliability, and reduce security issues, other things being equal. Openness and collaboration can also increase awareness, education, and workforce development, cornerstones of US and South Korean IoT strategies and policies. *Openness is not the inverse of security; each can strengthen the other and build trust in products and ecosystems.*

Bolster stability, resilience, and ties between key regional partners, the United States and South Korea

The United States and South Korea have a long history of economic, technological, and political cooperation over the last few decades. South Korea is one of few advanced, democratic, capitalist economies in Northeast Asia. The United States and South Korea stand to benefit from stronger economic ties, amid a sea of less predictable, less ideologically compatible nations. High-tech exports are a large segment of South Korean exports, and a large segment of US imports. Improved security, resilience, and trustworthiness of IoT improves the national security and economies of both nations.

US and South Korean strategies and policies for cyberspace and for IoT favor openness and collaboration, in addition to strengthening cybersecurity.

CONCLUSION

It is certain that governments, companies, and individuals will increasingly adopt and depend on IoT devices. Failure to address the safety and security issues inherent in such dependence allows accidents and adversaries to undermine public safety, the economy, and national and international security. The United States and South Korea together have a great deal of control over—and responsibility for—assuring the *global* benefits of IoT.

Collaboration between these two nations to raise the bar for cyber safety and security improves the chances of success, and benefits both economies, by hastening progress. In the absence of such a collaborative effort, progress will be delayed, allowing others to take the lead. The future looks bright for the United States and South Korea, if the promise of the Internet of Things holds. If IoT cybersecurity is done right, the United States and South Korea can make the world *safer, sooner, together.*

---

21 For instance, the president's commission report stated bluntly "The United States must lead a global push to drive security and secure development concepts into IoT design and development." See Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry*, Public Health Emergency, June 2, 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.Health Care Industry Cybersecurity Task Force.

22 For instance, see "Master Plan for Building the Internet of Things (IoT) That Leads the Hyper-Connected, Digital Revolution," Ministry of Science, ICT and Future Planning, May 8, 2014, http://www.kiot.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf; "IoT Common Security Principles v 1.0," Ministry of Science, IT and Future Planning, September 27, 2016, https://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=IoT_%EA%B3%B5%ED%86%B5%EB%B3%B4%EC%95%88%EC%9B%90%EC%B9%99_V1(%EC%9B%B9%EC%9A%A9).pdf.

23 "The Future Has Arrived — It's Just Not Evenly Distributed Yet," Quote Investigator, January 24, 2012, https://quoteinvestigator.com/2012/01/24/future-has-arrived/.

RECOMMENDATIONS FOR INCREASED COOPERATION

Align incentives to favor cyber safety and security by design

As demonstrated above, there is a coalescing set of practices known as security by design. These practices collectively decrease operational risk and cost, as well as cut down on externalities that pay dividends to the broader economy. However, initial costs for these devices may be higher than for those without built-in security. External forces can rebalance incentives for buyers and sellers to allow better accounting for full costs and risks.

These forces may also include specific policies to bolster incentives for or reduce barriers to replacing less safe and secure IoT devices with those that are safer and more secure. This type of action tends to be particularly useful in addressing externalities, among the hardest problems to address in a free market. The US Health and Human Services (HHS) Health Care Industry Cybersecurity Task Force has proposed a program for medical devices similar to the 1990s "Cash for Clunkers" program for cars.[24] This step would need to be coupled with a set of requirements for both targeted devices, and their replacements, to ensure those devices most likely to cause harm are replaced, and that the replacements are significantly better.

The US legislative or executive branch should also study the impact of increased barriers or negative incentives for unsafe IoT devices or components. Some products and components, such as chlorofluorocarbons and lawn darts, are already banned or restricted from import and sale in the United States because they are considered unsafe. Unpatchable IoT devices have been compared to lawn darts, a toy that proved deadly and has been banned by several countries.[25] And the aforementioned HHS task force recommended evaluating a Montreal Protocol–like approach to preserve patient safety.[26] While increasing tariffs and trade restrictions may raise costs (or reduce availability) of lower-quality goods, overall costs of ownership, operation, and maintenance may be expected to decrease. And US trade with South Korea may, in fact, fare better under such an arrangement, as products and components from their companies tend to be of higher quality and cost, as compared with many of their global competitors.

Evaluate new models of improving IoT cybersecurity

The United States and South Korea can collaborate by jointly funding, researching, and evaluating these new models, promoting adoption of the successful ones. As the US president's commission report pointed out, "as our cyber and physical worlds increasingly converge, the federal government should work closely with the private sector to define and implement a new model for how to defend and secure this infrastructure."[27] And Executive Order 13800[28] called for new approaches to national cyberdefense. The United States can collaborate with South Korea on this path.

Given the two nations' strong manufacturing experiences, and the nature of the Internet of Things, one of these evaluations may center on continuous improvement processes applied to IoT. Over the past few decades, lean manufacturing practices have transformed the automotive industry, increasing quality, reducing cost, and speeding time to market. Similar practices have only recently become prevalent in the IT industry, and for some early adopters in the IoT industry.[29] If the results of continuous improvement hold for the Inter-

24 "Cash for Clunkers" offered credit towards a new car for those trading in their older cars. This practice was designed to stimulate the economy and reduce the level of pollution by getting higher-emissions vehicles off the road. Problems in implementation meant that these objectives may not have been realized. Effects, similarities, and differences should be accounted for if a similar program is tried. See Atif Mian and Amir Sufi, "The Effects of Fiscal Stimulus: Evidence from the 2009 'Cash for Clunkers' Program," Working Paper, National Bureau of Economic Research, September 2010, http://www.nber.org/papers/w16351.pdf.

25 Corman, testimony on Cybersecurity.

26 The Montreal Protocol is a highly successful international trade agreement that reduces the market for ozone-depleting chemicals. See Duncan Brack, "The Use of Trade Measures in the Montreal Protocol" in *Protecting the Ozone Layer* (Springer, Boston, MA, 1998), 99–106, https://doi.org/10.1007/978-1-4615-5585-8_14.

27 Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry*, United States Government, June 2017, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

28 Executive Order No. 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," White House, May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

29 These practices are often called DevOps, and when cybersecurity is included, DevSecOps or Rugged DevOps. A good infographic and overview can be found in "Infographic: DevOps Lessons from Lean Auto Manufacturing," *DevOps*, February 2, 2017, https://devops.com/infographic-devops-lessons-lean-auto-manufacturing/. See also Gene Kim, Kevin Behr, and George Spafford, *The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win*, 1st Edition (IT Revolution Press, 2013).

BOX 3. CYBER SAFETY AND SECURITY BY DESIGN

While there is no authoritative list of practices considered cyber safe or secure by design, it is worth highlighting a few commonalities in corporate practice and US government policy documents. Many of these are consistent with standards, proposed legislation, industry guidelines, and other documents previously issued by the US government. Some of the processes, capabilities, and ongoing practices are described below.

- Software update mechanism. Software tends to age like milk rather than wine, unless it is updated.[1] A built-in capability to accept a security update gives operators a much greater capability to prevent and respond to security or safety incidents. One of the most mature capabilities in the IT industry is to deliver prompt, agile, and secure updates.
- Coordinated vulnerability disclosure policy. Software vulnerabilities are an inevitable byproduct of software development. Those who accept reports of security vulnerabilities have a defensive advantage over those who discourage such reports.
- Isolation and segmentation. Isolation of critical operational components from networked components improves resilience of IoT devices against hazardous and hostile conditions, and can allow the device to function, perhaps in a diminished capacity, when failure occurs.
- Secure development life cycles. Secure software and hardware development standards and frameworks help manufacturers accelerate maturity of their processes. Practices such as those documented by the International Organization for Standardization, the National Institute of Standards and Technology, Microsoft, and others include key elements such as adversarial resilience modeling (sometimes called threat modeling), fault tree analysis, penetration testing, software and hardware traceability, and component analysis.
- Changeable credentials. Any adversary who knows—or can guess—an IoT device's password can gain access. Hardcoded passwords hamstring defenders and are often publicly available on the internet and in product manuals.
- Forensically sound evidence capture. Devices that have the capability to capture and preserve evidence of tampering or operational deviations greatly facilitate safety and security investigations, especially when this evidence is, itself, tamper resistant.

1 Andy Ozment and Stuart E. Schechter, *The Security of OpenBSD: Milk or Wine?*, Massachusetts Institute of Technology, December 2006, https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/061223_Schechter-Ozment.pdf.

net of Things, citizens and companies in the two countries will enjoy similar effects through fewer software defects, less elective complexity, greater traceability, improved ability to forecast cost and risk, and more agile responses to security issues. This strategy not only aligns with emerging industry best practices, it matches principles laid out in US policies and in South Korean strategy.

Other promising approaches apply advanced capabilities and practices to improving security-by-design capabilities. For instance, a Defense Advanced Research Projects Agency project[30] underway now seeks to automatically detect, determine, and enforce safe and secure configurations in complex systems. This could allow operators to more closely match system configuration with principles of least-privilege and minimized complexity, as well as inform manufacturers of optimal defaults. These practices would greatly reduce the attack surface presented to adversaries, increasing defenders' efficiency.

30 Jacob Torrey, "Configuration Security (ConSec)," Defense Advanced Research Projects Agency, accessed December 31, 2017, https://www.darpa.mil/program/configuration-security.

Improve transparency throughout the supply chain

Internet of Things device makers and operators alike struggle with managing security vulnerabilities. Transparency can help both stakeholder groups distinguish products and components and account for the full cost and risk of decisions. Both of these properties enhance free market forces to shape cybersecurity and safety capabilities.

The United States and South Korea can collaborate to promote, refine, and standardize the Software Bill of Materials (SBOM) and other forms of transparency for IoT cyber safety and security. Buyers who can analyze the composition of goods can factor their quality and provenance into their decision-making. The US president's Commission on Enhancing National Cybersecurity called for a "nutrition label" for IoT cybersecurity, and Executive Order 13800[31] called for "Supporting Transparency in the Marketplace." There has been other work in labelling, and it seems to be coalescing around the concept of an SBOM.

An SBOM allows buyers to understand the amount and complexity of software, as well as known software defects. Further, when vulnerabilities or end of life for these components become known, the owner and operator can quickly tell whether, where, and how they are affected. The Mayo Clinic, Exxon,[32] the Financial Services Information Sharing and Analysis Center,[33] the Financial Services Sector Coordinating Council,[34] Underwriters Laboratories,[35] and others have published processes, guidance, and standards. Congressional bills,[36] hearings,[37] and direction,[38] as well as executive action[39] also have specified SBOMs.

Promote greater education and societal participation in IoT security

The United States and South Korea can collaborate to share knowledge and practices, which would increase the percentage of new workforce entrants in many fields with some exposure to cybersecurity. Both the United States and South Korea call for greater awareness, knowledge, experience, and education in IoT security.[40] While labeling can greatly assist in making the general public aware, more technically inclined individuals often benefit from more diverse and extensive resources. Some formal programs exist, such as cybersecurity courses for computer science students in college and high school, as well as academic research programs. There is also a large and growing number of people learning informally, through independent experimentation and research. Formal and informal capacity building should be supported and promoted.

Universities provide an ideal forum for teaching cybersecurity principles, as well as developing expertise. However, a surprising percentage of university students—even those studying computer science and engineering—graduate without having any formal education on cybersecurity. This must change. Instilling students with an understanding of basic cybersecurity principles and postures greatly improves their marketable skillset and increases their awareness of more secure methods. Curricula that include education on defensive programming, restricted codebase languag-

31 Executive Order No. 13800.

32 Dan Perrin, "A New Narrative on Cyber Security," *The Hill*, May 4, 2016, http://thehill.com/blogs/congress-blog/technology/278712-a-new-narrative-on-cyber-security.

33 Third Party Software Security Working Group, *Appropriate Software Security Control Types for Third Party Service and Product Providers*, White Paper (Financial Services Information Sharing and Analysis Center, October 2015), https://www.fsisac.com/sites/default/files/news/Appropriate%20Software%20Security%20Control%20Types%20for%20Third%20Party%20Service%20and%20Product%20Providers.pdf.

34 Financial Services Sector Coordinating Council, *Purchasers' Guide to Cyber Insurance Products*, 2016, https://www.fsscc.org/files/galleries/FSSCC_Cyber_Insurance_Purchasers_Guide_FINAL-TLP_White.pdf.

35 "Cybersecurity," Underwriters Laboratories Cybersecurity Assurance Program, industries.ul.com/cybersecurity.

36 Mark R. Warner, US Senator from the Commonwealth of Virginia, "Senators Introduce Bipartisan Legislation to Improve Cybersecurity of 'Internet-of-Things' (IoT) Devices," press release, August 01, 2017, www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36. For the bill, see Mark Warner, "Internet of Things (IoT) Cybersecurity Improvement Act of 2017," Pub. L. No. S.1691 (2017), https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017.

37 "Cybersecurity of the Internet of Things," Hearing before the Subcommittee on Information Technology, House of Representatives, 115th Congress 1 (2017), https://oversight.house.gov/hearing/cybersecurity-internet-things/.

38 Energy and Commerce Committee, "Walden Asks HHS to Convene Sector-Wide Effort to Develop Software Bill of Materials for Health Care Technologies," press release, US House of Representatives, November 16, 2017, energycommerce.house.gov/news/press-release/walden-asks-hhs-convene-sector-wide-effort-develop-software-bill-materials-health-care-technologies/.

39 Joshua Higgins, "NTIA's 2018 Cyber Agenda Will Focus on 'Software Component Transparency,' IoT Security," *Inside Cyber Security*, December 27, 2017, https://insidecybersecurity.com/daily-news/ntia%E2%80%99s-2018-cyber-agenda-will-focus-%E2%80%98software-component-transparency%E2%80%99-iot-security.

40 Including, most recently, Executive Order 13800.

Apple's HomePod speaker. *Photo credit*: Martin Hajek/Flickr.

es, static and dynamic testing tools, the Rugged Handbook and Rugged Implementation Guide,[41] and other practices greatly improve students' ability to code securely. Competitions such as the Atlantic Council's Cyber 9/12 Student Challenge[42] and the National Collegiate Cyber Defense Competition[43] encourage students from many disciplines to learn and apply cybersecurity principles and practices in their own fields of study.

The United States and South Korea can study and learn from each other's experience with cybersecurity education. Primary and secondary education in the United States increasingly rely on computers, tablets, mobile devices, and IoT. Many schools have classes with technology at the center. South Korea runs a series of cybersecurity high schools[44] that have implemented informal educational programs and facilities that teach technology primitives, encourage skills building, and develop accurate mental models, hence creating a more cybersecurity-savvy population.

In the United States, the nonprofit Hak4Kidz,[45] Safe and Secure Online,[46] and Hacker Highschool[47] teach children and young adults how technology works, how to safeguard themselves online, and some basic skills that can help build suitability for the IT and cybersecurity workforce. Maker- and hackerspaces provide safe venues where individuals can learn how technology works and create in a high-collaboration environment. Hackerspaces are like modern-day tinkerer's labs,

41 "Home," Rugged Software, www.ruggedsoftware.org.

42 Atlantic Council Cyber 9/12 Student Challenge, Atlantic Council, www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12.

43 "Home," National College Cyber Defense Competition, nationalccdc.org.

44 Among around twenty high schools in South Korea specialized in IT, the listed are the most representative schools in cybersecurity: Hansei Cyber Security High School (www.hansei.org), Sunrin Internet High School (www.sunrint.hs.kr), Dongil Technical High School (www.di.hs.kr), Korea Digital Media High School (www.dimigo.hs.kr), Semyeong Computer High School (www.smc.hs.kr), and Buil Electronics and Design High School (http://buil.hs.kr).

45 "Home," Hak4Kidz, www.hak4kidz.com.

46 "Home," Safe and Secure Online, www.safeandsecureonline.org.

47 "Home," Hacker High School, www.hackerhighschool.org.

where experimentation and failure lead to innovations that become patents, startups, art projects, and other societal benefits. These facilities can also serve as independent testing labs for IoT devices, similar to the several cyber ranges in the United States, and the Korea Internet & Security Agency's (KISA) IoT testing lab.

The South Korean government and private sector can accelerate the benefits from civil society initiatives, which can help IoT device makers improve cybersecurity cost-efficiently. The international Open Web Application Security Project frameworks are widely used globally to improve cybersecurity and in procurement standards. BuildItSecure.ly[48] provides advice, guidance, reference models, and other resources for Kickstarter-sized companies that cannot afford this expertise internally. And I Am The Cavalry,[49] a grassroots initiative with global reach, has developed frameworks for industries to improve cyber safety, as well as helped bring together various stakeholders in high-trust, high-collaboration environments to bridge gaps between experts in different domains. These initiatives fill the gap where the public sector cannot act, and the private sector will not act.[50] However, adoption by South Korean companies and individuals is lower than in other countries, as there is little awareness, little participation, and few Korean-language translations.

The US and South Korean governments should lead by promoting and incentivizing engagement with civil society initiatives, as well as hacker- and makerspaces.[51] Document translation would reveal emerging global practices to the South Korean market more quickly and bring insights back to the global initiatives. Inclusion of these materials in government outreach (such as KISA's work with small businesses) and academic courses could further improve awareness of the latest global expertise to South Korea's domestic market. The government could also look to confer social and/or financial rewards for individual and corporate participation, such as public recognition, certifications, competitions, or prizes. Participation in these groups and spaces would build South Korean domestic capabilities, global influence, and integration into international cybersecurity research communities.

South Korean white hat security researchers are already known as some of the best in the world, yet they remain a relatively untapped resource at home and in the United States. Where these researchers find security flaws and can report them in good faith, manufacturers, owners, and operators can improve the security and safety of IoT devices. New markets, companies, and services are emerging to accelerate these defensive practices, such as Vulnerability Coordinators and Bug Bounty programs, which bolster both the US and South Korean economies and the security of IoT devices. In addition, this type of informal education and expertise-building has produced many of the current and future generations of IoT security experts (including the author). Yet legal restrictions and other barriers chill investigation and reporting of these flaws.

South Korea and the United States can take steps together and individually to greatly increase cooperation between their organizations, companies, and workforces. The Korea-US Free Trade Agreement, which includes provisions of the original US Digital Millennium Copyright Act (DMCA), should be updated to reflect rules that unlock both security research and business models.[52] This would remove barriers for highly skilled South Korean white hat security researchers to participate in programs such as Hack the Pentagon and Microsoft's BlueHat Prize. These programs, in turn, could serve as models for the South Korean private sector and government to learn from. The South Korean government can play a leading role in making this practice more culturally acceptable by ensuring vulnerability disclosure is viewed as a natural part of a continual improvement process.[53]

48 "Goals," Build It Secure, www.builditsecure.ly.

49 "I Am The Cavalry Cyber Safety Outreach," I Am The Cavalry, www.iamthecavalry.org.

50 Paraphrased from Eli Sugarman in Commission on Enhancing National Cybersecurity, *Panelist Statements* (Meeting of the Commission on Enhancing National Cybersecurity, Berkeley, CA: University of California, Berkeley, 2016), 13. https://www.nist.gov/sites/default/files/documents/2016/09/12/june21_panelist_statements.pdf.

51 For instance, through the Korean Ministries of Technology, Industry, and Energy, and of Science and ICT, along with the US Departments of Commerce and State.

52 Aaron Alva, "DMCA Security Research Exemption for Consumer Devices," Blog, Federal Trade Commission, October 28, 2016, https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices.

53 Sometimes such programs are viewed as failures—which carry a high cultural stigma that would discourage adoption—by South Korean software developers and companies. One of the authors informally collaborated on a Sunchon University effort to reframe startup failures in a similar way, in order to increase entrepreneurialism and innovation in South Korea.

Share resources, experiences, and expertise among governments, corporations, and independents

Foster collaboration where the United States and South Korea have shared interests, and where investments can benefit both nations. Both countries share similar threats from more- and less-predictable parties in cyberspace, including ideological, criminal, and state adversaries. Sharing information among law enforcement, intelligence agencies, industry players, and other stakeholders can improve the knowledge and defensive postures of both countries.

Long-established organizations, like Computer Emergency Response Teams, help governments, academia, and industry coordinate on emerging cyberattacks, vulnerabilities, and other internet issues. Newer organizations, such as Information Sharing and Analysis Centers and Organizations, can similarly play an important role for industry segments and geographic areas. **These organizations are primarily comprised of US firms, and the South Korean government could encourage more South Korean firms to join as well.**

The United States and South Korea can also coordinate on investments that can serve a common good. Where knowledge gained from cyber ranges and testing labs can benefit both societies, it makes sense to share. And collaborations at each other's facilities can allow researchers to share testing methods and experience, and build relationships. Similarly, collaborating on startup incubators could serve both markets by building experience and market value. South Korea has launched at least two such incubators in Northern Virginia, and the United States can do the same in South Korea.

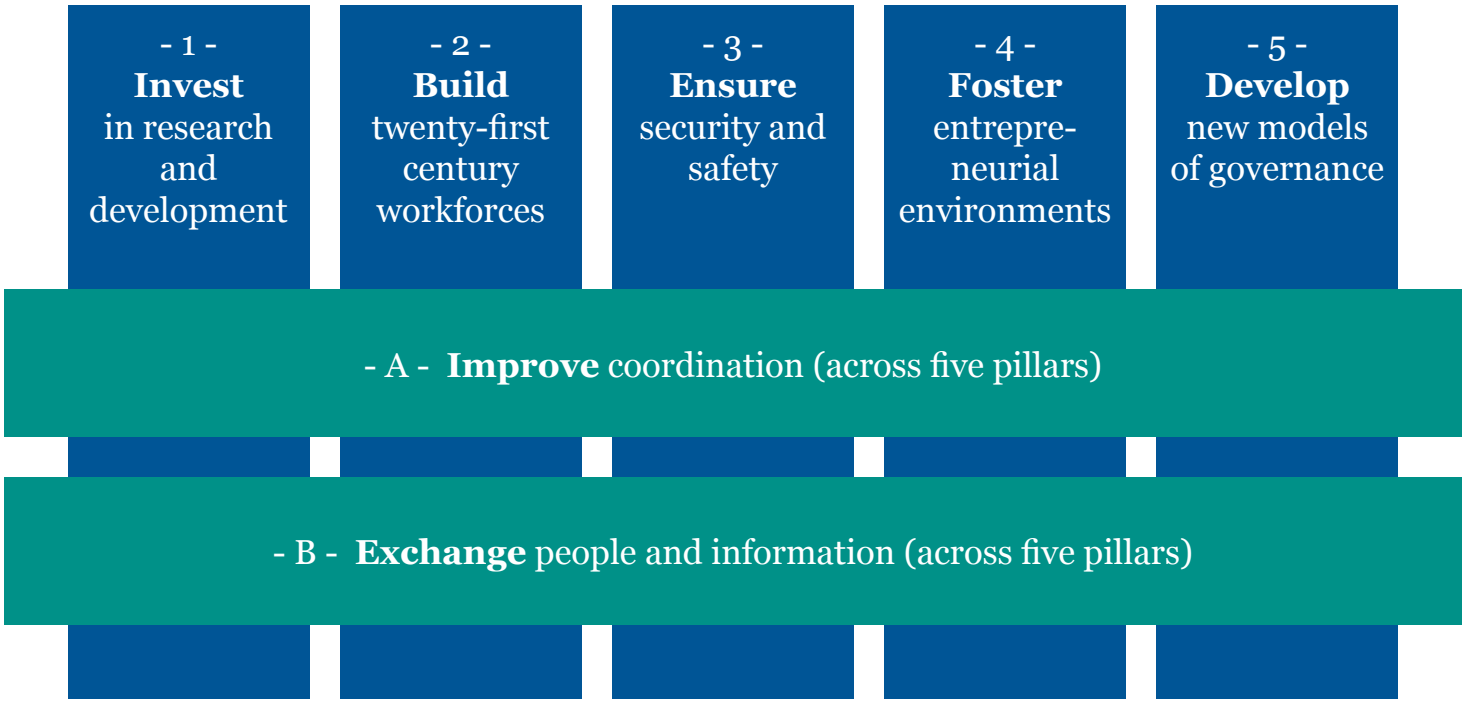
***

The Atlantic Council wishes to thank Nuri Jeon for her invaluable contribution to this chapter: researching Korean-language policy documents and ensuring recommendations are optimized for both US and South Korean contexts.

RECOMMENDATIONS FOR INCREASED US-REPUBLIC OF KOREA COOPERATION

Based on the recommendations in each chapter, a strategic framework for building a Smart Partnership emerges. This framework includes five areas in which the United States and the Republic of Korea (hereafter South Korea) can focus their collaboration: (1) investing in research and development; (2) building twenty-first-century workforces; (3) ensuring security and safety; (4) fostering entrepreneurial environments; and (5) developing new models of governance. Two building blocks support these five pillars: (A) improving coordination and (B) exchanging people and information. The recommendations included within each pillar are relevant for stakeholders in government, private industry, academia, and civil society. The United States and South Korea will need to work together across disciplines and at multiple levels to successfully navigate the Fourth Industrial Revolution's disruptive changes.

A Strategic Framework for Building a Smart Partnership



1. INVEST IN RESEARCH AND DEVELOPMENT

Investment in both basic and applied research and development (R&D) is one of the fundamental building blocks for maintaining a competitive advantage in emerging and cutting-edge technologies like artificial intelligence (AI), biotechnology, and the Internet of Things (IoT). Governments traditionally have more tolerance for risk taking on basic research, which typically has a longer time horizon before any breakthroughs can be easily commercialized. By contrast, the private sector prefers research and development that can yield new products and services over the near-to-medium term. For the United States and South Korea to gain the most returns on their investment in R&D, these countries must work together to identify appropriate areas for investment; align their programs and establish joint initiatives; leverage civil society and other stakeholders; and reduce barriers to cooperation wherever they exist. Below are some of the key recommendations of this report that relate to investing in research and development.

Identify priority areas for R&D.

» Two candidates for pre-commercialization research are advanced computing, which includes quantum computing, and brain science. (Chapter 1)

» Korea's Ministry of Trade, Industry, and Energy and the US Department of Energy should develop a joint committee of experts to develop a research agenda to increase the use and utility of AI in smart grid development and deployment. (Chapter 1)

» Establish intergovernmental collaboration in the area of research and clinical response to cancer. (Chapter 4)

» Applications of advanced biotechnologies such as synthetic organisms, gene drives, and germline editing could be good subjects for technical collaborations between the United States and South Korea. (Chapter 3)

» Both governments have opportunities to shape the future of biotechnology research with regards to synthetic organisms and the development of new datasets that can be mined for medical advances. (Chapter 3)

Align programs and establish joint initiatives.

» Align research programs to maximize discoveries that can benefit the public good, such as health and the environment. (Chapter 1)

» The Korea Institute for Advancement of Technology (KIAT) should work with the US Agency for International Development's (USAID's) Global Development Lab and other appropriate development agencies to help build AI-enhanced infrastructure in selected developing countries. (Chapter 1)

» South Korea's government should host an annual AI algorithm competition. Possible topics include the application of AI algorithms to the sectors in which South Korea wants to apply AI, or areas in which there are AI needs in South Korean industry. (Chapter 2)

  - The Netflix Prize was an open competition for the best collaborative filtering algorithm to predict user ratings for films, based on previous ratings without any other information about the users or films. The Kaggle competition is a challenge in which companies and researchers post data, and statisticians and data miners attempt to produce the best models for predicting and analyzing the data. (Chapter 2)

» Expand engagement between the US National Institutes of Health and South Korea's Biobank Project on precision medicine. (Chapter 4)

» The United States and South Korea could build a joint bilateral scientific competition in the area of advanced biotechnology similar to the United States-China EcoPartnership,[1] which focused on sustainability.

» There could be joint research projects and funding streams to study a virus that is of mutual concern to the United States and South Korea. The Middle East respiratory syndrome coronavirus (MERS-CoV) could be a good candidate. Multiple vaccine candidates could be tested in a collaborative fashion, or tools to help advance MERS-CoV research could be developed and jointly shared between the United States and South Korea. (Chapter 3)

Leverage civil society.

» Catalyze civil society organizations, companies, and individuals around the responsible development of convergent biotechnologies to scale applications that address global challenges. (Chapter 4)

» Facilitate collaboration between US and South Korean philanthropies and civil society organizations to advance scientific research. (Chapter 4)

» Enable partnerships between US and South Korean hospitals around clinical trials to leverage South Korea's high-quality and cost-competitive biomedical infrastructure.[2] (Chapter 4)

Address barriers to research.

» Enhance the efficiency of data centers of biotechnology-centered research agencies to overcome the challenge of storing massive amounts of biological information. (Chapter 3)

» Develop software solutions that can effectively manipulate such large amounts of biological data. (Chapter 3)

---

1 "EcoPartnerships," United States-China EcoPartnerships Program, accessed November 28, 2017, https://ecopartnerships.lbl.gov/.

2 "Review of 2014 Clinical Trial Approvals in Korea," Korea National Enterprise for Clinical Trial, accessed November 28, 2017, http://en.konect.or.kr/whykorea/fns.htm.

» Make data amenable to processing; information for bioinformatics analysis needs to be in a computable form. (Chapter 3)

» Update and modernize the US-Korea Free Trade Agreement (KORUS FTA) to reflect rules that unlock security research and bolster businesses models. This would remove barriers for highly skilled South Korean white hat security researchers to participate in programs such as Hack the Pentagon. The South Korean government can play a lead role in making this practice more acceptable by ensuring vulnerability disclosure is part of a continual improvement process. (Chapter 6)

2. DEVELOP TWENTY-FIRST-CENTURY WORKFORCES

As disruptive technologies change the landscape of work in the twenty-first century, the United States and South Korea will need to remain proactive in ensuring their workforces have the necessary knowledge, skills, and abilities to remain competitive in the global marketplace. Developing twenty-first-century workforces will require a collaborative effort among government, industry, and academia that offers training to citizens early and often, so they remain technically literate and therefore less prone to reacting negatively toward new technologies. In addition, promoting diversity and inclusion in the science and technology space is a critical factor for success and cannot be overlooked. Finally, innovative training and education mechanisms should be considered, as current models may prove insufficient for developing a twenty-first-century workforce.

Collaborate and engage.

» Establish public-private partnerships at the municipal and local levels that develop artificial intelligence and machine learning training programs in locations where South Korean and/or US technology companies are established. (Chapter 1)

» The private sector must work with educational institutions to develop a next-generation workforce capable of providing the needed technical know-how and expertise. (Chapter 1)

  - One example is the central role that Intel Corporation has played in working with local Vietnamese institutions in Ho Chi Minh City to locally train engineers as workers in their plants. (Chapter 1)

» Engage citizens on topics related to convergent biotechnologies to create a more technically literate workforce and mitigate potential social backlash against the disruptive potential of advanced biotechnology. (Chapter 4)

Promote diversity and inclusion.

» KIAT and the National Science Foundation should develop a series of exchanges on increasing the female workforce in artificial intelligence/machine learning (AI/ML) R&D. (Chapter 1)

» Focus on the implications of AI for women and underrepresented groups in the R&D ecosystem and share experiences and best practices. (Chapter 1)

Implement innovative training and education mechanisms.

» Develop innovative mechanisms not only to further the training of researchers, but also to provide "executive education" for researchers in related fields, promote cross-fertilization of fields, and help already-trained researchers transition into areas where interest is high and funding is more plentiful. (Chapter 3)

» Maker- and hackerspaces provide safe venues—such as highly collaborative environments—where individuals can learn how technology works and have the freedom to create. Experimentation and failure can lead to innovations that become patents, startups, art projects, and other societal benefits. These facilities can also serve as independent testing labs for IoT devices. (Chapter 6)

» Competitions can encourage students from many disciplines to learn and apply cybersecurity principles and practices in their own fields of study. (Chapter 6)

» Social and/or financial rewards conferred for individual and corporate participation in civil society initiatives, such as public recognition, certifications, competitions, or prizes, can build South Korean domestic capabilities, global influence, and greater integration into international cybersecurity research communities. (Chapter 6)

» Governments should partner with universities to develop curricula on IoT, data science, cybersecurity, and artificial intelligence for high school and higher education, offer training opportunities to businesses, and create scholarship programs focused on STEM education. (Chapter 5)

» Curricula in universities should include defensive programming, restricted codebase languages, and static and dynamic testing tools. (Chapter 6)

3. ENSURE SAFETY AND SECURITY

When developing these new technologies, it is also important to consider the implications for safety and security. As artificial intelligence, biotechnology, and the Internet of Things will affect nearly all aspects of human life, getting the safety and security aspects right is paramount. The United States and South Korea can work closely together in this area to develop international safety standards and encourage their adoption.

Improve Biosafety.

» Encourage other nations to promote industry-wide screening standards, champion a common code of conduct for suppliers of DNA, and develop mechanisms so that more of the gene synthesis market performs screening, and has a place to report suspicious orders. (Chapter 3)

» Increase intrinsic biosafety, in which biosafety is built into the organism, so that synthetic organisms cannot escape boundaries that are set for them. (Chapter 3)

- A joint initiative between the United States and South Korea could provide the structure, timeline, and political importance to the work that is required to get these safety standards achieved. (Chapter 3)
- Safety standards for new biotechnology applications, such as synthetic organisms, gene drives, and germline editing, are still in flux, and should be a focus of collaboration. (Chapter 3)

» Expand security cooperation between the United States and South Korea on issues related to biotechnology to focus on both deliberate and natural biological threats. (Chapter 3)

- Encourage more countries to take a multisectoral approach through a variety of means, such as military-to-military conferences with other nations from Southeast Asia or the development of a Joint External Evaluations supplement with a military focus. (Chapter 3)

Strengthen Cyber Safety and Security.

» Favor security by design. (Chapter 6)

- Create a "cash for clunkers" program for medical devices, ensuring that those devices most likely to cause harm are replaced, and that the replacements are significantly better. (Chapter 6)
- Apply advanced capabilities and practices to improving security by design, such as automatically detecting, determining, and enforcing safe and secure configurations in complex systems. (Chapter 6)

» Promote, refine, and standardize a Software Bill of Materials and other forms of transparency for IoT cyber safety and security. (Chapter 6)

- Create a "nutrition label" of cybersecurity products. (Chapter 6)

» Make better use of South Korean white hat security researchers to improve the security and safety of IoT devices. (Chapter 6)

- Accelerate practices such as Vulnerability Coordinators and Bug Bounty programs. (Chapter 6)

4. FOSTER ENTREPRENEURIAL ENVIRONMENTS

The United States and South Korea have highly entrepreneurial private sectors that are at the cutting-edge of technological innovation. Given that often it is the private sector that leads the way in technological progress, whether through new products, services, or processes, it is critical for the United States and South Korea to ensure the private sector's continued operation in a global business-friendly environment. To foster an entrepreneurial ecosystem, the two countries should work together to streamline regulations, share best practices, develop standards, and improve commercialization.

Streamline regulations and ensure compliance.

» South Korean and US automobile companies should consider developing a consortium on autonomous vehicles. Such a partnership could be critical for developing common regulations, creating data-sharing protocols, and standardizing rules of the road for autonomous vehicles at the level of the manufacturer. (Chapter 1)

- A useful modeling example could include the California Fuel Cell Partnership, which was created to accelerate the infrastructure and standards for hydrogen fuel-cell vehicles. (Chapter 1)

» Leverage Samsung's selection in September 2017 by the US Food and Drug Administration to be one of nine companies—only two of which were international companies—to participate in a digital health software pre-certification pilot program,[3] forming the basis for synergistic regulations in South Korea. (Chapter 4)

» Another important opportunity for bilateral coordination between the United States and South Korea lies in minimizing or eliminating certain requirements and regulations across the border for IoT products and systems. (Chapter 5)

Share best practices and develop standards.

» Share best practices to ensure compliance with the European Union's (EU's) General Data Protection Regulation, which will apply to all companies processing and holding personal data of subjects residing in the EU, regardless of the company jurisdiction. (Chapter 4)

» Actively promote the universal adoption of a common, flexible framework, created through robust public-private collaboration, which promotes best practices for cybersecurity governance and risk management. (Chapter 5)

- Leverage existing international bodies or conventions to rename or recast the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework as a more international framework (rather than a US-based one) to increase global adoption. (Chapter 5)

» National policies and initiatives should support research that identifies the most cost-effective IoT cybersecurity measures. Identifying not only *best* practices but also the most *cost-effective* best practices will encourage and facilitate industry's voluntary adoption of cybersecurity measures as much as possible. (Chapter 5)

Improve commercialization.

» South Korea's high internet penetration rate could allow it to serve as a test-bed to scale mobile health technologies and integrate them into the existing healthcare system with the country's growing smart city infrastructure. (Chapter 4)

» Providing opportunities and a more fluid process for scientists, engineers, researchers, and others to commercialize their findings could bring discoveries to market sooner and ensure more rapid distribution. (Chapter 4)

» Collaborating on startup incubators could serve markets in the United States and South Korea by building experience and market value. South Korea has launched at least two such incubators in northern Virginia, and the United States can do the same in South Korea. (Chapter 6)

5. DEVELOP NEW MODELS OF GOVERNANCE

Scientific breakthroughs and emerging technologies continue to test the limits of existing social, ethical, and legal norms. As new and disruptive technologies continue to sprint forward, discussions around the governance of these technologies fail to keep up. Without hampering the innovation currently unfolding, the United States and South Korea must focus on the implications that these new technologies have for norms and values. Together, these countries need to work to ensure that artificial intelligence, biotechnology, and the Internet of Things are developed in a safe and responsible manner. This may require new models of governance to address concerns brought about by these technologies. As two of the world's leading technological innovators, the United States and South Korea have a strong stake in shaping and influencing the social, ethical, and legal norms that will govern the technologies of the twenty-first century—after all, these governance issues will also have significant economic and security implications.

» Identify ways to bring South Korean companies into the Partnership on AI. Their participation and expertise would help develop more informed norms and standards. (Chapter 1)

- "With the increasing role of the private sector in developing norms and standards for AI, partnerships that bring together the leaders in this area are more relevant to policy development. The Partnership on AI—an indus-

3 US Food and Drug Administration, "FDA Selects Participants for New Digital Health Software Pre-certification Pilot Program," released September 26, 2017, https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm577480.htm.

try-launched initiative to bring together the leading companies working on AI development, norms, and applications—is currently leading the effort to develop private sector governance over AI/ML. As of February 2018, no South Korean companies are involved in this partnership. Given the large number of South Korean companies in leadership roles in this space, their participation and expertise would help develop more informed private sector policy discussions." (Chapter 1)

» Expand trilateral engagement with partners such as Japan, Germany, and the European Union to engage on technical, legal, and ethical norms, principles, codes of conduct, and data and privacy standards that could underpin advanced biotechnologies. (Chapter 4)

  - South Korea's recent launch of the Fourth Industrial Revolution Committee and Workshop in collaboration with Germany could be expanded to include the United States. (Chapter 4)

» Developing shared legal and ethical norms, principles, codes of conduct, and standards could allow for more fluidity between each nation's products and customers. (Chapter 4)

» The principles of security and privacy by design should be pursued and promoted whenever possible, reinforcing the notion that security and privacy are foundational issues, which should be reflected in practice from the very beginning of production conception and design, rather than as afterthoughts. (Chapter 5)

A. IMPROVE COORDINATION

Broadly improving coordination between the United States and South Korea is one of two focus areas that cuts across the five pillars of the strategic framework. The United States and South Korean governments can use several forums, mechanisms, and communications channels, and should include a multidisciplinary group of stakeholders.

» Ensure that the Joint Committee Meetings on Science and Technology Cooperation resume and that the appropriate experts from both countries participate. (Chapter 1)

» Commit to reestablishing the high-level bilateral US-South Korean Information and Communication Technology (ICT) Policy Forum and use it to better coordinate on AI/ML-related policy development. (Chapter 1)

» Highlight advanced biotechnologies as an area of cooperation in future dialogues in the Senior Economic Dialogue. (Chapter 4)

» Coordinate multilateral collaboration through fora such as the United Nations around neuroscience R&D in recognition of the robust domestic efforts underway in the United States through the US Brain Initiative and South Korean Brain Research Institute. (Chapter 4)

» Discuss bilateral issues related to information technology and data hurdles related to convergent technologies at the ICT Policy Forum. (Chapter 4)

» Develop a fusion center, which would create regular interactions on biotechnology topics related to relevant government agencies as well as the private sector and develop an advanced biotechnology track in the Group of Twenty; work through the Organisation for Economic Co-operation and Development; or work through the renegotiation of the KORUS FTA. (Chapter 3)

» Establish a technology and policy dialogue that focuses on synthetic organisms, gene drives, and germline editing, providing an opportunity for South Korea and the United States to avoid earlier mistakes and promulgate the safe development of agricultural biotechnologies. (Chapter 3)

» Establish a center of excellence in IoT cybersecurity to engage in R&D, applications development, standards development, training, and policy development. (Chapter 5)

» Create a university consortium to collaborate on technology development projects that would be funded by governments where companies validate new technologies through pilot tests or commercialization. (Chapter 5)

» The private sectors in both countries should address the challenges and opportunities in IoT at the IoT Dialogue[4] launched by Samsung, Intel, and other leading industry associates in 2017. Discussions should include policies related to mobile

4 Samsung Newsroom, "Technology Industry Leaders Release National Strategy to Maximize US Economic and Societal Benefits from the Internet of Things," released October 3, 2017, https://news.samsung.com/us/iot-us-economic-societal-benefit-national-strategy/.

health, wearable technology, and healthcare data protection. (Chapter 4)

B. EXCHANGE PEOPLE AND INFORMATION

Cutting across each of the five pillars is a need to increase the exchange of people and information between the United States and South Korea. By exchanging scientists, researchers, and students and sharing industry best practices, both countries can benefit from closer people-to-people interactions.

To invest in research and development:

» Create venues for premier scientists in areas of advanced biotechnology to exchange information and explore opportunities to collaborate with promises of expanded access to government facilities and resources. Sharing information between scientists could cultivate longer-term research collaborations that leverage the comparative advantages of different nations. (Chapter 4)

» Reinvigorate efforts to collaborate on the US Biden Cancer Initiative[5] with Japan and South Korea—including through research and data sharing—that could result in more rapid innovation in treatments. (Chapter 4)

» Learn from the successes of the Johnson & Johnson Innovation Centers—a model of private sector–led efforts to spur innovation by supporting startups and small and medium-sized enterprises—to expand access to existing expertise and facilities.[6] (Chapter 4)

» Incentivize citizen scientists from both countries to expand participation in technical competitions such as those coordinated by the Defense Advanced Research Projects Agency, USAID Global Development Lab, NIST's Global Cities Teams Challenge,[7] and South Korea's Smart Challenge projects. (Chapter 4)

To build twenty-first-century workforces:

» The two countries should develop jurist exchange programs in AI/ML including South Korean and US law schools. Develop a cadre of jurists capable of dealing with the issues that will arise related to ethics, international trade, and the economy. (Chapter 1)

» South Korea should make a targeted effort to recruit Fulbright Scholars in Science, Technology, and Innovation[8] and build a network to connect existing South Korean researchers in the United States, which include several hundred doctorate-level scientists based out of the National Institutes of Health and in labs funded by the National Science Foundation. (Chapter 4)

» The United States can study and learn from South Korea's experience with cybersecurity schools. South Korea runs a series of cybersecurity high schools and informal educational programs that teach technology and encourage skill-building. (Chapter 6)

» Knowledge gained from cyber ranges and testing labs can benefit both societies, and it makes sense to share. Collaborations at each other's facilities can allow researchers to share testing methods and experiences, and build relationships. (Chapter 6)

To ensure safety and security:

» Sharing information among law enforcement, intelligence agencies, industry players, and other stakeholders can improve the knowledge and defensive postures of both countries. (Chapter 6)

- The South Korean government could encourage more South Korean government agencies and firms to join organizations like Computer Emergency Response Teams, which help government, academia, and industry coordinate on emerging cyberattacks, vulnerabilities, and other internet issues, and Information Sharing and Analysis Centers and Organizations, which similarly play an important role

5 Biden Cancer Initiative, accessed November 28, 2017, https://bidencancer.org/.

6 "About Us: Vision, Family, Leadership," Johnson & Johnson Innovation, accessed November 28, 2017, https://www.jnjinnovation.com/about-us.

7 Sokwoo Rhee, Martin Burns, and Cuong Nguyen, *Global City Teams Challenge 2016*, NIST Special Publication 1900-01, accessed November 28, 2017, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-01.pdf.

8 "The Fulbright Scholar Program: Science, Technology and Innovation," Council for International Exchange of Scholars, accessed November 28, 2017, https://www.cies.org/fulbright-scholar-program-science-technology-and-innovation.

for industry segments and geographic areas. (Chapter 6)

To encourage entrepreneurial environment:

» Translate English-language documents to make emerging global practices available for the Korean market and bring new insights back to the global initiatives. Include these materials in government … and academic courses to further increase awareness of the latest global expertise within Korea's domestic market. (Chapter 6)

To develop new models of governance:

» Facilitate collaboration between US and South Korean philanthropies and civil society organizations, exploring the legal, social, and ethical issues surrounding advanced biotechnologies. (Chapter 4)

AUTHOR BIOGRAPHIES

Dr. Vaughan Turekian

Senior Director of Science and Technology for Sustainability Program, National Academies of Sciences, Engineering, and Medicine

Dr. Vaughan Turekian is the senior director of the Science and Technology for Sustainability (STS) Program at the National Academies of Sciences, Engineering, and Medicine. Prior to joining the STS program, Dr. Turekian served as the science and technology advisor to the US secretary of state from September 2015 to 2017. Dr. Turekian drew upon his background in atmospheric chemistry and extensive policy experience to promote science, technology, and engineering as integral components of US diplomacy. Previously, he was chief international officer for the American Association for the Advancement of Science (AAAS) and the director of AAAS's Center for Science Diplomacy. In this capacity, he worked to build bridges between nations based on shared scientific goals, placing special emphasis on regions where traditional political relationships are strained or do not exist. As editor-in-chief of *Science & Diplomacy*, he published original policy pieces that have served to inform international science policy recommendations. Dr. Turekian holds a BS in geology and geophysics and international studies from Yale University and a MS and PhD from the University of Virginia where he focused on the transport and chemistry of atmospheric aerosols in marine environments.

Dr. Taehee Jeong

Senior Data Scientist, Xilinx

Dr. Taehee Jeong is a senior data scientist at Xilinx. He is currently teaching a class on deep learning at San Jose State University. His research areas are machine learning, deep learning applications in manufacturing, quantitative methods and statistics, data mining, and data analytics. He is focusing on machine learning and deep learning applications in the semiconductor industry. He has extensive experience applying quantitative methods and statistics and machine learning algorithms in industry. He has many years of professional and academic research experience working at various institutions, universities, and companies such as Xilinx, Western Digital, Seagate Research, and LG Electronics Institute of Technology.

Dr. Gigi Kwik Gronvall

Senior Scholar, Johns Hopkins Center for Health Security;
Associate Professor, Johns Hopkins Bloomberg School of Public Health

Dr. Gronvall is a senior scholar at the Johns Hopkins Center for Health Security and an associate professor in the department of environmental health and engineering at the Johns Hopkins Bloomberg School of Public Health. She is an immunologist by training. Dr. Gronvall's work at the center addresses the role of scientists in health security—how they can contribute to an effective technical response against a biological weapon or a natural epidemic. She is particularly interested in developing policies that will boost the safety and security of biological science activities while allowing beneficial research to flourish. Dr. Gronvall is a member of the Threat Reduction Advisory Committee (TRAC), which provides the secre-

tary of defense with independent advice and recommendations on reducing the risk to the United States, its military forces, and its allies and partners posed by nuclear, biological, chemical, and conventional threats. She has testified before Congress about the safety and security of high-containment biological laboratories in the United States and served on several task forces related to laboratory and pathogen security. Dr. Gronvall received a BS in biology from Indiana University, Bloomington.

Dr. Elizabeth Prescott

Professor of the Practice and Director of Curriculum, Science, Technology, and International Affairs, Walsh School of Foreign Service, Georgetown University

Dr. Elizabeth "Libbie" Prescott works at the intersection of science, technology, and international affairs at Georgetown University's Edmund A. Walsh School of Foreign Service. Most recently, Dr. Prescott served as deputy director and education portfolio lead for the MD5 National Security Technology Accelerator based out of the National Defense University at the US Department of Defense. Prior to that, she worked at the US Department of State, served as counselor and strategic advisor to the Science and Technology (S&T), adviser to the US secretary of state, and was S&T adviser to the assistant secretary of state for the Bureau of East Asian and Pacific Affairs. Outside of government, Dr. Prescott has served as practice head for biosecurity at the Eurasia Group; as a research fellow at the International Institute for Strategic Studies-US; as a fellow at the National Academy of Science's Board on Science, Technology, and Economic Policy; and has consulted for the strategy division of the National Health Service in the United Kingdom. Dr. Prescott has her doctorate in molecular biology from the University of Oxford, Balliol College and dual degrees with high honors in economics and molecular and cell biology from the University of California, Berkeley.

Dr. Gwanhoo Lee

Professor of Information Technology and Analytics, Kogod School of Business, American University

Dr. Gwanhoo Lee is a professor of information technology and analytics in the Kogod School of Business at American University. He is an advisor to Samsung Economic Research Institute (SERI) and a mentor for the Korea Innovation Center of the Korean Ministry of Science and ICT. He has consulted for the World Bank on ICT strategy in developing countries including Russia and Kyrgyzstan. From 2004 to 2016, he directed the Center for IT and the Global Economy that engages senior executives from the private and public sectors in exchanging knowledge and experience in digital business and economy. In 2016, he co-founded the Kogod Cybersecurity Governance Center that aims at creating knowledge on governance and managerial aspects of cybersecurity. Dr. Lee earned his doctorate in management information systems from the Carlson School of Management at the University of Minnesota and his BS and MS degrees in industrial engineering from Seoul National University in Korea.

Ms. Rebekah Lewis

Director, Kogod Cybersecurity Governance Center, American University

Ms. Rebekah Lewis is the director of the Kogod Cybersecurity Governance Center (KCGC) at American University's Kogod School of Business (KSB) in Washington, DC. In addition to her role with the KCGC, Lewis also teaches and conducts research related to cybersecurity governance, law, and policy. She previously served as a cybersecurity and information assurance attorney for the US National Security Agency and practiced law in the Washington office of Latham & Watkins. Lewis also has experience at the International Telecommunication Union (ITU) in Geneva, Switzerland.

Mr. Beau Woods

Cyber Safety Innovation Fellow, Atlantic Council

Mr. Beau Woods is a cyber safety innovation fellow with the Atlantic Council, a leader with the I Am The Cavalry grassroots initiative, and founder/CEO of Stratigos Security. His focus is the intersection of cybersecurity and the human condition, primarily around cyber safety, ensuring the connected technology that can impact life and safety is worthy of our trust. Over the past several years in this capacity, he has consulted with automakers, medical device manufacturers, healthcare providers, cybersecurity researchers, US federal agencies and legislative staff, and the White House. Prior to joining the Atlantic Council, Mr. Woods founded the security consultancy, Stratigos Security, to advise large enterprises, small businesses, and NGOs on information security strategy and development. Prior to that, Mr. Woods spent five years with Dell SecureWorks, where he advised commercial clients on information security and built up the security consulting services practice. Mr. Woods graduated from the Georgia Institute of Technology with a BS in psychology.

ACKNOWLEDGMENTS

The Atlantic Council would like to thank the following policy practitioners, business leaders, and subject matter experts for contributing their insight and analysis to this project:

» **Robert A. Atkinson**, *President*, Information Technology and Innovation Foundation

» **Megan Frisk**, *Foreign Affairs Officer, Office of the Science and Technology Advisor to the Secretary*, US Department of State

» **David Gunning**, *Program Manager, Information Innovation Office*, Defense Advanced Research Projects Agency

» **David K. Han**, *Senior Scientist in Artificial Intelligence*, Army Research Laboratory

» **He Yujia**, *Visiting Fellow, Scowcroft Center for Strategy and Security*, Atlantic Council

» **Hweonbae Hwang**, *Visiting Fellow, Scowcroft Center for Strategy and Security*, Atlantic Council

» **Franklin D. Kramer**, *Distinguished Fellow, Scowcroft Center for Strategy and Security*, Atlantic Council

» **Adriane LaPointe**, *Senior Policy Advisor, Office of International Affairs, National Telecommunications and Information Administration*, US Department of Commerce

» **Carol D. Linden**, *Director, Office of Regulatory Science and Innovation, Office of the Chief Scientist/Office of the Commissioner*, US Food and Drug Administration

» **Robert A. Manning**, *Senior Fellow, Scowcroft Center for Strategy and Security*, Atlantic Council

» **Taisuke Mibae**, *Visiting Senior Fellow, Scowcroft Center for Strategy and Security*, Atlantic Council

» **Nicholas Montella**, *Manager, Japan and Korea*, U.S. Chamber of Commerce

» **Jim Pannucci**, *Director, Partnership Development Office*, Frederick National Lab for Cancer Research

» **Jongwon "JP" Park**, *Chief Strategy Officer*, EYL Inc.

» **Eleonore Pauwels**, *Director, the AI Lab and Senior Research Associate*, Wilson Center

» **Nathaniel Schaefle**, *Bilateral Affairs Program Analyst, Office of Science and Technology Cooperation*, US Department of State

» **David A. Wollman**, *Deputy Director, Smart Grid and Cyber-Physcial Systems Program Office, National Institute of Standards and Technology*, US Department of Commerce

This report represents the conclusions of the authors only. While the individuals acknowledged above offered their expertise and insight during private discussions on each chapter of the report, their participation and their acknowledgement here do not represent an endorsement of this text in whole or part. Additionally, those acknowledged here have participated in their individual, not institutional, capacities.

The Atlantic Council would like to thank the Korea Institute for Advancement of Technology for their support of this project.

The Atlantic Council also would like to thank the following individuals for their work on this report: Barry Pavel, Miyeon Oh, Mathew Burrows, Robert A. Manning, HuiHui Ooi, Diya Li, Samuel Klein, Beryl Thomas, He Yujia, Shaun Ee, Mina Kim, Cameron Douglas, Ellen Riina, Heeji Kim, Emily Dean, Joanna Jaworska, and Bailey Wong. This project would not have been possible without the work and support of each of these individuals. Special thanks to the Atlantic Council publication team: Susan Cavan, Sarah DeLucia, and Romain Warnault.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org