UC San Diego
SCHOOL OF GLOBAL POLICY AND STRATEGY
21st Century China Center

Asia Society | CENTER ON U.S.-CHINA RELATIONS

MEETING THE CHINA CHALLENGE:

A New American Strategy for Technology Competition

by the Working Group on Science and Technology in U.S.-China Relations

Peter Cowhey, Chair

A project of the 21st Century China Center under the auspices of the Task Force on U.S.-China Policy

Co-chairs: Susan Shirk and Orville Schell

NOVEMBER 16, 2020

ABOUT THE WORKING GROUP ON SCIENCE AND TECHNOLOGY IN U.S.-CHINA RELATIONS

The bipartisan Working Group on Science and Technology in U.S.-China Relations is chaired by Peter Cowhey, Dean of UC San Diego's School of Global Policy and Strategy, and comprised of twenty-eight China specialists and exerts in science and technology from academia, industry, and think tanks, including several former government officials.

Organized by the UC San Diego 21st Century China Center, the Working Group operates under the auspices of the Task Force on U.S.-China Policy, which is co-chaired by Susan Shirk from UC San Diego and Orville Schell from the Asia Society's Center on U.S.-China Relations.

Working Group members met in person three times in San Diego, Washington D.C. and San Mateo between September 2019 and March 2020. After March 2020, the Working Group switched to virtual meetings, and divided into four small groups to examine sector-specific policies and draft the section reports. Throughout, the Working Group kept its focus on China's evolving science and technology policy and practice, the challenges the People's Republic of China (PRC) presents to the United States, and the debates in the United States over the complex trade-offs between national security, competitiveness, and openness in the context of the broader innovation ecosystem.

The intent of the Working Group was to create a guide for the transition team for the next president. It sets forth broad policy objectives as well as specific recommendations for a new and integrated approach to competition by the U.S. in four domains of science and technology: fundamental research, 5G digital communications, artificial intelligence and biotechnology.

21ST CENTURY CHINA CENTER

The mission of the 21st Century China Center is to produce and disseminate impactful evidence-based research about China, and to enhance U.S.-China relations by advancing scholarly collaboration, convening policy discussions, and actively communicating with policy makers and the general public in both countries.

Asia Society | CENTER ON U.S.-CHINA RELATIONS

The Center on U.S.-China Relations was founded in 2006 and is based at Asia Society's New York headquarters. The center undertakes projects and events which explore areas of common interest and divergent views between the two countries, focusing on policy, culture, business, media, economics, energy, and the environment.

School of Global Policy and Strategy
University of California San Diego
9500 Gilman Drive # 0519
La Jolla, CA 92093-0519
https://china.ucsd.edu/

ACKNOWLEDGEMENTS

This work would have been impossible without the contributions of many dedicated individuals and organizations, especially Lei Guang, the executive director of the 21st Century China Center. I am deeply grateful to Peter Cowhey who was persuaded to chair the Working Group in what is to him an extremely busy and demanding year; to my intellectual partner and co-chair of the Task Force Orville Schell; and to all the members of the Working Group on Science and Technology in U.S.-China Relations, who spent many months exploring in detail the challenges and opportunities presented by competition with China and offering their candid views and insights. Special thanks to Elsa Kania for drafting the COVID text boxes and to Arthur Bienenstock, Karl Eikenberry, Peter Michelson, Barry Naughton, Jason Matheny, and Robert Friedmann for corralling the large and small groups to draft the four case studies.

I am grateful for the comments from external readers, including Doug Beck, Sam Bozzette, Jose W. Fernandez, Erica R.H. Fuchs, Jimmy Goodrich, Don Rosenberg, and several others who were generous with their time and knowledge, and candid with their critiques. These individuals strengthened this work greatly but bear no responsibility for its ultimate content.

I would like to extend a special thanks to Robert Daly, director of the Kissinger Institute on China and the United States at the Wilson Center, and James Cross, director of Franklin Venture Partners, for their felicitous arrangement of meeting venues for the Working Group in Washington D.C. and Silicon Valley.

Several individuals from UC San Diego provided invaluable management and creative support to this project from beginning to end, working to ensure that everything ran smoothly, from the off-line and online meetings, to communication, editing, design, and production of the final report. I want to thank Christine Clark, Nicole Daneshvar, Rosemarie Pi'ilani Fernandez, Iva Kostova, Amy Robinson, Sam Tsoi, Simeng Zeng and especially, Lindsay Morgan, for her sharp editing.

I am grateful to Laura Chang and Michael Laha, colleagues from the Asia Society's Center on U.S.-China Relations, who answered every query quickly and made sure the report would receive maximum exposure to the public and policy community.

Finally, I want to acknowledge the generous support from the Carnegie Corporation of New York (CCNY) that made this study possible. I want to thank Dr. Stephen Del Rosso, Program Director in International Peace & Security at CCNY, for his unfailing support to the Center and the activities led by the Task Force on U.S.-China Policy.

Susan L. Shirk

Research Professor and Chair, 21st Century China Center
UC San Diego School of Global Policy and Strategy

MEMBERS OF THE WORKING GROUP

- **Charlene Barshefsky,** Senior International Partner at WilmerHale
- **Arthur Bienenstock,** Professor of Photon Science, Emeritus and former Dean of Research, Stanford University and former Associate Director for Science, Office of Science and Technology Policy
- **Jessica Chen Weiss,** Associate Professor of Government, Cornell University
- **Tai Ming Cheung,** Director, UC Institute on Global Conflict and Cooperation, UC San Diego
- **Mark Cohen,** Director, UC Berkeley Center for Law and Technology
- **Peter Cowhey,** Dean, UC San Diego School of Global Policy and Strategy
- **Wendy Cutler,** Vice President, Asia Society Policy Institute
- **Robert Daly,** Director, Kissinger Institute on China and the U.S., Wilson Center
- **Karl Eikenberry,** Former U.S. Ambassador to Afghanistan and Lieutenant General, U.S. Army, Retired
- **Robert Friedman,** Vice President for Policy and University Relations, J. Craig Venter Institute
- **Melanie Hart,** Senior Fellow and Director of China Policy, Center for American Progress
- **Yasheng Huang,** Epoch Foundation Professor of International Management, MIT Sloan School of Management
- **Elsa Kania,** Adjunct Senior Fellow, Technology and National Security Program, Center for a New American Security
- **Arthur Kroeber,** Partner and Head of Research, Gavekal and founder, Gavekal Dragonomics
- **Eric Loeb,** Executive Vice President, Government Affairs, Salesforce
- **Anja Manuel,** Co-Founder and Principal, Rice, Hadley, Gates & Manuel LLC
- **Jason Matheny,** Director, Center for Security & Emerging Technology, Georgetown University
- **Evan Medeiros,** Penner Family Chair in Asian Studies and Cling Family Distinguished Fellow in U.S.-China Studies, Walsh School of Foreign Service, Georgetown University
- **Peter Michelson,** Professor of Physics and Luke Blossom Professor in the School of Humanities and Sciences, Stanford University
- **Barry Naughton,** So Kwan Lok Chair and Professor, UC San Diego School of Global Policy and Strategy
- **Samm Sacks,** Cyber Policy Fellow, New America; and Senior Fellow, Yale Law School Paul Tsai China Center
- **Orville Schell,** Arthur Ross Director, Center on U.S.-China Relations, Asia Society
- **Andrew "Drew" Senyei,** Physician and Venture Capitalist; Managing Director, Enterprise Partners Venture Capital, Retired
- **Susan Shirk,** Research Professor and Chair, 21st Century China Center, UC San Diego School of Global Policy and Strategy
- **Helen Toner,** Director of Strategy at Center for Security and Emerging Technology, Georgetown University
- **Ken Wilcox,** Emeritus Chairman, Silicon Valley Bank
- **Robert Work,** Distinguished Senior Fellow for Defense and National Security, Center for a New American Security, and former Deputy Secretary of Defense
- **Keith Yamamoto,** Professor and Vice Chancellor for Science Policy and Strategy, UC San Francisco

ACRONYMS

AAU	Association of American Universities
API	Active Pharmaceutical Ingredients
ATIS	Alliance for Telecommunications Industry Solutions
BARDA	Biological Advanced Research Projects Agency
CCSA	China Communications Standards Association
CFIUS	Committee on Foreign Investment in the United States
CISA	Cybersecurity and Infrastructure Security Agency
CNMPA	China's National Medical Products Administration
DARPA	Defense Advanced Research Projects Agency
DOE	Department of Energy
EU	European Union
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FIRRMA	Foreign Investment and Risk Review Modernization Act
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IAP	Inter-Academy Partnership
ICT	Information and Communications Technology
IP	Intellectual Property
IPR	Intellectual Property Right
ITU	International Telecommunication Uni
NASEM	National Academies of Sciences, Engineering and Medicine
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
ORAN	Open Radio Access Network
OSTP	Office of Science and Technology Policy
PRC	People's Republic of China
R&D	Research and Development
S&E	Science and Engineering
S&T	Science and Technology
SBIR	Small Business Innovation Research
STEM	Science, Technology, Engineering, and Mathematics
STTR	Small Business Technology Transfer
TEVV	Testing, Evaluation, Verification, and Validation
TWAS	World Academy of Sciences
USDA	U.S. Department of Agriculture
USPTO	U.S. Patent and Trademark Office
vRAN	Virtualized Radio Access Network
WHO	World Health Organization
WTO	World Trade Organization

CONTENTS

FROM THE CHAIR

Since its launch in fall 2019, the Working Group on U.S.-China Science and Technology Relations truly became a meeting of minds among experts on China, foreign policy, economics, and science and technology. We came from businesses, universities, and think tanks. Many had prior expertise in government. Many were deeply rooted in the science and technology community. Together, we undertook a shared voyage of discovery.

We started by recognizing that the growing tensions between the United States and China reflected deep problems that required solutions. At the same time, we worried that many of the policy discussions had not defined the problems clearly enough to yield effective remedies. Some policy proposals could impose costs far larger than the benefits while still not ameliorating the long-term problem.

Our search for a more productive policy mix followed a two-pronged strategy. The entire Working Group clarified our common understanding of the underlying risks and benefits in the existing U.S.-China foreign policy and science and technology relationship. We ended up with three foundational principles to guide our finer-grained policy analyses.

1. We must strengthen U.S. innovation capabilities in a robust and sustained way, from increased funding for fundamental research to selective upgrading of our production system;

2. We should tighten risk management that is targeted on both current and future security threats and illicit behavior;

3. We should preserve, as much as possible, the benefits of an open, ethical, and integrated global knowledge system and innovation economy.

These principles are complementary. The successful realization of each principle depends on the implementation of the other two.

Our second prong of work involved dividing into four small groups to craft detailed case studies applying these principles to fundamental research, artificial intelligence, 5G broadband, and biotechnology. Each study yielded detailed conclusions and policy recommendations. The specifics varied significantly by case, but also had substantial overlaps that we highlight in the Working Group's general recommendations.

Beyond our recommendations, this undertaking revealed a deeper challenge for the foreign policy community focused on the paramount relationship with China. The community has not mastered the nuances of science and technology issues sufficiently. This challenge to its core competence is reminiscent of a similar moment in the Cold War. Charting strategy for the Cold War once required foreign policy experts to achieve reasonable fluency in the sometime arcane logic of deterrence theory and nuclear force capabilities. The evolving U.S. and China relationships won't be bordered by an "iron curtain" or a preoccupation with avoiding nuclear war. Instead it will feature rivalry for global leadership mixed with shared interests in such global issues as economic growth and stability, climate change, and public health.

Permeating every facet of the U.S.-China relationship will be crucial capabilities in science and technology that will feature both intense rivalry and necessary cooperation. During our work together, the foreign policy experts discovered that a good deal of the conventional wisdom about these issues reflects a flawed understanding of deeper dynamics in science and technology. The technological experts came to realize that foreign policy problems don't neatly yield to (theoretically) perfect, logical solutions, but reflect both internal political dynamics in China and the relative power positions of the U.S. and China.

In short, the expert community has serious homework to do if it is to get right these foundational issues for the bilateral relationship, and thus for global well-being. This report doesn't answer all the key questions, but we hope that it is an example of the work that must, and can, be done.

Peter Cowhey

PREFACE

Innovation in science and technology (S&T) is a core American strength. The United States has been the undisputed global technology leader since the end of World War II, but today, our preeminence faces three major interlinked challenges: The United States has allowed the foundations for its technological leadership to erode. It faces formidable competition from the People's Republic of China (PRC)—a country that has deployed full state power, and sometimes used illegal means, to build an innovation system to gain on the United States. And it has overreacted to the competition challenge from China, and in doing so, is poised to damage its own innovation ecosystem, which flourishes in an environment of global openness.

To confront these challenges, the United States needs a clear-eyed strategy for S&T innovation that enhances our national competitiveness and protects our national security. We must do two things, now: make needed investments in and policy adjustments for our S&T base at home; and craft a new approach to global cooperation that minimizes the security risks China poses without unduly sacrificing the benefits of openness.

The task is urgent. China's behavior under Xi Jinping raises fundamental concerns about the nature of China's global ambitions. Xi Jinping has vowed to modernize China's armed forces by 2035, and to transform China into world-class military power. China is using its growing military might to press its territorial claims against its neighbors and harass foreign vessels in international waters. In its foreign policy, Beijing uses its economic power in attempts to coerce sovereign governments, private companies, and overseas universities, media, and civil society organizations to conform to its political line. It is also constructing a surveillance state that threatens individual liberties in Xinjiang, Tibet, Hong Kong, and the rest of China.

In our view, China's pursuit to become a high-tech superpower is inextricably linked to its quest for regional dominance and global deference. Though the desire to develop China through innovation is legitimate, many of the ways in which the PRC government uses technology alarm the United States and other nations that hold liberal views of human rights and fair competition.

How China uses its technological prowess is one concern; the way it develops or acquires new technologies is another (White House Office of Trade and Manufacturing Policy 2018). China's well-resourced, winner-take-all approach to creating national champions in frontier technology is neo-mercantilist. Through massive subsidies far beyond the scale of other countries, and by shielding domestic firms from international competitors, China has enhanced its standing in global markets and damaged other countries, including the United States. Though China has increased its adherence to intellectual property rights (IPR) laws, it still employs a variety of illicit methods to acquire technological know-how from the U.S. and other countries.

China's changing behavior at home and on the world stage, coupled with its deviation from the norms of fair competition in S&T development, create economic and security risks for the United States and other countries and require forceful collective responses.

In this report, we make recommendations for a U.S. approach to China in four domains of science and technology. We envision a national strategy that will balance risks and opportunities over the long-term and that achieves three complementary objectives.

1. Self-strengthening: Bolster U.S. innovation capacities to stay competitive and secure.
2. Preserve Openness: Leverage a globally integrated S&T system to benefit the United States and the world.
3. Mitigate Risk: Tighten targeted measures for risk management to address security threats and minimize costs to the United States.

THE UNITED STATES IS BETTER POSITIONED THAN YOU THINK

Some American politicians have panicked over what they see as a Chinese technological juggernaut that is surpassing the United States. They see the United States as falling dangerously behind China, and believe that China's technological advance was achieved solely through unfair competition and the pilfering of western technologies. They also believe that China's erasure of boundaries between commercial and military innovation, including the absorption of U.S. technology through worldwide business deals, represents an existential threat to U.S. national security. They conclude that the United States must preserve its prosperity and security by decoupling from China. The United States, as the thinking goes, must reduce or eliminate scientific and business collaboration with China in order to block its access to the crown jewels of American technology (The White House 2020a).

Our Working Group's assessment differs from the conventional wisdom on several fronts. We find that the United States is in better shape than the pessimists believe, especially when long-term technological trends are taken into account. The United States holds a lead in all the dynamically evolving fields examined in this report. The best way to sustain this leadership is to adopt a strategy that builds on America's asymmetric advantages, including our superior ability to operate and attract talent in an open global knowledge economy.

Given the complexity and urgency of the China challenge, it will be necessary to impose smart risk management strategies tailored to specific technologies. Some of the strategies may entail some limits on other countries' access to America's innovation system, but they are a precondition for continuing integration and open cooperation across borders. Moreover, as a necessary complement to risk management, we must pursue a robust strategy for correcting weaknesses that have crept into the U.S. system of basic science and applied technology development. In this report, our Working Group pinpoints priorities for remediation to shore up America's position on the frontiers of science and technology.

America must also foster collaboration with allies and friends. Strengthening U.S. domestic regulation of data privacy and security is an essential first step toward establishing global norms that undergird international collaboration with like-minded countries and set guidelines for engagement with China. We recognize that as long as we face a peer competitor that seeks to undercut our comparative advantages and pursue goals we do not share, it will be necessary to impose some limits on openness. We warn, however, that, if not carefully conceived, U.S. barriers to flows of talent, technology, investment, and knowledge will harm American security and competitiveness, and damage the global knowledge economy that enormously benefits the United States and the rest of world.[1]

Permitting the global technology system to bifurcate into hostile camps led by the United States and China would be self-defeating and impracticable. Engaging in a race to the bottom with China by emulating its statist and protectionist policies is a recipe for a weaker and less secure America.[2]

THE NATURE OF THE CHINA CHALLENGE IN SCIENCE AND TECHNOLOGY

China sees S&T capability as key to national power. Although the United States has always competed with other innovative nations, the China challenge of today is fundamentally different from past contests. Japan in the 1980s was a democratic ally whose economy did not match the scale of the United States, while China is an authoritarian country whose economy will soon overtake that of the United States. Economic and social ties between Russia and the United States were limited during the Cold War, while China's economy, universities, and other institutions have been enmeshed with those of the United States for decades.

> ***... the United States is in better shape than the pessimists believe, especially when long-term technological trends are taken into account.***

The China S&T challenge has five distinctive features:

First, it is financed and directed by the PRC government as a means to achieve regional dominance and global power. In 2009, China surpassed Japan to become the second largest funder of R&D in the world. In 2018, China spent $554.3 billion on R&D, only slightly below the level spent by the United States. That same year, China's share of global R&D (26.3 percent) approached the U.S. share (27.6 percent) (Congressional Research Service 2020). Over the next six years, Beijing plans to invest an additional $1.4 trillion of state and private funds in next-generation technologies (*Bloomberg News* 2020).

The Chinese government and Communist Party also invest substantially in expanding its pool of human talent. They operate more than

1 That knowledge is the key to economic growth, especially for wealthier economies, is an essential insight of modern economics (David Warsh 2007). For more information on how science and technology are especially vital for the US, see (Gruber and Johnson 2019).

2 A comparison can be made between our approach to U.S. science and technology that focuses on self-strengthening, targeted risk management, and openness, and the current Trump administration's approach that is articulated, most recently, in (The White House 2020b).

200 high-level talent recruitment programs in science and technology, which are run by numerous agencies, including China's National Science Foundation; the ministries of Science and Technology, Education, Human Resources and Social Security; and most prominently, the Party's Organization Department.[3] Many of these programs encourage scientists working abroad—most, but not all of whom are of Chinese origin—to support efforts to build China's S&T capacity through their research. While these programs are not illegal in the United States, they may serve as channels for the transfer of valuable research to China.

Second, China sometimes advances its position through illegal means. While China absorbs foreign technologies legitimately through licensing, foreign investments, and the return of overseas graduates, it also does so through cyber hacking of businesses and research institutes, technological espionage, and other forms of intellectual property (IP) theft. The PRC government committed to stop commercial cyber hacking in 2013, but Chinese intruders resumed operation after a brief hiatus.

Third, China is mounting a major effort to dominate the global technology standards of the future. The new "China Standards 2035" plan uses massive subsidies to promote the indigenous development of technologies and then employs economic diplomacy to enhance China's influence over the international bodies that set the crucial standards and norms for emerging technologies. China has already succeeded in placing many officials at international standard-setting bodies, including the current Secretary General of the International Telecommunication Union. China's rapidly growing influence not only provides commercial advantages for Chinese firms, but also gives its autocratic government a strong voice in shaping digital privacy norms and other vital standards that influence global telecom competitiveness and security policies.

Fourth, China has moved steadily to erase the boundaries between civilian commerce and national security prerogatives in global technology markets. While all countries cross these lines occasionally, democracies are usually dissuaded from doing so by a thicket of safeguards. In contrast, China has proclaimed in law that all of its citizens and corporations are obligated to assist China's national security agencies in matters related to national security, cybersecurity, and intelligence.

Finally, China is pursuing a military-civilian fusion (MCF) development strategy that makes it complicated for American S&T institutions to work with Chinese partners on any project that might have military applications. Xi Jinping personally directs the MCF initiative, and views it as essential to China's rise as a world-class military and technological power. A growing number of emerging technology intensive sectors are designated key areas for MCF investment under national plans (PRC State Council 2016; Nouwens and Legarda 2018). While MCF faces structural obstacles in China, it is important that U.S. policymakers put guardrails in place now to minimize security risks arising from the initiative. Appropriate safeguards will allow S&T interdependence to continue to the benefit of both countries.

While recognizing the challenges posed by the People's Republic of China, trying to shut China off from the United States and the global economy ultimately harms the United States. To remain truly competitive, U.S. firms need to operate at scale throughout the world; localize R&D to meet the needs of diverse, fast-growing markets; and hire the best talent wherever it is available. Global operations, including those in China, should support economic activity and job creation in the United States. American policymakers can and should strive to balance these complicated realities to promote the public interest.

U.S. openness also ensures a steady flow of badly needed global talent into the United States. America's ability to attract top talent is essential to its strength while broad restrictions on cross-border collaboration and immigration undermine American innovation. The best way to compete with an ever more capable and increasingly ambitious China is to protect as much of this open order as possible, while devising effective ways to contain the risks.

OUR APPROACH: SELF-STRENGTHENING, TARGETED RISK MANAGEMENT, AND OPENNESS

This report proposes a vigorous strategy to recalibrate the U.S.-China relationship in science and technology based on three policy goals: (1) Strengthening U.S. innovation capabilities, including increasing funding for fundamental research and upgrading our production system. (2) Tailoring risk management strategies to address security threats and counter illicit behavior. (3) Preserving, to the greatest degree possible, the open, integrated global S&T and commercial system.

3 See United States Senate Permanent Subcommittee on Investigations (2019, November 18) for more information on the description of the government-run talent training and recruitment programs.

Self-strengthening

The scientific and technological leadership capabilities of any country depend on domestic efforts to encourage discovery, innovation, and dynamic markets. Troublingly, the United States has under-invested in fundamental research and the training of domestic scientists and engineers for too many years. U.S. federal R&D support, relative to the size of gross domestic product (GDP), has declined steadily since the early 1960s, according to a 2019 Information Technology and Innovation Foundation (ITIF) report. The lowest level was reached in 2018 at 0.61 percent of GDP (Atkinson and Foote 2020). Since 1990, year-on-year federal R&D spending declined in 22 of 28 years as a percent of GDP. During roughly the same period, from 1991 to 2016, China increased its R&D expenditure thirtyfold, albeit from a smaller base (China Power team 2020).

This shortfall must be addressed. In light of the vanishing gap between American and Chinese R&D budgets, we advocate for increasing the level of U.S. federal R&D funding to at least its post-1976 average of 1 percent of GDP, if not higher.[4] Such resources are critical to America's fundamental research and early stage discovery. Our goal should be that combined government, industry, and university R&D funding exceed 3 percent of GDP, a target called for but not achieved by President Obama.

America must also address longstanding weaknesses in our commercial sector that undercut our competitiveness and national defense capabilities. As our case studies illustrate, policies that support disruptive technology innovators are vital to future American success. Equally important are policies that accelerate the movement of technologies from R&D to application. Regrettably, American policies have often ignored the potential of state-of-the-art manufacturing to complement our leadership in software, services, and cutting-edge science and engineering design. China, meanwhile, is facilitating experiments that integrate new hardware with software and services in every field, from medicine to transportation. This bundling of diverse capabilities into complete systems for complex missions is now a central feature of technology markets. U.S. policy efforts to selectively upgrade the manufacturing base and facilitate the development of new systems solutions are critical.

Enhancing our own national security innovation are also urgently needed. While policymakers focus on China's pursuit of military-civil fusion, they overlook the superior potential of America's own dual-use, civil-military innovation system. However, this system is under stress. During the Cold War, the U.S. Department of Defense (DOD) was often at the forefront of seeding new technology breakthroughs. Today, leading-edge technologies of military import frequently emerge from the civilian sector before DOD's procurement planning has fully embraced their significance. The loose coupling of the defense and commercial sectors in the United States encourages bold technology experiments, but it also makes for slow absorption by the military. There is a widely acknowledged need to more quickly embrace disruptive innovation from the civilian sector and reduce barriers for innovators outside traditional defense contractors and the Congressional appropriations system.

Targeted Risk Management

As long as China pursues its current strategy, the United States must address the security risks of S&T integration with China. But we reject the notion that an S&T divorce from China would eliminate most major risks. Policy action cannot reduce risk to zero, and a national security centered strategy aimed at eliminating all risk would be both unrealistic and destructive to our vibrant society, economy, and innovation ecosystem. In the end, America would be weaker—and therefore less secure. Moreover, most other countries, including U.S. allies and partners, would be unwilling to support a U.S. strategy that requires breaking off relations with China.

As an alternative to radical decoupling, we propose a highly targeted approach to risk management modeled on our experience with cyber security (Security Agency, n.d.). The cyber security consensus recognizes that, because the benefits of pervasive digital technology networks and applications are enormous,

... we advocate for increasing the level of U.S. federal R&D funding to at least its post-1976 average of 1 percent of GDP, if not higher.

4 The historical high since 1976 was in 1985 when federal funding for R&D was at 1.21% of GDP.

Policy action cannot reduce risk to zero, and a national security centered strategy aimed at eliminating all risk would be both unrealistic and destructive to our vibrant society, economy, and innovation ecosystem. In the end, America would be weaker—and therefore less secure.

trying to lock down the cyber infrastructure along national borders is ill-advised and likely to prove futile under any cost-benefit analysis. The best way to achieve resiliency and reduce risk is through effective monitoring and risk identification systems, selective buildup of U.S. capabilities, multiple layers of targeted safeguards, and redundancy of certain critical capabilities to allow faster recovery.

The risk management strategies we propose in this report tailor the lessons learned from cyber security to particular technology domains. They reflect the need for a sophisticated approach to risk management, informed by an accurate and granular understanding of the threat actors and activities of greatest concern in each technological domain. To be sure, some risks will require strict "lock downs," such as

As an alternative to radical decoupling, we propose a highly targeted approach to risk management modeled on our experience with cyber security.

those that exist for the creation of and access to military software systems. But, it is difficult to completely segregate complicated technology ecosystems in this manner and it greatly raises the cost and slows the speed of innovation. Therefore, tight controls of special points of vulnerability should be embedded within broader risk management schemes. Such a strategy will also enable us to share specific measures and coordinate with like-minded nations to keep the risks posed by China to a minimum.

Reaping the Benefits of Openness

America's openness and ability to attract top talent from all corners of the world gives us a great advantage over China. In contrast with America's receptivity and global network of allies and friends, China is relatively closed to immigration, has no allies, few collaborators, and a reputation damaged by its authoritarian politics and human rights abuses. If the U.S. government were to close our borders by restricting immigration indiscriminately, we would undermine the dynamic American innovation ecosystem that heavily relies on contributions by foreign talent. The best way to compete with an increasingly capable and ambitious China is to protect as much of this open order as possible while devising methods to contain the risks.

Since World War II, the expansion of the global knowledge economy has spurred growth and human well-being, not just in China or the United States, but worldwide. Firms and laboratories in India, Singapore, Brazil, and Vietnam play critical roles in inventing applications for many technologies; and their large numbers of skilled engineers and scientists are indispensable to global innovation.

The United States has proved itself particularly capable of drawing from the globally diverse pool of talent, and specifically Chinese S&T talent. American universities awarded 66,690 doctorates to Chinese students in science and engineering fields from 2000-2017; and their five-year and ten-year stay rate is at 83 percent and 90 percent respectively—the highest of all nations (Trapani and Hale 2019).[5] Many go on to become leading scientists and entrepreneurs in Silicon Valley, Cambridge, Seattle, and San Diego.

In the global knowledge economy, technological advancement—whether intended to tackle the risks associated with climate change or to advance new health technologies—depends on blending specialized capabilities from many sources. Once created, and regardless of where it is created, knowledge usually spreads despite government controls, allowing more countries to build on its foundation. Take biotechnology as an example: Biotech development promises to generate new scientific insights and tools to double the world's food supply and manage health risks

5 Stay rate is used by the National Science Foundation (NSF) to measure the proportion of foreign-born noncitizen recipients of

stemming from an increasingly urbanized and interconnected world. The creation and application of these tools are both inherently global tasks.

The United States cannot meet its technological goals if it isolates itself from the growing innovation capabilities outside its borders. In such a complex environment, the only viable leadership strategy is to race faster by investing in American innovation and welcoming talented individuals from all countries.

CONCLUSION

This report examines the challenge of targeted risk management and competitiveness policy by examining the case of fundamental scientific research, as well as developments in three fields of technological innovation: 5G, artificial intelligence (AI), and biotech. America currently possesses a competitive advantage in all these fields. We aim to sustain that edge.

We do not present a complete solution in each case. Instead, we begin each section by briefly referencing some of the major policy arguments circulating in Washington. We analyze the arguments to show where conventional wisdom falters or requires further elaboration. We then suggest measures to mitigate the gravest risks, strengthen U.S. competitiveness, and preserve the benefits of continued interdependence.

We recognize that the United States faces real and growing security threats from China. While we hope that radical decoupling will never be necessary, and understand that such a step would have dire consequences for the global and American innovation systems, we would be foolish to ignore the possibility that it may become unavoidable. Unless and until such a decision is made, the role of the scientific and tech community should be to pursue worldwide collaboration in accordance with practices that mitigate the risks from openness. It is the goal of our Working Group and this report to help define those practices and advise to what degree they should be applied in a rapidly changing geo-political environment.

U.S. science and engineering (S&E) doctorates who remain in the U.S. for employment after graduation. They are calculated every two years for the individuals who graduated 5 and 10 years earlier, respectively. Most foreign-born noncitizen recipients of U.S. S&E doctorates remain in the United States for subsequent employment.

SUMMARY OF POLICY RECOMMENDATIONS

This report challenges the conventional wisdom about how best to manage the science and technology contest between the United States and China. The United States is in a much stronger leadership position than many in the policy community assume, but requires new policies to uphold American security and enhance American strengths.

To protect against the risks posed by China and safeguard U.S. security and competitiveness, the United States must embrace three complementary policy goals:

1. Bolster U.S. innovation capabilities through meaures ranging from increased funding for fundamental research to selective upgrading of our production system.

2. Tailor targeted risk management measures to address current and future security threats.

3. Preserve as many of the benefits of an open, ethical, and integrated global knowledge system and innovation economy as possible.

These three policy goals are complementary to each other —the successful realization of one depends on the implementation of the other two. Preserving openness depends on improving risk management. Risk management is feasible only if it addresses functions within a strong, adequately resourced domestic innovation system. And strengthening the U.S. innovation system will be easier if we preserve an open, interdependent global system of S&T innovation.

> ***The policy recommendations presented in this report are most likely to succeed if they are designed and implemented collaboratively with like-minded countries.***

The policy recommendations presented in this report are most likely to succeed if they are designed and implemented collaboratively with like-minded countries. The four cases in this report—fundamental research, AI, 5G, and biotechnology—contain detailed policy recommendations. Here we present 16 policy recommendations that unify all four fields, organized under the three goals that guide our analysis.

BOLSTER U.S. COMPETITIVENESS

1. Putting Our Own House in Order

The United States must significantly expand investment in its S&T capabilities, and in basic research, in order to sustain its leadership in the face of the challenges from China. American policy errors, not Chinese actions, are responsible for U.S. weaknesses. The U.S. government should raise federal funding for research and development (R&D) to at least the historical average (since 1976) of 1 percent of GDP, and total R&D funding, including from government, university, and private sources, to at least 3 percent of GDP. In addition, an updated approach to Department of Defense (DOD) and NASA investments in dual-use and strategic technologies, such as AI and quantum computing, would benefit innovation.

U.S. advancement also requires action beyond traditional R&D funding. As a form of infrastructure investment, for example, the government should provide technical tools that no single company can provide effectively. The National Institute of Standards and Technology (NIST) should be charged with developing key evaluation and testing techniques for AI systems and make them available to all researchers and firms. In other cases, such as 5G technology, U.S. innovators would benefit from government procurement incorporating technical requirements that give a boost to new generations of innovators.

2. Double Down on the Distinctive U.S. Model of Commercial Innovation

China frequently relies on state-supported national champions, such as Huawei, to advance its global ambitions for leadership. The United States has taken a different approach historically, emphasizing innovation-fueled competition, especially by new market entrants. The United States, for example, revived its sagging technology leadership in the face of an earlier challenge from Japan by betting on disruptive innovation, often dubbed the "Silicon Valley" model. U.S. biotech leadership is similarly sustained by new market entrants. The United States should continue to support technology architectures and standards-setting processes that facilitate the entry of new innovators, as it did with its previous support of the Internet protocols.

3. Restore U.S. Leadership in Setting Global Technology Standards

Standards are the global roadmaps for applied innovation and related issues such as health, security, and safety. The U.S. technology industry has thrived under an international system of robust, voluntary, and industry led standards setting that has established formulas for intellectual property rights. U.S. trade policy has long supported this approach, and the United States has frequently challenged China at the World Trade Organization (WTO) when its measures threatened this formula. U.S. government policies that prevent active U.S. participation in standards setting are highly destructive. For example, export controls temporarily prevented the United States from participating in 5G standards setting, which reduced U.S. influence in defining the algorithms and technical requirements that will be adopted by all 5G products. The United States must engage in high-level diplomacy in key international institutions. Specifically, the United States should restore active U.S. participation in standards setting, and bolster participation by both U.S. private sector actors, especially smaller innovators, and experts from key U.S. government standards bodies, such as NIST. Confidence in U.S. government support for the protection of IP rights is an important incentive for participation by new entrants.

4. No Global Talent, No Global Leadership

America's long-standing fundamental advantage is its ability to attract the world's best talent to its universities and laboratories. Our analysis of basic research, AI, and biotech stresses that while the United States needs to grow a domestic pool of STEM (science, technology, engineering, and mathematics) talent at all skill levels—and improve the diversity of the pool—U.S. leadership will falter unless it continues to attract large numbers of students, scientists, and engineers from around the world. This openness carries risks, such as the risk of IP theft, but the benefits of being the global talent hub are significant. Some targeted risk mitigation strategies are appropriate, but the United States should avoid making America the "second choice" for top talent.

5. Chips are Fundamental

Digital innovation is transforming every aspect of basic research and applied technology innovation. Each case we examine is highly sensitive to America's, or its close allies', capacity for rapid progress in semiconductor development, and and dependent on a robust supply of alternatives from trusted sources. To be clear, we are not calling for exclusive reliance on these sources for chips; innovation will benefit from true global competition. Moreover, it is probably fanciful to think that the United States alone will dominate all advanced semiconductors. But the United States should assert overall leadership—or at least shared leadership—on every cutting-edge semiconductor technology, including both design and production capabilities. Appropriate R&D policies for bolstering fundamental innovation and supply chain capabilities (such as advanced manufacturing techniques) that are consistent with competitive market dynamics are essential. Trade and technology licensing policies can also be used appropriately to bolster these measures.

The United States should enhance its capabilities by funding R&D in advanced semiconductor capabilities, including manufacturing equipment and by providing incentives for the construction of state-of-the-art semiconductor manufacturing facilities in the United States (Keller, Goodrich, and Su 2020). In addition, the United States and its allies should impose strict export controls on the sale of semiconductor manufacturing equipment for advanced chips to all Chinese companies, private as well as state-owned, while continuing to allow the sale of finished chips to Chinese companies for civilian uses.

TARGET RISK MANAGEMENT

6. Define Policy Problems Precisely

Effective policies require a clear definition of the problem to solve, and carefully matching means to ends. For example, sanctioning advanced AI technology exchange with China will not improve China's human rights practices, as China can use pedestrian AI technologies to surveil its minorities and dissidents. Human rights is a values problem, not an AI problem, so AI is the wrong tool to apply.

7. Position for the Future

Policy discussions tend to focus on short-term considerations and immediate problems, which can prevent decisionmakers from taking longer-term trends and dynamics into account. As a result, many policy prescriptions fail to heed Wayne Gretzky's adage—skate to where the puck is going, not to where it is or was. For example, U.S. 5G policy focuses on first generation 5G equipment, despite the fact that 5G networks will evolve dramatically in ways that present new opportunities for American leadership. China's own model of innovation is constantly evolving as well. To succeed over the long term, U.S. policymakers should look ahead to where China is going and target technology options that are the key to American security and competitiveness over time.

8. Focus on Multi-Layered Risk Management Strategies, Not Exclusively on China

Evolving risks are more global and complex in nature than in the past. Given how globally interconnected data systems and supply chains are, broadly cutting off one "problem" country is virtually impossible. Moreover, global risks arise from diverse sources. Risk management strategies must therefore vigorously address immediate issues concerning China, but also insist on multiple layers of safeguards that apply to all nations.

9. Embrace a "Small Yard, High Fence" Philosophy

Government barriers that restrict the flow of human capital or foreign direct investment should be as targeted and limited as possible. For example, the United States should distinguish between broad-based commercial investments and a small set of strategic Chinese investments in early stage biotech ventures, and find the right policy tools to reduce risks without unduly driving talent and capital away from the United States. Universities should also protect security related research by either transferring it to national laboratories or to their own separate secure facilities with heightened personnel screening.

10. Establish New Technology Alliances

The United States should reinforce its leadership by collaborating with other technologically advanced countries—most of which are democracies—on research, production, and policy regulation. The United States used to be the largest market for new technologies. In those days, unilateral action by the United States to close off its market could cripple a new technology. But nowadays, major new technologies are being developed and finding markets outside the United States and other wealthy democracies. Collaboration on policies related to China is therefore critical for U.S. security and competitiveness. The necessary work includes licensing critical export technologies; cooperation to diversify supply chains; and assuring the cross-border flow of data used to develop AI. There is an urgent need to set common goals and create new mechanisms to coordinate policy with allies and like-minded countries.

11. Diversify Supply Chains

Our case studies reject the idea of the excluding China from all major supply chains. However, we strongly recommend diversifying sources of supply to improve resilience from risks ranging from natural disasters to sabotage or war. In some cases, such as in 5G, diversification will open the way to increased design and production in the United States by new market entrants.

12. Pursue Whole-of-Government Coordination

Whole-of-government coordination is essential for effective risk management. Balancing economic and security considerations is complicated, as short-term security measures may hinder long-term competitiveness. Effective risk management requires input from a variety of agencies and experts. Our report on biotechnology, for example, identifies a need for much higher-level coordination of key regulatory and funding policies. The report on fundamental research notes that security guidelines for scientific research issued by different agencies are inconsistent and officials often lack the scientific expertise needed to implement the guidelines sensibly.

PRESERVE OPENNESS

13. Vary Policies According to Technology Specific Risks and Benefits

Interdependence with China does not pose a uniform set of risks or benefits. Our examination of biotech and fundamental research shows that, in general, the benefits of interdependence vastly outweigh the risks to national security, and the best policy responses involve pairing openness with risk mitigation. AI and 5G present larger risks requiring new safeguards, but wholesale U.S. separation from China will not protect these dynamic technologies. Instead, practical cross-domain policy responses are needed to balance gains from openness with risk management safeguards. For example, U.S. leadership in AI benefits from engagement with diverse data-intensive operations around the world. Yet large amounts of desired data will flow across 5G networks that contain Huawei equipment and

are connected to billions of smart devices subject to hacking by states, terrorists, and cyber criminals. This will require the risk management approach highlighted in recommendation eight.

14. Negotiate Reciprocity to Stabilize Interdependence

When the traditional safeguards of multilateral agreements falter, as they have recently, selectively relying on the principle of reciprocity to manage the United States' competitive and even adversarial relations may help preserve technological interdependence with China and prevent the bifurcation of the world economy and technology standards. Reciprocity guidelines may be desirable for access to biomedical and AI data, as well as patenting in some cases. Rules requiring reciprocity can also be a springboard for negotiated understandings of mutually acceptable terms for exchange and commerce.

15. Collaboratively Develop the Ethics of Responsible Science

U.S. dominance in science and technology in recent decades gave America a large influence over the norms and values of the scientific community. As science research and talent disperses, the United States must reinforce the importance of ethical scientific conduct. This task should begin in our own laboratories with training on ethical scientific conduct (including respect for IP), and should extend to the complicated choices surrounding the use of new technologies such as AI or gene editing tools. Ethics training is an important tool for responding to concerns about security in our labs. Our studies also recommend that these efforts extend to collaborating with the global scientific community to refine these norms. Joint training between American and Chinese universities could help inculcate common standards of research integrity and narrow ethical gaps.

16. Revive Rules and Institutions for Promoting International Commerce and Technological Cooperation

International institutions provide opportunities for renewed American leadership and action. For example, the United States can challenge Chinese export subsidies through actions undertaken with alliance partners within the WTO. The United States should also convene a group of like-minded countries to ensure that trade remedies can address the massive domestic subsidization programs undertaken in China that artificially create first mover advantages for Chinese companies. The United States and its partners must reclaim their leadership roles in leading scientific institutions and inter-governmental bodies, such as the International Telecommunication Union and the World Health Organization, so that we can balance the benefits of international interdependence with enhanced security and competitiveness. To shore up existing international institutions, the United States can also help to build new complementary arrangements focused on particular concerns about technology outside the purview of these institutions.

01

MAINTAINING U.S. LEADERSHIP IN FUNDAMENTAL RESEARCH

Even during the height of the Cold War, Soviet and U.S. scientists collaborated on basic physics and other research.

KEY POINTS

- Open exchange and collaboration drive spectacular scientific breakthroughs; they are essential to scientific and technological innovation in the United States. Collaboration with Chinese researchers should continue, but with safeguards that address security risks from China and other countries.
  - Universities should implement strict reporting requirements for faculty and researchers who collaborate with Chinese counterparts, including disclosures of foreign funding, and conflict-of-interest and conflict-of-commitment activities.
  - The government should cordon off highly sensitive research to be performed only in off-campus vetted institutions, such as national laboratories.
  - The government should investigate, punish, and condemn espionage, intellectual property theft, and other illicit activities by China.
- The United States cannot maintain its leadership in fundamental research—and the commercial technology it drives—unless it substantially increases support for basic research by increasing federal research and development funding to 1 percent of GDP.
- The United States should urgently boost the domestic supply of STEM talent—including by implementing a vigorous financial aid program to increase participation of U.S. citizens and permanent residents in undergraduate and graduate STEM education—while continuing to attract the best and the brightest to American universities.
- The United States should establish an international consortium to develop, with allies and like-minded countries, technology policies toward China, and to establish common ethical principles for the conduct of research.

Fundamental scientific research is the key that underlies the technological advances that have benefited Americans and all of humanity. Open international collaboration—including joint research with scientists overseas, sharing data and findings through peer reviewed publication, and welcoming foreign students and researchers to American universities—is essential for scientific progress. The United States' success as the global leader in scientific and technological innovation has been achieved by its open exchange and collaboration across national borders.

An open research environment nurtures critical thinking and creativity, which is foundational to the American system of research and innovation. Institutions of higher learning in the United States attract the largest number of internationally mobile students. According to a 2020 National Science Foundation (NSF) report, international students make up a significant proportion (around 36 percent) of science and engineering doctorate recipients, including half or more of the doctorates in engineering, mathematics and computer sciences (B. Khan, Robbins, and Okrent 2020).

Spectacular scientific breakthroughs have been achieved by large-scale international collaborations involving investments and data collection from countries all over the world. Contemporary examples abound: from the CERN particle accelerator; the U.S.-led Event Horizon Telescope network, which formed a virtual Earth-sized telescope to study black holes; and the LIGO-Virgo gravitational wave detectors; to the Human Genome Project, and the Kavli Foundation's international program of research institutes and initiatives. Moreover, advances in basic scientific knowledge are often accompanied by the development of novel technologies that further advance knowledge (Romer 2018)—for example, the world would not have the laser without foundational work in physics done in Europe by Plank and Einstein.[1] The virtuous cycle of scientific breakthroughs and technological advances have driven long-term economic growth for the United States, and indeed for the world.

1 The theoretical underpinnings of the laser technology that were developed by Max Planck (light as electromagnetic radiation) and Einstein (emission) were created in the beginning of the 20th century. The laser was invented in 1960 and considered "a solution looking for a problem." Now it covers a myriad of activities ranging from medical tools (e.g. surgery) to telecommunications (e.g. optic fiber).

However, in reaction to China's rise, a new viewpoint is emerging that challenges international collaboration in fundamental science and engineering research. Faced with illicit technology transfer and IP theft by China, this viewpoint argues that the United States should severely limit international scientific collaboration, including by restricting the flow of talent from China to the United States.

The U.S. government is right to be concerned about foreign espionage and IP theft by the government of China. In concert with allies and like-minded countries, the U.S. should investigate, punish, and condemn such acts and seek to induce changes in China's long-term behavior through counter-espionage, law enforcement, diplomatic pressure, and professional training in scientific integrity.

But drastic limitations to foreign collaboration would not preserve American security. They would severely curtail open inquiry, especially if they are applied broadly across new technologies.[2] They would significantly weaken university based scientific research and impede the flow and training of the talented students U.S. industry needs. The presumed benefits of reducing illicit activities would be far outweighed by the losses incurred (John Deutch 2019).

Even during the height of the Cold War, Soviet and U.S. scientists collaborated on basic physics and other research.[3] Despite Eastern Bloc efforts to steal technology to enhance their military capabilities, the Reagan administration determined that the products of federally funded, university based research in science and engineering should remain unrestricted to the maximum extent possible. The 1985 National Security Decision Directive 189 (NSDD-189) rule protecting universities' open research environment has been reaffirmed by subsequent administrations and still governs basic and applied research today.[4]

To preserve security and enhance U.S. strengths, U.S. universities and government regulators must continue to promote the key drivers of transformational research, namely openness and collaboration, by attracting international students, including those from China, and encouraging diversity in our own science and technology workforce.

A Changed Research Landscape

The need for internationalized scientific research is greater today than ever before. But the entire global S&T system has changed, with much of the advanced work now done outside the United States and Europe. Given this expansion of the global knowledge economy, and the rest of the world's embrace of Chinese advances, the U.S. ability to stop knowledge from spreading is virtually nonexistent.[5]

American investment in scientific research has also been lagging. In 2019, the federal government spent only $83.4 billion on basic and applied research, with about 16.3 percent going toward computer science, mathematics, and physical sciences (Pece 2020). Total U.S. national R&D funding has declined as a percentage of U.S. gross domestic product (GDP) in the past two decades, while China has substantially stepped up its efforts. Similarly, the U.S. share of global R&D expenditures has declined from 41 percent in 2000 to 28 percent

... the entire global S&T system has changed, with much of the advanced work now done outside the United States and Europe.

2 Careful security assessments must be done, but worst case analysis can easily unbalance risk assessment. For example, see (Lindsay 2020) for the intelligence implications of quantum computing.

3 For example, the 'Lacy-Zarubin Agreement' of 1957 initiated people-to-people exchanges and evolved into a Interacademy Scientific Exchanges that were renewable every two or three years (Krasnyak 2019). These exchanges lasted decades. In the aftermath of the Cold War, American and Russian scientists and engineers collaborated to mitigate potential nuclear threats (e.g: loose nukes and nuclear materials) after the Soviet Union break up (Hecker 2016).

4 Basic science research is included in the scope of "fundamental research" as defined by National Security Decision Directive 189 (NSDD-189): "'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." The policy states: "It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted...No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes."

5 A good indicator of the expansion of the global knowledge economy beyond North America and Europe is the sharp increase in Asia's share of global R&D expenditures. (Congressional Research Service 2020; Segal and Gerstel 2019).

in 2018, while China's share increased from 4.5 percent to more than 25 percent over the same timeframe (Congressional Research Service 2020; Segal and Gerstel 2019). Though the private sector in the United States invests substantially in R&D, most funding is for applied research and experimental development to commercialize existing technology, rather than basic research.

The nature of open science has also changed, and with it, its impact on scientific collaboration. The policy thinking that basic science should be open, while applied technology can be restricted, is no longer relevant. The lag time from fundamental research to application has shortened in many fields. The translational speed in certain areas, such as life sciences, has accelerated while in others, such as artificial intelligence, the boundaries between basic science and applications are thin and porous.

The practice of open science raises legitimate questions about collaboration with scientists from countries like China, whose governments do not share common values and norms about scientific exploration, collaboration, IP protection, human rights, and ethical science. This recognition calls for caution and a more calibrated approach to manage the risks, in coordination with allies and like-minded countries. Instead of restricting international collaboration, the U.S. government should sustain it, subject it to appropriate risk management measures, and prioritize long-term critical investments at home in public education, research, infrastructure, and innovation.

Below, we lay out a strategy that accomplishes all three objectives: maintaining U.S. strength in fundamental research, minimizing the risks, and preserving the global knowledge economy. First we describe the drivers of U.S. leadership in S&T innovation; next we identify risks to U.S. dominance and security; and third we offer targeted policy recommendations for the U.S. government, national labs, and universities.

SECURING U.S. LEADERSHIP IN SCIENCE

American researchers benefit enormously from collaboration with foreign scientists, including scientists from China. A recent study published in *Higher Education* finds that collaboration has enabled the United States to increase its scientific influence, leverage its resources, and recruit world-class talent (J. J. Lee and Haupt 2020). Several studies find that the most cited—and therefore impactful—publications are from international collaborations (Leydesdorff et al. 2014; Wagner, Leydesdorff, and Bornmann 2014; Leydesdorff, Bornmann, and Wagner 2015; Sugimoto et al. 2017; White 2019; Pohl 2020).[6] The scientific accomplishments of PRC-born scientists are particularly noteworthy; Chinese scientists have received numerous medals and honors, including Dirac Medals, McArthur Awards, Fields Medals, National Medals of Science, and election to the National Academies of Science, Engineering, and Medicine.

The more diverse the U.S. science and engineering (S&E) workforce, the more certain we can be of our future as an innovation nation. While investment in domestic science, technology, engineering and mathematics (STEM) education and diversification of the S&E workforce must be major priorities, the United States should also compete to attract the best scientists from around the world. An effective immigration policy that ensures a sustained flow of high-skilled talent to the United States is vital for the American economy and leadership position. According to the annual report by the Silicon Valley Leadership Group, the Silicon Valley workforce was 38 percent foreign born in 2018, with Chinese immigrants among the top three largest groups (Silicon Valley Leadership Group 2020).[7] Moreover, 67 percent of Silicon Valley's new tech talent aged 25-44 was Asian, with the majority from China and India (Joint Venture Silicon Valley Institute for Regional Studies 2020). Students from China make up a large fraction of those pursuing graduate studies in engineering, physics, information technology, and biotechnology in the United States.[8] U.S. research in these fields would slow considerably without their participation.

According to an NSF study, more than 80 percent of Chinese students awarded advanced degrees remain in the United States (Amy Burke 2019; Trapani and Hale 2019), becoming an important part of the American STEM workforce. Even after foreign researchers return to home country, they continue to contribute to advancing foundational knowledge and benefit fundamental research in the United States through collaboration and co-publication (Cong Cao et al. 2019). In addition, studying and working in the United States inculcates

6 Publications indicate growing impact of international collaboration. U.S. articles involving international collaborators rank considerably higher than all other U.S. publications in field-weighted citation impact analyses of contributions from several universities. The largest fraction of U.S. S&E articles with international co-authors are with authors from China (25.71%) followed by the United Kingdom (13.29%).

7 In comparison, about 17% of the workforce was foreign-born in the entire country in 2018.

8 Between 2000 and 2017, students from China received almost one-third of all doctorates awarded in STEM disciplines, with 32% of all the doctorates awarded in science and engineering, 34% in engineering, 38% in physical sciences and 36% in computer science. See (Trapani and Hale 2019) for more information.

researchers with values of ethical science and open knowledge-sharing, which are then shared and spread around the world.

Finally, collaboration allows the United States to monitor research in China. One serious risk of halting collaboration is that the United States may be caught off guard by major advances in China.

MANAGING THE RISKS OF COLLABORATION

To preserve an open research environment at home, we must manage the risks of international collaboration. China's huge, state-dominated economy, its questionable political and military intentions, and its slow progress in IP protection make it a formidable and threatening competitor.[9]

The U.S. government therefore has a legitimate concern that a hostile China may take advantage of our open research system. Indeed, there is some indication that this is already happening. In recent years, there have been reports of researchers at U.S. universities inappropriately transferring ideas and intellectual property to China in the name of collaboration; of U.S. scientists' clandestine participation in the Chinese government-run talent programs; and of the unauthorized provision of research materials and confidential information to China (U.S. Senate Permanent Subcommittee on Investigations 2019).

Collaborating with China introduces four types of risks:[10]

1. Inappropriate information transfer by researchers. Unauthorized disclosure of confidential information contained in research proposals or manuscripts under review for government agencies or scientific publishers, damage the integrity of reviewing systems and, in some cases, constitutes the theft of research ideas. In the worst case, these efforts constitute spying. Such illicit actions undermine trust and credibility—the basic building blocks of open science.

2. Failure to declare personal or research funding from China. U.S. funding agencies and universities use conflict of interest and conflict of commitment policies to ensure the integrity of research and the protection of intellectual property. For this reason, they require that researchers list funding from other sources in both proposals and university documents. Failure to declare such funding may indicate deliberate inappropriate action.

3. Reverse brain drain—graduate students and researchers take knowledge and capabilities back to China. Talent is mobile. According to NSF surveys, the United States continues to be the most attractive destination for international talent, with the intention-to-stay rate at 85 to 90 percent for Chinese STEM PhD graduates in 2017 (Zwetsloot, Feldgoise, and Dunham 2020). The PRC government seeks to counter that U.S. advantage through official talent programs such as the Thousand Talent Plan that offers graduates lucrative incentives to return to China. Though these programs are not illegal or illegitimate in themselves, the returnees may be expected by the state to undertake research to advance national military and internal repressive capabilities.

4. Commercial and military applications of basic science: Fundamental research often happens near the beginning of a complex innovation chain that ultimately leads to impactful application. The innovation chain involves universities, government agencies and national laboratories, and the commercial and financial enterprises. Leadership in some key areas such as in semiconductor research, development, and production begins with basic science, but then involves myriad other players. Openness in basic science enables the "out of the box" thinking that characterizes the most impactful fundamental research, which then drives the rest of the innovation chain. Downstream risks, often unanticipated in the early stage of scientific research, should be managed without inhibiting fundamental research, which thrives on openness and international collaboration.

POLICY RECOMMENDATIONS

To secure our leadership in science and technology, the U.S. government should fund fundamental research generously and at appropriate levels for each field (Gruber and Johnson 2019; Hadley and Manuel 2020). The United States should continue to support an open research environment by welcoming international students and researchers, engaging in international basic science collaboration actively and strategically, and competing vigorously for top global talent. Targeted risk mitigation strategies should be implemented to manage the four categories of risks described above. Below we lay out some specific recommendations for U.S. universities and government regulators.

9 Illicit information transfer and IP theft were not uncommon in America's early history, but the U.S. government never implicitly or explicitly embraced them (M. W. Peng et al. 2017; Huang, Yukon and Smith, Jeremy 2019).

10 See, for example, (Lauer 2020) for numerical data on violations.

Recommendations for the U.S. Government:

1. Invest to secure U.S. leadership in fundamental research. The U.S. federal spending on R&D in basic research is at a historic low. The government should support bipartisan initiatives like the Endless Frontier Act (H.R. 6978 / S.3832) and boost federal funding for basic research to at least 0.3 percent of GDP. Adding applied research and development, we advocate for combined federal R&D funding of 1 percent GDP or higher. Only then can we begin to reverse the trend of declining government R&D spending and secure the United States' leadership in fundamental research and technological innovation.

2. Support IP protection to encourage private R&D investment. Most R&D in the United States is driven by the private sector, which, beholden to shareholders, typically invests only if a return on investment is likely. In basic research, investment is often risky and and long term. With IP theft becoming an increasing issue in China and world-wide, protecting U.S. IP assets through diligent IP enforcement in the United States is critical.

3. Help U.S. students study STEM. The federal government should implement a vigorous financial aid program to increase participation of U.S. citizens and permanent residents in undergraduate and graduate STEM education, as Steve Hadley and Anja Manuel have proposed (Hadley and Manuel 2020). Such a program could be modeled after Eisenhower-era scholarships post-Sputnik. This would boost domestic supply of STEM talent and reduce the nation's dependence on foreign talent. To substantially reduce direct dependence on foreign talent and increase the flow of domestic talent requires sustained and substantial investments in many areas.

4. Fix the STEM immigration system. The Federal government should be entrusted with the primary responsibility of preventing those deemed inappropriate for graduate studies in the United States from participating in research at U.S. universities. The U.S. visa system has established mechanisms for performing this critical gate-keeping function, but greater capacity and expertise is needed. The U.S. government should exercise its responsibility in a manner that maximizes U.S. universities', and industries', access to talent without compromising national security. And the U.S. immigration system should be reformed to facilitate not only the recruitment but also the integration of researchers with advanced STEM degrees so they contribute to our research base.

The U.S. government should avoid blanket prohibitions of all scientists and researchers from China. To maximize U.S. national strength, the U.S. should allow Chinese students and researchers to work in areas deemed "strategic"—such as quantum computing, AI, semiconductors, and synthetic biology—but with appropriate safeguards. Proposals such as the Secure Campus Act (H.R 7033 and S.3920) would obstruct fundamental research progress without obvious benefits to the security of the United States.[11]

The United States must prioritize critical, sustained investments at home in public education, research, infrastructure, and innovation (Magsamen and Hart 2019). However, it is unlikely that increases in domestic enrollments will quickly compensate for a sharp reduction of international talents. In any case, we do not see increased domestic enrollment and international recruitment as an either-or choice.

The United States should continue to support an open research environment by welcoming international students and researchers, engaging in international basic science collaboration actively and strategically, and competing vigorously for top global talent.

5. Use the power of classification to protect highly sensitive research; and ensure such research is performed in vetted institutions. In keeping with NSDD-189, the government should adopt a "small yard, high fence" approach and classify research in select, carefully limited dual-use fields. Once identified, such research should be transferred from universities to institutions such as national laboratories that are equipped to manage both classification and interactions among vetted researchers. This would prohibit foreign nationals from participating in these

11 The proposed Secure Campus Act would bar Chinese nationals from receiving student or research visas to the US for graduate or post-graduate studies in STEM fields. It would also prohibit Chinese nationals and participants in China's foreign talent recruitment programs to receive or work on federal R&D grants in STEM fields.

few carefully selected and narrowly defined research areas.

The government should determine which small number of fields should be classified in collaboration with scientists. A starting point could be the criteria proposed by Sacks (2019) for export control: (i) they are essential to military technology, (ii) there is scarcity of knowledge about the technology, and (iii) the United States is truly at the forefront of that technology development (Sacks 2019).

6. Establish ethical principles for the conduct of research. To maintain an open fundamental research environment, the United States should continue to play a leading role in establishing frameworks for the ethical conduct of research and data sharing for the global scientific community. And the United States should lead by example.[12] Leaders of the U.S. scientific community should engage with their counterparts in China to discuss ethical norms for research and best practices to guide the conduct of scientific research collaborations between scientists in China, the United States, and elsewhere.[13]

7. Create consistent guidelines. Currently, multiple U.S. government agencies promulgate rules about international science collaboration and conflicts of interest.[14] These must be harmonized and clarified, so universities can follow them appropriately, including heightened attention to reciprocity and standards for information and data exchange that can be important inputs to advances in the age of big data. Both the Association of American Universities (AAU) and the Office of Science and Technology Policy (OSTP) are already working on this issue.[15]

8. Improve domain expertise in the FBI and intelligence community. The Federal Bureau of Investigation (FBI) is tasked with monitoring violations of research principles, so it is imperative that it has a staff appropriately trained to understand science and technology in many domains. The FBI should be informed about fundamental distinctions between basic science and specific technological applications, and be advised to obtain the counsel of domain experts in its investigative cases. With limited additional funding, the FBI could hire experts to ensure guidelines are policed appropriately so as to reduce overreach and prosecution of innocent individuals.[16]

9. Create an international consortium to coordinate technology policies toward China. None of the proposals in this report will fully address the security and technological challenges unless there are similar compatible regulations in all technologically advanced allied countries. A variety of thoughtful proposals for international coordinating groups (with relatively small memberships from technologically sophisticated democracies) have surfaced that could guide this effort. These proposals agree that, among their tasks, international coordinating groups should collaboratively identify critical technologies; harmonize risk management strategies (such as export controls and foreign investment screening); and build consensus with leadership in civil society (such as science organizations) on science research guidelines (Manuel, Singh, and Paine 2019; Rasser et al. 2020). Importantly, these proposals avoid advocating for measures that would fundamentally undermine the underlying principles of international trade and investment developed through the WTO system. Instead, they focus on coordination of national regulatory and R&D policies and thereby preserve key foundations of

Create an international consortium to coordinate technology policies toward China.

12 AI principles have been developed during the last years. Some notable ones are the Asilomar Principles (2017), the OCDE AI Principles (May 2019), the G20 (July 2019), and the U.S. Principles (February 2020). The US could spearhead this area with likeminded countries that have sizable AI strategies including France, Germany, and South Korea.

13 For example, the American Physical Society leadership is engaged in discussions with leading physicists in China about impediments to collaboration in basic research -see more information on ("China & APS," n.d.)

14 For example, in research-security related definitions. See more information on (Association of American Universities 2020).

15 AAU (Association of American Universities 2020) and APLU (Association of Public and Land-grant Universities, n.d.) provide a summary of the actions taken to address concerns regarding security and foreign influence on campus.

16 For example, Xiaoxing Xi, Professor of Physics at Temple University, was arrested at gunpoint in May 2015 by the FBI on charges of sharing technology secrets with collaborators in China. The case ended with the FBI dropping all the charges in September 2015 (Matt Apuzzo 2015).

international openness while squarely addressing the challenges outlined in this report.

Beyond working with friends and allies, the United States should also actively engage with multilateral organizations such as the InterAcademy Partnership (IAP) and the World Academy of Sciences (TWAS), which are increasingly important venues for international coordination.

Recommentations for U.S. Universities:

1. Strengthening and implementing university rules. U.S. universities should take action to ensure adherence to their conflict of interest, conflict of commitment, code of conduct, and required reporting policies. U.S. universities should also implement and/or update processes and mechanisms to screen and vet international projects.[17] The government should ensure implementation through periodic audits, with the goal of minimizing inappropriate behavior while avoiding excessive red tape.

2. Recognize the blurry boundaries and accelerating translational speed between basic and applied research, and commercial and national defense applications. The evolution from basic science to application is far from straightforward, so basic science may have defense applications that cannot be foreseen by scientific researchers. Since the boundary is sometimes fuzzy, an ongoing dialogue between academia, government, and industry is essential. Broad brush restrictions on international exchange are generally futile in the end, and they slow down scientific progress for all parties. For example, U.S. researchers are unable to collaborate on quantum information science with their Chinese counterparts, because the field is deemed to be of potential military use. Nonetheless, Chinese advances in the area now have the potential to surpass the United States.[18]

3. Train faculty and researchers, including graduate students and visiting scholars, in the appropriate conduct of research. Openness requires honesty, transparency, and integrity. All U.S. institutions and scientists involved in basic research should recommit themselves to these principles and to adhering to their institution's conflict of interest, conflict of commitment, code of conduct, and required reporting policies. In addition, U.S. research universities should regularly train faculty and senior researchers to distinguish between appropriate and inappropriate collaborations, and to handle conflicts of interest and commitment. Research universities should also be required to regularly instruct all foreign and domestic students and visiting researchers to raise awareness about illegal spying and the consequences of such activities, including criminal prosecution. Universities should expand their training in scientific ethics beyond traditional research integrity issues and include conflicts of interest and commitment (JASON, 2019). Joint training between American and Chinese universities could help inculcate common standards of research integrity and narrow ethical gaps.

CONCLUSION

The principal goal of fundamental research is to advance human knowledge. U.S. leadership in early stage innovation depends on its ability to continue to lead the world in new frontiers of research and to attract the most talented students worldwide. The success of this approach depends on the openness and freedom of U.S. society—which are two of America's most important asymmetric advantages—and on an effective government-academia partnership to manage the inherent risks of international collaboration.

Preserving America's security and ensuring American leadership in fundamental scientific research requires a strong commitment to openness, coupled with smart risk mitigation. Closing up the U.S. research system and stymying collaboration will harm the United States, causing us to fall behind and become a second-rate nation in science and technology.

17 For example, on April 3, 2019 MIT implemented a new review process for 'elevated risk' international proposals (Lester 2019).

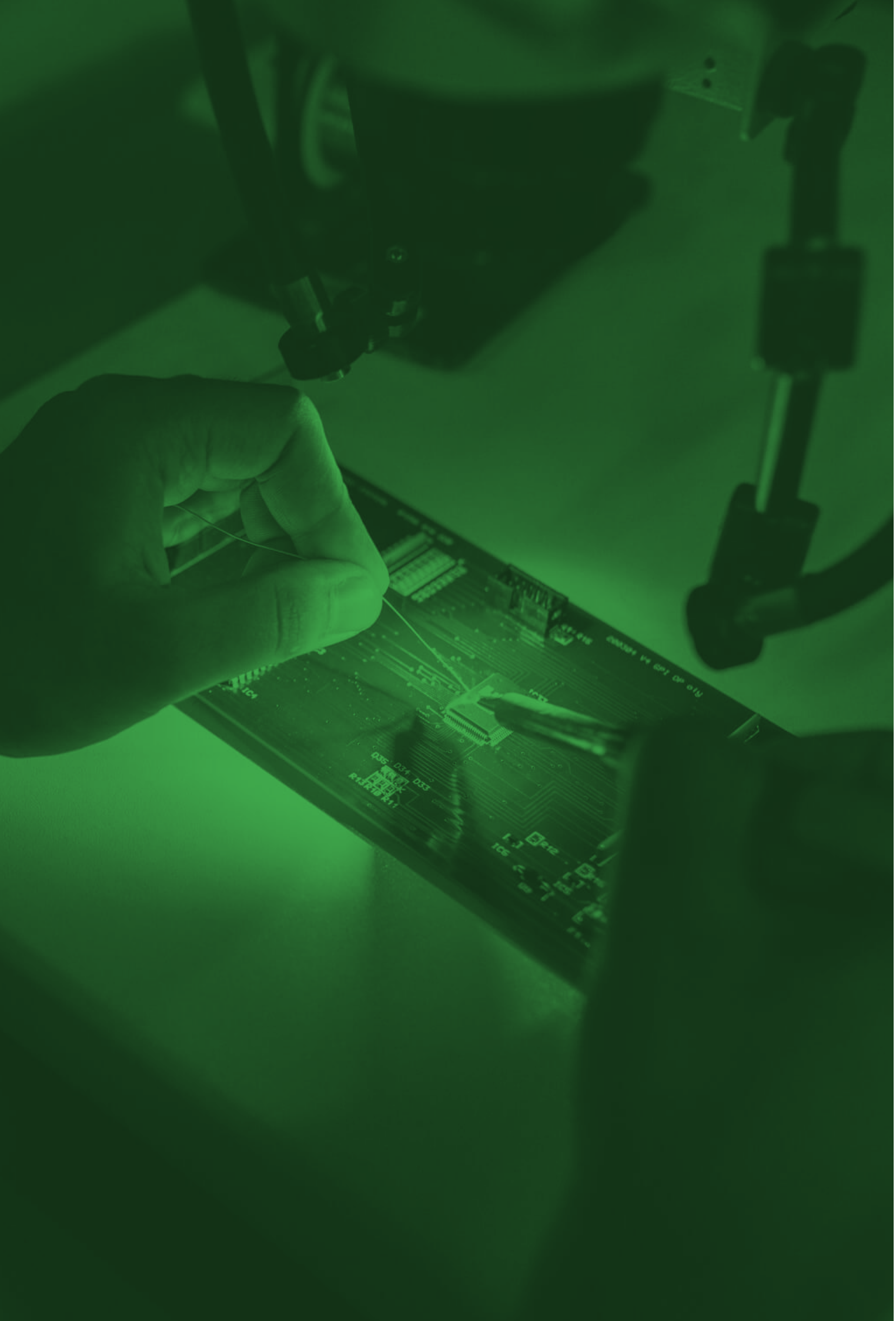
18 NSF defines quantum information science (QIS) as "an emerging field with the potential to cause revolutionary advances in fields of science and engineering involving computation, communication, precision measurement, and fundamental quantum science."(NSF Quantum Information Science Working Group 1999). See also (John Costello 2017).

COVID BOX 1

U.S. CHINA COMPETITION IS HERE TO STAY; BUT SAVING LIVES DURING A PANDEMIC REQUIRES THE TWO COUNTRIES TO WORK TOGETHER.

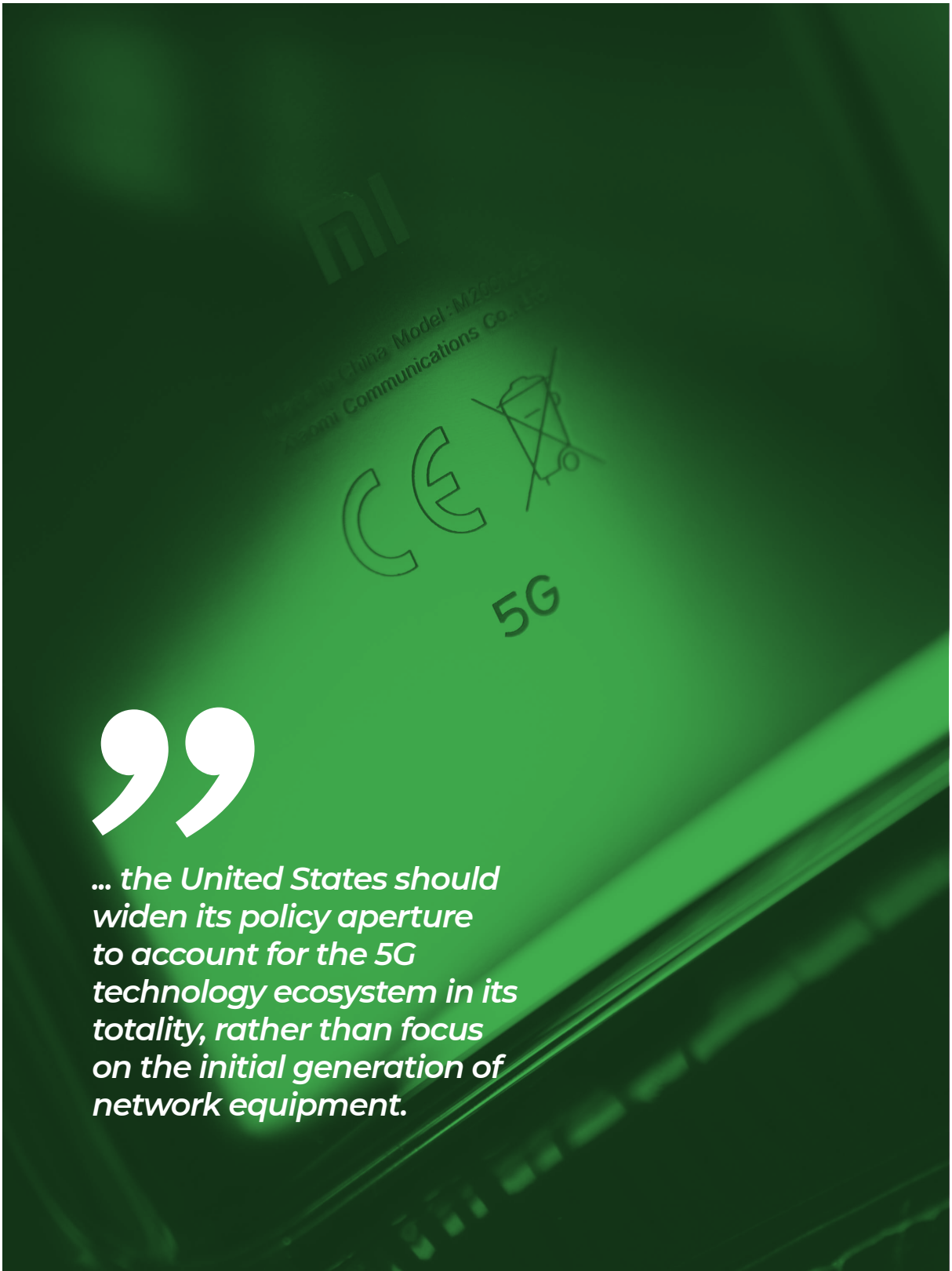
The COVID-19 pandemic has resulted in a new nadir in U.S.-China relations. The initial delays and lack of transparency by China's Party-state contributed to the rapid global diffusion of the novel coronavirus. Beijing has launched campaigns of propaganda in an attempt to change the narrative about that reality. Meanwhile the White House also has sought to deflect criticism of its poor management of the pandemic by blaming China. Misinformation, disinformation, and conspiracy theorizing in both countries have exacerbated tensions.

Prior to this pandemic, global public health was regarded as a likely arena of productive engagement for China and the United States. In the past, the two countries had been able to combine forces to confront global public health threats such as H1N1 flu and Ebola. Instead, the mistrust and hostility that has flared up against the backdrop of the global pandemic have further undermined the prospects for cooperation or even minimal coordination between the two governments.



02

A 5G STRATEGY FOR AMERICA: U.S. OPTIONS AND THE CHINA CHALLENGE



> *... the United States should widen its policy aperture to account for the 5G technology ecosystem in its totality, rather than focus on the initial generation of network equipment.*

KEY POINTS

- 5G technology is a fundamental, evolving infrastructure technology. It will enable future specialized networks to respond instantaneously to the needs of innovative applications for capacity, speed, and reliability.
- Contrary to conventional wisdom, the United States is strongly competitive in the underlying technological drivers of 5G as it evolves. A smart U.S. strategy to enhance U.S. security and competitiveness will shape the evolution of 5G in ways that fit these strengths.
- The United States should not attempt to win a race between Huawei and a new American national champion. Instead, the United States should adopt a forward-looking strategy to enable a variety of new entrants to enter the 5G innovation space successfully. This strategy would erode dependence on a single equipment provider for the entire 5G network by facilitating the emergence of open and modular architectures such as ORAN or vRAN. Diversifying suppliers will also make it easier to manage both immediate security risks, and complex future threats to the 5G ecosystem as it shifts from a single-vendor model to a more competitive and diverse interoperative system.
- Huawei's prominence in the global technology market presents a special challenge. The risks associated with Huawei can justify a ban on some products by some countries, but total global exclusion of Huawei is not feasible—nor is Huawei the only risk. Instead, the United States should pursue a layered approach to risk mitigation that maximizes network reliability and security and manages the espionage and sabotage risks in the applications and end-user devices that interact deeply with these networks.
- 5G standards are critical. The United States should deflect Beijing's attempt to dominate the standards process through government coordination of Chinese firms. The United States should play a leadership role in the inter-governmental process, while enabling more U.S. firms to fully participate in the voluntary, transparent, industry led and intellectual property-protecting consensus process for setting standards. Enabling participation of innovative U.S. firms will require a variety of incentives to support and encourage their entry to the 5G space, and participation in the standards process.
- The United States should use diplomacy to coordinate with other allies and like-minded countries to counter market-distorting subsidies by the Chinese government to its telecom companies.

Fifth generation (5G) mobile broadband telecommunications will become a fundamental component of the world's communication and information technology infrastructure over the next five to ten years. 5G's value goes far beyond its capacity to deliver greater speed and bandwidth to individual users. 5G systems will enable future specialized networks to respond instantaneously to the needs of specific applications for capacity, speed, and reliability.

5G will enable many more specialized end-use solutions in industry and manufacturing, transportation, agriculture, healthcare, and any number of public and private applications. These solutions will operate "locally" but be integrated into the broader network and Cloud computing infrastructures. For example, remote surgeries can be carried out using local virtual reality applications, combined with Cloud computing resources. Moreover, these applied networks can be anywhere, not just where terminals are attached to high-volume fiber optic cables. 5G will also make massive machine-to- machine networking among sophisticated devices like robots (sometimes called the "Internet of Things") into the dominant network use.[1]

5G's development is vital for the future prosperity and security of the United States. However, to date, uncritical acceptance of two false premises have hampered 5G policy discussions. One is that the United States is badly behind China in the key drivers of this blossoming technology. The second is

1 Some policy analysts insist that US policy should look forward to 6G. It is difficult to forecast what 6G would entail. 5G is an ecosystem whose design is already underway, a more tractable target for policy intervention. That said, our recommendations assume trends in technology that will position the U.S. to excel in 5G and 6G.

that the core security risk revolves around the role of Huawei hardware, particularly radio base stations, in the 5G network. Neither premise is a good basis for effective policymaking.

This report argues that the United States should widen its policy aperture to account for the 5G technology ecosystem in its totality, rather than focus on the initial generation of network equipment. While there are short-term concerns about security that require careful attention, the United States should adopt a forward-looking strategy and anticipate new and emerging configurations of 5G technology. This future configuration poses different security risks and competitive opportunities while operating in a global market where China will remain an important factor. As is said in hockey, we must "skate to where the puck is going, not where it is or has been."

A forward-looking approach has two implications. First, although concern about 5G communications has focused mostly on the current generation of infrastructure equipment, it is equally important that the United States maintain its traditional leadership position in foundational 5G research and development and standards (Manuel and Hart 2020). 5G standards serve as the blueprint of the 5G ecosystem—they are implemented by *all* 5G products, including chipsets, devices, and infrastructure equipment. They define the algorithms and technical requirements that make wireless communications systems work.

Second, 5G networks are likely to adapt dramatically over the next few years, from networks that rely on updated versions of legacy telecom equipment and systems, to a diverse ecosystem in which operators can source components from a variety of companies, with standard interfaces allowing them to work together in a single network. This new ecosystem may well rely more heavily on software to deploy and operate 5G networks, reducing the need for operators to purchase and maintain expensive hardware.

China will challenge the U.S. in both areas: in shaping the new 5G ecosystem, and in the potential transition from hardware- to software-centered technologies. In response, U.S. policymakers should stay especially focused on the end goal—U.S. security and prosperity originating from participation in global markets—and use policy to drive in that direction, rather than primarily focusing on the market as it looks today. 5G networks could evolve dramatically in ways that present new opportunities for American leadership in the medium to long term.

The following discussion addresses two areas that require new policy. First, economic and technology policies should address the medium-term evolution of 5G networks. If government policy facilitates a fair process and invests in a few key capabilities, the United States will be able to maintain its traditional standards leadership while the features of the emergent network will play to American strengths. This evolution will help the United States respond to the challenge presented by Chinese state-sponsored and/or subsidized companies.

Second, while the emerging 5G standards have some strong new security features, the security challenge will become significantly more complex as the number of local networks and access points grows exponentially in the Internet of Things. China poses a unique security threat that requires an immediate U.S. response to the technology in the early stage of 5G rollout—but it is not the only security threat. The United States should focus on a comprehensive risk management strategy for the evolving 5G ecosystem. We need to recognize that Chinese companies will remain part of the global supply chain into the future and take action to mitigate risks based on this (realistic) expectation of the global ecosystem.

> ***... the United States should adopt a forward-looking strategy and anticipate new and emerging configurations of 5G technology ... As is said in hockey, we must "skate to where the puck is going, not where it is or has been.***

We offer detailed policy recommendations in the final section.

STANDARDS AND THE LONG-TERM 5G ECOSYSTEM

The development of 5G required groundbreaking inventions to enable its revolutionary advances. As a new technology system in its earliest iteration, 5G technologies will continue to evolve rapidly, thereby creating a technological upheaval that offers opportunities and risks for the United States. The "recipes" that allow many innovators to coordinate their ideas for hardware and software and make them interoperable are

the 5G technology standards. The first two releases of 5G standards have already been finalized and the third 5G release is currently under development.[2] 5G standards collectively define the new technology's features and requirements implemented in all 5G products. They include protocols for security, such as how to deploy encryption and decryption for signaling over 5G networks. In short, standards are critical for charting the technology's future, and therefore have vital implications for U.S. security and competitiveness.

Good governance principles in standard-setting are essential for maintaining the merit-based evaluation and selection of the best technologies. In the past, the process achieved global acceptance of its recommendations

from common international standards set by consensus—U.S. interests may be at risk due to overt and covert government coordination of Chinese firms even as U.S. influence has waned. In particular, Chinese companies have been pressured to vote as blocks in favor of Chinese standards contributions, irrespective of technical merit, and large teams from government-subsidized Chinese firms have flooded some standards processes. This Chinese strategy may cause a process intended to be technocratic to become politicized in ways that are counterproductive to its legitimacy.

To illustrate the challenge, as Chinese participation has increased, many large U.S. firms have reduced their role in standards bodies; smaller new firms with advanced

Good governance principles in standard-setting are essential for maintaining the merit-based evaluation and selection of the best technologies.

while conforming to the long-standing U.S. position of supporting a voluntary, transparent, industry led consensus for setting standards. It also operated under a reasonable and balanced intellectual property (IP) rights system that respected IP rights and innovation.

In recent years the PRC government decided that promoting Chinese standards in global standards bodies via the work of Huawei and other Chinese companies is key to realizing techno-nationalist goals for technological ascension. Viewed in this context, Huawei is in the vanguard of the Chinese effort to establish dominance in both the number and significance of Chinese patents that are deemed "standard essential" to 5G standards (Strumpf 2019). American and other non-Chinese firms still hold a significant share of these essential patents.[3] Going forward, however, it is in the U.S. interest to deflect Beijing's attempt to dominate the standard-setting process.

To be clear, while Chinese participation in the global system is desirable—the world benefits

technologies find participation in the standards process challenging and costly. Currently, 55 companies participate in the standards process under the U.S. umbrella, Alliance for Telecommunications Industry Solutions (ATIS); by contrast, the China Communications Standards Association (CCSA) has 128 member as of 2020.[4] The number of European organization members also dwarfs those of the United States. Moreover, the standards process has long involved a government-to-government component for some matters, exemplified by the International Telecommunication Union (ITU). The PRC government has put resources into achieving prominent leadership roles in these intergovernmental processes to increase its influence. Therefore, bolstering American participation is vital.

The impact of the standards system on the evolution of 5G plays out in concert with the dynamics created by the commercial marketplace. The initial deployment of 5G hardware is, with very limited exceptions, being implemented with upgrades to traditional cellular network infrastructure equipment

2 Standards emerge primarily under the umbrella of 3GPP (the 3G Partnership Project), the organization that sets 5G standards under the International Telecommunication Union, or ITU. Separately, the O-RAN Alliance is leading a critical effort to develop common standards for a truly open and interoperable fronthaul interface within the radio access network (RAN), which 3GPP has thus not addressed. Many new market entrants are calling for 3GPP to adopt the O-RAN fronthaul interface as a common global standard.

3 The purpose of this Working Group is not to settle debates about the significance of the total number of patents in 5G standards versus an emphasis on the technological significance of specific patents. This group agrees that China has set a policy goal of being the overall leader in setting global 5G standards. The question for us is how to respond.

4 See ("Membership," n.d.) for 3GPP membership; CCSA full membership, at 644, can be found on its official website ("CCSA Membership," n.d.)

supplied by incumbents such as Huawei, Ericsson, Nokia, and Samsung. These networks run on a mostly closed (proprietary) hardware system that gives incumbent equipment providers a great deal of discretion in designing detailed system architecture. Huawei has the largest global market share by far. Huawei's success owes both to its engineering prowess in radio access networks (RAN) and core networks, and to the robust subsidies provided to Huawei's customers by the PRC government and generous loans from state banks (Hart and Link 2020). The question now is how a new set of entrants can transform this arena into a more technologically innovative space that would, as a by-product, advance American economic and security interests.

New entrants will face obstacles. For one, subsidized Chinese prices slow down the transition process by providing cheap equipment that is easy to integrate with existing networks, and depress the economics of market entry for new innovators. Many network operators feel they have no alternative to Huawei equipment because it is costly and technically difficult to switch proprietary network equipment systems. Moreover, given their dominant position, Chinese companies have incentives to slow down the emergence of more efficient solutions in the standards process that would enable new market competitors.

A sound policy strategy would embrace two shifts in the unfolding standards for 5G. First, there is a growing global coalition of companies, including major information technology firms and American network operators, seeking to push the market from its current single-vendor model (where operators largely buy their equipment from one vendor and cannot easily mix and match) to a more diverse, interoperable ecosystem (called an Open Radio Access Network, or "Open RAN"). ORAN architecture would ensure an open network whose design facilitates the mixing and matching of offerings from various hardware and software providers. This modular design would facilitate movement away from forced vertical integration, and thus from reliance on any one 5G infrastructure supplier such as Huawei.

Second, many companies are developing server-based systems based on "Cloud computing" that rely more heavily on software to deploy and operate 5G networks. This approach also shifts many of the command and control functions of the network (a key security stress point) to Cloud computing that instructs the network on how to meet the needs for the task at hand, including guidance on routing and security measures. This is called the virtualized radio network approach or vRan. It is one in which U.S. firms are poised to play a leadership role because of American capabilities in making the mobile chips, servers, and software architectures used in Cloud computing, as well as its enormous strength in software applications.

The United States has a unique opportunity to take advantage of these technical evolutions. Multi-vendor interoperability, i.e., the ability of different standards-compliant hardware and software systems to operate together seamlessly in 5G, is particularly important. Many industry players are pushing the market in that direction—though some incumbents, including Huawei, oppose. A move toward interoperability makes sense for both technical evolution and open market competition. U.S. competitiveness improves because a more open market creates opportunities for disruptive technology, such as virtualization, and for new market entrants, most of whom conduct R&D and manufacturing in the United States. It will also bring more choices and opportunities to manufacturing critical components in the United States and other secure locales, thus reducing certain security risks.

A look back to the upheavals in computing and networking that occurred in the 1990s offers useful lessons for the evolution of 5G. The then-new Internet provided an "open" (i.e., non-proprietary) software architecture (the Internet protocols), creating a "modular" system in which any supplier of hardware or software could plug into the Internet and provide specialized capabilities. Specialized suppliers could still use proprietary technology within their individual components (such as computers and routers), but they were designed for "plug and play" in an open and modular network. In both hardware and software, formerly dominant proprietary and vertically integrated systems, such as IBM mainframes and AT&T communications networks, gradually gave way to networks of desktops and servers (fueled by ever more powerful semiconductors) plus new software systems that provided faster and cheaper solutions. While not perfectly seamless, control of information technology (IT) shifted substantially to software, specialized equipment, and semiconductor specialists who could deliver their solutions across many different hardware systems. As a result, networked IT evolved from expensive, highly specialized hardware systems—similar to the hardware network devices dominating 5G today—to today's world of pervasive information applications, such as the apps on our cellphones.

Innovation-fueled competition, especially by new market entrants, created disruptive innovation, which resulted in an explosion of competition and new solutions, fueled by new specialized hardware and software suppliers.

The productivity of the entire ecosystem increased because of the complementarity of various advances.[5] Moreover, this Internet architecture ultimately reinforced U.S. competitiveness in IT, which was then being challenged by Japanese firms who clung to extensive vertical integration for IT.

If the global 5G ecosystem shifts to an ORAN architecture, we expect similar dynamics. The current oligopoly structure with four major equipment vendors—Nokia, Ericsson, Huawei, and Samsung—will weaken and many companies will be able to provide equipment and software in a mix-and-match ecosystem. That shift creates opportunities for new market entrants from the United States and elsewhere to prosper, which will make it harder for China or any other nation to suppress competition or carve out a dominant position for its national champions. A further benefit of a more diverse supply ecosystem is that it reduces risks to security created by any major firm.

The potential benefits of 5G ORAN and vRAN technologies will not materialize automatically. The ingenuity of American firms alone is not enough—appropriate policy measures are required to realize the benefits. Below we lay out this policy agenda with specific recommendations.

UNDERSTANDING SECURITY RISKS IN THE SHORT AND LONG TERM

While the 5G standards and technology themselves have built-in advanced security features, and ORAN and vRAN architectures provide security alternatives to traditional "black box" infrastructure, any new technology can present additional vulnerabilities. The defense of U.S. security demands a robust response, not only to protect the network today, but also to ensure security in an even more complex future. That means tackling increasingly complex security threats in both hardware and software, as well as leveraging underlying security protocols and algorithms in the foundational 5G technology standards.

In terms of hardware, billions of new end-use devices will originate from China or from small new providers whose information security practices rarely match those of technology giants. No matter what the United States and its closest allies do, much of our traffic will touch networks where Huawei or ZTE equipment is installed, or will be part of the Internet of Things interacting with the network. So too, the flows of data in a future 5G-enabled ecosystem will be complex and not readily separated or segmented by nation. Each of these touchpoints constitutes a potential network vulnerability. Given this reality, a "zero trust" paradigm becomes a necessity.[6] Any solution focused on the United States or a few countries will not eliminate much of the risk, nor will an exclusive focus on threats from China address the largest long-term risks.

Even the most basic discussion of network security must take into account threats both from state actors and from cyber criminals, who are becoming as capable as nation-states on some fronts. Moreover, there are qualitatively different threats, ranging from espionage to sabotage, which require different responses.

Huawei's prominent role in the global market presents a special challenge. Already, Huawei is present within over 90 networks.[7] Partly owing to the generous financing by Chinese state banks to its customers, Huawei can provide a rapid and low-cost transition to 5G that is understandably attractive to many countries. Security experts worry that hidden "backdoors" in Huawei equipment or software could present all three of the most malign types of risk: espionage, sabotage, and dependence. Espionage centers on the ability to intercept messages and collect sensitive information at scale. Sabotage involves the ability to bring down the entire communications network in a time of extreme tension or war or to use the threat thereof as a means of coercion. Dependence refers to the types of direct and indirect power and influence that an actor can exercise over decisions on other tech choices, such as facial recognition technology, based on possessing a near-monopoly on certain types of critical infrastructure equipment. These risks are different but related, and all require serious attention.

Despite the special challenge of Huawei, we should not fall into the trap of thinking that banning Huawei is the key to a secure network in the long term. On balance, the risks presented by Huawei can justify a ban, particularly for nations that see China as a competitor or potential adversary. Yet total global exclusion is not feasible, and it is certainly

5 For example, networked personal printers and Excel spreadsheets made personal computers more valuable.

6 Zero trust frameworks assume that firewalls do not secure the data and applications flowing through the network. As a result, constant monitoring and security safeguards exist within the network. For example, through varying designs, each user and device must be thoroughly authenticated and access to various resources and data flows on the network may be segmented for security reasons.

7 Huawei is especially strong in numerous developing country markets. It has almost 30% of the world market for RAN equipment, making it number one in the business (Pongratz 2020).

not a coherent or complete solution to the multifaceted challenges of 5G security.

A layered approach to risk mitigation with regard to Huawei is thus justified. Such an approach should recognize that there are different security needs depending on network activity and applications. To date, the United States, Australia, the United Kingdom, Japan, Canada, India, and Sweden have essentially eliminated Huawei as an option for their core infrastructure. France and Germany may follow. However, many countries will opt out of a total ban on Huawei, and U.S. pressure may have limited leverage. The cost of asking countries to discard low-cost Huawei equipment for improved security during the transition to full 5G networks is relatively high, and many may fear falling behind in a so-called "race to 5G." Instead, the U.S. government should offer countries and their telecom networks incentives to deploy 5G standard security features at the outset, and to consider new approaches such as ORAN and/or vRAN as their networks evolve. These new architectures reduce both capital and operational expenses for 5G, making it easier to replace legacy Huawei equipment with the assistance of competing vendors vRAN.

Beyond the immediate challenge of Huawei security risks, the long-range nature of threats associated with 5G requires a targeted risk management strategy. The goal is both to maximize network reliability and security and to manage the security in the use-cases and applications that interact deeply with these networks. Network technology, applications, and end-user devices are continuously evolving; so too, are the risks. We need a flexible approach that can evolve to respond to shifting risks across all layers of the network and its applications. We should prioritize the deployment of security features and options incorporated in 5G global standards.[8] We should also work with allies and network users (e.g., healthcare, automotive) to agree on a multi-layered system of security safeguards, building on initial progress toward consensus via the Prague Proposals (Prague 5G Security Conference 2019). This could include identifying particular items in future global supply chains for the 5G ecosystem that require coordinated security safeguards. Priority effort should go to creating with the European Union (EU) and like-minded nations an approach that could become the *de facto* global framework, as has also been recommended by other case studies in this report.

PROSPERITY WITH SECURITY: POLICY RECOMMENDATIONS FOR ACHIEVING THE 5G TECHNOLOGIES THAT WILL BEST SERVE THE UNITED STATES

The emerging technology ecosystem in its totality must be the primary focus of U.S. policy efforts. Policy action is required in two broad areas that have very different risk and return profiles.

The first policy objective is to ensure that the emerging 5G network evolves according to principles that provide for a secure and stable network and play to American strengths in the evolving technology ecosystem. In the long run, this is the most fundamental objective, and there is still time to organize a strong and coherent government strategy.

Broadly, this demands leadership in developing 5G standards in a manner consistent with an ORAN architecture, while providing space for disruptive approaches such as vRAN. The U.S. government should also undertake selective policy interventions to fuel R&D critical for setting 5G standards while incentivizing market entry by a range of specialist firms with new solutions that can thrive in a radically reinvented network. This is how the United States prospered in IT after the Internet emerged in the late 1960s. In some cases (such as how networks protect data privacy), policy choices must be made strategically against Chinese preferences, but the overall objective goes beyond China.

The second policy objective is to address both immediate security threats and the even more complex future threats as we move to full 5G with ORAN and vRAN networks. The United States faces not only a critical short-term need but also a long-term challenge. Current efforts focusing on Huawei equipment are important but they have also distracted

A targeted risk management strategy may start with Huawei, but it should go well beyond the issue of who controls traditional network hardware.

8 In the past China has sometimes ordered deployment of Chinese created standards for suppliers in China. The US Government has rightly opposed these actions.

from long-term fundamental considerations. A targeted risk management strategy may start with Huawei, but it should go well beyond the issue of who controls traditional network hardware.

In the following, we present four detailed recommendations that fall under two categories, with the first two recommendations aiming to facilitate a robust 5G network that will contribute to American prosperity, and the last two recommendations designed to mitigate the range of security threats in espionage, sabotage, and dependence.

1. Participate actively in the standards-setting process to lead in foundational technologies as well as to achieve an open and modular architecture.

1A. The United States should provide support to reinforce existing standard-setting procedures and good governance principles, and renew strong American participation. The U.S. government should strongly support U.S. and other companies to engage fully in standard-setting institutions. For example, expanded U.S. government funding and staffing to enable standards groups to meet in the United States would reduce barriers to participation by smaller companies.

1B. The U.S. government should support the Department of Commerce, especially its National Institute of Standards and Technology (NIST), and other U.S. government agencies to take a much more active role in the development of balanced standards policies and processes, as well as 5G technology standards, thereby leveraging NIST's expertise in cybersecurity. However, NIST should not direct standards choices. At the same time, the Department of State should lead a long-term effort, in cooperation with allies, to strengthen U.S. participation and leadership in the ITU because of its important role in 5G development.

1C. The U.S. government should adopt policies that incentivize U.S. firms to invest in long-term R&D, which is critical to leading in foundational technology standards. The United States should make a vigorous effort to incentivize and support companies conducting their R&D and manufacturing in the United States, particularly small-to-medium sized companies seeking to become new market entrants by leveraging potentially disruptive 5G shifts to interoperability and virtual networks. Incentivizing the R&D efforts of U.S. firms requires that the U.S. government be diligent in pursuing its traditional policy support for IP rights in the setting of standards.

2. Adopt a targeted approach to improving U.S. leadership in the 5G ecosystem.

2A. The United States should not try to win a "national champions race" by creating a national champion in telecom equipment. No "new Lucent" can solve the fundamental competitive challenges. Such an approach is ill-suited to the technological evolution of 5G as well as the U.S. political and market system. If Washington deems it important to bolster Huawei competitors in legacy RAN equipment, it should consider U.S. government financing, such as from the Export-Import Bank, for bids by trusted firms that in the near term have capacity to produce and price at sufficient scale to be a reliable alternative to Huawei.

2B. A key objective must be to establish a global market for current and future technology products that is not distorted by massive subsidies. The United States should coordinate with other affected countries on whether distortions of markets due to large-scale subsidies warrant the use of countervailing duties or other actions at the WTO or in other forums. This can be complemented by diplomatic discussions among interested parties about correcting problems.

The United States should not try to win a "national champions race" by creating a national champion in telecom equipment.

2C. The United States should reduce dependence on China for strategic 5G-related components by diversifying suppliers. The U.S. strategy should target more diversified design and production by U.S. or allied firms, especially new entrants, to more quickly reduce the level of reliance on China. For example, China is a critical supplier of 5G radios and antennas, which the United States will need in the future, even if a vRAN approach reduces hardware needs. New American market entrants with specialized components can diversify this hardware base. One likely candidate for facilitating market entry is supporting the ORAN Alliance negotiations—particularly those aiming to develop common standards for a truly open and interoperable radio access

network—currently underway among a wide array of IT companies.

2D. To further bolster U.S. innovation and leadership in world 5G markets, the U.S. government should encourage new entrants, through government procurement preferences and targeted U.S. government support for research in particular technological capabilities. This would be similar to the innovation strategy that stimulated the early Internet economy. High on the list should be:

- Pass major government measures to buttress U.S. leadership in underlying semiconductor technologies, particularly by supporting secure production arrangements and incentives for R&D.
- Greatly expand R&D support for 5G ORAN and vRAN test beds. This will accelerate the design and scaling of network capabilities and innovative end-use applications by a diverse array of participants, including systems integrators who will customize network and IoT systems. To keep test beds competitively neutral, consider using universities, national laboratories, or other large U.S. government facilities.
- Leverage U.S. government procurement to reinforce ORAN and vRAN standards. The United States must ensure that future procurement of 5G systems, including for government facilities and military installations, provide opportunities for start-up firms to experiment with innovative applications.

2E. Freeing up traditional mobile radio spectrum for 5G deployment is important. Even more critical is removing barriers to developing millimeter wave spectrum, and the equipment necessary to enable it, because it is essential to many of the biggest technology uses. This is especially important given China's ability to scale quickly, unhindered by government limitations on where network equipment can be deployed. Federal and local partnerships should remove regulatory obstacles to 5G networks, leverage spectrum sharing and de-conflict competing uses. For example, federal facilities could be opened up for installations of the millions of small antennas necessary for using the millimeter wave spectrum.

2F. Use the 5G roll-out to provide network access to all Americans. This investment should be an integral element of the post-COVID-19 stimulus and recovery program, along with measures to develop a more robust workforce in 5G through jobs training programs. The U.S. government must also expand programs to ensure that universal broadband service is available in under-served communities, and to facilitate a long-term transition to tele-work and e-learning for students. In the course of doing so, U.S. companies will "learn by doing" to accelerate innovative solutions in the 5G ecosystem.

3. Adopt targeted risk management strategies to address a broader spectrum of possible security breaches, including the risk of espionage from non-trusted network equipment.

3A. Hardware-based risks of eavesdropping are significant, but they are not limited to Huawei RAN equipment. For example, Huawei already has a 21 percent share of global fiber optic networks, including a significant U.S. presence (Network Telecom Information Research Institution 2019). Fiber optical service nodes have information processing roles that provide opportunities to monitor message flow. Comprehensive monitoring of hardware risks should be sustained and intensified across the entire information and communications technology (ICT) ecosystem: there is no easy substitute.

3B. More widespread encryption, including increased reliance on end-to-end encryption of important communications, is essential to guard against eavesdropping.

3C. The biggest espionage dangers will continue to be hacking by both state actors, some with sophisticated cyber capabilities, and individuals. This is true even when human vulnerabilities from spear-phishing and social engineering are considered. Dangers include targeting and exploiting vulnerabilities within the systems and the equipment of other companies. Because ORAN and vRAN may have new vulnerabilities, and the number of 5G devices deployed for IoT will be huge, risk management by intense network monitoring, identity management, and training users on security is essential (Rose, Eldridge, and

... the U.S. government should encourage new entrants, through government procurement preferences and targeted U.S. government support for research in particular technological capabilities.

Chapin 2015).

4. Manage the long-term risks of sabotage and dependence through diversification.

4A. While a ban on Huawei is feasible in some key countries, especially allies and partners, this is a global networking challenge that requires multifaceted solutions. Considering that Chinese components, user terminals, and software will be intermixed among the billions of connected end users of 5G globally, a total global market ban on Huawei and other Chinese suppliers is not practical.

4B. Prioritize working with allies to agree on a multi-layered system of security safeguards. The objective is to permit secure cooperation and data interchange among countries that use cellular infrastructure from trusted vendors, while providing added security where countries may not have installed trusted vendor hardware and software. Common approaches to strengthening supply chain security for critical components and software should be emphasized. Priority should be given to creating a joint approach with the EU and other technologically sophisticated democracies that can become a global framework, building upon the Prague Proposals. Such an approach should:

- Create a multi-layered system of security safeguards based on robust risk management principles, such as robust security monitoring capabilities; practices for security information sharing among networks; systems for increasing redundancy in network functions (as a safeguard against failures); and resiliency in restoring networks. 5G is designed for reliability and security, and its deployment should leverage that design.
- Incentivize all deployed radio network equipment to meet certain requirements for "open interconnection" (the Open RAN architecture). Once the network's intelligence moves out of traditional network equipment, no one vendor can easily bring down the network. Faster movement to an open network with diverse new suppliers may bolster security.
- Recommend a set of risk mitigation protocols for countries that use Huawei equipment. The protocols might include regular monitoring of Huawei software as a first step and limited scope for Huawei equipment (as in the initial British approach of explicitly banning Huawei equipment from core parts of the network, such as intelligence, military, and nuclear installations). A requirement that Huawei radio base stations use secure chip sets supplied by approved vendors could also be part of such protocols.

CONCLUSION

The strategic approach described here intends to accomplish many objectives simultaneously by recognizing the complexity of the 5G challenge posed by China. A focus both on accelerating 5G deployment and transitioning to a more open architecture will provide Americans access to a fast and secure digital network and provide American businesses access to the full features of the Internet of Things. These are the keys to future productivity gains to bolster the U.S. economic recovery. Such measures will also provide American technology firms—including new market entrants and those conducting substantial R&D and manufacturing in the United States—a strong competitive basis for participating in the world 5G market.

American firms, and American Internet traffic, are deeply entangled in a world market and network system that cannot be hermetically sealed off from Chinese technology firms' hardware and software system products. Co-existence is necessary. Furthermore, the United States cannot be a leader in the long-term 5G ecosystem if it does not operate at a global scale and reap the benefits of the diversity of innovations that will spring up around the world.

As a result, the United States needs policies that embrace global openness but reduce the competitive threat from state-supported firms such as Huawei. At the same time, a multi-layered security strategy can substantially reduce the threats of foreign espionage and sabotage, along with the many other sources of security risks, in a world in which 5G networks, and the Internet of Things that they support, will be interconnected, complex, and enabling of major data flows across national borders.

A focus both on accelerating 5G deployment and transitioning to a more open architecture will provide Americans access to a fast and secure digital network and provide American businesses access to the full features of the Internet of Things.

COVID BOX 2

A TARGETED APPROACH IS NEEDED TO KEEP RISKS TO MINIMUM.

The Chinese government has sought to exploit the pandemic situation in order to enhance its global influence including by promoting the notion of the "health silk road" as a new element of the One Belt, One Road initiative. If China is among the first countries to develop a viable vaccine, then Beijing also might engage in "vaccine diplomacy" in providing access to supplies preferentially to extend its geopolitical influence, despite promises to ensure equitable access. The Trump administration might try to do the same thing. China has belatedly committed to join COVAX, the World Health Organization-backed effort to deliver vaccines to low income countries, but the U.S. has not only refused to join but has also withdrawn from the WHO.

As the pandemic continues, Beijing and Washington are locked in a race to develop the first vaccines and effective treatment for the disease. U.S. government agencies allege that China is trying to hack vaccine data and steal COVID-19 research. There are inherent risks of scientific collaboration with China too, as the Chinese government restricts data sharing by its scientists, and it provides lax supervision to the detriment of maximum safety and research integrity. Such risks are real. They need to be weighed against huge potential benefits for the humanity. Targeted counter measures should be taken to mitigate such risks.

03

BOLSTERING U.S. STRENGTH IN ARTIFICIAL INTELLIGENCE

China is a formidable player in AI, but by most measures, the United States still leads, and draws on a set of strengths that China lacks and is unlikely to acquire in the near future.

KEY POINTS

- China's exalted advantage in AI is over-rated. The United States remains a global leader in AI technology and draws on a set of strength that China lacks and is unlikely to acquire in the near future. The only area where China is unambiguously a world leader is facial recognition, due to strong support from the government for social control purposes.
- The importance of data as a general-purpose strategic resource has been greatly exaggerated. Infinite amounts of data are not infinitely better; the law of diminishing returns applies. Prudent policies can assure U.S. researchers and firms have the necessary magnitude and variety of data they need to excel in AI.
- The AI ecosystem is global and AI research progress thrives on openness. While specific AI applications are protected by existing laws, broadly restricting collaboration, or the open sharing of research with Chinese AI researchers, would slow down AI progress in the United States.
- The United States should adjust immigration policies to ensure the country remains the global hub for human capital and talent for AI development.
- Targeted measures against organizations aiding human rights abuses in China is more effective than broad restrictions of access to U.S. AI technology.
- Semiconductors are foundational to AI. The United States should enhance its capabilities by investing more in advanced semiconductor manufacturing equipment and by constructing state-of-the-art semiconductor manufacturing facilities in the United States.
- The United States should work with allies and partners to shape international norms around the democratic use of AI.

Artificial intelligence (AI) is a general purpose technology with the potential to significantly affect most sectors of the economy.[1] We already see promising applications in scientific innovation, healthcare, energy, and transportation. Advances in technologies such as speech recognition, translation, natural language processing, and image processing can be broadly applied, spurring economic growth and enabling new applications that are hard to forecast. Consider how electricity not only led to artificial light, but also to high-rise buildings and modern telecommunications. AI is likely to cause transformations of comparable scale, with important implications for governance.

Because AI may be critical for future technological and economic leadership, some have raised concerns that China's industrial policy, intellectual property (IP) theft, and "data advantage" give it a significant edge over the United States.[2] This narrative is typically accompanied by policy proposals that emphasize restricting immigration and closing off U.S. technology development. While there are

> ***The only area where China is unambiguously a world leader is facial recognition, due to strong support from the PRC government for social control purposes.***

legitimate security concerns regarding AI, we believe that many policy responses miscalculate the sources of AI strength and undermine U.S. leadership.

China is a formidable player in AI, but by most measures, the United States still leads, and draws on a

1 Much of this chapter is based on (Toner 2019).

2 Some significant examples include (K.-F. Lee 2018; Allison 2019; Vincent and Schmidt 2017; Savage and Scola 2019).

set of strengths that China lacks and is unlikely to acquire in the near future. The only area where China is unambiguously a world leader is facial recognition, due to strong support from the PRC government for social control purposes. The United States can sustain its leadership in AI by doubling-down on a strategy that emphasizes investment in research and infrastructure, relatively open technology development, high-skilled immigration, and alliances with democratic states (Cohen and Fontaine 2020; Rasser et al. 2020). This strategy requires maintaining global research norms of openness, maintaining the U.S. status as the global hub for computer technology and engineering talent, instituting targeted risk mitigation strategies, and strengthening U.S. global leadership.

We elaborate on this strategy by addressing four debates concerning U.S.-China competition in AI: the degree to which an open research system advantages or disadvantages the United States; the role of human capital; whether China has a data advantage; and the role of international standards. We close with recommendations for U.S. federal policy that emphasize a risk management approach to global interdependence.

THE ADVANTAGE OF OPEN GLOBAL RESEARCH

Since well before the beginning of the AI boom in 2012, the field has been characterized by strong norms of open publishing. The vast majority of AI research has been published on arXiv.org, a freely accessible repository for scientific papers maintained by Cornell University. The norm of openness is so strong that most major technology companies with AI research labs, including Google, Facebook, Amazon and Microsoft, allow researchers to freely publish much of their work. However, as commercial competition intensifies over time, and as research progresses toward application, that openness may lessen.

The open, distributed environment accelerates research progress in several ways. Researchers in one lab can easily test and build on results published by another; researchers in different labs (and different countries) can easily collaborate on projects; researchers moving between jobs need less time to get settled with their new organization's research and practices; and less experienced researchers can use online resources to teach themselves and quickly get to a level where they can contribute their own insights.

The openness of the AI ecosystem may seem undesirable to policymakers concerned with protecting U.S. technological advantages. A natural impulse is to seek ways to close off external access to U.S. research, perhaps drawing inspiration from nuclear energy or rocketry research. Recent instances of IP theft from U.S. companies and universities show that we must be clear-eyed about espionage on the part of the PRC, and our institutions must be more vigilant about security than they have been in the past. JASON, an independent government advisory group made up of top scientists, makes a strong case for expanding disclosure requirements for funding and affiliations, and producing more detailed project risk assessments, particularly in sensitive research areas (JASON 2019).

While constructive risk mitigation strategies are required, broadly restricting external access to U.S. AI research would be counterproductive. Specific AI applications of concern are already protected by export controls, including military and law enforcement technologies.[3] Because these applications represent such a small fraction of AI's potential uses, and non-sensitive applications hold such promise for promoting U.S. growth and prosperity, measures that attempt to broadly restrict access to AI research—for example, export controls or other restrictions on collaborative research that are not highly targeted—are likely to backfire in two mutually reinforcing ways.

Since well before the beginning of the AI boom in 2012, the field has been characterized by strong norms of open publishing.

First, measures that restrict collaboration or

3 AI systems specifically built for applications of concern (such as censorship, surveillance, and munitions development) already fall under existing controls on software and data relevant to controlled items. Creating restrictions for broader AI categories would likely cast an overly wide net. For example, restricting natural language processing algorithms in general would cover not only AI-based censorship systems, but also the use of AI for translation, poetry generation, improving search engine results, and many other applications (Flynn 2020).

open sharing of research are likely to slow down the pace of research progress within U.S. university and corporate labs, damaging their standing on the world stage and reducing their market share. Second, because AI researchers are highly mobile, any such measures enacted in the United States are likely to prompt researchers to seek employment overseas, where they can continue their work unencumbered, including in the growing AI sectors of Canada and the UK, which are actively taking measures to recruit AI talent. Such dynamics also would further incentivize U.S. corporations to move more of their AI research groups to other countries, which will weaken the positive spillover between corporate and university research in the United States.

HUMAN CAPITAL DRIVES AI PROGRESS

Access to skilled researchers and engineers is a key area of competition in the field of AI. The United States' unique ability to attract and retain foreign talent is a key American advantage—and perhaps its most important advantage for AI. More than half of computer and mathematical scientists with doctoral degrees working in the United States were born abroad (59 percent). Many of these workers come to the United States as international students and prefer to stay in the United States after completing their studies. More than 83 percent of Chinese and Indian students in the United States receiving S&E doctorate degrees say they intend to stay in the United States after graduation, and their "actual stay rate" is between 83 and 90 percent for five or ten years respectively (Amy Burke 2019). This status quo reflects the high quality of the U.S. commercial and research environment, as well as the attractiveness of the liberty, openness, and prosperity found here.

China is working hard to catch up, however, with government initiatives like the Thousand Talents Plan,and educational programs described in the April 2018 Artificial Intelligence Innovation Action Plan [for] Institutions of Higher Learning, which aim to step up the training of indigenous talent, and encourage Chinese abroad to return home (Zweig and Wang 2013; Zweig and Kang 2020; Zwetsloot 2020).

A strategic approach to U.S. AI policy would seek to leverage our asymmetric advantages and solidify our place as the global hub for AI talent. China's reporting on AI competition highlights "a severe brain drain of outstanding AI talents" to the United States as a key weakness for China (Q. Peng and Li 2019). Unfortunately, recent changes in the U.S. immigration environment risk eroding this advantage. American policies that restrict the inflow of top-tier research talent from China are a dream come true for PRC leaders. As one PRC state media put it, its technology ecosystem "stands to gain enormously from a U.S. visa clampdown and are eagerly waiting for such curbs to be implemented." (Teixeira 2020) Restrictive U.S. immigration policies do more than any Thousand Talents Plan ever could to bolster China's technological prowess.

THE MYTH OF CHINA'S DATA ADVANTAGE IN AI

China is often said to have a "data advantage" in AI, due to China's large population and its relatively lax data regulations. This claim is misleading in two ways, and a poor basis for U.S. AI policy.

First, the idea of data as a general-purpose strategic resource ("the new oil") has been greatly exaggerated (Chahal, Fedasiuk, and Flynn 2020). While it is true that data are an important input to AI systems, one particular set of data is not generically useful for training any kind of system. Any given AI application requires data relevant to the specific problem it is trying to solve. For example, data on consumers' purchasing history are valuable for predicting future purchasing behavior, but not for locating missiles in satellite imagery. To assess competitive advantages in data, one needs to identify specific applications of concern, consider what data would be required to train those systems, and determine whether China has an abundance of that type of data.

Moreover, the sheer volume of data does not automatically generate advantages. In many applications, there are diminishing marginal returns to increasing the amount of data—i.e., a dataset with 100 million examples might achieve close to the same performance of a dataset with 200 million. In other applications, real-world data can even be a hindrance by limiting the exploration of possible

The United States' unique ability to attract and retain foreign talent is a key American advantage—and perhaps its most important advantage for AI.

solutions. For example, the Go-playing system AlphaGo Zero learned only from self-play and outperformed systems that were trained on historical games. Even in cases where system performance substantially improves with more data, the United States is well-positioned in several security domains because the United States has far more platforms and bases than China, in many more environments, collecting military relevant data from many more sensors. When it comes to data quality (i.e., accuracy, structure, and storage), the United States also appears to be at an advantage relative to China in many industries (Sheehan 2019).

Moreover, the sheer volume of data does not automatically generate advantages.

Second, the data advantage proposition overlooks constraints on the availability of consumer data in China. As in the United States, awareness of and concern about data privacy is rising among Chinese consumers, and China's government is actively developing laws and regulations in response. This push is part of the country's larger effort to build a complex governance regime for cyberspace and information and communications technology (ICT).[4] Currently, the regime appears to be modeled heavily on the European Union's General Data Protection Regulation (GDPR), but appears to be somewhat more permissive than GDPR in order to be more business friendly (Sacks n.d.).

In contrast to growing protection of consumer data, China does not restrict its *government's* ability to surveil its citizens or access their data. All signs indicate that the government will continue to use intrusive techniques to surveil, monitor, and oppress its population, including the techniques involved in the brutal treatment of Muslim Uighurs in Xinjiang.[5] These activities represent gross human rights violations that deserve the attention of the U.S. government and public. Ironically, this powerful surveillance system neither requires nor currently involves powerful AI to succeed. The technologies used in Xinjiang and elsewhere are widely available tools for data analysis, along with checkpoints, search and seizure, eavesdropping, and traditional human intelligence. In other words, the PRC government's repressive capacity is not dependent on—but can be enabled by—cutting-edge AI surveillance techniques.

As such, general restrictions on China's access to U.S. AI technology, such as export control measures, are unlikely to affect China's capability to use technological means for authoritarian governmental purposes. Instead, the United States should implement targeted measures against organizations aiding human rights abuses—for example, by continuing to add companies involved in producing surveillance goods for use in Xinjiang to the Department of Commerce's Entity List (US Department of Commerce 2019)—while working with allies and partners to shape international norms around the democratic use of AI.

Taking human rights seriously in foreign policy, and not simply using these issues as an excuse for geopolitical maneuvers, has been an important part of U.S. foreign policy. Many tactics, including sanctions and technology controls, can be part of a principled human rights strategy. We should avoid, however, an overly blunt "all thumbs no fingers" approach to AI talent and data restrictions. At the same time, U.S. policy should also consider how AI development affects our own efforts to advance human rights at home, including pressing issues of racial and economic justice.

AI STANDARDS AS SOFT POWER

China understands the power of influencing widely implemented technology standards and has aggressively sought to drive the development of the global standards for AI, as they have in the case of 5G and other technologies. One of the most prominent aspects of this push was the release of an in-depth white paper on AI standards in January 2018, which included contributions from over two dozen Chinese companies, associations,

4 This data privacy regime generally seeks to protect consumer privacy from technology companies working in China. A standard called the Personal Information Security Specification took effect in May 2018 and forms the first piece of the regime. We are not suggesting that the constraints on Chinese firms will reach those on firms in many democracies, but this development should be part of our understanding of big data in China.

5 For example, this recent Human Rights Watch report for a detailed description of one strategy to collect and use citizen data in Xinjiang. See more information in (Wang 2019).

and academic organizations (Ding, Triolo, and Sacks 2018). Another was a meeting held in Beijing in April 2018, where this white paper was presented to Subcommittee 42, a group that sits within two internationally respected standards bodies: the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (Ding, Triolo, and Sacks 2018).

While few formal, top-down standards yet exist for AI systems, the widespread use of specific platforms to develop and deploy AI models provides a key opportunity to influence the technology. The most widely used AI platforms are developed by U.S. companies. Prominent examples include two software libraries for deep learning: Tensorflow and Pytorch, developed by Google and Facebook, respectively. They are by far the most widely used platforms of their kind, including in China—despite attempts by Chinese companies to release their own versions, such as Baidu's PaddlePaddle or SenseTime's Parrots. Platforms like these provide the United States with a form of AI-relevant soft power.

POLICY RECOMMENDATIONS TO ENHANCE U.S. COMPETITIVENESS IN AI

To enhance U.S. competitiveness in AI, the United States should strengthen its asymmetric advantages: its status as the hub of human capital and talent in AI development; its effective use of targeted risk mitigation strategies to protect sensitive applications of AI; its advantages in data quality and volume; and its influence over the AI ecosystem, including through standards and platforms.

Specific recommendations:

1. Increase the National Science Foundation funding for basic research in AI to $1.8 billion—about $1 billion more than the NSF's 2021 fiscal year budget request to Congress. Increased funding will ensure that the United States continues to drive global AI research and development. Basic research is the backbone of the American advantage in AI, but no major federal effort has been made to strengthen that backbone during the current wave of progress in deep learning—in contrast to many other countries, especially China.

Federal support is particularly crucial in areas where the commercial sector is likely to underinvest. These include research to improve the safety and security of AI systems, such as robustness (ensuring safe performance under a range of conditions, including interference by adversaries); assurance (ensuring AI systems can be understood and controlled); and specification (ensuring the system behaves as intended by the operator) (Ortega, Maini, and DeepMind safety team 2018). Foundational research in these areas would also contribute to the development of testing, evaluation, verification, and validation (TEVV) for AI, which is currently a significant barrier to widespread use of AI in safety critical settings, including defense applications.

2. Increase National Institute of Standards and Technology (NIST) funding for AI testing, evaluation, verification, and validation by $50 million for fiscal year 2021, doubling the White House fiscal year 2020 budget request. NIST has primary responsibility for developing and implementing standards for reliable, robust, and trustworthy AI (National Institute of Standards and Technology 2019), as well as international benchmarking. NIST is also well-positioned to coordinate interagency and public-private collaboration on AI TEVV.

3. Ensure that the United States and its allies lead in technologies at the base of the AI supply chain. Semiconductors are foundational to AI, and the semiconductor supply chain has two significant bottlenecks that advantage democratic states: more than 95 percent of semiconductor design tools are produced by U.S. companies, and more than 90 percent of semiconductor manufacturing equipment is produced by U.S., Dutch, and Japanese companies. As long as China lacks the most advanced equipment, it will be unable to achieve supply chain independence (S. M. Khan and Flynn 2020). The United States should enhance its capabilities by funding R&D in advanced semiconductor manufacturing equipment and providing incentives for the construction of state-of-the-art semiconductor manufacturing facilities in the United States.

The United States should enhance its capabilities by funding R&D in advanced semiconductor manufacturing equipment and providing incentives for the construction of state-of-the-art semiconductor manufacturing facilities in the United States.

In addition, the United States and its allies should impose stricter export controls to all PRC firms on the semiconductor manufacturing equipment necessary to make advanced AI

chips at or below 45nm.[6] Better controls on production technology would provide a more secure foundation for allowing U.S. firms to sell semiconductors, still subject to export controls, to PRC firms.

4. Ensure the United States remains the top destination for global talent by recruiting top students to U.S. universities and improving the immigration options available to AI researchers and engineers. This includes lifting numerical limits on H-1B visas and/or green cards for those working in AI fields while maintaining appropriate vetting processes; creating a clear path from student/scholar status to permanent residence; and reducing processing times and application burdens (Arnold 2019).

5. Mitigate the risks of technology transfer through targeted countermeasures. The vast majority of Chinese students who come to the United States represent a boon for American competitiveness and a loss to China, but targeted policies should be put in place to screen out high-risk individuals. Such policies could include increasing intelligence resources for visa screening and post-entry review, reforming transparency requirements on funding sources, and coordinating with universities to establish and disseminate research security best practices. In line with known cases of security violations, these efforts should focus primarily on researchers and less on bachelor's and master's students who are not engaged in research activities.

As a further risk mitigation measure, the United States and its allies, particularly the intelligence alliance, Five Eyes, should pursue an alliance on technology policy with technologically sophisticated democracies (as proposed in other sections of this report), that would ensure that intelligence agencies give sufficient priority to assessing and forecasting competitors' developments in AI, and prevent illegal technology transfers. On balance, the United States gains much from its open research environment, but we must be cognizant that China, as a lagger, gains an advantage by accessing these innovations.

6. Strengthen U.S. global leadership by drawing on our alliances with other democratic nations. The United States and its allies are responsible for two-thirds of global R&D (Flagg 2020), and most of the development and production of key technologies essential to AI. A coordinated multilateral approach to investment, AI standards (including rules to assure cross-border data flows, subject to privacy protection), and the trade of technologies that are important to machine learning will be much more successful than any unilateral approach. In addition, by investing in computing methods such as homomorphic encryption, differential privacy, and federated learning, we can provide asymmetric advantages to democracies (Hwang 2020).

CONCLUSION

The United States' leading position in AI rests on a unique set of strengths. A strategic approach to this technology must embrace the United States' ability to train, attract, and retain highly skilled researchers and engineers, who are critical for AI research, development, and deployment. Investing in trustworthy AI and working together with like-minded allies can further bolster U.S. advantage. While targeted countermeasures to protect against espionage and technology transfer are needed, promoting basic research within AI's open, international ecosystem is equally important. In order to retain and strengthen its global leadership, the United States must recognize and invest in its distinct advantages.

6 These controls may also need to be applied to software and design services for semiconductor manufacturing. Nanometers (nm) are the metric for measuring the size of transistors on a semiconductor chip. Shrinking transistor size is a fundamental goal of semiconductor manufacturing. The smaller the transistor, the more power efficient is the chip, for example. The 45 nm threshold is derived from Wassenaar agreement.

COVID BOX 3

BOTH COUNTRIES REAP LARGE BENEFIT FROM CONTINUING SCIENTIFIC COOPERATION DESPITE TENSION.

Strikingly, although tensions between the U.S. and Chinese governments have intensified, cooperation in scientific research has continued. By some estimates, research collaboration to address COVID-19 has actually increased. Despite a surge of nationalism in the course of COVID-19 crisis, "scientific globalism" appears to have prevailed so far. Open-access publications and international collaboration has risen despite the tensions.

Based on initial estimates, China and the United States have been leading in scientific publications related to COVID-19. They are producing proportionally more global articles together after the pandemic than before the outbreak. These two countries have tended to collaborate more with each other than any other, in ways that appear to be mutually beneficial, and that pattern appears to be continuing in COVID-19 research. There are compelling reasons to encourage the continuation of such cooperation to the extent possible.

04

U.S.-CHINA COMPETITION AND COLLABORATION IN BIOTECHNOLOGY

Much as chemistry and physics dominated the 20th century, transformative advances in biotechnology will shape the course of the coming decades.

KEY POINTS

- The United States has dominated the biotechnology industry since it emerged in the 1970s and remains ahead of China by most metrics in biotech development. But China has identified biotechnology as a top priority for future development. Its massive investment threatens U.S. primacy.
- A loss of U.S. leadership in the sector would have grave impacts on American competitiveness and security, and on global progress. The loss of American leadership would challenge the norms and institutions that underlie open, ethical, and internationally collaborative biotech research—at a time of dramatic changes in biotechnology with major societal implications (e.g. CRISPR gene editing).
- Robust scientific collaboration between the United States and China in biotechnology is vital for addressing the world's pressing medical and public health problems. Given China's size and growing science and technology capabilities, the United States can also benefit from China's talent pool and its inclusion as part of a diversified supply chain.
- Collaboration with China carries risks. China's state-driven policies challenge accepted scientific norms and standard business practices and raise concerns. The United States should mitigate those risks by, among other things, pursuing greater reciprocity and harmonizing standards for exchange of information and biomaterials.
- The United States should invest more in U.S. biotech research and development; improve regulation and inter-agency coordination; strengthen domestic talent supply; promote manufacturing innovation; participate in international organizations; and reduce dependence and potential security threats.
- The United States should reform its interpretation of the intellectual property (IP) laws to allow important new forms of biotechnology eligible for patenting by aligning its practices with those of the European Union and China. Competing with China also requires vigorously protecting IP-intensive pharmaceutical products, blocking forced technology transfer by China, and launching additional manufacturing institutes for innovation, education, and collaboration.

The U.S. National Academies of Sciences asserted that the 21st century will be the century of biology (National Research Council 2009). Much as chemistry and physics dominated the 20th century, transformative advances in biotechnology will shape the course of the coming decades.

Perhaps nothing illustrates the importance of the biotech sector as clearly as the ongoing international emergency caused by the COVID-19 pandemic. As the world seeks tools to detect, treat, and prevent the novel coronavirus, innovation in biotechnology is the source of molecular diagnostics, antibody tests, therapeutics, and preventive vaccines. The world loses enormously from any political obstacles to international cooperation to develop this vital know-how. The World Health Organization's (WHO) Pandemic Influenza Preparedness Framework illustrates the benefits of early international collaboration. The world is made safer and healthier by agreements for data, materials, and benefit sharing prior to the emergence of a pandemic influenza outbreak (Shu et al. 2019; Huang, Yanzhong 2020). Any risk and benefit calculation about biotechnology, especially as it relates to biomedicine, must fully acknowledge the major gains from successful collaboration across all nations, including China.

While medicine is the "public face" of biotechnology, the field's reach extends to many other vital areas. Biotech is a global industry that the United States has dominated. A recent National Academies' report estimates that the bioeconomy accounts for about 5 percent of the U.S. gross domestic product (GDP)—about $1 trillion per year (The National Academies of Sciences, Engineering, and Medicine 2020). Maintaining that lead is important for American economic competitiveness. But of equal—or even greater—importance, continued advances in biotechnology are vital for addressing urgent societal challenges in health, food, energy, and environmental security that currently have no clear solutions in the face of global climate change and population growth. Global progress in biotechnology, led by the United States but involving concerted and collaborative efforts by scientists around the world, is essential to meet these challenges. The stakes are high.

There is growing concern within the U.S. biotechnology community that the PRC government's efforts in biotechnology, which are massively resourced, dwarf American programs and create vulnerabilities in the U.S. research and production base. We share that concern. However, a broad-brush characterization of the problem diverts attention from vital distinctions that should inform policy strategies.

First, while there are potential national security risks associated with the misuse of biotechnology, such as the development of bio-weaponry or bio-terrorism, the benefits from cooperation are enormous, and the ethical imperatives for making rapid progress to address global challenges are urgent. It is thus vital to maintain scientific engagement while adopting a prudent and targeted strategy of risk management.

Second, the field of biotechnology covers a wide range of life sciences and technology with four important dimensions, discussed below. Although many of the examples discussed below are from biomedicine, a productive and comprehensive strategy should concentrate on each dimension separately.

Bioeconomy

Bioeconomy refers to the sector of the U.S. economy that includes a wide range of products and services, including healthcare solutions such as biologics (i.e., drugs made from living organisms), vaccines, and diagnostics; genetically modified crops; and bio-based industrial products such as biochemicals, biomaterials, and ingredients for biopharma.

Biosecurity and Biodefense

The biotech sector is on the frontlines of efforts to respond to pandemics such as COVID-19, and to combat a wide variety of infectious diseases that affect both humans and animals. Biosecurity policy focuses on such vital tasks as developing desperately needed antibiotics, which are losing effectiveness due to antimicrobial resistance. At the same time, advances in biotechnology could be exploited by terrorists and nation-states for nefarious purposes. The process of safeguarding against such risks will remain an important concern for U.S. biodefense policy.

Digital Biology and Precision Medicine

Medicine has become increasingly digital in the years since the first draft of the human genome in 2000. Advances in precision medicine depend on "digital biology" and bioinformatics: wide-scale human genome sequencing, matched with digital health records and electronic monitoring, using artificial intelligence and other big data analytic methods to glean unique insights that enable more sophisticated treatments. Moreover, we are at the very early stages of developing biotech tools and techniques to alter the DNA of human somatic cells for prevention or treatment of disease. The manipulation of germline (i.e., inheritable) DNA, made possible by new tools (e.g., CRISPR), is a particularly important area to monitor.

Basic Science and Engineering

Enabling technologies such as DNA sequencing, CRISPR, and synthetic biology, and advances in biodefense and the bioeconomy, are all the fruits of basic science. Improved understanding of molecular biology, cell biology, genetics, and other areas of basic biology powers advances in biotechnology. Going forward, such advances will be inextricably entwined with AI, data science, nanotechnology, microfluidics, and other emerging technologies, creating critical synergies that will drive future progress.

KEY RISKS AND CHALLENGES FROM CHINA

U.S. scientists and engineers have been at the forefront of advances in biological research and development since the biotechnology sector emerged in the 1970s. U.S. scientists and research institutions have taken the lead in establishing values and standards for the biotech sector's aspirations, while restraining irresponsible or unethical applications, including those of interest to military and security forces. Even as biotech has become more globalized, American investigators and institutions have remained instrumental in forging global collaboration and maintaining open scientific standards.

However, China's faster growing economy, its sizable STEM-educated workforce, and rapid scientific progress raise the possibility that China could catch up or even surpass the United States in certain domains of biotechnology in the future. China included a blueprint for its biotech sector development in its "Made in China 2025" national strategic plan,[1] and its 13th Five-Year Plan includes additional measures for biotechnology innovation that

1 For example, in bio-pharmaceuticals, one of four target areas, MIC 2025 sets goals to develop "antibody drugs, antibody coupling drugs, new structural proteins, polypeptide drugs, and new vaccines", "technologies to support personalized medicine", and "breakthroughs in new technologies like 3D bio-printing and induced pluripotent stem cells."

target the four areas mentioned above. Biotech is also recognized as a key dual-use technology in China's plans and policies for military-civil fusion. As the PRC government looks for "new growth points" as its economy recovers from the disruption of COVID-19, among the strategic emerging industries recognized as key domains for investment is the biotech industry, including advances in innovative vaccines, synthetic biotechnology, and pharmaceutical innovation (Kania et al. 2020).

Any loss of U.S. leadership in biotechnology would be a grave concern because of its potential impact on American economy and security. However, even more consequential could be the resultant challenge to the norms and institutions built by the United States and its allies to secure an open, ethical, and internationally collaborative research enterprise in biotechnology. The boundaries between basic research and commercialization in this field are more porous than in many others. Thus, successful innovation requires tight linkages between research norms and business practices.

Any loss of U.S. leadership in biotechnology would be a grave concern because of its potential impact on American economy and security ... even more consequential could be the resultant challenge to the norms and institutions ... to secure an open, ethical, and internationally collaborative research enterprise in biotechnology.

We see three key biotechnology related challenges and risks facing the United States:

1. China's massive investment and efforts (licit and illicit) to catch up threatens U.S. primacy in biotechnology, an industry and domain of technology that the United States has dominated, and whose norms and institutions American research has helped to shape, since its origins.

There are ongoing Chinese efforts to expropriate critical research and technology from U.S. biotech research and commercial enterprises, including recent attempts to target multiple American companies involved in the development of vaccines, diagnostics, and treatments for the novel coronavirus. These efforts have included illicit means of luring away U.S. researchers, replicating U.S. research programs, and establishing "shadow laboratories" in China, thereby creating conflicts of interest (and possible IP theft) on the part of American researchers that are especially troubling in the late stages of R&D.

China is complementing its efforts to gain commercial advantage with rules that hinder foreign investment in biotech. For example, the Chinese drug approval policies disadvantage foreign innovators by granting earlier marketing approvals for Chinese companies and generic drugmakers. In addition, market access for foreign firms is often conditioned on technology transfer. If left unchanged or unchallenged, these practices could restrict or even exclude overseas innovators, or lead to persistent large-scale technology transfer to China, if innovative overseas companies opt to pursue collaboration on unfavorable terms in order to gain access to the Chinese market.

2. China has launched well-coordinated policies for its biotechnology development, which may negatively impact U.S. interests. China's state-driven policies challenge accepted scientific norms and standard business practices in global biotech development. The state-imposed pressures on individual scientists and enterprises to contribute to China's indigenous biotech development can create perverse incentives that raise concerns about the risks of collaboration, from illicit commercial practices to potential spillover to military application.

In addition, China has imposed—and is intensifying—constraints on access to Chinese data and biomaterials, including genetic information, epidemiological data, test data for drugs, and a ban on shipping research biomaterials. These measures create two problems. First, these policies may create asymmetries that are damaging or disadvantageous to U.S. interests, especially as Chinese researchers and enterprises seek to gain access to foreign sources of data, including from the United States, without reciprocity. Second, data sharing is vital during pandemics, particularly at early stages, when pathogens of pandemic potential are just emerging. During global pandemic crises, mechanisms should be put in place to remove or at least lower the routine impediments to data and materials sharing and scientific collaboration. Voluminous pre-existing constraints on access make it hard to promote timely global cooperation among researchers.

3. A high concentration in China of the global supply lines of certain pharmaceutical products creates risks of unintentional disruption or willful severance to impose

cost. Given China's size and growing scientific and technological capabilities, the United States can benefit from China's inclusion as part of a diversified supply chain for essential pharmaceutical ingredients and other biotechnological goods and services. However, U.S. dependence on China poses risks. For example, 97 percent of all antibiotics in the United States are imported from China (Abdoo 2019). A new framework for collaboration should monitor asymmetric risks and benefits to ensure global health and enable sustained international collaboration.

To meet these challenges, the United States should first and foremost increase investment in biotech R&D in order to maintain its leadership. The U.S. government should enact policies that help to train more domestic students, attract international talent, and strengthen the U.S. bioeconomy and biotech innovative ecosystem. At the same time, it should tackle the risks created by the aggressive, well-coordinated, and well-resourced Chinese state efforts to develop China's bioeconomy and biotech industries. Finally, in the interest of new discoveries and public health, the United States should maintain robust scientific collaboration with Chinese scientists for mutual and global benefits, while also expanding research cooperation with allies and partners.

MAINTAINING STRONG U.S. LEADERSHIP IN BIOTECHNOLOGY

Today, the United States is far ahead of China in biotechnology by most metrics, including the number of triadic (U.S., European, and Japanese) patents related to biotechnology, clinical trials for biologics, and the share of the world's biotechnology crops and biofuels production. A global executive opinion survey of biopharma competitiveness and investment ranks China well behind the United States and only midway among newcomer biotechnology markets (Pugatch Consilium 2019). However, China has the capacity to create a larger bioeconomy workforce than the United States, and by one estimate, private investment in Chinese biotech companies exceeds that of the United States (Cumbers 2020).

In the realm of R&D, China seems to be following a classic "catch-up" trajectory, similar to other technology fields, where China introduces new talent and technologies, digests, absorbs, and re-innovates. China's investments in several important areas, such as precision medicine and stem cell research, appear greater than those by the United States. China's total science and engineering R&D expenditures are still somewhat less than those of the United States, but China's annual increase in R&D since 2000 has been four times greater. No data are available to compare biotechnology related R&D expenditures by China relative to the United States, but the situation is likely similar: lower R&D expenditures at present, but a faster rate of increase. President Xi Jinping's call for innovation and elevation of biosecurity as a national imperative in the wake of the COVID-19 pandemic may accelerate these trends.

To ensure that the United States maintains its lead despite China's enhanced policy attention and investments, the U.S. government must dedicate greater attention and resources to this vital sector. Improving American competitiveness and sustaining U.S. primacy in biotechnology requires the United States to increase domestic investment to strengthen our own innovation capabilities.

A serious commitment to an American bioeconomy strategy is vital to the task of countering and competing with China's state-driven policies, and requires leadership from the Executive Office of the President. While such efforts began in the Obama administration (The White House 2012), and have continued under Trump (Office of Science and Technology Policy 2019), additional attention and significant investment will be needed.

> ***Today, the United States is far ahead of China in biotechnology by most metrics.***

We recommend three groups of actions:

1. Improve the coordination of U.S. policy on biotechnology and the bioeconomy, and increase support for R&D.

The United States must elevate the importance of biotechnology within the Executive Branch. The director of the Office of Science and Technology Policy (OSTP) should appoint an assistant director for biotechnology and the bioeconomy who can coordinate interagency initiatives.

Additionally, the National Institutes of Health (NIH), National Science Foundation (NSF), Department of Energy (DOE), Defense

Advanced Research Projects Agency (DARPA), and the Biological Advanced Research Projects Agency (BARDA)—the key federal funders of biotechnology research—should increase investment in biotechnology-related R&D, especially in precision medicine and synthetic biology:

- The field of precision medicine, broadly defined, is a particularly promising domain for major investments. Initiatives in the area would deploy AI-enabled and machine learning-powered knowledge to aggregate, integrate, and analyze vast amounts of data from basic science, clinical, personal, environmental, and population health settings. It would help aggregate data across silos to better understand biological processes and define disease mechanisms, while developing and delivering more precise diagnostics, therapeutics, and prevention measures.

- Synthetic biology, also called "engineering biology" versus "biological engineering," is a recent approach to biotechnology that combines science, technology, and engineering to accelerate the understanding, design, redesign, manufacture, or modification of genetic materials, living organisms, and biological systems. This is among the most promising and rapidly expanding area of biotechnology, with applications in biomedicine, agricultural biotechnology, bioenergy, and biomanufacturing.

2. Strengthen the development of domestic talent in bioscience.

As in other fields of science and engineering, greater attention must be devoted to incentivizing, training, and retaining U.S. biosciences talent, educating American students, and continuing to welcome foreign-born students.

To build a more robust pipeline for talent, OSTP and federal agencies such the Department of Education and NIH should dedicate special STEM education and training grants to cultivating talent and generating interest among K-12 students. This should include promoting greater diversity and inclusion in the field through dedicated programs to recruit and support students of color in the life sciences. Increased funding is also needed to support graduate studies and postdoctoral research in the high-priority domains of biological sciences and biotechnology.

3. Strengthen the U.S. innovation ecosystem for biotechnology.

U.S. intellectual property (IP) laws require reform to better enable commercialization of diagnostics and other biotechnology products in ways that contribute to the American competitive advantage.

- The United States requires a robust and flexible patent system to secure and promote investments in a range of biotech inventions. The U.S. Patent and Trademark Office (USPTO) and the courts are rendering ineligible for patent protection a host of computer-implemented and biotech-related inventions under an expansive view of the Patent Law regarding patent eligible subject matter. The USPTO should reconsider its patent eligibility criteria to better align with its counterparts in the European Patent Office and China's National Intellectual Property Administration, so as not to disadvantage American companies.[2]

- There is also an urgent need for regulatory improvements in a few key areas: The U.S. government should re-evaluate restrictions that appear to disadvantage U.S. stem cell- and fetal tissue-based research, which are critical to enabling advances in medical research that are vital to American healthcare and competitiveness. Additionally, the Food and Drug Administration (FDA) should strengthen programs to regularly inspect Chinese and other foreign suppliers of active pharmaceutical ingredients (APIs) and enhance other quality control mechanisms to ensure safety and quality. Currently the principal focus of FDA regulatory oversight is on pharmaceuticals in finished dosage form.

- The U.S. government should also launch additional manufacturing institutes under the multiagency "Manufacturing USA" program to advance manufacturing innovation, education, and collaboration in biotechnology. The goal of these institutes is to develop next-generation manufacturing capabilities and required talent. Currently there are 14 public-private institutes, but only three focus on biotechnology related manufacturing.

- Finally, OSTP should explore mechanisms

2 Notably, between 2014 and 2017, the USPTO rejected 17,743 applications that were filed in the US, China and Europe, of which 1,310 claimed the same or similar inventions that had granted by the EPO, in China, or both but were rejected in the United States. Among those, 618 were directed to diagnosis or treatment of disease, 150 involved cancer treatment, 103 involved healthcare and information technology applications, and 64 involved personalized medicine. These inventions covered a wide range of cancers and illnesses. See The data is drawn from (Madigan and Mossoff 2019).

to support biotech startups to enable the successful transition from promising research to new biologic, diagnostic, or technology companies with demonstrated medical and commercial potential. While Chinese startups are often assured of state funding for these stages, U.S. biotech startups face the chronic problem of the "valley of death," i.e., the failure of transition due to the lack of adequate funding and resources in early stages of commercialization. Examples of possible remedies include expansion of the U.S. Small Business Administration's Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs to include earlier phases of research by smaller companies.

The United States should aggressively pursue greater reciprocal rules and harmonized standards for exchanging information and biomaterials.

Mitigating Risk from China's State-driven Policies

Strengthening the U.S. domestic capabilities is the first step toward maintaining U.S. leadership in biotechnology. Another important area for U.S. policy action is to counter PRC government policies and actions that pose grave risks to U.S. biotech development. The United States can mitigate these risks if it acts now. In this section, we discuss these risks in detail and offer practical solutions for addressing them.

4. Ensure that U.S.-China collaboration in biotech protects American interests, with greater attention to reciprocity and ethical science.

- The United States should aggressively pursue greater reciprocal rules and harmonized standards for exchanging information and biomaterials. The selective use of economic reciprocity rules, i.e., rules that apply equally to both sides, is a critical tool for protecting the values and interests of the United States and its allies. However, the United States alone is unlikely to achieve adequate leverage without a multilateral approach that involves substantive coordination with allies and partners.
- As suggested in the fundamental research section, the U.S. government should release guidelines for best practices for its scientific engagement with China that reflect U.S. values and ethical concerns. These guidelines should address (1) joint research with dual-use potential; (2) collaborations with elements of the Chinese military and public security apparatus; and (3) engagement with institutions enabling human rights abuses, such as those in Xinjiang.

5. Diversify U.S. supply chains in biological inputs and products to ensure resilience to potential sources of disruption, by China or any other country. The United States should not and cannot eliminate China completely from its pharmaceutical and biomedical supply chains. However, U.S. policy should develop supply chains that are geographically diverse and resilient against potential disruptions caused by disease, natural disasters, or political tensions. The U.S. government should conduct a government-wide review of U.S. vulnerabilities to supply chain disruptions, followed by an analysis of how to strengthen the U.S. domestic industrial base.

6. Take actions to counter and change Chinese government practices that weaken protections for IP-intensive pharmaceutical products.

- Although China agreed to significantly amend its pharmaceutical-related IP laws and regulations as part of the Phase 1 U.S.-China Trade Agreement, the final outcomeis not known. The U.S. government should closely monitor the Phase 1 agreement and use the agreement's enforcement provisions to ensure full compliance with its terms.
- The U.S. government should aggregate data to address concerns from individuals, and research and business organizations, in concert with like-minded countries, about harmful Chinese industrial practices in order to shield U.S. firms and individuals from retaliation over their complaints about Chinese practices. Retaliation by the PRC government against U.S. firms or individuals for invoking their rights under trade agreements should not be tolerated, and should be met by forceful action.

7. Pursue robust countermeasures to China's forced technology transfer efforts in the biotech sector. This includes increasing the U.S. government's long-term capacity to monitor and respond to competition from China, whether it emanates from

government technology promotion or illicit commercial behavior, particularly cases of economic espionage and theft of U.S. data and sensitive biomedical information. Potential countermeasures include:

- The U.S. government should continue to increase efforts to monitor Chinese investments in the United States. The U.S. Congress took a positive step in passing the Foreign Investment and Risk Review Modernization Act (FIRRMA), which calls for review of non-majority investments in "critical technologies." The Committee on Foreign Investment in the United States (CFIUS), the body which implements FIRRMA, should also increase its capacity to monitor Chinese venture capital (VC) investment in the biotech sector, since VC investors may have access to proprietary information or can unduly influence strategic direction in early biotech startups. Further measures to increase the transparency of investments, such as requiring greater information disclosure by investors and confirmation of "beneficial ownership," are desirable.
- The U.S. intelligence community and law enforcement agencies should improve their capacity to engage with academia and industry to discuss and raise awareness of the potential risks from China's talent recruitment efforts such as the Thousand Talents Plan. We endorse the recommendations in the fundamental research section of this report regarding research integrity, conflicts of interests, and commitment rules.
- The U.S. government and private and public research laboratories should cooperate in criminal investigations and support active monitoring of patent filings, "shadow labs," and research publications to alert U.S. entities of patent fraud and IP theft carried out by a foreign country, including China.
- The Cybersecurity and Infrastructure Security Agency (CISA) should implement a rapid response program to support and strengthen the cyber security of companies deemed critical to U.S. pandemic response and vaccine development.

Maintaining Robust but Strategic Collaborations for the Global Good

Although the United States will need to manage risks prudently, cooperative relationships in biotechnology should be maintained and improved, to the extent possible and in line with U.S. values and interests. Robust scientific collaboration between the United States and China in biotech is vital for the global good.

8. Maintain scientific collaborations with China on urgent or shared challenges.

- The U.S. government should coordinate regular dialogues among the various U.S.-China working groups in the FDA, NIH, U.S. Department of Agriculture (USDA), and other agencies, as well as industry and academia, to identify productive opportunities for cooperation.
- As the COVID-19 crisis illustrates, the search for vaccines and anti-viral compounds is an international effort that will enhance global welfare. Collaboration with our allies and partners—and even with our rivals when the circumstances warrant—will likely yield a more effective portfolio of products more quickly than competition alone.
- The United States should strengthen collaboration between the U.S. FDA and China's National Medical Products Administration (CNMPA), including harmonizing standards and regulations where possible. However, harmonization of regulatory systems (e.g., clinical trials and drug acceptance) must be conditioned on reciprocity on policy and implementation by China.
- Future advances in fields such as precision medicine will provide global benefits, and can be accelerated through global cooperation. But collaboration and engagement with China must be conditioned on reciprocity and remediation of incidents of exploitation. Cooperation can be modeled on the policies and algorithms developed for responsible and secure sharing of genomic and health-related data by the nongovernmental Global Alliance for Genomics and Health. The United States and China should work together with both

Collaboration with our allies and partners—and even with our rivals when the circumstances warrant—will likely yield a more effective portfolio of products more quickly than competition alone.

the WHO and professional bodies such as the Inter-Academy Partnership (IAP) of the National Academies of Sciences, Engineering and Medicine, to promulgate global ethical guidelines and regulations for human genome editing.

9. Strengthen U.S. participation in biotechnology related multilateral organizations and agreements.

The United States should reengage and regain its position of collaborative leadership by actively participating in international health and biological organizations such as the WHO, Biological and Toxin Weapons Convention, and the Convention on Biological Diversity, despite these organizations' flaws. U.S. withdrawal from the WHO, if sustained, could badly damage U.S. interests while creating a vacuum in which Beijing could increase its influence. In addition to international bodies, professional organizations such as the IAP, which comprises 140 academies of science, engineering, and medicine from around the world, is another important venue for international coordination.

> ***The potential benefits of U.S.-China cooperation are enormous, and the ethical imperatives for making rapid progress to address the global pandemic are urgent.***

CONCLUSION

Biotechnology is a vast field whose advances will shape the course of innovation in the coming decades. The United States is clearly the leader in the field, but its dominant position is under challenge because of declining R&D investments and talent development, and the rise of a formidable competitor in China. To maintain leadership, the United States must begin by increasing financial and human capital investment in the sector, as it should in other areas examined in this report. The U.S. government should also pursue policies that will catalyze innovation in frontier science and technologies such as precision medicine and synthetic biology; advance the bioeconomy; and provide robust biosecurity against possible attacks by terrorists, rogue nations, and emerging infectious diseases.

The PRC government's efforts in biotechnology do create vulnerabilities for the U.S. research and production base. The United States should insist on the practice of ethical science, condition biomaterials exchange and data sharing with China on reciprocity, take effective measures to counter China's IP theft, and diversify its supply lines for pharmaceutical products and medical equipment to minimize dependence on China. But American policymakers should also keep in mind the huge benefits of U.S.-China collaboration in biotechnology for solving the world's pressing medical and public health problems.

The COVID-19 pandemic offers a useful lesson. Research collaboration to address COVID-19 has remained strong among the American and Chinese scientists, despite heightened tension between the two governments. The potential benefits of U.S.-China cooperation are enormous, and the ethical imperatives for making rapid progress to address the global pandemic are urgent. Maintaining openness while adopting a prudent and targeted strategy of risk management is thus vital.

COVID BOX 4

U.S. MEDICAL SUPPLY CHAINS FAILED, AND COVID DEATHS SURGED: IT'S TIME TO INVEST IN U.S. CAPABILITIES.

While China's national response to control the pandemic achieved relative success despite the negative externalities for the economy, the dysfunction that has characterized the U.S. response has weakened the American economy and the appeal of its political system. U.S. soft power and influence have suffered because of fumbling efforts at home. The American withdrawal from the World Health Organization also has created a vacuum that may benefit China's influence within international institutions.

Chinese leaders regarded the crisis as a test for their system of governance. After the relative success of their response, CCP propaganda has characterized the Party-state model as having demonstrated its "system advantage." By contrast, the United States has seen its confidence rattled by its poor performance, especially compared to prior expectations of American preparedness. For instance, Nature magazine blames the lack of effective response in the U.S. on "political meddling, disorganization and years of neglect of public-health data management."

Sudden shortages of masks, gowns, gloves, and other medical supplies have further exposed the U.S. vulnerability caused by over-dependence on a China-centered supply chain for pharmaceutical products and medical equipment. These shortfalls will likely become an impetus for greater indigenization of supply chains and production.

Yet, the United States has built an unparalleled ecosystem of scientists, entrepreneurs, doctors, and investors in the biotech sector that leads the world in scientific discoveries and significant triadic patents, clinic trials, and novel therapeutics. As of September 2020, for example, the United States owns or is the largest external funder of eight of the 13 most advanced and promising vaccine candidates for COVID-19. The United States continues to enjoy primacy in biotechnology; continuing investment by the government and industry will maintain its leadership into the future.

REFERENCES

Abdoo, Mark. 2019. *Exploring the Growing U.S. Reliance on China's Biotech and Pharmaceutical Products.* https://www.fda.gov/news-events/congressional-testimony/exploring-growing-us-reliance-chinas-biotech-and-pharmaceutical-products-07312019.

Allison, Graham. 2019. "Is China Beating America to AI Supremacy?," December 22, 2019. https://nationalinterest.org/feature/china-beating-america-ai-supremacy-106861.

Amy Burke. 2019. "Science and Engineering Labor Force." NSB-2019-8. Science and Engineering Indicators 2020. National Science Board, National Science Foundation. https://ncses.nsf.gov/pubs/nsb20198/immigration-and-the-s-e-workforce#stay-rates-of-u-s-s-e-doctorate-recipients.

Arnold, Zachary. 2019. "Immigration Policy and the U.S. AI Sector." Center for Security and Emerging Technology. https://cset.georgetown.edu/research/immigration-policy-and-the-u-s-ai-sector/.

Association of American Universities. 2020. "AAU Submits Response to JCORE Request for Information on the Research Environment," January 27, 2020. https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/JCORE_FRI_COMMENTS_1.27.20.pdf.

Association of Public and Land-grant Universities. n.d. "Science and Security." https://www.aplu.org/projects-and-initiatives/research-science-and-technology/science-and-security/.

Atkinson, Robert D., and Caleb Foote. 2020. "Federal Support for R&D Continues Its Ignominious Slide. Information Technology & Innovation Foundation (ITIF)." August 26, 2020. https://itif.org/publications/2019/08/12/federal-support-rd-continues-its-ignominious-slide.

Bloomberg News. 2020. "China's Got a New Plan to Overtake the U.S. in Tech," May 20, 2020. https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech.

"CCSA Membership." n.d. China Communications Standards Association.

Chahal, Husanjot, Ryan Fedasiuk, and Carrick Flynn. 2020. "Messier than Oil: Assessing Data Advantage in Military AI." Center for Security and Emerging Technology. https://cset.georgetown.edu/research/messier-than-oil-assessing-data-advantage-in-military-ai/.

"China & APS." n.d. American Physical Society. https://www.aps.org/programs/international/map/china.cfm.

China Power team. 2020. "Is China a Global Leader in Research and Development?" *China Power* (blog). October 28, 2020. https://chinapower.csis.org/china-research-and-development-rnd/.

Cohen, Jared, and Richard Fontaine. 2020. "Uniting the Techno-Democracies: How to Build Digital Cooperation." *Foreign Affairs,* November 2020. https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

Cong Cao, Jeroen Baas, Caroline S Wagner, and Koen Jonkers. 2019. "Returning Scientists and the Emergence of China's Science System." *Science and Public Policy* 47 (2): 172–183. https://academic.oup.com/spp/article/47/2/172/5658550.

Congressional Research Service. 2020. "Global Research and Development Expenditures: Fact Sheet." Fact Sheet R44283. Congressional Research Service. https://fas.org/sgp/crs/misc/R44283.pdf.

Cumbers, John. 2020. "China's Plan To Beat The U.S. In The Trillion-Dollar Global Bioeconomy." *Forbes,* February 3, 2020. https://www.forbes.com/sites/johncumbers/2020/02/03/china-now-out-invests-america-in-the-global-bioeconomy-by-30/?sh=5fb96c377440#135046537440.

David Warsh. 2007. *Knowledge and the Wealth of Nations: A Story of Economic Discovery.* New York: W. W. Norton & Company.

Ding, Jeffrey, Paul Triolo, and Samm Sacks. 2018. "Chinese Interests Take a Big Seat at the AI

Governance Table." *New America Cybersecurity Initiative* (blog). June 20, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.

Flagg, Melissa. 2020. "Global R&D and a New Era of Alliances." Center for Security and Emerging Technology. https://cset.georgetown.edu/research/global-rd-and-a-new-era-of-alliances/.

Flynn, Carrick. 2020. "Recommendations on Export Controls for Artificial Intelligence." Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/Recommendations-on-Export-Controls-for-Artificial-Intelligence.pdf.

Gruber, Jonathan, and Simon Johnson. 2019. *Jump-Starting America: How Breakthrough Science Can Revive Economic Growth and the American Dream.* PublicAffairs.

Hadley, Stephen, and Anja Manuel. 2020. "How to Use the next Stimulus to Counter China." *The Washington Post,* May 11, 2020.

Hart, Melanie, and Jordan Link. 2020. "There Is a Solution to the Huawei Challenge." Center for American Progress. https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/.

Hecker, Siegfried S., ed. 2016. *Doomed to Cooperate: How American and Russian Scientists Joined Forces to Avert Some of the Greatest Post-Cold War Nuclear Dangers.* Bathtub Row Press.

Huang, Yanzhong. 2020. "The U.S. and China Could Cooperate to Defeat the Pandemic Instead, Their Antagonism Makes Matters Worse." *Foreign Affairs,* March 24, 2020. https://www.foreignaffairs.com/articles/china/2020-03-24/us-and-china-could-cooperate-defeat-pandemic.

Huang, Yukon, and Smith, Jeremy. 2019. "China's Record on Intellectual Property Rights Is Getting Better and Better. Carnegie Endowment for International Peace." *Foreign Affairs,* October 16, 2019. https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/

Hwang, Tim. 2020. "Shaping the Terrain of AI Competition." Center for Security and Emerging Technology. https://cset.georgetown.edu/research/shaping-the-terrain-of-ai-competition/.

JASON. 2019. "Fundamental Research Security." National Science Foundation. https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

John Costello. 2017. *Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications.* https://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony_Final2.pdf.

John Deutch. 2019. "Assessing and Responding to China's Innovation Initiative." In Technology and National Security: Maintaining America's Edge, edited by Leah Bitounis and Jonathon Price. The Aspen Institute.

Joint Venture Silicon Valley Institute for Regional Studies. 2020. "2020 Silicon Valley Index." Joint Venture Silicon Valley. https://jointventure.org/download-the-2020-index.

Kania, Elsa, Ngor Luong, Caroline Meinhardt, Ben Murphy, Dahlia Peterson, Helen Toner, Graham Webster, and Emily Weinstein. 2020. "New Chinese Ambitions for 'Strategic Emerging Industries,' Translated." *New America Cybersecurity Initiative* (blog). September 29, 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/new-chinese-ambitions-strategic-emerging-industries-translated/.

Keller, Devi, Jimmy Goodrich, and Zhi Su. 2020. "The U.S. Should Be Concerned with Its Declining Share of Chip Manufacturing, Not the Tiny Fraction of U.S. Chips Made in China." SIA Blog (blog). July 10, 2020. https://www.semiconductors.org/staff/jimmy-goodrich/?feed.

Khan, Beethika, Carol Robbins, and Abigail Okrent. 2020. "The State of U.S. Science and Engineering." NSB-2020-1. Science and Engineering Indicators 2020. National Science Board, National Science Foundation. https://ncses.nsf.gov/pubs/nsb20201/.

Khan, Saif M., and Carrick Flynn. 2020. "Maintaining China's Dependence on Democracies for

Advanced Computer Chips." Center for Security and Emerging Technology. https://cset.georgetown.edu/research/maintaining-chinas-dependence-on-democracies-for-advanced-computer-chips/.

Krasnyak, Olga. 2019. "How U.S.-Soviet Scientific and Technical Exchanges Helped End the Cold War." *American Diplomacy* (blog). November 2019. http://americandiplomacy.web.unc.edu/2019/11/how-u-s-soviet-scientific-and-technical-exchanges-helped-end-the-cold-war/.

Lauer, Michael S. 2020. "ACD Working Group on Foreign Influence on Research Integrity Update." National Institutes of Health, June 12. https://acd.od.nih.gov/documents/presentations/06122020ForeignInfluences.pdf.

Lee, Jenny J., and John P. Haupt. 2020. "Winners and Losers in US-China Scientific Research Collaborations." *Higher Education* 80 (July): 57–74. https://link.springer.com/article/10.1007/s10734-019-00464-7.

Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley and the New World Order.* Houghton Mifflin Harcourt.

Lester, Richard. 2019. "New Review Process for 'elevated-Risk' International Proposals," April 3, 2019. https://orgchart.mit.edu/node/214/letters_to_community/new-review-process-elevated-risk-international-proposals.

Leydesdorff, Loet, Lutz Bornmann, and Caroline Wagner. 2015. "Recent Developments in China-U.S. Cooperation in Science." *Minerva,* April. https://arxiv.org/abs/1404.6545.

Leydesdorff, Loet, Loet Leydesdorff, Han Woo Park, and Wagner, Caroline. 2014. "International Coauthorship Relations in the Social Sciences Citation Index: Is Internationalization Leading the Network?" *Journal of the Association for Information Science and Technology.* 65 (10): 2111–26. https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.23102.

Lindsay, Jon R. 2020. "Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage." *Security Studies* 29 (2): 335–61. https://www.tandfonline.com/doi/full/10.1080/09636412.2020.1722853.

Madigan, Kevin, and Adam Mossoff. 2019. "Five Years Later, the U.S. Patent System Is Still Turning Gold to Lead." *IP Watchdog* (blog). December 15, 2019. https://www.ipwatchdog.com/2019/12/15/five-years-later-the-us-patent-system-is-still-turning-gold-to-lead/id=116984/.

Magsamen, Kelly, and Melanie Hart. 2019. "Limit, Leverage, and Compete: A New Strategy on China." Center for American Progress. https://www.americanprogress.org/issues/security/reports/2019/04/03/468136/limit-leverage-compete-new-strategy-china/.

Manuel, Anja, and Melanie Hart. 2020. "How the West Could Win a Technological 'Shadow War' with China." *Los Angeles Times,* June 11, 2020. https://www.latimes.com/opinion/story/2020-06-11/china-5g-global-standards-war.

Manuel, Anja, Pavneet Singh, and Thompson Paine. 2019. "Compete, Contest and Collaborate: How to Win the Technology Race with China." In . A Proposal Developed for the Technology and Public Policy Projec. Stanford University Freeman Spogli Institute for International Studies. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/manuel_et_al_china_tech_race_101619_final_updated_0.pdf.

Matt Apuzzo. 2015. "U.S. Drops Charges That Professor Shared Technology With China." *New York Times,* September 11, 2015. https://www.nytimes.com/2015/09/12/us/politics/us-drops-charges-that-professor-shared-technology-with-china.html.

"Membership." n.d. 3GPP: A Global Initiative. https://www.3gpp.org/about-3gpp/membership.

National Institute of Standards and Technology. 2019. "Artificial Intelligence Standards." *Federal Register,* May 1, 2019. https://www.federalregister.gov/documents/2019/05/01/2019-08818/artificial-intelligence-standards.

National Research Council. 2009. *A New Biology for the 21st Century.* Washington, DC: The National Academies Press. https://www.nap.edu/catalog/12764/a-new-biology-for-the-21st-century.

Network Telecom Information Research Institution. 2019. "The Top 10 Competitiveness Enterprises in the Optical Communications Industry of Global and China Market." 2019. http://list.nti.news/.

Nouwens, Meia, and Helena Legarda. 2018. "China's Pursuit of Advanced Dual-Use Technologies." Research Paper. International Institute for Strategic Studies. https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance.

NSF Quantum Information Science Working Group. 1999. "Quantum Information Science An Emerging Field of Interdisciplinary Research and Education in Science and Engineering." Report of the NSF Workshop. Arlington, VA: National Science Foundation. https://ncses.nsf.gov/pubs/nsb20206/.

Office of Science and Technology Policy. 2019. "Summary of the 2019 White House Summit on America's Bioeconomy." The White House Office of Science and Technology Policy. https://www.whitehouse.gov/wp-content/uploads/2019/10/Summary-of-White-House-Summit-on-Americas-Bioeconomy-October-2019.pdf.

Ortega, Pedro A., Vishal Maini, and DeepMind safety team. 2018. "Building Safe Artificial Intelligence: Specification, Robustness, and Assurance." *DeepMind Safety Research* (blog). September 27, 2018. https://medium.com/@deepmindsafetyresearch/building-safe-artificial-intelligence-52f5f75058f1.

Pece, Christopherr. 2020. "Federal R&D Obligations Increase 8.8% in FY 2018; Preliminary FY 2019 R&D Obligations Increase 9.3% Over FY 2018." NSF 20-308. NCSES InfoBrief. National Science Foundation. https://www.nsf.gov/statistics/2020/nsf20308/nsf20308.pdf.

Peng, Mike W., David Ahlstrom, Shawn M. Carraher, and Weilei Stone Shi. 2017. "History and the Debate Over Intellectual Property." *Management and Organization Review* 13 (1): 15–38.

Peng, Qian, and Hualing Li. 2019. "Examining the Five Shortcomings of China's AI Talent System." *Xinhua News Agency,* August 28, 2019. http://www.gov.cn/xinwen/2019-08/28/content_5425310.htm.

Pohl, Hans. 2020. "Organizing Internationalization at Stanford University: Managing Top-Down and Bottom-Up Initiatives." CALIE Papers. The Swedish Foundation for International Cooperation in Research and Higher Education. https://calieproject.files.wordpress.com/2020/04/cp-5-internationalisation-at-stanford-hans-pohl-final.pdf.

Pongratz, Stefan. 2020. "Huawei and ZTE Increased Their Revenue Shares While Nokia and Cisco's Revenue Shares Declined for the Full Year 2019 Telecom Equipment Market." March 2, 2020. https://www.delloro.com/the-telecom-equipment-market-2019/.

Prague 5G Security Conference. 2019. "The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World." Government of the Czech Republic. https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

PRC State Council. 2016. "State Council Notice on the Publication of the National 13th Five-Year Plan for S&T Innovation." http://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm. https://cset.georgetown.edu/research/state-council-notice-on-the-publication-of-the-national-13th-five-year-plan-for-st-innovation/.

Pugatch Consilium. 2019. "Ascending to the Peak of Biophamaceutical Innovation: Biopharmaceutical Competitive & Investment (BCI) Survey." Pugatch Consilium. https://www.pugatch-consilium.com/reports/BCI_2017_Report.pdf.

Rasser, Martijn, Rebecca Arcesati, Shin Oya, Ainikki Riikonen, and Monika Bochert. 2020. "Common Code: An Alliance Framework for Democratic Technology Policy." Washington, DC: Center for a New American Security. https://www.cnas.org/publications/reports/common-code.

Romer, Paul. 2018. "The Deep Structure of Economic Growth." *Paul Romer* (blog). 2018. https://paulromer.net/deep_structure_growth/.

Rose, Karen, Scott Eldridge, and Lyman Chapin. 2015. "The Internet of Things: An Overview." Internet Society. https://www.internetsociety.org/resources/doc/2015/iot-overview.

Sacks, Samm. n.d. "China's Emerging Cyber Governance System." *CSIS* (blog). n.d. https://www.csis.org/chinas-emerging-cyber-governance-system.

———. 2019. *Smart Competition: Adapting U.S. Strategy Toward China at 40 Years.* New America. https://docs.house.gov/meetings/FA/FA00/20190508/109457/HHRG-116-FA00-Wstate-SacksS-20190508.pdf.

Savage, Luiza Ch., and Nancy Scola. 2019. "'We Are Being Outspent. We Are Being Outpaced': Is America Ceding the Future of AI to China?," July 18, 2019. https://www.politico.com/story/2019/07/18/global-translations-ai-china-1598442.

Security Agency. n.d. "Cybersecurity." Cybersecurity. https://www.cisa.gov/cybersecurity.

Segal, Stephanie, and Dylan Gerstel. 2019. "Research Collaboration in an Era of Strategic Competition." CSIS. https://www.csis.org/analysis/research-collaboration-era-strategic-competition.

Sheehan, Matt. 2019. "Much Ado About Data: How America and China Stack Up." *MacroPolo* (blog). July 16, 2019. https://macropolo.org/ai-data-us-china/?rp=e.

Shu, Yuelong, Ying Song, Wang Dayan, and Carolyn Greene. 2019. "A Ten-Year China-US Laboratory Collaboration: Improving Response to Influenza Threats in China and the World, 2004-2014." *BMC Public Health* 19 (520). https://doi.org/10.1186/s12889-019-6776-3.

Silicon Valley Leadership Group. 2020. "Silicon Valley Competitiveness and Innovation Project - 2020 Update." A Dashboard and Policy Scorecard for a Shared Agenda of Prosperity and Opportunity. Silicon Valley Community Foundation. https://www.svcip.com/files/SVCIP%202020%20-%20FINAL%203.9.2020.pdf.

Strumpf, Dan. 2019. "Where China Dominates in 5G Technology." *The Wall Street Journal,* February 26, 2019. https://www.wsj.com/articles/where-china-dominates-in-5g-technology-11551236701.

Sugimoto, Cassidy R., Nicolas Robinson-Garcia, Dakota S. Murray, Alfredo Yegros-Yegros, Rodrigo Costas, and Vincent Larivière. 2017. "Scientists Have Most Impact When They're Free to Move." *Nature Comment,* October 4, 2017. https://www.nature.com/news/scientists-have-most-impact-when-they-re-free-to-move-1.22730.

Teixeira, Alessandro Golombiewski. 2020. "The End of U.S. Tech Dominance? Foreign Talent Must Not Be Turned Away at the Door." *China Global Television Network (CGTN),* June 22, 2020. https://news.cgtn.com/news/2020-06-22/The-end-of-U-S-tech-dominance-Foreign-talent-must-not-be-turned-away-RvDoAmydfq/index.html.

The National Academies of Sciences, Engineering, and Medicine. 2020. *Safeguarding the Bioeconomy.* Washington, DC: The National Academies Press. https://www.nap.edu/catalog/25525/safeguarding-the-bioeconomy.

The White House. 2012. "National Bioeconomy Blueprint." The White House. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf.

———. 2020a. "United States Strategic Approach to the People's Republic of China." Washington, DC: The White House. https://www.whitehouse.gov/articles/united-states-strategic-approach-to-the-peoples-republic-of-china/.

———. 2020b. "National Strategy for Critical and Emerging Technologies." https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

Toner, Helen. 2019. *Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy.* Center for Security and Emerging Technology. https://cset.georgetown.edu/research/technology-trade-and-military-civil-fusion-chinas-pursuit-of-artificial-intelligence/.

Trapani, Josh, and Katherine Hale. 2019. "Higher Education in Science and Engineering." Science and Engineering Indicators. National Science Foundation, National Science Board. https://ncses.nsf.gov/pubs/nsb20197/international-s-e-higher-education.

US Department of Commerce. 2019. "U.S. Department of Commerce Adds 28 Chinese Organizations to Its Entity List." U.S. Department of Commerce. https://www.commerce.gov/news/press-releases/2019/10/us-department-commerce-adds-28-chinese-organizations-its-entity-list.

U.S. Senate Permanent Subcommittee on Investigations. 2019. “Threats to the U.S. Research Enterprise: China’s Talent Recruitment Plans.” Washington, DC: United States Senate Permanent Subcommittee on Investigations Committee on Homeland Security & Government Affairs. https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China’s%20Talent%20Recruitment%20Plans%20Updated2.pdf.

Vincent, James, and Eric Schmidt. 2017. Eric Schmidt says America needs to ‘get its act together’ in AI competition with ChinaThe Verge. https://www.theverge.com/2017/11/1/16592338/eric-schmidt-google-ai-competition-us-china.

Wagner, Caroline, Loet Leydesdorff, and Lutz Bornmann. 2014. “The European Union, China, and the United States in the Top-1% and Top-10% Layers of Most-Frequently-Cited Publications: Competition and Collaborations.” *Journal of Informetrics* 8 (3): 606–17. https://www.sciencedirect.com/science/article/abs/pii/S1751157714000509?via%3Dihub.

Wang, Maya. 2019. “China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App.” Human Rights Watch. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass#.

White House Office of Trade and Manufacturing Policy. 2018. “How China’s Economic Aggression Threatens the Technologiesand Intellectual Property of the United States and the World.” White House Office of Trade and Manufacturing Policy. https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

White, Karen. 2019. “Publication Output: U.S. Trends and International Comparisons.” NSB-2020-6. Science and Engineering Indicators. Alexandria, VA: National Science Foundation, National Science Board. https://ncses.nsf.gov/pubs/nsb20206/.

Zweig, David, and Siqin Kang. 2020. “America Challenges China’s National Talent Programs.” No. 4. Center for Strategic and International Studies. https://www.csis.org/analysis/america-challenges-chinas-national-talent-programs.

Zweig, David, and Huiyao Wang. 2013. “Can China Bring Back the Best? The Communist Party Organizes China’s Search for Talent.” *The China Quarterly* No. 215 (September): 590–615.

Zwetsloot, Remco. 2020. “China’s Approach To Tech Talent Competition: Policies, Results, and the Developing Global Response.” The Brookings Institution. https://www.brookings.edu/research/chinas-approach-to-tech-talent-competition/.

Zwetsloot, Remco, Jacob Feldgoise, and Josh Dunham. 2020. “Trends in U.S. Intention-to-Stay Rates of International Ph.D. Graduates Across Nationality and STEM Fields.” Center for Security and Emerging Technology. https://cset.georgetown.edu/research/trends-in-u-s-intention-to-stay-rates-of-international-ph-d-graduates-across-nationality-and-stem-fields/.

UC San Diego
SCHOOL OF GLOBAL POLICY AND STRATEGY
21st Century China Center

Asia Society
CENTER ON U.S.-CHINA RELATIONS