The American AI Century:
A Blueprint for Action

December 2019

Martijn Rasser, Megan Lamberth, Ainikki Riikonen,
Chelsea Guo, Michael Horowitz, Paul Scharre

Bold. Innovative. Bipartisan.

1152 15th Street NW
Suite 950
Washington, DC 20005

CNAS.ORG / @CNASDC
T: 202.457.9400
F: 202.457.9401

ACKNOWLEDGMENTS

The authors thank Zach Arnold (Research Fellow, Center for Security and Emerging Technology [CSET]), Tarun Chhabra (Senior Fellow, CSET), Jack Clark (Policy Director, OpenAI), Melissa Flagg (Senior Fellow, CSET), Michael D. Gariss (Senior Computer Scientist, National Institute of Standards and Technology), Saif Khan (Research Fellow, CSET), Jason Matheny (Founding Director, CSET), Igor Mikolic-Torreira (Director of Analysis, CSET), Doug Rand (Senior Fellow, Federation of American Scientists, and Cofounder, Boundless Immigration), and Remco Zwetsloot (Research Fellow, CSET) for their thoughtful feedback and suggestions.

A special thanks to the members of the Center for a New American Security (CNAS) Task Force on Artificial Intelligence and National Security, whose insights helped to shape the scope and breadth of our analysis. The views expressed in this report are those of the authors alone and do not represent those of the task force or its members.

Thank you to CNAS colleagues Loren DeJonge Schulman, Maura McCarthy, and Melody Cook for their role in the review, production, and design of this report. Finally, thank you to Monika Bochert for her assistance in reviewing and finalizing the report. Any errors that remain are the responsibility of the authors alone.

ABOUT THE AUTHORS

Martijn Rasser is a Senior Fellow in the Technology and National Security Program at CNAS. Mr. Rasser served as a senior intelligence officer and analyst at the Central Intelligence Agency. Upon leaving government service, Mr. Rasser was Chief of Staff at Muddy Waters Capital, an investment research firm. More recently, he was Director of Analysis at Kyndi, a venture-backed AI startup. Mr. Rasser received his BA in anthropology from Bates College and his MA in security studies from Georgetown University.

Megan Lamberth is a Research Assistant for the Technology and National Security Program at CNAS. Prior to joining CNAS, Ms. Lamberth was a Brent Scowcroft Fellow at the Aspen Strategy Group, where she helped spearhead the planning and execution of the Aspen Strategy Group Summer Workshop and two sessions of the Aspen Ministers Forum. Ms. Lamberth received her MA in international affairs from the Bush School of Government & Public Service at Texas A&M University. She graduated from Sam Houston State University with a BA in criminal justice.

Ainikki Riikonen is a Research Assistant for the Technology and National Security Program at CNAS. Before joining CNAS, Ms. Riikonen worked at the Department of Defense's Near East South Asia Center for Strategic Studies, where she supported security cooperation programs on regional security issues for participants from North Africa, the Middle East, Central Asia, and South Asia. Previously, she interned at the National Consortium for the Study of Terrorism and Responses to Terrorism, where she researched foreign nuclear and radiological programs. Ms. Riikonen holds a degree in international relations from the University of St Andrews and is currently studying for an MA in security studies at Georgetown University.

Chelsea Guo is the former Joseph S. Nye Jr. Intern with the Executive Team at CNAS. Prior to joining CNAS, Ms. Guo worked as a research analyst at the Open Philanthropy Project and a policy intern at the Future of Humanity Institute, where she focused on issues related to advanced AI and great power competition. She currently is pursuing an M.Phil in politics (political theory) at Oxford University. Ms. Guo graduated cum laude from Yale University with an MS/BS in molecular, cellular, and developmental biology and a BA in political science, with distinction in both majors.

Michael C. Horowitz is a professor of political science and the interim director of Perry World House at the University of Pennsylvania. He is also an Adjunct Senior Fellow at CNAS. He received the 2017 Karl Deutsch Award from the International Studies Association, presented annually to a scholar under age 40 who is judged to have made the most significant contribution to the study of international relations and peace research. Professor Horowitz is coauthor of the book *Why Leaders Fight* and author of *The Diffusion of Military Power: Causes and Consequences for International Politics*. His research interests include technology and global politics, military innovation, the role of leaders in international politics, and forecasting. He has published in a wide array of peer-reviewed journals, as well as more popular outlets such as *The New York Times* and Politico. Professor Horowitz previously worked for the Office of the Undersecretary of Defense for Policy in the Department of Defense. He is also a Life Member of the Council on Foreign Relations. He has held fellowships at the Weatherhead Center, Olin Institute, and Belfer Center at Harvard, where he received his PhD in government. Professor Horowitz received his BA in political science from Emory University.

Paul Scharre is a Senior Fellow and Director of the Technology and National Security Program at CNAS. He is the award-winning author of *Army of None: Autonomous Weapons and the Future of War*, which won the 2019 Colby Award and was named one of Bill Gates' top five books of 2018. Mr. Scharre formerly worked in the Office of the Secretary of Defense, where he played a leading role in establishing policies on emerging weapon technologies. He led the working group that drafted DOD Directive 3000.09, establishing DOD's policy on autonomy in weapon systems. Mr. Scharre is a former infantryman, sniper, and reconnaissance team leader in the Army's 75th Ranger Regiment and completed multiple tours to Iraq and Afghanistan. He holds an MA in political economy and public policy and a BS in physics, both from Washington University in St. Louis.

ABOUT THIS REPORT

This report is produced as part of the CNAS Artificial Intelligence and Global Security Initiative, which explores how the artificial intelligence (AI) revolution could lead to changes in global power, the character of conflict, and crisis stability. The initiative also examines the security dimensions of AI safety and prospects for international cooperation. For more information on this initiative and other reports in this series, visit cnas.org/AI.

This publication was made possible in part by a grant from Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the authors.

REPORTS IN THIS SERIES

Other reports of the CNAS Artificial Intelligence and Global Security Initiative include:

"Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security" by Gregory C. Allen (February 2019)

"Strategic Competition in an Era of Artificial Intelligence" by Michael Horowitz, Elsa B. Kania, Gregory C. Allen, and Paul Scharre (July 2018)

"Artificial Intelligence and International Security" by Michael Horowitz, Paul Scharre, Gregory C. Allen, Kara Frederick, Anthony Cho, and Edoardo Saravelle (July 2018)

"Artificial Intelligence: What Every Policymaker Needs to Know" by Paul Scharre and Michael Horowitz (June 2018)

"Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power" by Elsa B. Kania (November 2017)

Reports are available online at http://cnas.org/AI.

TABLE OF CONTENTS

FOREWORD **2**

EXECUTIVE SUMMARY **3**

SUMMARY OF POLICY RECOMMENDATIONS **4**

I. INTRODUCTION **7**

II. CREATE AN AMERICAN AI FUTURE **8**

III. LEAD IN RESEARCH & DEVELOPMENT **8**

IV. HARNESS AMERICA'S TALENT PIPELINE **13**

V. COUNTER ILLICIT TECHNOLOGY TRANSFER **20**

VI. PROTECT AMERICA'S EDGE IN AI HARDWARE **23**

VII. SHAPE GLOBAL NORMS FOR AI USE **26**

VIII. IMPROVE GOVERNMENT READINESS **29**

IX. LEAD IN AI STANDARDS-SETTING AND MEASUREMENT **32**

X. CONCLUSION **36**

APPENDIX **37**

ENDNOTES **42**

FOREWORD

By Robert O. Work

We find ourselves in the midst of a technological tsunami that is inexorably reshaping all aspects of our lives. Whether it be in agriculture, finance, commerce, health care, or diplomatic and military activities, rapid technological advancements in fields like advanced computing, quantum science, AI, synthetic biology, 5G, miniaturization, and additive manufacturing are changing the old ways of doing business. And AI—the technologies that simulate intelligent behavior in machines—will perhaps have the most wide-ranging impact of them all.

This judgment is shared by many countries. China, Russia, members of the European Union, Japan, and South Korea all are increasing AI research, development, and training. China in particular sees advances in AI as a key means to surpass the United States in both economic and military power. China has stated its intent to be the world leader in AI by 2030 and is making major investments to achieve that goal.

The United States needs to respond to this technological challenge in the same way it responded to prior technology competitions, such as the space race. U.S. leadership in AI is critical not only because technology is a key enabler of political, economic, and military power, but also because the United States can shape how AI is used around the world. As this report explains, while AI can be used for incredible good by societies, it already is being abused by authoritarian states to surveil and repress their populations. And advances in AI technology are enabling future malign uses, such as launching sophisticated influence attacks against democratic nations. The United States must make sure it leads in AI technologies and shapes global norms for usage in ways that are consistent with democratic values and respect for human rights.

This CNAS report offers sensible ways to ensure U.S. leadership in the coming "AI century." If you are seeking a primer on AI or a long argument about its import, look elsewhere.[1] This report has a bias for action. It is built around a list of concrete recommendations, segmented into seven sections, with concise rationale and explanation for each. Together, the recommendations provide the framework for a national strategy for AI leadership.

U.S. leaders would do well to read, consider, and implement them.

EXECUTIVE SUMMARY

The United States excels when it pursues big ideas. It is one of the few countries in the world that can rally its resources and its human capital to achieve the most ambitious of goals. The United States stands at the cusp of another such moment. Prudent policy decisions today will help to protect and cement America's lead in AI for decades. Together these actions will help to ensure that the coming AI century is an American one, a new technological era where America's national security—and that of U.S. allies and partners—is more secure, its economy is poised to flourish, and its norms and values underpin AI technologies worldwide.

American leaders in government and industry should commit to harnessing the country's science and technology base through greater research and development (R&D) funding and by pursuing international collaboration with like-minded partners. These leaders also must dedicate resources to prepare future generations by building up America's human capital. Educators will require new skills to teach the future American work force as part of updated K-12 curricula.

Human capital investments must go beyond those born in the United States. International talent is a cornerstone of American innovation. Immigrants and their children play an outsize role in the U.S. technology ecosystem, producing many of the United States' leading scientific minds and founding many of the country's most iconic companies. Congress and the executive branch must address outdated and constricting immigration laws to continue to encourage the world's best AI talent to study, work, and stay in the United States.

America's openness and opportunities are among its greatest attributes. Malign actors also use these qualities against it. Illicit technology transfer is a serious problem that erodes U.S. competitiveness and costs the U.S. economy hundreds of billions of dollars. Countering this widespread theft is imperative, as is the need to do so in a manner consistent with U.S. freedoms and values.

The United States must protect its technological competitiveness further by controlling exports and securing and diversifying supply chains of advanced AI-specific hardware. U.S. action also is needed to promote government readiness to assure that the country is prepared for the likely transformative impact of AI on U.S. national security, the U.S. economy, and American society. Finally, U.S. leadership in setting global AI norms, standards, and measurement is essential to promote AI ethics, safety, security, and transparency in accordance with U.S. interests.

The specific recommendations that flow from our analysis of these issues are detailed in this report. Together they form the strategic foundation needed to make the current U.S. vision for AI, and continued American leadership in AI, a reality.

SUMMARY OF POLICY RECOMMENDATIONS

Research and Development

1) Boost yearly U.S. government funding of AI R&D to $25 billion by FY2025
    - Spending at this level is realistic and doable: $25 billion is equal to less than 19 percent of total federal R&D spending in the FY20 budget.
    - Basic research funding, which is foundational to game-changing technological achievements is under pressure; the U.S. government is the largest funder.

2) Incentivize private sector AI R&D with tax credits and easing access to government datasets
    - America's corporations are a key comparative advantage in sustaining overall leadership in AI.
    - Data scarcity is a common barrier to entry for AI researchers at universities and startups.

3) Promote international R&D collaboration
    - Decades of experience show that joint work with foreign researchers can be done with great benefit and little detriment to U.S. economic and national security.

Human Talent

4) Increase public and private sector AI and science, technology, engineering, and math (STEM) education and skills training
    - To remain competitive, the United States needs a national human capital strategy for technology.

5) Increase funding opportunities for university researchers
    - Federal grants to academia decreased from their 2011 peak of $45.5 billion to $40.9 billion in 2017.

6) Raise the cap for H1-B visas; remove the cap for advanced-degree holders entirely
    - International talent remains a critical backbone of the country's technological ecosystem.
    - U.S. technology firms currently rely heavily on temporary-hire foreign workers to fulfill critical shortages in STEM occupations.

7) Amend the Department of Labor Schedule A occupations list to include high-skilled AI technologists
    - Updating the Schedule A occupations list to include high-skilled AI technologists would streamline the permanent residency sponsorship process for employers.

8) Create a new program that couples visa grants to ten-year open-market work commitments
    - This approach would attract foreign students already highly predisposed to remain in the United States, target specific AI-related disciplines, and eliminate the cost and uncertainty of extending job offers to qualified foreign nationals by removing employer sponsorship requirements.

Illicit Technology Transfer

9) Provide more cyber defense support to small firms
    - Small and medium businesses in general are more vulnerable to cyber attacks.

10) Authorize consular officials to act on risk indicators for espionage to screen out high-risk individuals before they arrive
    - Broader screening is required beyond simply PLA-sponsored individuals or sensitive research projects because AI is highly dual-use.

11) Improve collaboration between U.S. counterintelligence experts and universities
    - Associations representing U.S. universities have expressed desire for better engagement with the national security community on counterintelligence threats, among other issues.

AI Hardware

12) Increase the availability of affordable compute resources
    - The high cost and limited availability of compute is often a barrier to entry for startups and researchers in academia.

13) Establish multilateral export controls on semiconductor manufacturing equipment (SME)
    - Limiting the diffusion of SME to China, which looks to indigenize advanced semiconductor fabrication, is essential to protecting America's edge in semiconductors.
    - Multinational cooperation is necessary as other SME leaders are located in Japan, South Korea, Singapore, and the Netherlands.

14) Boost domestic semiconductor manufacturing with retooling incentives
    - Some fabs need to retool every 2-3 years to stay competitive and these costs are burdensome.

15) Secure semiconductor supply chains through public-private partnerships
    - The U.S. military and intelligence community have special needs for security that go above and beyond what is available in commercial facilities, yet they lack the scale of demand to make a purely government-dedicated foundry possible.

16) Diversify semiconductor fabrication by creating an international fab consortium with key allies
    - A consortium with allies should share the cost burden of building new semiconductor foundries to ensure a trusted and diverse supply chain.

AI Norms

17) Lead in establishing norms for appropriate AI use
    - The United States has unparalleled influence and authority on the global stage and is in a unique position to set an example for the world on how AI should and should not be used.

18) Collaborate with allies and partners on norms for AI use
    - Alliances and partnerships with like-minded countries will help to ensure that responsible stewardship of AI becomes the global norm.

19) Protect U.S. research from supporting human rights violations by modernizing export controls
    - Due to the dual-use nature of facial recognition and other biometrics-detection technology, U.S. organizations are at risk of indirectly contributing to human rights violations through research collaborations, technology exports, and investments.

Government Readiness

20) Prioritize talent management with hiring reforms and AI-related training
    - Talent management in an era of AI will require attracting and retaining top talent with technical AI expertise. Government officials require training to responsibly and effectively use AI applications, and to craft policy and inform acquisitions.

21) Allocate funding for federal agencies to implement AI
    - The American AI Initiative falls short in that it does not establish budget targets.
    - Increases in spending beyond what existing budgets can support is needed to ensure that agencies don't lag on AI implementation.

22) Modernize IT processes
    - Consolidating data centers and standing up cloud services will be required to ensure the U.S. government can update systems; manage, leverage, and share data; have access to compute; and manage a technical work force.

23) Define what is AI
    - Setting a definition for AI for federal government purposes will improve standards setting, formulating measurements, appropriations of AI-related funding, and tracking AI spending across government.

AI Standards & Measurement

24) Establish an NSTC Subcommittee for AI Standards & Measurement
    - The central importance of standards and measurement to fostering AI technologies that are safe, secure, reliable, and comport with U.S. norms and values warrant a stand-alone subgroup dedicated to the issue.

25) Establish a permanent horizon scanning effort devoted to AI
    - Tracking global progress in AI is necessary to hedge against technology surprise.

I. INTRODUCTION

AI, the technologies that simulate intelligent behavior in machines, likely will create dramatic opportunities for the U.S. economy, national security, and our health and well-being. Unfortunately, without policy action, the United States is at risk of ceding its leadership in AI. China, European Union member states, Japan, South Korea, and Russia are increasing spending on AI R&D and training new researchers to leverage AI. Some—Russia, most notably—seek to develop autonomous robotic weapons to replace human soldiers on the battlefield. Most of these countries do not just have AI strategies but have begun implementation in a way that threatens America's technological edge. This report recommends concrete actions to ensure that the United States remains the leader in AI, to promote the development of standards in line with U.S. interests and values, and to anticipate and prepare for security challenges.

These policy recommendations build on existing U.S. AI policy, including the Executive Order on Maintaining American Leadership in Artificial Intelligence (February 2019) and *The National Artificial Intelligence R&D Strategic Plan: 2019 Update* (June 2019). The executive order highlights the need for using AI to promote economic and national security, fostering technological breakthroughs, development of technical standards, skills training for workers and researchers, international collaboration, and investments in R&D. The 2019 AI R&D plan lays out eight high-level strategic concepts that identify federal R&D priorities. Both documents identify U.S. strengths, challenges, opportunities, and priorities.

The legislative branch also contributes to laying out a high-level vision. The U.S. Congress mandated the establishment of the National Security Commission on Artificial Intelligence (NSCAI) in the 2019 National Defense Authorization Act (NDAA), recognizing the need for a comprehensive national approach to AI. The commission was created as an independent body to "review advances in artificial intelligence, related machine learning developments, and associated technologies" in order to "comprehensively address the national security and defense needs of the United States."[2] NSCAI released its interim report on November 4, 2019, identifying five lines of effort on which the U.S. government should focus: R&D investments, national security applications of AI, training and recruiting AI talent, protecting and building upon U.S. technical advantages, and promoting global AI cooperation. Underpinning these areas of focus is the clear-eyed recognition that the United States is in a strategic competition, and that AI is at its center.

This report presents specific next steps to ensure the U.S. government's vision for sustained AI leadership becomes reality. It offers policy recommendations to strengthen U.S. competitiveness in AI through increased R&D spending and international collaboration; building American human capital through education and immigration reforms; tackling academic and industrial espionage; improving U.S. government readiness for widespread AI adoption; investing in AI-specific hardware at home and restricting exports of semiconductor manufacturing equipment; promoting the development of safe, transparent, explainable, reliable, secure, and resilient AI; and keeping abreast of global AI developments to prevent technology surprise.

The report is divided into eights sections that feature analysis of the issue at hand and provide corresponding policy recommendations. An appendix provides an overview of ongoing AI initiatives across the U.S. government.

II. CREATE AN AMERICAN AI FUTURE

The United States is approaching a consequential decision point in its history: how to address AI's looming impact on the American economy and society writ large. AI technologies will fundamentally alter how people interact with machines, devices, and each other. AI will change how we learn, how we work, how we treat illness, how we wage war. AI promises great opportunities. It also poses tremendous risks. How the United States prepares for this new era will determine whether American society can reap the benefits while mitigating the threats.

The path of least resistance is that of the status quo. It is the laissez-faire approach that is popularly thought to have served America well. In that narrative, the United States became the wealthiest and most powerful country in the world based on a unique mix of freedom, ingenuity, hard work, optimism, and a bit of luck. There is a certain comfort in this American exceptionalism. The current U.S. vision for AI as expressed by the Trump administration reflects this sentiment with its faith in industry, innovative spirit, and its hands-off approach to guidance and funding.

This path is fraught with risk, however, because it takes for granted U.S. leadership by underplaying the effort, expense, and vision it took to get here. American technological leadership is not guaranteed. The United States of today is rooted in investments in education, science, R&D, and infrastructure made decades ago. On its current trajectory, with a shrinking share of global R&D spending, human capital shortfalls, and the rapid rise of a near-peer competitor, the United States cannot continue to coast. America's ability to harness AI to the fullest extent possible is at stake. Falling short would squander economic and societal benefits and expose the United States to avoidable risks and challenges.

Instead, bold action is needed to reinvigorate America's competitiveness and position the United States for success. That framework for action is detailed in the pages that follow. This pathway includes decisions that will require tradeoffs and political fortitude. Success also will require long-term commitments from policymakers, academia, and private industry. Achieving the American AI Century depends on a whole-of-society approach spanning decades.

III. LEAD IN RESEARCH & DEVELOPMENT

Greater investments in AI R&D are essential to maintaining American leadership in AI. Throughout the 20th century, the federal government played a critical role in fueling technological innovation by funding pivotal basic research. Government funding was essential to developing the transistor, the Global Positioning System, and the Internet—inventions that transformed the world economy. Yet over the past several decades, federal government spending on R&D as a percentage of GDP declined from about 1.2 percent in 1976 to around 0.7 percent in 2018.[3] This is a worrisome trend as the federal government remains the main funder of basic research.[4] Government support again could be pivotal both in fostering new AI breakthroughs and ensuring that the U.S. government has access to those breakthroughs.

> **Government funding was essential to developing the transistor, the Global Positioning System, and the Internet—inventions that transformed the world economy.**

U.S. government entities already are pursuing important AI R&D initiatives. The National Science Foundation funds an array of basic research and partners with stakeholders across government, academia, and the private sector to foster advances in the field.[5] The National Institutes of Health are incorporating deep learning to improve disease screening and natural language processing for information retrieval and discovery.[6] In 2018, the Defense Advanced Research Projects Agency (DARPA), the Department of Defense organization charged with developing emerging technologies, launched a $2 billion multi-year campaign to incentivize the creation of a range of new AI capabilities and applications.[7]

Unclassified federal government spending on defense AI R&D in FY2020 will be about $4 billion, according to a Bloomberg analysis from March 2019.[8] In September 2019, the White House announced an FY20 non-defense AI R&D budget request of nearly $1 billion.[9]

In contrast, the level of Chinese government spending on AI R&D is not clear. Complete annualized figures for Chinese government spending are not publicly available. Instead, only announcements of planned, multi-year spending offer a window into the scale of overall government R&D spending at the national, provincial, and local levels.[10] For instance, two Chinese cities alone announced the creation of RMB 100 billion (approximately $15 billion) multi-year AI development funds while Beijing unveiled plans for a $2 billion AI research park in 2018.[11]

The United States enjoys robust private sector R&D funding. Precise figures are hard to discern because companies typically do not divulge details for R&D expenditures in their financial statements and privately-owned firms do not have such reporting requirements. That said, looking at overall R&D expenditures by major AI-intensive companies gives a sense of the scale of private investments in AI R&D. The combined 2018 R&D expenditures by U.S. firms Alphabet, IBM, Facebook, Microsoft, and Amazon was $80.5 billion.[12]

China's tech giants also report significant R&D investments, although they are considerably smaller than those of their U.S. counterparts. Leading Chinese AI firms Alibaba, Baidu, and Tencent collectively spent $9.1 billion on R&D in 2018.[13] These firms are also major investors in Chinese AI startups.[14]

In contrast, Europe is a laggard. Combined R&D spending by the EU (national governments and private investments) is projected to be EUR 20 billion (approximately $22.1 billion) in 2020, up from about EUR 3.7 billion (approximately $4.1 billion) in 2016.[15]

The United States' dominant position in startup funding, a key driver of technological innovation, is starting to erode. In 2017, the U.S. share of global AI startup funding was less than half of the world's total—ceding the lead to China—for the first time ever.[16] This happened despite venture capital funding of American AI startups growing at a 36 percent compound annual growth rate since 2013.[17]

Min Wanli, Alibaba's Chief AI Scientist, speaks with CNBC's Arjun Kharpal on a panel at CNBC's East Tech West conference. While the U.S. is still the leader in private sector R&D investment, Chinese firms, such as Alibaba, Baidu, and Tencent, are rapidly increasing their investments. (Dave Zhong/Stringer/Getty Images)

Figures are clearer for all national R&D spending, beyond simply AI, and indicate worrisome trends. Other countries are outpacing the United States with faster growth of their national R&D budgets. Total U.S. national (public and private) R&D expenditures as a share of GDP have been mostly stagnant since 1996. China quadrupled its R&D expenses as a share of GDP over the same time frame, and countries like Israel and South Korea also significantly ramped up spending.[18] As a result, the U.S. share of global R&D has declined over the past several decades, falling from 69 percent in 1960 to 28 percent in 2016. From 2000 to 2015, the United States accounted for 19 percent of global R&D growth, while China accounted for 31 percent.[19] China is on track to top the United States in total R&D investments (in purchasing power parity-adjusted dollars) as soon as 2019.[20]

R&D is a key driver of long-term economic growth.[21] The Congressional Budget Office reaffirmed in 2018 that federal R&D spending is a positive influence on private R&D spending and increases macroeconomic growth.[22] Authors of a ten-year study of 28 EU economies concluded that a 1 percent increase in R&D expenditure as a percentage of GDP would cause an increase of real GDP growth rate of 2.2 percent.[23]

The United States gains further benefits from federal R&D spending through effective technology diffusion. Technology transfers from the public to the private sector are stipulated in several laws.[24] This legislation gives ownership and title to federally funded research by universities and small businesses and has resulted in thousands of spin-off companies, increased technology transfer, and greater innovation.[25] Under these laws, the U.S. receives government royalty-free access to the research.[26]

To strengthen U.S. competitiveness in AI, Congress and the White House should:

Boost yearly U.S. government funding of AI R&D to $25 billion by FY2025
Congress and the White House should work together to increase federal AI R&D spending to $25 billion in five years. This target represents a fivefold increase over FY2020 but is affordable. It would still represent less than 19 percent of the amount requested for all unclassified R&D in the president's FY20 budget. A large jump in spending on a specific line item also has precedent: The president's FY19 budget requested an $18.1 billion increase in defense R&D over FY18.[27]

Given the central role AI technologies likely will play in economic growth, geopolitics, and global security, and the sharp growth in global spending on AI, this is a modest sum in relative terms. In FY2020, the United States is poised to spend nearly $59 billion in unclassified defense R&D alone

(including AI R&D).[28] For historical perspective, the five-year Manhattan Project cost $23 billion in 2018 dollars.[29] The 1960–1973 Apollo program cost $288.1 billion when adjusted for inflation, and NASA spent $490 billion in total over those 13 years, an average of $37.7 billion a year.[30]

The priority should be to fund high-risk/high-reward basic science research—areas where private industry has little incentive to invest but that hold tremendous potential for valuable new knowledge. Breakthroughs in software, such as novel AI techniques that address the limitations of existing AI methods, and hardware, such as next-generation semiconductor technologies and superconducting artificial neurons, could be game-changers that provide the United States with a continuing technological edge.[31]

Leading up to the Apollo 11 Saturn V launch on July 16, 1969, the U.S. government invested billions in R&D funding during the 13-year Apollo program, demonstrating the power of targeted government R&D investment for breakthroughs in technology advancement. The U.S. government will need to similarly increase its R&D investment to spur new breakthroughs in artificial intelligence. (NASA/Getty Images)

The federal government should adopt a phased approach to increasing funding levels, so that the resources are spent effectively and responsibly. The departments and agencies that receive federal R&D monies (primarily DOD, HHS, DOE, NASA, NSF, USDA, VA, DOT, DOI, DHS, EPA) will require time to plan for expanded research agendas and to formulate relevant metrics to measure progress and effectiveness.

Incentivize AI R&D in the private sector

America's private sector is a key comparative advantage in sustaining overall AI leadership by the United States. Policymakers have a number of ways to stimulate further R&D activity by corporations while adhering to free market principles. First and foremost is maintaining the PATH Act of 2015, which permanently extended the federal R&D tax credit.[32] It offers strong incentives to conduct and expand R&D by reducing tax liabilities.

Second is standardizing and making current and future government datasets more readily available to the private sector and academia to facilitate training of machine learning models, as the Trump administration's AI executive order proposes. The government's Project Open Data is a major step in making data discoverable and usable.[33] Doing so will help to address data scarcity problems, especially for entities with significant resource constraints such as startups or some university researchers, by expanding the number of open-source high-quality datasets.[34]

Third is exploring additional stimulants of private sector R&D activity. A comprehensive survey of R&D incentives in use around the world provide additional options for policymakers to consider to enhance U.S. competitiveness:[35]

- Accelerated depreciation of qualifying R&D assets
  - Allows greater deductions in the earlier years of an asset

  - Can be used to minimize taxable income
  - Purpose: encourage more frequent investments in, and upgrades to, R&D assets such as labs and equipment.

- R&D expenses super-deduction tax incentive
  - Allows a taxpayer to deduct qualified R&D expenses from its net income
  - Can be used to minimize taxable income
  - Purpose: promote increased R&D spending by corporations.

- Cash grants, low interest loans
  - Provide funds for qualified R&D activity through non-repayable funds or loans with favorable terms and conditions
  - Purpose: provide capital to entities pursuing high-risk/high-reward research, which often face barriers to obtaining funding.

- Tax exemptions and reductions for qualified tech transfer
  - Can be used to minimize taxable income
  - Purpose: promote cross-industry technology diffusion and spin-off company creation to boost innovation.

- Patent-related incentives such as reduced tax rates on income from intangible assets[36]
  - Lower tax rates on assets that do not derive their value from physical attributes, such as software and chemical formulas
  - Purpose: promote R&D of intangible assets, which often have a longer development timeline and a higher risk of failure.

Promote international R&D collaboration

As an open democratic society with world-class universities, research institutes, and corporations, the United States makes for an attractive partner in joint R&D. Decades of experience show that joint work with foreign researchers can be done with great benefit and little detriment to our economic and national security. President Trump's executive order is right to emphasize the importance of collaborating with international partners.

The benefits of international collaboration include cost sharing; aligning complementary knowledge, experience, and know-how; improved interoperability; developing norms and principles; and more efficient standards setting. The United States joining the Organization for Economic Cooperation and Development (OECD) in adopting global AI principles was an important step in the right direction because it shows U.S. support for international norms in developing trustworthy AI.[37] This helps foster global cooperation and promotes values such as human rights.

> **Global AI issues—ensuring AI is safe, transparent, explainable, reliable, and resilient—are especially well suited to broad international research cooperation.**

The United States is fortunate to have most of the world's leading AI powers as allies and partners. The United Kingdom, France, Japan, Singapore, and South Korea, for example, have committed $100s of millions to AI R&D.[38] Toronto is a global AI hub. Each of these locales, and numerous others, are prime candidates for mutually beneficial cooperation. Global AI issues—ensuring AI is

safe, transparent, explainable, reliable, and resilient—are especially well suited to broad international research cooperation.

Mechanisms to promote multinational collaboration range from personnel exchanges to establishing cooperative international R&D centers at home and abroad. Such collaborative relationships can be encouraged by enhancing visa and work permit regimes, providing grants and loans, and organizing multinational innovation prize competitions. Such competitions could be modeled on DARPA's series of Challenges and the XPRIZE competitions, which have successfully tackled some of the toughest science and engineering problems, including in AI.[39]

IV. HARNESS AMERICA'S TALENT PIPELINE

American Talent

Homegrown talent is key for the U.S. AI ecosystem. U.S. leadership in AI begins with STEM education at the K-12 level. The U.S. government has taken positive, albeit belated, strides in improving K-12 STEM education and should continue to expand these efforts. In 2018, the National Science & Technology Council (NSTC) published its Strategy for STEM Education, which built on prior efforts to promote computational literacy like the recent follow-through of the 2016 Computer Science for All initiative.[40]

The U.S. government will need to prioritize and invest more in K-12 STEM and computer science education in order to build a robust AI workforce for the future. (Ariel Skelley/Getty Images)

The initiative's original funding request for $4 billion was never realized, but the federal government's attention to the matter likely contributed to state and local efforts to improve computational literacy programs.[41] In 2017, President Trump signed a presidential memorandum which directed the Department of Education to devote $200 million to STEM and computer science annually.[42] Technology companies promised another $300 million to support the initiative, well short of the proposed target. Meanwhile, the Department of Education prioritized funding exclusively for computer science for the first time in 2019.[43] Yet, while programs to promote computer science have slowly expanded, initiatives specific for building AI skills lag.[44]

Building American AI talent also relies on having a robust teaching base at universities, but that teaching base is losing its faculty to private companies due to greater resources.[45] Computer science faculty at universities who leave academia for private companies and the number of new PhDs who choose industry jobs rose from 38 percent to 57 percent in the last decade.[46]

This trend may be even steeper in the deep learning field.[47] This exodus harms U.S. leadership in AI now and over the long term because it decreases the expert base available for training the next

generation of AI talent. Faculty and advanced PhD students selecting into industry in ever greater numbers drains the community of expertise available to train the next generation of AI experts and occurs at the expense of longer-term research projects important to breakthrough innovation. Faculty leaving academia for industry also harms long-term innovation potential. A study published in 2019 concluded that when professors left their teaching positions for the private sector, their students became less likely to start a company and those who did raised less money.[48]

In addition to higher salaries, those leaving academia for the private sector cite access to compute, data, research funding, and high-impact projects as draws.[49] Some companies are taking steps to preserve the faculty bases that build their talent pipelines, for example by establishing fellowships and consortiums or allowing professors to rotate between responsibilities.[50] The U.S. government, in its National Artificial Intelligence Research and Development Strategic Plan, calls for long-term investments in AI research and the release of publicly available datasets to fill some of this resource gap.[51]

Apple hosts an "Hour of Code" workshop for third grade students in New York City in 2015. Some employees at technology companies like Apple have begun teaching computer science classes and workshops to K-12 students, which helps foster interest in STEM subjects from an early age. (Andrew Burton/Getty Images)

Corporate America can further assist in ensuring they will have access to future elite talent and promote U.S. AI leadership in the long term by helping to teach the next generation. Tech leaders including Microsoft, Google, and Amazon make employees available to teach computer science skills such as coding to high school students, particularly in underserved areas.[52] Such initiatives help to nurture the future AI industry.

In addition to cultivating the experts responsible for future cutting-edge breakthroughs, the United States will need to facilitate the talent necessary for implementing and managing AI solutions. This part of the talent base will not necessarily require doctorates so much as relevant bachelor's and master's degrees for literacy in AI applications. These application-savvy coders will comprise the bulk of the workforce. AI leadership will require both programmers with bachelor's and master's degrees and smaller numbers of elite talent.

To ensure the United States has the requisite homegrown talent, the White House and Congress should:

Increase public and private sector AI and STEM education and skills training
The White House's strategy for STEM education includes plans to cultivate the talent pipeline early with such measures as building computational thinking and teaching data science. It would benefit, though, from emphasis on increasing general AI literacy specifically.[53]

Congress should provide more funding for NSF to expand grant-giving to school districts to develop new AI-focused curricula and associated resources such as professional development of teachers. In addition, Congress should appropriate the requested $4 billion for the Computer Science for All initiative or a new analogous effort.

To remain competitive, the United States needs a national human capital strategy for technology and must invest in improved education in STEM. The NSTC should build on its 2018 Strategy for STEM Education by presenting a detailed plan to execute their recommendations, task specific government agencies, and fund reforms.[54] Additionally, Congress should provide tax credits for companies that offer relevant STEM training to employees, students, and teachers, either internally or through third parties.[55]

Education is governed largely at the local and regional levels, but the federal government plays an important role in agenda-setting. It can shape progress in AI not just by providing resources but by empowering AI as a national priority and a focus area for education.[56]

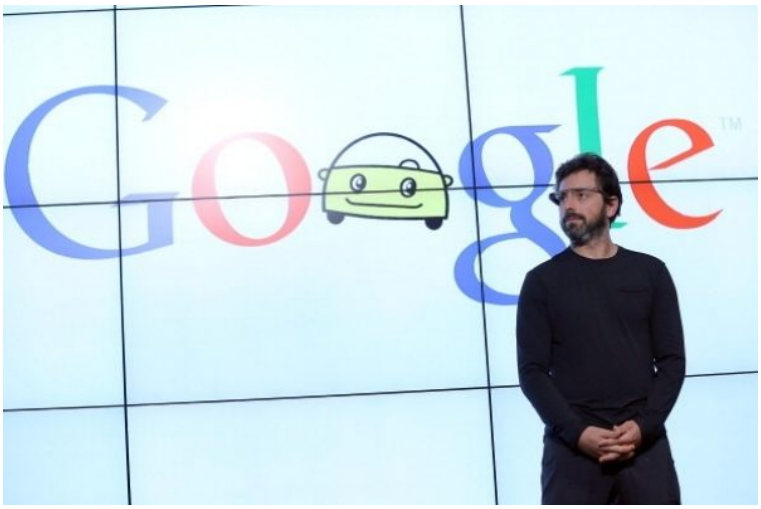
Increase funding opportunities for university researchers

Congress should increase R&D funding for AI research at universities. Federal grants to academia decreased from their 2011 peak of $45.5 billion to $40.9 billion in 2017. The value of those grants dropped even more in real terms.[57] Researchers have directly cited stagnant AI R&D funding as an incentive to move to private industry.[58] Adequate funding is especially important for machine learning because it is resource intensive. Training a single model can cost tens of thousands of dollars for compute resources alone.[59] Increasing AI R&D funding not only will keep more professors at universities; it will enable them to pursue longer-term research in important areas that may be less of a priority for industry research.

International Talent

Immigrants long have been a source of innovation in the United States. Throughout the country's history, high-skilled immigrants have contributed to some of the nation's most transformative technologies. Today is no different. International talent remains a critical backbone of the country's technological ecosystem. Immigrants founded one-quarter of the technology start-ups in the United States, and immigrants and their children founded nearly half of U.S. Fortune 500 companies, including Apple, Google, General Electric, and IBM.[60]

High-skilled immigrants play an indispensable role in American AI. More than half of the country's top AI talent base is composed of foreign nationals.[61] With too few STEM-educated Americans and higher employment growth in STEM careers compared to the overall job market, U.S. technology firms currently rely heavily on temporary-hire foreign workers to fulfill critical shortages in STEM occupations.[62]



Sergey Brin, cofounder of Google, is an industry leader and immigrant from the Soviet Union. Brin illustrates the success and importance of international talent for America's technological ecosystem. (Justin Sullivan/Getty Images)

While labor market indicators suggest a shortage of AI talent, estimates of exact numbers vary considerably.[63] More reliable tallies from the broader discipline of computer science and STEM-focused occupations generally hint at the scale of the issue. Within the United States alone, more than 300,000 cyber-related positions currently go unfilled, and this number is projected to skyrocket to an estimated 1.8 million unfilled positions by 2022.[64] Within the STEM field overall, a 2018 study by Deloitte and the National Association of Manufacturing estimates a need for 3.5 million STEM jobs by 2025, with more than 2 million of those positions going unfilled due to a lack of skilled talent.[65]

Even if the United States undertakes a robust—and fully funded—STEM education program, immigrants will remain an invaluable component of the U.S. talent base. It will take a generation to develop a new cohort of American-born scientists and engineers, while high-skilled immigrants can be recruited immediately, resolving acute workforce shortages today. Additionally, immigration allows the United States to draw on the best and brightest from around the world. In a global competition for AI talent, the United States has a natural advantage in the fact that many want to come and work in the United States. Washington should capitalize on this advantage by maximizing opportunities to recruit high-skilled immigrants to work in the United States.

Despite the need for international talent in AI research and development, immigration mechanisms for working in the United States are insufficient and the process for entry is often cumbersome. Since the passage of the Immigration Act of 1990, the immigration cap has remained stagnant, while the U.S. labor force has grown by 30 percent to around 163 million people.[66] For high-skilled immigrants, visas and green cards are scarce and difficult to acquire.

U.S. technology companies have relied most heavily on H-1B visas to recruit qualified immigrants. Established in 1990, the H-1B visa program was designed as a short-term solution to address labor shortages in particular areas, allowing employers to hire temporary employees with specialized knowledge.[67] As the Internet Age unfolded, the demand for high-skilled labor continued to rise. Subsequently, the U.S. technology sector—with great need for computer science specialists—began using the H-1B visa program to hire international talent.[68]

Today, the available number of H-1B visas is capped at 85,000 per year, with 20,000 visas designated for those with graduate degrees.[69] While this cap has remained at 85,000 since 2005, the number of H-1B applications has skyrocketed, peaking in 2017 at 236,000 applications, though declining to

199,000 in 2018.[70] The denial rate for new applicants has grown from 6 percent in FY2015 to 32 percent in FY 2019. The denial rate for visa renewals also has increased since 2017.[71]

The recent decline in H1-B applications and the increase in denial rates may be a consequence of new policies enacted by the Trump administration. In 2017, President Trump signed the "Buy American and Hire American" executive order, which directed the Department of Homeland Security to award H-1B visas to the "most skilled or highest-paid" workers.[72] This led the U.S. Citizens and Immigration Services to reevaluate the kinds of work and educational experiences that constitute a "specialty."[73] In past instances where temporary visa denial rates increased, employers have reported "time lost due to the increase in denials," and that the impact of these denials have cost "millions of dollars in project delays and contract penalties."[74]

During a visit to a manufacturing facility in Wisconsin President Trump signed the "Buy American and Hire American" Executive Order, which made changes to the H-1B visa program. U.S. technology companies rely heavily on H-1B visas to recruit international talent. (Scott Olson/Getty Images)

While the H-1B visa program is the dominant pathway to hire temporary employees, the Optional Practical Training (OPT), which allows F-1 student visa holders to work in the United States following graduation, is a critically important program for retaining international talent. Student visa holders studying in STEM fields are allowed to work in the United States for up to three years after graduation, and there is no cap on work permits granted under the OPT program.[75]

In recent years, various lawmakers have called for the limitation or elimination of the OPT program.[76] This would be a mistake. The OPT program is the country's largest source of temporary high-skilled immigrant talent.[77] In 2016, 172,000 work permits were granted under the OPT program for F-1 visa holders studying STEM, up from 73,000 in 2014.[78]

> **The OPT program is the country's largest source of temporary high-skilled immigrant talent.**

Issues with the available immigration pathways shape the extent to which the United States is a beacon for highly talented individuals from around the world, including China. From 2005 to 2015, nearly 87 percent of Chinese doctoral students studying in the United States planned to remain following graduation.[79] Today, while a large fraction of top-tier Chinese AI researchers stay to work at American institutions, the overall total number of Chinese graduates remaining after graduation is shrinking.[80] In 2016 there was a nearly 57 percent growth in Chinese international students across all fields of study returning home compared to 2011 numbers.[81] China's evolving technological

ecosystem and the numerous obstacles to obtaining a worker visa in the United States are likely major factors in this decline.[82]

Given the structure of the AI labor market and the demonstrated need signaled by employers, policies to attract and retain the next generation of top STEM researchers is essential to long-term U.S. competitiveness.

To ensure the United States attracts the best AI talent in the world, Congress should:

Reform the H-1B visa application process
The U.S. Congress should work to reform the H1-B visa process to make it more suitable for hiring and retaining international talent.

First, Congress should raise the overall cap of available H-1B visas and remove the cap for advanced-degree holders entirely. By raising the current cap and removing the limit on advanced-degree applicants, Congress would address, partially at least, the striking imbalance between H-1B petitions and available H-1B visas. The annual limit on H-1B visas was exceeded the past 16 years, and thus, by limiting the H-1B visa cap, the United States is arbitrarily restricting a major source of talent for U.S. companies.[83] This is an unfortunate example of government intervention in the marketplace that constrains American innovation.

The exact shortage of AI technologists in the United States is difficult to quantify, but it is clear that while the number of AI job postings continues to increase, the number of job seekers has leveled off.[84] While the motivation to keep the H-1B cap low is to protect American workers, this is unneeded and detrimental for the AI and computer science fields, where the demand in the marketplace far outweighs the available U.S.-born researchers.[85] In order to meet demand, America's AI talent base for the upcoming generation will need to draw heavily on foreign nationals who choose to live and work in the United States, and Congress should provide sufficient opportunity for U.S. companies to recruit talent from abroad.

Second, Congress should simplify the process of applying for an H-1B visa to make it easier for start-ups and smaller tech companies to hire necessary international talent. The H-1B application process is expensive and requires extensive documentation from the applicant's potential employer. Consequently, technology giants with greater personnel and resources—Amazon, Microsoft, Intel, and Google—make up a significant percentage of approved H-1B petitions.[86] Therefore, in addition to raising the cap on available H-1B visas and simplifying the process, Congress should earmark a percentage of these visas for smaller technology firms and start-ups.

Create new ways to recruit high-skilled immigrants
In addition to reforming the H-1B visa process, Congress and the White House should identify alternative mechanisms to recruit and retain international AI talent.

First, the Department of Labor (DOL) should amend its list of Schedule A occupations to include high-skilled AI technologists. Under Schedule A authorities, DOL has authority to determine whether there are insufficient numbers of American workers for a specific occupation and that the hiring of foreign nationals will not negatively impact U.S. workers.[87] As the need for AI technologists far outweighs the number of available U.S. AI scientists, this would be an appropriate occupation for Schedule A designation. If AI specialists were added to the list of Schedule A

occupations, employers seeking to sponsor a foreign national for a green card could forgo the first step in the permanent residency process and proceed directly with the I-140 filing process, saving both time and resources for the employer and employee.[88]

Second, Congress should create a new program to attract qualified international students and retain them for the American AI workforce. This proposal is different from the "staple a green card to a diploma" concept popularized by *New York Times* columnist Thomas Friedman in that it is more targeted, requires up-front commitment on the part of the program participant, and frees the applicant from requiring employer sponsorship.[89]

The program as envisioned consists of three phases. In the first phase, an international student applies for an "F-prime" dual intent student visa.[90] To obtain such a visa, the student must be accepted into a pre-approved AI-related graduate-level academic program, be successfully screened and vetted by the FBI and the State Department, and commit to working in an AI-relevant field in the United States for a minimum of ten years upon graduation.[91] The F-prime visa is guaranteed for the duration of the student's program of study as long as the student meets certain academic criteria.

The second phase begins upon completion of graduate school. The program participant is provided a ten-year conditional open-market EB-1 green card, the so-called "genius visa" for immigrants with extraordinary skills in their field. Like status quo EB-1 green cards, this new subcategory would have no labor certification or employer sponsorship requirement and allow the individual to work for any U.S. employer, but unlike a typical EB-1, it would not last indefinitely.

U.S. immigrants attend their naturalization ceremony to become American citizens. Immigrants are the bedrock of American ingenuity and innovation. The U.S. government should reform existing immigration pathways and create new ones to recruit additional high-skilled immigrants for STEM and computer science jobs. (John Moore/Getty Images)

In phase three, after nine years of employment in the United States, the participant is eligible to commence the petition to remove the conditions on residence (permanent green card) or apply for naturalization. Unconditional permanent residency or citizenship would be granted upon the successful completion of the ten-year employment period.

The program would have three key benefits. First, through the considerable up-front commitment, it attracts the best and brightest foreign students who are already highly predisposed to live, study, work, and remain in the United States. Second, unlike the "stapled green card"' approach, it is targeted for specific AI-related disciplines. Third, by removing employer sponsorship requirements, you solve the "start-up visa" problem by eliminating the cost and uncertainty of extending job offers to qualified foreign nationals.

V. COUNTER ILLICIT TECHNOLOGY TRANSFER

The United States needs to double down on protecting American intellectual property. Historically, adversaries and allies alike have pursued U.S. technologies to improve their military or economic comparative advantage including Russia, Japan, France, Israel, and South Korea.[92] China is the primary point of reference here, however, because of the sheer scale of its ongoing collection efforts. China is an increasingly capable espionage actor, and is actively collecting information from America's government, corporations, nonprofits, and colleges and universities. It employs a range of methods, both legal and illegal, to appropriate U.S. technology including U.S. company insiders, employees of Chinese firms partnering with U.S. companies, cyber espionage, foreign direct investment, and academic solicitation.[93]

In July 2019 FBI Director Christopher Wray stated, "There is no country that poses a more severe counterintelligence threat to this country right now than China . . . and I don't say it lightly."[94] He further noted that the Bureau had around 1,000 investigations involving attempted theft of U.S. intellectual property (IP). The White House, in its 2017 National Security Strategy, also highlighted the importance of the issue.[95] One concrete action the administration recommended was to strengthen the Committee on Foreign Investment in the United States (CFIUS), which was accomplished in 2018 through the passage of the Foreign Investment Risk Review Modernization Act of 2018. The bill cited factors such as the national security risks of increasing control of certain assets by foreign entities, and to what extent a transaction would expose sensitive U.S. citizen data to foreign governments, as considerations.[96]

Private Sector

China's efforts to illicitly obtain American technologies and know-how are vast and effective. One in five U.S. companies reported IP theft by China in 2018.[97] The United States Trade Representative calculates that the annual cost of "the theft of trade secrets could be as high as $600 billion."[98] This figure does not incorporate the full cost of patent infringement, nor the estimated $400 billion per year lost to economic espionage via cyber attacks.[99]

> **The United States Trade Representative calculates that the annual cost of "the theft of trade secrets could be as high as $600 billion."**

To counter the theft of U.S. technology from American companies, Congress should:

Provide more cyber defense support to small firms

Congress should increase funding for efforts supporting cyber defense at smaller firms active in critical technology areas. Small and medium business in general are more vulnerable to cyber attacks.[100] One effective initiative worth expanding is the Department of Homeland Security's National Cybersecurity and Communications Integration Center and the Critical Infrastructure Cyber Community Voluntary Program.[101] The Department of Homeland Security's Inspector General found that the department is overall behind on assessing its cybersecurity workforce and forming a strategy to build that workforce.[102] As it builds its strategy, it should build in measures specifically catered toward supporting the U.S. innovation base.

Academia

Countering Chinese espionage and other forms of technology transfer in academia poses vexing challenges. The United States needs to blunt Chinese collection efforts without undermining civil liberties or the free and open environments of American universities. FBI Director Wray called China's efforts a "whole of society threat" to the dismay of many universities that stressed the importance of openness, inclusion, and the contributions of international students.[103] Lee Bollinger, president of Columbia University, went so far as to say that monitoring foreign-born students "is antithetical to who we are."[104] Rather than generate friction between itself and universities, the U.S. government should build dialogue with universities to understand their concerns and look for mutually agreeable solutions. The open environment at universities is important because it is foundational to U.S. innovation. At the same time, this openness is being exploited by China. The United States needs solutions that are consistent with American values while guarding against espionage and illicit or otherwise unintended technology transfer.

The U.S. government can support universities by bringing awareness to *specific* methods and technologies of interest. Focusing on methods and targeted technologies can create avenues for action that avoid profiling Chinese national students. This approach also would mitigate collateral risks of racial profiling of the Chinese-American and larger Asian-American communities. More than half of the top AI talent in the United States is composed of foreign nationals, and Chinese nationals who study and decide to stay in the United States form an important part of this research community.[105]

General-purpose technologies such as AI, which are inherently dual-use, create an additional challenge to counterespionage efforts because they are less likely to be safeguarded by classification protocols and because espionage actors may have more claims to plausible deniability. Despite this, the U.S. government can take steps to help protect the technology innovation community, especially universities, against illicit technology transfer.

To address the threat posed by academic solicitation, the U.S. government should:

Authorize consular officials to act on risk indicators for espionage

The U.S. State Department, FBI, and intelligence community should collaborate to protect open research environments by screening out high-risk individuals before they arrive. Possible risk factors include whether an individual is funded by China's government, including the People's Liberation Army (PLA), or cites highly specific research interests relating to defense technologies.

Disallowing PLA researchers is one place to start. The Australian Strategic Policy Institute estimates that 500 military scientists from China have been sent to the United States since 2007 and that "research collaboration with the PLA . . . comes with significant security risks while offering unclear benefits."[106] The U.S. State Department should work with the intelligence community to identify other risk factors, and Congress should legislate to authorize visa denials accordingly.

Legislators recently have proposed both actor-based and technology-based approaches to improve visa screening. The People's Liberation Army (PLA) Visa Security Act would prohibit F or J visas for PLA employed, funded, or sponsored individuals, and the Protect Our Universities Act of 2019 would mandate background screening of students seeking to work on "sensitive research projects."[107] Both proposals are sensible measures and should be implemented, but broader

screening also is required beyond simply PLA-sponsored individuals or sensitive research projects. AI is highly dual-use and has both commercial and military applications. Data-informed policies should help to protect universities against individual academic espionage risks while mitigating potential negative effects to open campus environments.

Improve collaboration with colleges and universities

The FBI should increase collaboration with universities and information sharing on academic espionage threats. Universities have a strong interest in preventing countries such as China from unfairly exploiting research by their faculty. Universities and the FBI both already are implementing measures to address security concerns on campus and combat academic espionage.[108] Greater dialogue is urgently needed between investigators and academics to better understand the scope of the problem and solutions. Positive action is under way: In September 2019, the White House OSTP published an open letter to the U.S. research community to highlight the issue of research security. OSTP announced its plan to hold meetings at academic institutions across the country to discuss lines of efforts such as coordinating outreach and engagement and assessing and managing risk.[109] The Securing American Science and Technology Act of 2019 supports this approach and calls for OSTP to convene meetings on best practices.[110] Universities are taking their own steps to address the issue. The Association of American Universities (AAU) and Association of Public & Land-Grant Universities (APLU) sent a letter to universities in April 2019 on best practices for protecting against intellectual property theft and academic espionage.[111] More should be done, however, to ensure greater coordination between universities and the national security community on this important topic.

In February 2018, the FBI disbanded the National Security Higher Education Advisory Board (NSHEAB), which had existed since 2005 to establish lines of communication between universities and the national security community on counterintelligence threats, among other issues. Since then, members of Congress and American education leaders have publicly expressed concern about the FBI's decision to disband the NSHEAB and the need for a reconstituted organization to perform its functions.[112] In April 2018, the American Council on Education (ACE) sent a letter to the FBI director on behalf of 15 different American education associations and councils requesting engagement with the national security community in a forum similar to the NSHEAB.[113] Similarly, in April 2018 the ACE, AAU, APLU, and Council on Government Relations released a joint statement expressing support for the NSHEAB and a desire for a similar forum.[114] U.S. government officials also have expressed support for such a mechanism of collaboration between universities and the national security community. The Commissioner of the U.S.-China Economic and Security Review Commission said the board was "vital and should be reinstated," and FBI officials signaled in 2018 they were exploring creating a similar group.[115]

The FBI should reconstitute the NSHEAB or a similar body to increase awareness and cooperation on countering espionage in U.S. academia.[116] Many universities would support this reconstitution and it would provide a valuable mechanism for coordination between universities and the national security community on sharing information on threats and actions to counter academic espionage.

Other agencies that work on technology transfer should build dialogue with universities as well. The Department of Commerce Bureau of Industry of Security already engages in training with colleges and universities to raise awareness of export control laws. Although export controls may not be suitable for AI software, the Department of State's Bureau of International Security and Nonproliferation can use its expertise in dual-use technologies.[117] Working off the Department of

Commerce trainings as a model, the Department of State should work with researchers to identify red flags for dual-use technologies. As one PLA researcher said, foreigners "can be asked to develop an algorithm but not briefed on the details of how the algorithm would be used."[118] AI can be misused for malign ends but government experts can train university researchers to conduct due diligence of possible end uses. U.S. government collaboration with universities should not be limited strictly to security measures but should include knowledge-sharing on technologies themselves.

AI can be misused for malign ends but government experts can train university researchers to conduct due diligence of possible end uses.

VI. PROTECT AMERICA'S EDGE IN AI HARDWARE

AI systems require computational power ("compute") to run. Access to compute can make or break an AI project. Computational power rests in hardware, and like any other specialized physical object, hardware has its own design, fabrication, and supply chain considerations.[119] Availability of compute and supply chain dynamics therefore will drive national AI adoption potential, including the ability of a country to develop more advanced systems. U.S. policymakers should regard hardware as an equal part of the talent-data-hardware triad and work to boost American leadership and security in this space.

The U.S. government has ongoing efforts to create compute infrastructure for research, to increase hardware supply chain security, and to develop next generation AI-optimized chips. Sound policies in all three areas are required to protect America's technological leadership.

To support research, the White House's American AI Initiative directs federal agencies to allocate compute resources for AI-applications and R&D.[120] A number of U.S. government supercomputers built for AI applications, like the Department of Energy's Center for Accelerated Application Readiness, have opened applications to the public for research projects.[121] For hardware development, the National Science Foundation has jointly funded projects, for instance with DARPA, to develop next-generation chips.[122]

To address supply chain security, the Department of Defense has a Trusted Foundry program. It sought to accredit microelectronics sources as "trusted" if they could assure the integrity of persons and processes for chips' chain of custody.[123] As of 2016, the program boasted about 20 foundries, with IBM running the facilities responsible for the vast majority of leading-edge custom-made chips.[124] These facilities lost their eligibility, however, when GlobalFoundries, a U.S.-based but United Arab Emirates–owned company, purchased them.[125] For lack of alternative options, the Department of Defense signed a seven-year contract with GlobalFoundries to continue purchasing microchips.[126] The Government Accountability Office (GAO) says that the Department of Defense is still seeking "new approaches to retain trustable, leading-edge capabilities."[127]

U.S. government efforts to build and deploy hardware are outlined in the American AI Initiative, the White House's National Artificial Intelligence Research and Development Strategic Plan, and some agency-specific projects.[128] Congress and the administration should do more to make compute available, to mitigate supply chain risks, to build the next generation of AI-optimized chips, and to protect America's edge by limiting the diffusion of advanced semiconductor manufacturing equipment.

To preserve and promote America's advantage in AI hardware, Congress and the White House should:

Increase the availability of affordable compute resources

The U.S. government has a long history of building high-performance computers and awarding grants for researchers who require compute for their projects. It should supplement these existing efforts by using innovative approaches to facilitate access to affordable compute resources. While most researchers will not require exascale computing like that offered by Oak Ridge National Laboratory's next supercomputer, compute even for smaller projects is expensive.[129] It often poses a barrier to entry for start-ups, universities, and colleges. Smaller institutions like high schools doing the basic training of the next generation of AI leaders often only can afford the bare essentials.[130] For example, the cloud computing cost for AlphaGo Zero—the improved version of DeepMind's AlphaGo—by itself cost around $35 million.[131] AlphaStar, DeepMind's AI program that beat a top professional human player at the Starcraft II strategy game, cost as much as $100 million.[132]

The U.S. Department of Energy's Oak Ridge National Laboratory (ORNL) unveils its most powerful scientific supercomputer. Supercomputers provide the U.S. government with massive amounts of compute, and the government is working to give researchers in academia increased access to compute. (ORNL/Carlos Jones/Flickr)

To help address the compute access gap, the National Science Foundation is building relationships with cloud computing providers through the "Enabling Access to Cloud Computing Resources for CISE (Computer and Information Science and Engineering) Research and Education" program and the "Exploring Clouds for Acceleration of Science (E-CAS)" project.[133] NSF should expand these projects, and Congress should increase funding for them.

Congress also can incentivize companies to donate compute resources to universities. The compute used in the largest training runs doubles every three and a half months, and demand will likely increase.[134] The U.S. government operates a number of compute facilities that are open to university researchers, but increasing capacity will be necessary to satisfy growing demand. In Massachusetts, a number of top universities partnered with the state government and the private sector to establish the Massachusetts Green High Performance Computing Center, which houses a number of high-end computer systems available to researchers.[135] State and federal agencies partnered to build the infrastructure necessary to support the center. Additionally, the project benefited from the federal New Markets Tax Credit Program that promotes private capital investment in low-income regions.[136] Tax incentives for donated or discounted compute resources could increase universities' access to commercial compute resources, especially at a time when more companies seek relationships with academia.

Establish multilateral export controls on semiconductor manufacturing equipment (SME) and increase federal R&D funding for next-generation hardware

The United States has a major global lead in semiconductor design and should enact multilateral export controls, in concert with allies and partners, to protect its competitive edge in hardware. China is currently heavily dependent on imports of foreign-manufactured semiconductors to meet

internal demand. As part of its Made in China 2025 plan, China is looking to reduce its reliance on foreign chips by ramping up domestic semiconductor production.[137] Yet this desire to indigenize production is a major source of strategic leverage for the United States.

To accomplish this goal, China needs foreign imports of semiconductor manufacturing equipment (SME), which are the equipment and tools needed to establish a chip fabrication facility, or foundry.

The global SME market is highly centralized, with the United States, Japan, and the Netherlands accounting for 90 percent of global SME market share.[138] In key areas the market is even more concentrated. A single Dutch company is the sole supplier of extreme ultraviolet lithography machines required to make the latest generation of semiconductors.[139] Nearly the entire global supply of photoresists, chemicals essential to the production of semiconductors, is produced by a handful of companies based in the United States, Germany, Japan, and South Korea.[140]

The Commerce Department and State Department should work with key allies and partners (the Netherlands, Japan, South Korea, and Singapore) to establish multilateral export controls on SME, restricting sales to China. While export controls on semiconductors themselves should be rare and targeted, such as the action against Huawei and a handful of other companies linked to the Chinese military, the United States should enact broad restrictions on sales of SME to China, working in concert with allies and partners, in order to sustain the U.S. advantage in hardware.

> **The United States should enact broad restrictions on sales of SME to China, working in concert with allies and partners, in order to sustain the U.S. advantage in hardware.**

One risk to SME export controls is that they deprive U.S. companies of profits they currently use to invest in R&D. Chinese investments in domestic chip fabrication have buoyed the SME industry, accounting for much of the recent market growth.[141] U.S. companies must continue to invest in next-generation techniques to remain global leaders. As chip designs approach the atomic limit of silicon and Moore's Law comes to an end, chip companies are searching for the next breakthrough that will lead to a new generation of computing hardware. In order to ensure continued U.S. leadership in semiconductors, the federal government should increase R&D in next-generation chip design, fabrication, and packaging. Enacting the following two recommendations also would offset SME revenue losses.

Boost domestic semiconductor manufacturing with retooling incentives

Reinvigorating the Trusted Foundry program would be a positive step for U.S. leadership in AI hardware and help to ensure a secure supply chain. Building plants for semiconductors is expensive—an advanced fabrication facility can cost up to $20 billion.[142]

A feasible alternative to all-new facilities to revive this part of the Trusted Foundry Program is to support retooling of existing U.S.-based foundries to facilitate leading-edge hardware. Some fabs need to retool every two to three years to stay competitive, and these costs are burdensome.[143] Several companies already have requested funding to upgrade fabrication facilities in order to supply the government.[144] The United States should identify the U.S.-owned domestic facilities most suitable for retooling and develop a long-term funding plan to rebuild a trusted leading-edge semiconductor manufacturing capacity.

Secure semiconductor supply chains

The United States should work with U.S. industry leaders to explore novel public-private partnerships to ensure trusted semiconductor supply chains and work with key allies to establish an international fab consortium to diversify semiconductor fabrication. The United States is a global leader in semiconductor design, with U.S.-headquartered firms accounting for roughly half of the global market, but most fabrication occurs overseas.[145] This heavy reliance on overseas production presents risks of disruption or vulnerabilities introduced into the supply chain.[146] For example, chip production at Taiwan Semiconductor Manufacturing Company was disrupted briefly in 2018 when a computer virus made its way onto fabrication equipment.[147] Taiwan in particular is a major locale for semiconductor fabrication, accounting for over 70 percent of fabrication in "pure play foundries."[148] Taiwan is a major target of Chinese hackers and potential insider threats and a potential flashpoint for conflict.[149]

Employees at SK HYNIX Inc., South Korea's largest semiconductor company, work on a production line at a plant in Icheon, South Korea. Semiconductor supply chains are increasingly global, and their chains of custody pose challenges for security verification, which is of growing concern for the U.S. Department of Defense. (Pool/Getty Images)

The costs of establishing a new foundry are significant, on the order of $10–20 billion, making on-shoring costly even with potential government subsidies.[150] Additionally, the U.S. military and intelligence community have special needs for security that go above and beyond what is available in commercial facilities, yet they lack the scale of demand to make a purely government-dedicated foundry profitable.[151] The DOD and intelligence community should explore novel approaches for public-private partnerships with U.S. companies to build the capability for trusted design, fabrication, packaging, and testing. Additionally, the United States should establish an international fab consortium with allies to share the cost burden of building new semiconductor foundries to ensure a trusted and diverse supply chain. Member nations should include the global leaders in semiconductor manufacturing equipment: the United States, Japan, and the Netherlands.

VII. SHAPE GLOBAL NORMS FOR AI USE

The applications of AI can do incredible good for societies. It can optimize city systems, study employment patterns to give insights to policymakers, and revolutionize biotechnology. Technology in general can be used to make human life easier but only if it is subjected to informed policy and good governance. Increasingly, AI-enabled technologies are being abused by authoritarian states to exert control over their populations. In some cases, U.S. research and academic and private institutions have been complicit in enabling these abuses.[152]

Myriad potential risks arise with AI technologies. AI's general purpose and dual-use nature increase the risks of misuse and accidents. Risks of misuse involve the possibility of individuals or groups using AI systems in an unethical way, while accident risks are the potential harms that stem from AI systems behaving in unexpected ways.[153] AI also poses structural risks, meaning that AI technologies have the capacity to shape the political, economic, or social environment in disruptive or harmful ways.[154] Conversely, factors derived from structure, such as competitive advantages, also could influence how actors use AI, including by creating perverse incentives, such as actors racing to develop the technology first and taking shortcuts on safety.

As AI increasingly is incorporated into technologies that impact Americans' daily lives, the potential for misuse, accidents, and structural risks increases. Facial, image, and speech recognition algorithms are becoming more accurate, ubiquitous, and affordable every day. While they strengthen law enforcement capabilities, these technologies also raise concerns about civil liberties. Speech generation and synthetic media can be used in art, but also to spread disinformation and undermine the public's trust in truth and facts.

American leadership, alongside other democratic nations, in shaping international AI norms is essential to ensuring these technologies are developed and used in ways that align with democratic interests and values. The administration and Congress should:

Lead in establishing norms for appropriate AI use
The United States must be a leading voice on the how AI should and should not be used. As an open democratic society and the world's preeminent economic and military power, the United States has unparalleled influence and authority. U.S. society must determine how to strike a balance between concerns surrounding the use of AI systems, such as the debate over facial recognition technology. The United States is one of the few countries in the world where the interplay between civil society, government, and corporations will determine the processes to manage such thorny questions. It is vital to get this right, not just for the sake of American society, but to set an example for the world.

The U.S. government should pursue leadership in establishing norms for AI. In October 2019, the Defense Innovation Board (DIB) proposed a series of AI ethics principles, that if adopted by the Pentagon, will help guide the Defense Department's use of AI in combat and noncombat systems.[155] These principles can serve as a model for how the U.S. government, led by OSTP, guides the development and use of AI systems. The U.S. government also should collaborate with AI technologists who conduct research on AI safety, risk mitigation, and misuse. Not only does the U.S. government need to develop guiding norms for AI use, they will need to develop implementation methods and accountability mechanisms for abiding by them.

Collaborate with allies and partners on norms for AI use
The United States cannot go it alone. Working with allies and democratic partners will be essential to setting global norms on AI use at a time of growing AI competition. The implications of AI for global stability are too great.

The United States signaled its commitment to trustworthy AI that respects human rights and democratic values by endorsing the OECD AI principles.[156] In a speech at the OECD forum where those principles were endorsed, U.S. Chief Technology Officer Michael Kratsios called "on every

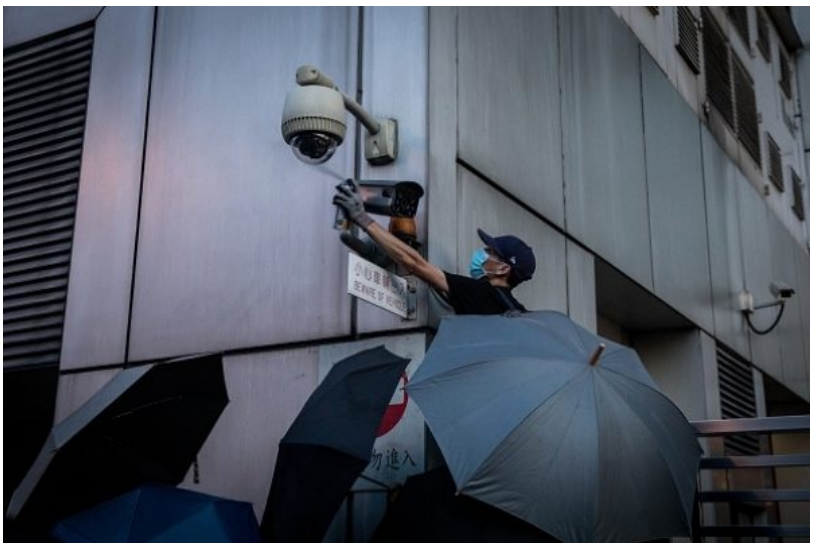
nation that shares our values to join with us to develop AI and make our countries stronger, the world safer, and our people more prosperous and free."[157]

Alliances and partnerships with like-minded countries will ensure that responsible stewardship of AI becomes the global norm. Concerted cooperative action will encourage other nations to follow suit and place pressure on outliers.

Protect U.S. research from supporting human rights violations

AI already is being used to strengthen autocratic rule and suppress minority populations. The most egregious example to date is in China. The Chinese Communist Party is conducting human rights abuses against Uyghurs in Xinjiang and is using AI-enabled technology to do it. The state has detained more than a million Uyghurs in detention camps.[158] Those not in camps are trapped in cities where neighborhoods are cordoned by facial recognition gates that determine who may pass, who may not, and who will be detained on sight.[159] Data doors pick up identifying cell phone information for people walking through them, and citizens are required to have government spyware installed on their phones.[160]

The Chinese government has forcibly collected other kinds of data to track Uyghurs as well, including gait data, voiceprint data, and genetic data.[161] Cameras track vehicles wherever they go and automatically identify license plates at gas stations.[162] The authorities use the Integrated Joint Operations Platform to aggregate this data, along with information about religious practices and other activities for their easy reference.[163] China's government is extending its watchful eye over the rest of the country with data-based initiatives like the Golden Shield Project, Sharp Eyes, and plans for a nationwide voiceprint recognition database.[164] China has engineered a new approach to authoritarianism supercharged by AI. It has been holding workshops abroad about its digital practices and selling surveillance technologies to other states; its approach is likely to proliferate over time.[165]



A protester covers a security camera during a march in Hong Kong against the extradition bill. The Chinese government is using AI-enabled technologies to collect mass amounts of biometric data to track and surveil its population. (Chris McGrath/Getty Images)

Due to the dual-use nature of facial recognition and other biometrics-detection technology, U.S. organizations are at risk of indirectly contributing to these human rights violations through research collaborations, technology exports, and investments.[166] Several U.S. companies and universities already have been implicated, sometimes inadvertently, and have withdrawn deals or agreements. In September 2019, the U.S. Department of State circulated draft guidance for the export of surveillance hardware and software.[167] While sensible, the guidelines are not mandatory. Stronger action is needed.

To prevent U.S. AI companies from enabling human rights abuses, Congress should modernize P.L. 101-246, Title IX, which "restricts the U.S. licensing of exports and re-exports of crime control and crime detection equipment and instruments listed in the Export Administration Regulations to China."[168] This modernization should include hardware incorporating AI-enabled biometric identification technologies such as facial, voice, and gait recognition. Additionally, the White House should levy further sanctions on and expand the Department of Commerce Entity List to include businesses and entities that provide oppressive technology, training, or equipment to authoritarian regimes implicated in human rights abuses.[169] In October 2019, the Trump administration placed eight Chinese technology companies on the Entity List for their involvement in human rights violations in Xinjiang and put visa restrictions on Chinese officials complicit in these activities.[170] Congress also should consider legislation to prevent U.S. entities from investing in companies that are building AI tools for oppression, such as Chinese AI company SenseTime.[171]

The United States can exert further pressure by invoking the Global Magnitsky Act to sanction foreign individuals involved with human rights abuses.[172] These actions are necessary to provide guardrails around legitimate U.S.-China AI cooperation and ensure that U.S. organizations do not contribute inadvertently to human rights abuses.

VIII. IMPROVE GOVERNMENT READINESS

With its American AI Initiative, the administration has identified the prerequisite building blocks for the implementation of a national AI strategy. According to the Government Artificial Intelligence Readiness Index published by the Oxford Institute, the United States is the fourth most "ready" country in the world on this front. These factors include strong governance, availability of quality data, technical skills, and robust public services. The report highlights the United States' "highly skilled workforce, innovation-friendly regulatory environment, and access to technological infrastructure and data" as positive developments.[173]

The administration's AI R&D Strategic Plan, executive order on AI, and long-term research efforts like DARPA's AI Next campaign are strengths to build upon.[174] In Congress, H.R. 4174 mandated the establishment of a Chief Data Officer Council at the Office of Management and Budget to coordinate best practices and data-sharing across the government.[175] The OPEN Data Act requires federal organizations to publish information in standardized machine-readable formats, which increases data quality and availability as standard practice.[176] These developments satisfy many of the organizational and data infrastructure requirements for AI adoption, but more is needed to achieve long-term U.S. objectives.

To ensure U.S. government agencies can take full advantage of AI resources, Congress and the cabinet-level departments should:

Prioritize talent management

Talent management in an era of AI will require managing three different, but related, challenges. First, it is necessary for the U.S. government to attract and retain top talent with technical AI expertise. Second, many national security professionals will require training in AI so that they can responsibly and effectively use AI applications. Third, government officials including senior leaders, policymakers, and procurement officials will need a working knowledge of AI functionality, uses,

and limitations to craft policy and inform acquisitions. Rotational programs to distribute talent around the government and career trajectories built around AI systems management as a profession would further bolster the federal government's human capital. The United States also needs to develop novel ways to bring outside AI experts into the government, even if for short periods of time. Temporary assignments, fellowships, and other opportunities (including recognition and public discussion of the results of such assignments) that make it easier for external technical and policy experts to serve may help ensure that the government has the AI expertise it needs.

> **The United States also needs to develop novel ways to bring outside AI experts into the government, even if for short periods of time.**

One model the U.S. government has used to employ digital talent is through short-term "tours of service."[177] Some initiatives are government-wide, like the U.S. Digital Service (USDS), which places technologists in a variety of projects and agencies. Some projects are security-oriented; for example, the Defense Digital Service component facilitated the Hack the Pentagon bug bounty program. Other projects showcase how applying talent to project-based approaches can modernize government processes. USDS has completed projects to optimize Department of Veterans applications for cloud and to increase digitization of Department of Homeland Security casework. Individual agencies also have undertaken term-based efforts. The National Institutes of Health (NIH), in its Strategic Plan for Data Science, announced its intention to recruit data scientists from industry and academia for one- to three-year "national service sabbaticals" at NIH projects.[178] These "tours of service" and "Data Fellows" concepts could serve as models for kickstarting AI implementation as the government continues to establish its longer-term personnel needs.

Cyber experts, technologists, and data scientists participate in the U.S. Navy's #HackTheSky hackathon. The participants were tasked with hacking into the code that controls the Naval Postgraduate School's fleet of autonomous swarming drones. The U.S. government hosts an array of events like this one to spur collaboration among government officials, researchers, and those in the private sector. (Victoria Ochoa/U.S. Navy)

U.S. policymakers need to recognize, however, that the pool of AI talent willing and able to serve in government will remain limited unless obstacles in hiring and employment practices are addressed. On-and-off ramps for the federal workforce are limited by both policy and culture. Federal employees no longer seek a three-decade career within a single agency—younger personnel have different expectations of career management. Likewise, many evolving fields (from STEM to regional expertise) benefit enormously from experts who can refresh their knowledge and experience in and out of government, with simplified paths of return. To create a flexible and permeable workforce, in the short term OPM should work with Congress and federal agencies to change present policies to allow prior government employees

to be rehired noncompetitively at any level for which they are qualified.[179] Just as importantly, agencies should remove barriers to talent movement between departments and agencies—including excessive and delaying security clearance transfers. Finally, federal agencies should enable more seamless on-ramps for internship and fellowship programs.[180]

Additionally, the government should examine how existing talent acquisition processes can be expanded to include AI specialists. To highlight one success case, the Department of Defense's Cyber Excepted Services has cut hiring times in half for new employees and is being leveraged for AI professionals as well.[181] To recruit recent graduates into government, the CyberCorps: Scholarship for Service could serve as a model. The program awards scholarships contingent upon working for government in cybersecurity positions following graduation.[182] The program could be expanded to target AI talent for both security and non-security functions.

Another effort to emulate is the Defense Digital Service. It employs best practices from the business world to quickly bring the best available technology into the department.[183] With its cadre of top private sector technologists on temporary government assignments, it launched the federal government's first bug bounty program and open source coding collaboration, to name a few successful projects.[184]

The U.S. Air Force Kessel Run initiative presents another novel approach to attracting and retaining talent. Rather than being located on a military base, personnel are based in Cambridge, Massachusetts, creating a work environment more akin to a technology start-up instead of the stereotypically staid government office.[185] U.S. government entities across the board will need to think creatively about how to entice AI talent to work in the public sector to compete with the perks, flexibility, and higher salaries offered by tech sector firms.

Allocate funding for federal agencies to implement AI

The American AI Initiative called upon agencies to prioritize AI within their budgets. The request has had some successes, like the Department of Energy's April 2019 announcement of $20 million specifically to expedite the implementation of AI and machine learning into energy technologies and design.[186]

The American AI Initiative falls short in that it does not establish budget targets. Agencies could lag on AI implementation without dedicated financial support. This hands-off approach by the administration further risks disjointed and incoherent efforts that will likely result in needless frustration and inefficiencies.

Most importantly, increases in spending beyond what existing budgets can support is needed. Front-end requirements include much higher R&D funding, data infrastructure upgrades, and talent acquisition. Rebalancing limited budgets to implement AI could displace critical mission and research areas within agencies.[187] Such displacement risks agencies relabeling other ongoing projects as AI-related where they can.

The White House should work with Congress to ensure agencies are allocated sufficient appropriations for AI implementation. The American AI Initiative is a good start, but ensuring much greater funding and coordinated congressional support will cement AI as a national priority.

Modernize IT processes

AI implementation by the U.S. government depends on the ability to update systems; manage, leverage, and share data; have access to compute; and manage a technical workforce. This will require consolidating data centers and standing up cloud services.

The U.S. government is making progress in recognizing the challenges in this area. For example, the GAO has suggested updates to IT practices that would be conducive not only to government efficiency but to AI adoption. The GAO recommended data center consolidation, modernization of legacy systems, and management of the IT workforce.[188] Separately, the Defense Innovation Board's Software Acquisition and Practices (SWAP) study endorsed updates to the Department of Defense's software acquisition processes.[189] Congress folded in elements of the SWAP study into the National Defense Authorization Act (NDAA) for FY 2020.[190] Following through on these measures, with continued cross-government leadership, will set the conditions for adopting AI.

The cloud will be important to AI implementation. According to the Department of Defense Cloud Strategy, "The algorithms used to inform decisions are dependent on the Department's data and information being organized, secure, and visible in a common environment."[191] AI depends on an aggregation of data and on compute; cloud solutions can deliver both. The U.S. government needs to optimize its data management in order to implement AI. The government is tackling data consolidation from a number of angles already through legislation like the 2014 Federal Information Technology Acquisition Reform Act, cross-government modernization efforts like the GAO's Improving the Management of IT Acquisitions and Operations initiative, and agency projects like the Department of Defense's Cloud Strategy and Joint Enterprise Defense Infrastructure (JEDI) cloud.[192] Some agencies are farther ahead than others, but the overall trajectory toward virtualization and cloud services—whether Software as a Service, Platform as a Service, or Infrastructure as a Service—seems positive.[193]

IX. LEAD IN AI STANDARDS-SETTING AND MEASUREMENT

AI Standards

AI should be safe, reliable, secure, and resilient. Government agencies also should continue to fund research of explainable and transparent AI systems. Standardization of AI techniques is required to define these qualities and provide the foundation for their measurement and regulation, where required. The United States long has been a leader in standards-setting, such as in telecommunications.[194] U.S. leadership in global AI standards-setting will help ensure that AI implementations play to our strengths and comport with our interests and values.

> **U.S. leadership in global AI standards-setting will help ensure that AI implementations play to our strengths and comport with our interests and values.**

In August 2019, the National Institute of Standards and Technology (NIST), part of the Department of Commerce, published a plan for how federal agencies should engage in AI standards.[195] This leadership role was mandated by the Trump administration's American AI Initiative.[196] Outside of the U.S. government, the American National Standards Institute (ANSI) is one of the leading national organizations focused on standards-setting both in the United States and abroad. A subgroup within ANSI, the International Committee for Information Technology Standards, is working specifically on developing standards in AI.

ANSI and NIST are engaged in the nascent international standards-setting effort. Working groups now are debating such topics as trustworthiness in AI, big data, AI use cases and applications, and governance implications of AI.[197]

Measuring AI

Measurement is how the AI research community orients itself and prioritizes research. Some measurement-focused initiatives, like the "ImageNet competition," have helped define field-wide progress in areas such as image recognition.[198] Other initiatives, like New York University's language-focused "GLUE" benchmark, have themselves become catalysts for further research. After various people submitted AI systems that maxed-out performance on GLUE, NYU built a new, harder benchmark called "SuperGLUE," which is serving to further catalyze progress.[199]

Benchmark tests are necessary to understand the performance of an AI system. With the breadth of technologies, functions, and capabilities that comprise AI, devising quantitative measurement schema poses a challenge. As a result, current tests for measuring AI range from vague and conceptual to well defined and mature. The AI Index has compiled some of the best examples of efforts to track progress of AI research.[200]

An example from the established end of the AI research spectrum is the F1 score—a function of precision and recall—that is used widely to evaluate natural language processing models. On the other end of the spectrum is the concept of computational creativity, the ability of a computer to create new ideas from existing information or to solve a problem it hasn't encountered before. Scientists still argue over what "creativity" means or whether it's possible for computers, let alone how to measure it. [201]

Moreover, AI measurement methodologies are not static. As technologies mature, and expectations of machine intelligence change, many tests that make sense today will not be as relevant a few years from now. Periodic reexaminations—at least every five years—and updates of testing methodologies will be necessary to ensure that AI systems are functioning optimally.

Take the example of the stalwart Turing Test, often used to test how well chatbots can mimic humans. Over half a century old, it is less meaningful today as a means to measure machine intelligence. Experts have proposed new tests of artificial creativity and intelligence such as Lovelace 2.0 and Winograd Schema Challenge as alternatives to Turing.[202] Winograd itself has shortcomings due to language- and data-based biases, according to a group of researchers. In July 2019, researchers announced a new, much larger challenge and associated dataset called WINOGRANDE that addresses these deficiencies.[203] We should expect further improvements to this new schema as knowledge and capabilities grow.

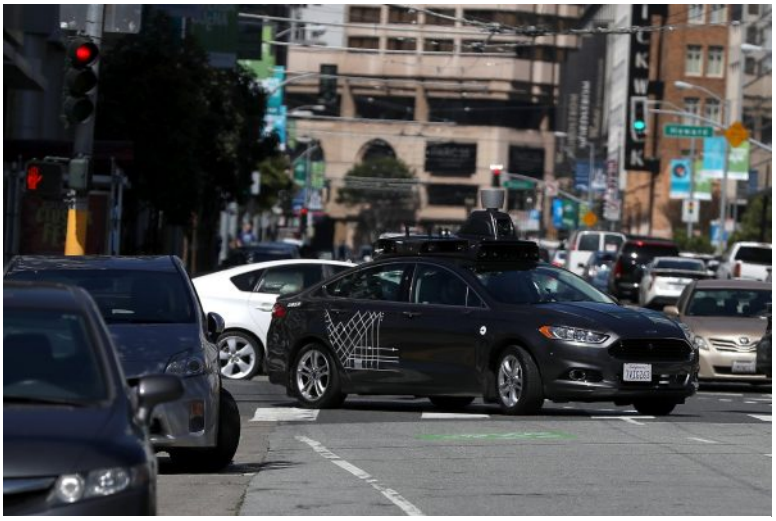
U.S. government involvement in standards-setting and measurement is important because policymakers will have direct access to the quantitative information needed for better, evidence-based decisionmaking. It further helps government experts identify areas where targeted grants—such as academic research on quantifying AI "robustness" and "trustworthiness"—would help to establish well-defined and effective metrics.

> **U.S. government involvement in standards-setting and measurement is important because policymakers will have direct access to the quantitative information needed for better, evidence-based decisionmaking.**

Codified tests to measure performance, functionality, and capabilities of AI systems are important and necessary. To make sure the United States is a global leader in AI metrics and to promote widespread adoption of AI solutions, the White House Office of Science and Technology Policy should:

Establish an NSTC Subcommittee for AI Standards & Measurement
Co-chaired by OSTP and NIST, the subcommittee would be created under the existing NSTC Select Committee on AI, whose mandate is to "prioritize and promote AI R&D, leverage federal data and computing resources for the AI community, and train the AI-ready workforce."[204] AI testing and standards are currently the purview of the NSTC Subcommittee on Machine Learning and Artificial Intelligence, which has a broader charter centered on monitoring the state-of-the-art in ML/AI and sharing of best practices between government agencies.[205] The central importance of standards and measurement to fostering AI technologies that are safe, secure, and reliable, and that comport with U.S. norms and values, warrants a stand-alone subgroup dedicated to the issue. This subcommittee would be most effective under the more focused NSTC Select Committee on AI.

It should bring together subject matter experts and stakeholders from government, academia, and private industry to formulate AI standards, identify AI metrics requiring measurement, identify AI risks, adopt existing performance measures, and design and codify relevant measurement techniques when necessary.



Uber conducts a test of a self-driving car in San Francisco. Standards setting and measurement will be instrumental in ensuring that emerging technologies like autonomous vehicles are tested and evaluated throughout the technology's entire life cycle to ensure safety and reliability. (Justin Sullivan/Getty Images)

The subcommittee should be empowered to recommend what continuous testing, evaluation, and measurement can be done reliably in the private sector and academia, versus what should be conducted externally by governmental entities (e.g., aspects of telemedicine, medical device safety, and certain autonomous vehicle functions). Another function should be to identify measures around which academia and industry are beginning to coalesce. In these cases, the U.S. government could focus competitions to promote standardization and adoption of such measures.

This body should work in concert with the American National Standards Institute (ANSI) to ensure that new AI measuring techniques conform to U.S. AI standards. To be effective, the subcommittee

must have a permanent mandate so that it can review and update metrics and tests over time as needed.[206]

The subcommittee should partner with ANSI to develop a list of guidelines for government agencies and private companies to assess risk in the AI technologies they develop and deploy. The EU has a case study worth emulating. In 2018, the European Commission introduced draft ethical guidelines for trustworthy AI, prioritizing systems that impacted the user directly.[207] The subcommittee's guidelines should focus on the potential for misuse, the risk of accidents, and the possibility of negative structural or environmental impact.

Finally, Congress should appropriate funding to specific government agencies to join the subcommittee as a member.[208] This appropriation would cover staffing and travel costs, allowing government agencies to appoint representatives from among themselves to attend working group meetings for the subcommittee.

Define what is AI

The U.S. government should formulate a definition of AI for its purposes. This is a necessary first step: Doing so will facilitate standards-setting, formulate measurements, ease the appropriation of AI-related funding, and help to track the AI spending of government departments and agencies. A well-crafted definition will be richly descriptive, not pithy, to bound how it is interpreted. It will require addressing the subfields of AI, acknowledging the wide range of use cases, and identifying all relevant processes (e.g., reasoning, problem-solving, language-understanding). We recommend our proposed NSTC Subcommittee on AI Standards, Measurement & Risk determine this definition.

Hedge Against Technology Surprise

Being aware of and understanding global AI developments is essential to the United States maintaining its edge. Tracking global progress in AI is also necessary to help avoid technology surprise. While there is no standard definition of "technology surprise," broadly speaking it concerns major technological breakthroughs, discovery of a previously unknown research effort, an unexpected rapid development or advancement in a scientific or technical field, and/or an unanticipated novel use of existing technology.[209]

> **Tracking global progress in AI is also necessary to help avoid technology surprise.**

One way to minimize the risk of technology surprise is a methodology called horizon scanning. This technique incorporates research from a wide variety of sources with the goal of detecting change, exploring problems and challenges in emerging technology fields, and discerning trends. Numerous organizations are already applying horizon scanning to keep tabs on AI advances. OpenAI used horizon scanning techniques for its "AI and Compute" analysis.[210] The British nonprofits Jisc and the Center for the Future of Intelligence, and the Australian Council of Learned Academies use the technique to inform their analyses of AI research. [211]

In the United States, Stanford University publishes an annual AI Index that contains many indicators and data points useful for horizon scanning approaches.[212] The Chinese new media company Leiphone publishes a vast database of information on AI developments in China called AI Impact Factors Database (AI影响因子) that provides valuable insights.[213]

To reduce the risk of technology surprise, the White House Office of Science and Technology Policy should:

Establish a permanent horizon scanning effort devoted to AI
The U.S. government has several departments and agencies with staff experienced in horizon scanning, including DoD, DHS, and the intelligence community.[214] Relevant government agency representatives, along with participants from academia and the private sector should conduct regular meetings and workshops to discuss and analyze global AI trends and publish periodic unclassified and classified reports to inform policymakers and decisionmakers throughout the U.S. government.

This effort would function best if focused on specific case studies with important national security implications, and where non-public information offers critical insight—for example, measuring advancements in AI for the creation of autonomous drone movement systems and the development of adversarial AI capabilities.

X. CONCLUSION

The United States' position as the global leader in AI is under increasing pressure. Other countries, China especially, are outpacing the United States in growing their R&D budgets and investing more resources in human capital. Still, the United States holds important advantages with its extensive system of world-class universities and research institutes, leading technology companies, and a vibrant venture capital and private equity market to fund AI start-ups. It remains a place where people from around the world want to work and live.

The Trump administration articulated a strong strategic vision with its executive order and National R&D Strategy for AI. The next phase must be executing to achieve these goals. Implementing the recommendations in this report will help ensure that the United States is positioned for near-term and long-term success, and that this vision becomes reality.

The United States is at its best when it rises to the occasion to face a challenge head-on. By nurturing and capitalizing on U.S. advantages, and addressing the areas where America is starting to fall short, the United States can ensure this will be the American AI Century.

APPENDIX

Ongoing AI Initiatives Across the U.S. Government

The U.S. government is engaging in numerous lines of effort to advance artificial intelligence.[215] The Executive Branch and Congress are prioritizing AI through ongoing initiatives and projects, several of which are outlined below.

The White House

In February 2019, President Trump signed the "American AI Initiative" Executive Order (EO), identifying AI as an R&D priority for the U.S. government. The strategy, framed around five principles, directs implementing agencies to prioritize "sustained investment in AI R&D."[216] (1) The EO identifies the need for collaboration between the federal government, private industry, and academia. (2) It directs federal agencies to share more of their datasets and models for use by the AI research community. (3) The EO prioritizes AI education and workforce development to train the "next generation of AI researchers."[217] (4) It addresses public concerns over data security and privacy. (5) The initiative promotes increased collaboration with allies and partners, while protecting U.S. assets from acquisition by "strategic competitors and adversarial nations."[218]

The Office of Science and Technology Policy (OSTP)

The OSTP is orchestrating several AI projects and initiatives. These includes, but are not limited to: creating and co-leading the Select Committee on AI; co-leading and managing the Networking and Information Technology Research and Development program (NITRD) Machine Learning and AI Subcommittee; overseeing as part of the National Science and Technology Council (NSTC) the update to the National Artificial Intelligence Research and Development Strategic Plan; and leading the United States in international discussions on AI, including delegations to the 2017, 2018, and 2019 G7 Innovation and Technology Ministerial to promote AI R&D, as well as ongoing AI-related efforts in the OECD and in G20 ministerials.[219] The NITRD AI R&D Interagency Working Group, formed in June 2018, applies a "free market approach to scientific discovery" to harness the "combined strengths of government, industry, and academia," in order to best use this technology.

National Science & Technology Council (NSTC)

The National Artificial Intelligence and Development Strategic Plan

The National Science & Technology Council's Select Committee on Artificial Intelligence published an updated AI R&D strategic plan in June 2019.[220] Building off the original 2016 strategy, the plan identifies priority areas for federal government investment in AI R&D.[221] The strategy includes eight strategic priorities: (1) "Make long-term investments in AI research." (2) "Develop effective methods for human-AI collaboration." (3) "Understand and address the ethical, legal, and societal implications of AI." (4) "Ensure the safety and security of AI systems." (5) "Develop shared public datasets and environments for AI training and testing." (6) "Measure and evaluate AI technologies through standards and benchmarks." (7) "Better understand the national AI R&D workforce needs." (8) "Expand public-private partnerships to accelerate advances in AI."

NSTC issued a report reviewing federal AI R&D activities during the 2016-2019 timeframe in November 2019.[222]

America's Strategy for STEM Education
The promotion of STEM education is an ongoing priority for the Trump administration. In September 2017, President Trump signed a Presidential Memorandum for the Secretary of Education, with the goal of devoting approximately $200 million in grant funds every year to the promotion of STEM education, particularly in the field of computer science.[223] The Committee on STEM Education of the NSTC released a five-year strategic plan in December 2018 for STEM education, based on "a future where all Americans will have lifelong access to high-quality STEM education and the United States will be the global leader in STEM literacy, innovation, and employment."[224] This is a critical effort due to the importance of STEM education for developing the human capital the nation needs in AI and other high-tech fields.

National Security Commission on Artificial Intelligence
The U.S. Congress mandated the establishment of the National Security Commission on Artificial Intelligence in the 2019 NDAA, recognizing the need for a comprehensive national approach to AI. The commission was created as an independent body to "review advances in artificial intelligence, related machine learning developments, and associated technologies" to "comprehensively address the national security and defense needs of the United States."[225] The commission's focus areas include developments and trends in international cooperation and competitiveness, stimulating academic AI research with applications to national security, workforce and education incentives to attract leading talent in AI and machine learning, evaluating risks and ethical considerations associated with the military use of AI-enabled technologies, establishing data standards and incentivizing the sharing of training data, and potential mechanisms for managing the evolution of AI technologies.

Eric Schmidt, former head of Google's parent company Alphabet, serves as chairman of the commission and Robert O. Work, former Deputy Secretary of Defense, serves as vice chairman. The commission sent its initial report to Congress in July 2019.[226] On November 4, 2019, the NSCAI released its interim report which identified five lines of effort on which the U.S. government should focus: R&D investments, national security applications of AI, training and recruiting AI talent, protecting and building upon U.S. technical advantages, and promoting global AI cooperation.[227]

Congressional Artificial Intelligence Caucuses
In May 2017, the U.S. House of Representatives established a bipartisan AI caucus, with the mission to "inform policymakers of the technological, economic, and social impacts of advances in AI and to ensure that rapid innovation in AI and related fields benefits Americans as fully as possible."[228] In March 2019, a bipartisan group of U.S. senators announced the creation of their own bipartisan Senate Artificial Intelligence Caucus.[229] Recognizing the transformative potential of AI, the caucus will seek to connect congressional members to AI experts in the private sector and academia.[230]

The U.S. Department of Defense (DoD)

Joint Artificial Intelligence Center (JAIC)[231]
The 2018 National Defense Strategy (NDS) specifically identifies AI as an emerging technology with the potential to shape military power and as an arena of strategic competition. To prioritize AI throughout the Department, the DoD established the Joint Artificial Intelligence Center (JAIC) in June 2018 as a hub for AI research and development. In addition to launching a series of AI-centric

National Mission Initiatives, the JAIC is tasked with three central goals. The JAIC will "accelerate delivery and adoption of AI capabilities across DoD . . . establish a common foundation for scaling AI's impact," and "synchronize DoD AI activities, related AI and machine-learning projects" across the entire Department.[232] Since its inception, the JAIC has received approximately $90 million in funding.[233] In the FY 2020 budget, the JAIC will receive approximately $208 million in funding, about half of the amount the Pentagon first projected it would need to scale the center.[234]

Artificial Intelligence Strategy

The Department of Defense released its AI strategy, "Harnessing AI to Advance Our Security and Prosperity," in February 2019. The DoD framed its strategy around the concept of a "human-centered adoption of AI,"[235] the idea that humans play an essential role in the deployment and use of AI.[236] Specifically, the Department's strategy calls for the rapid delivery of AI-enabled technologies and prioritized collaboration with private industry, academia, and U.S. allies. It emphasizes the DoD's desire to lead in AI safety and ethics. The strategy also established the JAIC as the focal point of AI efforts across the entire Department.[237]

Defense Innovation Board

The Defense Innovation Board (DIB) recognizes the importance of maintaining America's technological advantage in AI, as well as ensuring these technologies are developed and used ethically and safely. In July 2018, the DIB's Subcommittee on Science & Technology was tasked with establishing a set of AI Principles for Defense, to ensure that the U.S. government develops and uses AI and related tools responsibly.[238] Over the duration of its study, the DIB has conducted a number of public listening sessions around the country, gathering input from a diverse group of stakeholders, inside and outside the U.S. government, focused on AI safety.[239] Additionally, the subcommittee directly engaged with organizations in the AI community committed to AI ethics and safety.

On October 31, 2019, DIB members voted and approved its proposed list of AI principles.[240] If adopted by the DoD, the principles will be used to inform future AI strategies, shape the JAIC's ongoing activities, and provide clarity to private sector companies that are considering partnering with the U.S. government.[241]

Defense Advanced Research Projects Agency (DARPA)

DARPA currently funds a "broad portfolio of AI R&D programs, ranging from basic research to advanced technology development."[242] In September 2018, DARPA announced an "AI Next" campaign consisting of a $2 billion-plus investment over five years in new and existing programs focused on attending to new capabilities and developing robust, explainable, high-performance, next-generation AI technologies. These include "automating critical DoD business processes, such as security clearance vetting or accrediting software systems for operational deployment; improving the robustness and reliability of AI systems; enhancing the security and resiliency of machine learning and AI technologies; reducing power, data, and performance inefficiencies; and pioneering the next generation of AI algorithms and applications, such as 'explainability' and common sense reasoning."[243]

U.S. Air Force

In September 2019, the U.S. Air Force unveiled its strategy for AI as an annex to the DoD's overarching AI strategy released in February 2019.[244] The Air Force's strategy identifies four focus areas: (1) "Drive down technological barriers to entry." (2) "Recognize and treat data as a strategic asset." (3) "Democratize access to artificial intelligence solutions." (4) "Recruit, develop, upskill, and cultivate our workforce." (5) "Increase transparency and cooperation with international, government, industry, and academic partners."[245]

Committee on Foreign Investment in the United States (CFIUS)

The 2019 NDAA includes the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA is designed to reform the Committee on Foreign Investment in the United States (CFIUS) review process since its last update in 2007. The legislation includes a significant expansion of the scope of transactions subject to review. The committee now can review investments in critical technology sectors even if they do not entail a controlling stake in the business. FIRRMA allows the committee to review foreign investments that provide access to non-public technical information, membership or observer rights on the board of directors, or involvement in substantive decisionmaking related to the use, development, or acquisition of critical technologies.[246] While FIRRMA does not specifically identify which technologies will be categorized as "essential to U.S. national security," it likely will empower the committee to review foreign investments in U.S. firms utilizing AI and associated hardware. News reports indicate that recent more aggressive CFIUS scrutiny over potential deals has led to a chilling effect on Chinese investments in emerging technologies in Silicon Valley.[247]

U.S. Department of Commerce Export Controls for AI

As part of the NDAA for Fiscal Year 2019, Congress enacted the Export Control Reform Act to facilitate the establishment of appropriate controls (including interim controls) on emerging and foundational technologies. Technologies often are placed on the Commerce Control List to protect sensitive U.S. technology.[248] Currently, AI falls under a "representative technology category" for which Congress currently is seeking to determine whether it is an emerging technology essential to the national security of the United States. AI and machine learning in this context refer to neural networks and deep learning, evolution and genetic computation, reinforcement learning, computer vision, expert systems, speech and audio processing, natural language processing, planning, audio and video manipulation technologies, AI cloud technologies, and AI chipsets.

Intelligence Community (IC) AIM Initiative[249]

The Office of the Director of National Intelligence (ODNI) publicly released its Strategy for Augmenting Intelligence Using Machines, or AIM Initiative, in late 2018. The AIM Initiative outlines opportunities to incorporate AI capabilities "in a manner that resolves key IC legal, policy, cultural, technical, and structural challenges."[250] The strategy proposes investment objectives, organized temporarily under immediate and ongoing, short-term, medium-term, and long-term efforts. Within this structure, the ODNI plans to implement IC-wide reforms regarding interagency collaboration, R&D, external partnerships, workforce, and transparency. Ultimately, the AIM Initiative represents an acknowledgement by the IC of the transformative effects AI will have on the production of intelligence and the need to adapt internal practices to retain analytical and operational advantages.

National Institute of Standards and Technology (NIST)

The U.S. Department of Commerce's NIST released its plan for "prioritizing federal agency engagement in the development of standards for artificial intelligence" in August 2019.[251] The plan was the product of President Trump's Executive Order on Maintaining American Leadership in Artificial Intelligence.[252] NIST's plan recommends the federal government "bolster AI standards-related knowledge, leadership, and coordination among agencies that develop or use AI; promote focused research on the trustworthiness of AI systems; support and expand public-private partnerships; and engage with international parties."[253]

U.S. Department of Energy's Office for Artificial Intelligence and Technology

The U.S. Department of Energy (DOE) established a new Office for Artificial Intelligence and Technology (AITO) in September 2019. In response to the Trump administration's executive order on AI, the DOE stood up the AITO to act as a coordinating body for the ongoing work on AI occurring across the Department. The AITO's mission is to, "accelerate the delivery of AI-enabled capabilities, scale the department-wide development and impact of AI, and synchronize AI activities to advance the agency's core missions, expand partnerships, and support American AI leadership."[254]

ENDNOTES

1. Paul Scharre and Michael Horowitz, "Artificial Intelligence: What Every Policymaker Needs to Know," CNAS, June 2018, https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know; Michael Horowitz, Paul Scharre, Gregory C. Allen, Kara Frederick, Anthony Cho, and Edoardo Saravalle, "Artificial Intelligence and International Security," CNAS, July 2018, https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security; and "Artificial Intelligence and Global Security," CNAS.org, https://www.cnas.org/artificial-intelligence-and-global-security.

2. 115th Congress, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," July 25, 2018, 329, https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf.

3. "Federal R&D as a Percent of GDP," American Association for the Advancement of Science, 2019, https://www.aaas.org/sites/default/files/2019-06/RDGDP.png.

4. "US R&D Spending at All-Time High, Federal Share Reaches Record Low," American Institute of Physics, November 8, 2016, https://www.aip.org/fyi/2016/us-rd-spending-all-time-high-federal-share-reaches-record-low.

5. "Artificial Intelligence (AI) at NSF," National Science Foundation, https://nsf.gov/cise/ai.jsp.

6. Susan Chacko, "Teaching Computers to Think," *National Institutes of Health,* 26 no. 4 (July-August 2018), https://irp.nih.gov/catalyst/v26i4/machine-learning.

7. "AI Next Campaign," Defense Advanced Research Projects Agency, https://www.darpa.mil/work-with-us/ai-next-campaign.

8. Chris Cornillie, "Finding Artificial Intelligence Money in the Fiscal 2020 Budget," Bgov.com, March 28, 2019, https://about.bgov.com/news/finding-artificial-intelligence-money-fiscal-2020-budget/.

9. National Science & Technology Council's Subcommittee on Networking & Information Technology Research & Development, *Supplement to the President's FY2020 Budget*, September 2019, https://www.whitehouse.gov/wp-content/uploads/2019/09/FY2020-NITRD-AI-RD-Budget-September-2019.pdf.

10. Thomas J. Colvin, Talla F. Babou, Keith W. Crane, Irina Liu, and Gifford J. Wong, "A Tentative Framework for Examining U.S. and Chinese Expenditures for Research and Development on Artificial Intelligence," D-10856, IDA, September 2019, https://www.ida.org/research-and-publications/publications/all/a/at/a-tentative-framework-for-examining-us-and-chinese-expenditures-for-r-and-d-on-ai.

11. Meng Jing, "Tianjin city in China eyes US$16 billion fund for AI work, dwarfing EU's plan to spend US $1.78 billion," Scmp.com, May 16, 2018, https://www.scmp.com/tech/innovation/article/2146428/tianjin-city-china-eyes-us16-billion-fund-ai-work-dwarfing-eus-plan; "Shanghai to set up multi-billion-dollar fund to develop AI," Chinadaily.com, September 18, 2018, http://www.chinadaily.com.cn/a/201809/18/WS5ba0ade9a31033b4f4656be2.html; and "Beijing to build $2 billion AI research park: Xinhua," Reuters, January 3, 2018, https://www.reuters.com/article/us-china-artificial-intelligence/beijing-to-build-2-billion-ai-research-park-xinhua-idUSKBN1ES0B8.

12. "Alphabet Inc. Form 10-K," U.S. Securities and Exchange Commission, December 31, 2018, https://abc.xyz/investor/static/pdf/20180204_alphabet_10K.pdf?cache=11336e3; "2018 Annual Report," IBM, 2018, https://www.ibm.com/annualreport/assets/downloads/IBM_Annual_Report_2018.pdf; "Annual Report 2018," Microsoft, October 2018, https://www.microsoft.com/en-us/annualreports/ar2018/annualreport; "Facebook Inc. Form 10-K," U.S. Securities and Exchange Commission, December 31, 2018, http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/a109a501-ed16-4962-a3af-9cd16521806a.pdf; "Facebook Research and Development Expenses 2009-2019 | FB," Macrotrends.net, https://www.macrotrends.net/stocks/charts/FB/facebook/research-development-expenses; and "2018 Annual Report," Amazon, 2018, https://ir.aboutamazon.com/static-files/0f9e36b1-7e1e-4b52-be17-145dc9d8b5ec.

13. "Alibaba Group Holding Limited Form 20-F," U.S. Securities and Exchange Commission, June 5, 2019, https://otp.investis.com/clients/us/alibaba/SEC/sec-show.aspx?Type=html&FilingId=13476929&CIK=0001577552&Index=10000; "Baidu Inc. Form 20-F," U.S. Securities and Exchange Commission, December 31, 2018, http://ir.baidu.com/static-files/4ce88b07-60fe-4561-9cc9-2b0e0ec9dfd6; and "2018 Annual Report," Tencent, 2018, https://www.tencent.com/en-us/articles/17000441554112592.pdf.

14. Karen Hao, "Three charts show how China's AI industry is propped up by three companies," Technologyreview.com, January 22, 2019, https://www.technologyreview.com/s/612813/the-future-of-chinas-ai-industry-is-in-the-hands-of-just-three-companies/.

15. "AI in Europe: Funding Hits €20 Billion," Next Generation Internet (NGI) Initiative, January 8, 2019, https://www.ngi.eu/news/2019/01/08/ai-in-europe-funding-hits-e20-billion/; Julia Fioretti, "EU to invest 1.5 billion euros in AI to catch up with US, Asia," Reuters, April 25, 2018, https://www.reuters.com/article/us-eu-artificialintelligence/eu-to-invest-1-5-billion-euros-in-ai-to-catch-up-with-us-asia-idUSKBN1HW1WL.

16. Dion Rabouin, "The world is catching up on AI," Axios.com, July 29, 2019, https://www.axios.com/us-share-artificial-intelligence-investment-cdf9bf0f-d036-4b21-b96b-7ab2e2d8332a.html; "China is Starting to Edge Out The US In AI Investment," CBInsights.com, February 12, 2019, https://www.cbinsights.com/research/china-artificial-intelligence-investment-startups-tech/; and Jeff Loucks, Susanne Hupfer, David Jarvis, and Timothy Murphy, "Future in the balance? How countries are pursuing an AI advantage," Deloitte.com, May 1, 2019, https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/ai-investment-by-country.html.

17. Jeb Su, "Venture Capital Funding for Artificial Intelligence Startups Hit Record High in 2018," *Forbes,* February 12, 2019, https://www.forbes.com/sites/jeanbaptiste/2019/02/12/venture-capital-funding-for-artificial-intelligence-startups-hit-record-high-in-2018/#2cdb3e0b41f7.

18. "Research and development expenditure (% of GDP), 1996-2017," The World Bank, 2017, https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS.

19. "Research and Development: U.S. Trends and International Comparisons" in *Science and Engineering Indicators 2018,* NSB-2018-1, National Science Foundation, January 2018, https://www.nsf.gov/statistics/2018/nsb20181/report/sections/research-and-development-u-s-trends-and-international-comparisons/highlights.

20. "National Science Board Statement on Global Research and Development (R&D) Investments NSB-2018-9," National Science Board news release, February 7, 2018, https://www.nsf.gov/nsb/news/news_summ.jsp?cntn_id=244465.

21. YiLi Chien, "What Drives Long-Run Economic Growth?" Federal Reserve Bank of St. Louis, June 1, 2015, https://www.stlouisfed.org/on-the-economy/2015/june/what-drives-long-run-economic-growth.

22. Sheila Campbell and Chad Shirley, "Estimating the Long-Term Effects of Federal R&D Spending: CBO's Current Approach and Research Needs," Congressional Budget Office, June 21, 2018, https://www.cbo.gov/publication/54089.

23. Svetlana Sokolov-Mladenović, Slobodan Cvetanović, and Igor Mladenović, "R&D expenditure and economic growth: EU28 evidence for the period 2002–2012," *Economic Research-Ekonomska Istraživanja*, 29 no. 1 (April 2016), https://www.tandfonline.com/doi/full/10.1080/1331677X.2016.1211948.

24. The Bayh-Dole Act, the Stevenson-Wydler Technology Innovation Act, and the Federal Technology Transfer Act of 1986.

25. Wendy H. Schacht, "The Bayh-Dole Act: Selected Issues in Patent Policy and the Commercialization of Technology," Congressional Research Service, December 3, 2012, https://fas.org/sgp/crs/misc/RL32076.pdf.

26. 35 U.S.C. § 207, "Domestic and foreign protection of federally owned inventions," https://www.govinfo.gov/content/pkg/USCODE-2011-title35/pdf/USCODE-2011-title35-partII-chap18.pdf.

27. "18. Research and Development," in *An American Budget: Analytical Perspectives*, Office of Management and Budget, Fiscal Year 2019, https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_18_research-fy2019.pdf.

28. "21. Research and Development," in *An American Budget: Analytical Perspectives*, Office of Management and Budget, Fiscal Year 2019, https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_21_research-fy2020.pdf.

29. "Manhattan Project," Wikipedia, https://en.wikipedia.org/wiki/Manhattan_Project.

30. "How much did the Apollo program cost?" The Planetary Society, http://www.planetary.org/get-involved/be-a-space-advocate/become-an-expert/cost-of-apollo-program.html.

31. Increased government support for AI research in academia is discussed further in the section "Harness America's Talent Pipeline."

32. Yair Holtzman, "U.S. Research and Development Tax Credit," *The CPA Journal,* October 2017, https://www.cpajournal.com/2017/10/30/u-s-research-development-tax-credit/.

33. Project Open Data, "Open Data Policy—Managing Information as an Asset," Project Open Data,, https://project-open-data.cio.gov/.

34. Stacy Stanford, "The Best Public Datasets for Machine Learning and Data Science," Medium.com, October 2, 2018, https://medium.com/towards-artificial-intelligence/the-50-best-public-datasets-for-machine-learning-d80e9f030279.

35. "Worldwide R&D Incentives Guide: 2018," EY.com, December 31, 2018, https://www.ey.com/Publication/vwLUAssets/ey-worldwide-rd-incentives-reference-guide-2018/$FILE/ey-worldwide-rd-incentives-reference-guide-2018.pdf.

36. See "How Taxes Affect the Incentive to Invest in New Intangible Assets," Congressional Budget Office, November 2018, https://www.cbo.gov/system/files/2018-11/54648-Intangible_Assets.pdf.

37. Fiona Alexander, "U.S. Joins with OECD in Adopting Global AI Principles," National Telecommunications and Information Administration, May 22, 2019, https://www.ntia.doc.gov/blog/2019/us-joins-oecd-adopting-global-ai-principles.

38. Tim Dutton, "An Overview of National AI Strategies," Medium.com, June 28, 2018, https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

39. "Prize Challenges," Defense Advanced Research Projects Agency, https://www.darpa.mil/work-with-us/public/prizes; "AI to Solve the World's Grand Challenges," XPRIZE Foundation, https://www.xprize.org/prizes/artificial-intelligence.

40. National Science & Technology Council Committee on STEM Education, *Charting a Course for Success: America's Strategy for STEM Education*, December 2018, https://www.whitehouse.gov/wp-content/uploads/2018/12/STEM-Education-Strategic-Plan-2018.pdf; and Megan Smith, "Computer Science For All," The White House, January 30, 2016, https://obamawhitehouse.archives.gov/blog/2016/01/30/computer-science-all.

41. Jacob Kastrenakes, "What happened to Obama's $4 billion in computer science funding?" Theverge.com, December 11, 2016, https://www.theverge.com/2016/12/11/13849766/obama-computer-science-for-all-funding.

42. "President Trump Signs Presidential Memo to Increase Access to STEM and Computer Science Education," Office of Science and Technology Policy, September 25, 2017, https://www.whitehouse.gov/articles/president-trump-signs-presidential-memo-increase-access-stem-computer-science-education/.

43. Code.org, "US Dept of Education Prioritizes Computer Science Funding," Medium.com, February 4, 2019, https://medium.com/@codeorg/us-dept-of-education-prioritizes-computer-science-funding-64d47807d1dc.

44. Baobao Zhang and Allan Dafoe, "General attitudes toward AI," in *Artificial Intelligence: American Attitudes and Trends,* (Center for the Governance of AI, Future of Humanity Institute, University of Oxford, January 2019), https://governanceai.github.io/US-Public-Opinion-Report-Jan-2019/general-attitudes-toward-ai.html.

45. Cade Metz, "When the A.I. Professor Leaves, Students Suffer, Study Says," *The New York Times,* September 6, 2019, https://www.nytimes.com/2019/09/06/technology/when-the-ai-professor-leaves-students-suffer-study-says.html; and Michael Gofman and Zhao Jin, "Artificial Intelligence, Human Capital, and Innovation," August 20, 2019, http://gofman.info/AI/AI_GofmanZhao.pdf.

46. Daniela Hernandez and Rachael King, "Universities' AI Talent Poached by Tech Giants," *The Wall Street Journal,* November 24, 2016, https://www.wsj.com/articles/universities-ai-talent-poached-by-tech-giants-1479999601.

47. Hernandez and King, "Universities' AI Talent Poached by Tech Giants."

48. Gofman and Jin, "Artificial Intelligence, Human Capital, and Innovation."

49. Roberta Kwok, "Junior AI researchers are in demand by universities and industry," *Nature International Journal of Science,* April 23, 2019, https://www.nature.com/articles/d41586-019-01248-w; and Ariel Procaccia, "Tech Giants,

Gorging on AI Professors Is Bad for You," Bloomberg.com, January 7, 2019, https://www.bloomberg.com/opinion/articles/2019-01-07/tech-giants-gorging-on-ai-professors-is-bad-for-you.

50. Hernandez and King, "Universities' AI Talent Poached by Tech Giants"; and Procaccia, "Tech Giants, Gorging on AI Professors Is Bad for You."

51. *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*, National Science & Technology Council's Select Committee on Artificial Intelligence, June 2019, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

52. Kate Stringer, "How the tech industry created a teaching corps for rural schools," Fastcompany.com, June 8, 2019, https://www.fastcompany.com/90361450/how-the-tech-industry-created-a-teaching-corps-for-rural-schools.

53. National Science & Technology Council's Committee on STEM Education, *Charting a Course for Success: America's Strategy for STEM Education*.

54. *Charting a Course for Success*; Smith, "Computer Science For All."

55. Stringer, "How the tech industry created a teaching corps for rural schools."

56. Kastrenakes, "What happened to Obama's $4 billion in computer science funding?"

57. Susan Decker and Alexandre Tanzi, "In Tech Race With China, U.S. Universities May Lose a Vital Edge," Bloomberg.com, March 1, 2019, https://www.bloomberg.com/news/articles/2019-03-01/in-tech-race-with-china-u-s-universities-may-lose-a-vital-edge.

58. Hannah Knowles, "CS research shifting toward industry," Stanforddaily.com, February 12, 2016, https://www.stanforddaily.com/2016/02/12/cs-research-shifting-toward-industry/.

59. Karen Hao, "Training a single AI model can emit as much carbon as five cars in their lifetimes," Technologyreview.com, June 6, 2019, https://www.technologyreview.com/s/613630/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/.

60. Sarah McBride, "One quarter of U.S. tech start-ups founded by an immigrant: study," Reuters, October 2, 2012, https://www.reuters.com/article/us-immigrants-startups-study-idUSBRE8910I020121002; Ian Hathaway, "Almost half of Fortune 500 companies were founded by American immigrants or their children," Brookings Institution, December 4, 2017, https://www.brookings.edu/blog/the-avenue/2017/12/04/almost-half-of-fortune-500-companies-were-founded-by-american-immigrants-or-their-children/; and "The 'New American' Fortune 500," Partnership for a New American Economy, June 2011, https://www.newamericaneconomy.org/sites/all/themes/pnae/img/new-american-fortune-500-june-2011.pdf.

61. Joy Dantong Ma, "The AI Race is Wide Open, If America Remains Open," MacroPolo.com, April 15, 2019, https://macropolo.org/us-china-ai-race-talent/.

62. "What does the S&E job market look like for U.S. graduates?" STEM Education Data—-National Science Foundation, https://www.nsf.gov/nsb/sei/edTool/data/workforce-03.html; and Ma, "The AI Race is Wide Open."

63. Remco Zwetsloot, Roxanne Heston, Zachary Arnold, "Strengthening the U.S. AI Workforce: A Policy and Research Agenda," Center for Security and Emerging Technology, September 2019, https://cset.georgetown.edu/wp-content/uploads/CSET-Strengthening-the-U.S.-AI-Workforce.pdf.

64. Frank J. Cilluffo and Sharon L. Cardash, "Unintended consequence: Federal cybersecurity workforce a potential casualty of the shutdown," Thehill.com, January 22, 2019, https://thehill.com/opinion/cybersecurity/426371-unintended-consequence-federal-cybersecurity-workforce-a-potential; and William Crumpler and James A. Lewis, "The Cybersecurity Workforce Gap," Center for Strategic and International Studies, January 2019, https://www.csis.org/analysis/cybersecurity-workforce-gap.

65. "Deloitte & Ella the Engineer Join Forces in New Comic Book Series to Spur Student Interest in STEM," Deloitte press release, February 26, 2019, https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-ellaengineer-comic-book-collab-stem.html.

66. Krishnadev Calamur, "The U.S. System for 'Skilled' Migrants Is Broken," *The Atlantic,* May 17, 2019, https://www.theatlantic.com/international/archive/2019/05/us-visa-system-skilled-migrants/589615/.

67. Neil G. Ruiz, "Key facts about the U.S. H-1B visa program," Pew Research Center, April 27, 2017, https://www.pewresearch.org/fact-tank/2017/04/27/key-facts-about-the-u-s-h-1b-visa-program/; and Calamur, "The U.S. System for 'Skilled' Migrants Is Broken."

68. NFAP Policy Brief, "H-1B Visas By the Numbers: 2017-2018," National Foundation for American Policy, April 2018, https://nfap.com/wp-content/uploads/2018/04/H-1B-Visas-By-The-Number-FY-2017.NFAP-Policy-Brief.April-2018.pdf.

69. Ruiz, "Key facts about the U.S. H-1B visa program."

70. Ruiz, "Key facts about the U.S. H-1B visa program."

71. NFAP Policy Brief, "H-1B Denial Rates: Past and Present," National Foundation for American Policy, April 2019, https://nfap.com/wp-content/uploads/2019/04/H-1B-Denial-Rates-Past-and-Present.NFAP-Policy-Brief.April-2019.pdf.

72. U.S. Citizenship and Immigration Services, "Buy American and Hire American: Putting American Workers First," USCIS.gov, https://www.uscis.gov/legal-resources/buy-american-hire-american-putting-american-workers-first. Since taking office in 2016, several of the Trump administration's immigration policies have made legal high-skilled immigration increasingly difficult. In January 2017, President Trump signed an executive order instructing the U.S. Department of State to suspend the U.S. Visa Interview Waiver Program, which allows frequent U.S. visitors to renew U.S. travel authorities without an in-person interview with a U.S. consular officer. In October 2017, the USCIS instructed its officers to "apply the same level of scrutiny" to H-1B extension requests that it does for initial H-1B petitions. This change increased the number of cases that must be reviewed by a USCIS officer, in turn causing processing delays. In May 2018, the U.S. Department of Homeland Security proposed removing the International Entrepreneur Rule (IER), an executive order signed by the Obama administration, which was set to begin in June 2017. The IER would have allowed immigrant entrepreneurs to remain in the U.S. for two and a half years to create a new company, with the possibility for extension if the company met certain metrics. Since 2017, the Trump administration has proposed eliminating the H-4 EAD Program, which grants work permits to spouses of H-1B visa holders. In the administration's spring 2019 regulatory agenda, it reiterated its call to eliminate this program. The removal of the H-4 EAD Program would impact an estimated 100,000 spouses who have obtained work permits. David Yanofsky, "Trump just made it harder for tourists to visit the US," Qz.com, January 27, 2017, https://qz.com/895149/trump-is-suspending-the-visa-interview-waiver-program/; "USCIS Updates Policy to Ensure Petitioners Meet Burden of Proof for Nonimmigrant Worker Extension Petitions," U.S. Citizenship and Immigration Services, https://www.uscis.gov/news/news-releases/uscis-updates-policy-ensure-petitioners-meet-burden-proof-nonimmigrant-worker-extension-petitions; "Removal of International Entrepreneur Parole Program; Proposed rule," 83 *Federal Register* 24415 (May 29, 2018), 24415-24427, https://www.federalregister.gov/documents/2018/05/29/2018-11348/removal-of-international-entrepreneur-parole-program; Jonathan Shieber, "Department of Homeland Security moves to finally rescind the International Entrepreneur Rule," TechCrunch.com, May 28, 2018, https://techcrunch.com/2018/05/28/department-of-homeland-security-moves-to-finally-rescind-the-international-entrepreneur-rule/; Stuart Anderson, "New Details and Problems Emerge With Trump Immigration Plan," Forbes.com, May 24, 2019, https://www.forbes.com/sites/stuartanderson/2019/05/24/new-details-and-problems-emerge-with-trump-immigration-plan/#1e2d6bf871f0; "Spring 2019 Unified Agenda of Regulatory and Deregulatory Actions," Office of Information and Regulatory Affairs, https://www.reginfo.gov/public/do/eAgendaMain; and Miriam Jordan, "Thousands of Indian Women Find Their American Dreams in Jeopardy," *The New York Times,* April 6, 2018, https://www.nytimes.com/2018/04/06/us/indians-h1b-visas-trump-immigration-wives.html.

73. Issie Lapowsky, "Visa Rejections for Tech Workers Spike Under Trump," Wired.com, April 25, 2019, https://www.wired.com/story/h-1b-visa-rejections-spike-under-trump/.

74. NFAP Policy Brief, "H-1B Denials and Requests for Evidence Increase Under the Trump Administration," National Foundation for American Policy, July 2018, https://nfap.com/wp-content/uploads/2018/07/H-1B-Denial-and-RFE-Increase.NFAP-Policy-Brief.July-2018.pdf.

75. Neil G. Ruiz and Abby Budiman, "Number of foreign college graduates staying in U.S. to work climbed again in 2017, but growth has slowed," Pew Research Center, July 25, 2018, https://www.pewresearch.org/fact-tank/2018/07/25/number-of-foreign-college-graduates-staying-in-u-s-to-work-climbed-again-in-2017-but-growth-has-slowed/.

76. Laura D. Francis, "Republican Lawmaker Pushing to End Foreign Grad Training Program," *Bloomberg Law,* June 12, 2019, https://news.bloomberglaw.com/daily-labor-report/republican-lawmaker-pushing-to-end-foreign-grad-training-program; and Stuart Anderson, "Latest on the Court Cases that Could Restrict Immigration, OPT, and H-1B Spouses," Forbes.com, July 10, 2019, https://www.forbes.com/sites/stuartanderson/2019/07/10/latest-on-the-court-cases-that-could-restrict-immigration-opt-and-h-1b-spouses/#12a57c1c44e3.

77. Ruiz and Budiman, "Number of foreign college graduates staying in U.S. to work climbed again in 2017, but growth has slowed."

78. Neil G. Ruiz and Abby Budiman, "Number of Foreign College Students Staying and Working in U.S. After Graduation Surges," Pew Research Center, May 10, 2018, https://www.pewresearch.org/global/2018/05/10/number-of-foreign-college-students-staying-and-working-in-u-s-after-graduation-surges/.

79. "2015 Doctorate Recipients from U.S. Universities," National Center for Science and Engineering Statistics, National Science Foundation, June 2017, https://www.nsf.gov/statistics/2017/nsf17306/static/report/nsf17306.pdf.

80. Matt Sheehan, "Chinese AI Talent in Six Charts," MacroPolo.org, May 28, 2019, https://macropolo.org/china-ai-research-talent-data/; and Matt Sheehan, "Who Loses from Restricting Chinese Student Visas?," MacroPolo.org, May 31, 2018, https://macropolo.org/who-loses-from-restricting-chinese-student-visas/.

81. Luke Kelly, "How China is Winning Back More Graduates from Foreign Universities than Ever Before," Forbes.com, January 25, 2018, https://www.forbes.com/sites/ljkelly/2018/01/25/how-china-is-winning-back-more-graduates-from-foreign-universities-than-ever-before/#52681e015c1e.

82. Sheehan, "Who Loses from Restricting Chinese Student Visas?"

83. NFAP Policy Brief, "H-1B Visas by the Numbers: 2017–2018."

84. Exact numbers for the AI talent pool both in the U.S. and abroad are difficult to quantify. In a 2017 report, Tencent estimated around 300,000 AI researchers and practitioners were employed in the industry, while the market demand for AI researchers was over one million. In Jean-Francois Gagné's 2019 Global AI Talent Report, he estimates a much lower figure at approximately 36,524 AI specialists worldwide. James Vincent, "Tencent says there are only 300,000 AI engineers worldwide, but millions are needed," Theverge.com, December 5, 2017, https://www.theverge.com/2017/12/5/16737224/global-ai-talent-shortfall-tencent-report; Jean-François Gagné, Grace Kiser, and Yoan Mantha, "Global AI Talent Report 2019,"JF Gagné, April 2019, https://jfgagne.ai/talent-2019/; "Report: Top 10 AI Jobs, Salaries and Cities," blog on Indeed.com, June 28, 2019, http://blog.indeed.com/2019/06/28/top-10-ai-jobs-salaries-cities/; Ann Saphir, "As companies embrace AI, it's a job-seeker's market," Reuters, October 15, 2018, https://www.reuters.com/article/us-usa-economy-artificialintelligence/as-companies-embrace-ai-its-a-job-seekers-market-idUSKCN1MP10D; and Bernard Marr, "The AI Skills Crisis and How to Close the Gap," Forbes.com, June 25, 2018, https://www.forbes.com/sites/bernardmarr/2018/06/25/the-ai-skills-crisis-and-how-to-close-the-gap/#17d80e1b31f3.

85. Caleb Watney, "To win the AI race, we need more humans," Thehill.com, August 14, 2018, https://thehill.com/opinion/cybersecurity/401773-to-win-the-ai-race-we-need-more-humans.

86. NFAP Policy Brief, "H-1B Visas By the Numbers: 2017-2018."

87. "Schedule A," U.S. Immigration Visa Center, http://www.us-immigrationvisa.com/immigration/employment-immigration/labor-certification/schedule-a; "Labor Certification for the Permanent Employment of Aliens in the United States; and Implementation of New System; and Proposed Rule," 20 *Federal Register* 656 (May 6, 2002), 30468-30469, https://www.govinfo.gov/content/pkg/FR-2002-05-06/pdf/02-10570.pdf.

88. Occupations under Schedule A authority are able to forgo the PERM Labor Certification process and proceed directly with the I-140 filing process with USCIS. The PERM Labor Certification is the first step in obtaining employment-based permanent residency and is a way for the Department of Labor to ensure there are insufficient US workers available to fill the available position. The I-140 filing process is the second step in the permanent residency process. Maggio Kattar, "The Three Stages of Employer Sponsored Permanent Residence via PERM," Maggio-kattar.com, https://maggio-kattar.com/three-stages-employer-sponsored-permanent-residence-perm/.

89. Thomas L. Friedman, "Invent, Invent, Invent," *The New York Times,* June 27, 2009, https://www.nytimes.com/2009/06/28/opinion/28friedman.html. Employee sponsorship and a higher-than-median salary are components of the pending Keep STEM Talent Act of 2019, introduced on October 4, 2019, in the House (H.R.4623) and Senate (S.1744). These stipulations could unintentionally disadvantage start-up companies and result in unintended wage disparities. U.S. Congress, House, *Keep STEM Talent Act of 2019,* H.R. 4623, 116th Cong., 1st sess., introduced in House October 8, 2019, https://www.congress.gov/bill/116th-congress/house-bill/4623/text; and U.S. Congress, Senate, *Keep STEM Talent Act of 2019,* S. 1744, 116th Cong., 1st sess., introduced in Senate June 5, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/1744/text.

90. F-prime is a nod to the F-1 student visa, which is a single intent visa. This means the foreign student intends to return to their home country upon completion of their academic program. Dual intent denotes that the foreign student will formally immigrate to the United States upon graduation from the approved academic program and obtain conditional permanent residency.

91. The program participant would be subject to periodic reinvestigations throughout the duration of the program for counterintelligence purposes. In the event of an early termination of the agreement by the program participant, a fine and visa restrictions would be imposed.

92. See John J. Fialka, *War by Other Means: Economic Espionage in America* (New York: W.W. Norton & Company, 1999).

93. "Suburban Chicago Woman Sentenced to Four Years in Prison for Stealing Motorola Trade Secrets Before Boarding Plane to China," U.S. Attorney's Office—Northern District of Illinois, Federal Bureau of Investigation, August 29, 2012, https://archives.fbi.gov/archives/chicago/press-releases/2012/suburban-chicago-woman-sentenced-to-four-years-in-prison-for-stealing-motorola-trade-secrets-before-boarding-plane-to-china; Rachel Lerman, "Jury awards T-Mobile $4.8M in trade-secrets case against Huawei," *The Seattle Times,* May 28, 2017, https://www.seattletimes.com/business/technology/july-awards-t-mobile-48m-in-trade-secrets-case-against-huawei/; "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investment in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," *Defense Innovation Unit Experimental (DIUx),* January 2018, https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf; and "Preventing Loss of Academic Research," Counterintelligence Strategic Partnership Intelligence Note (SPIN), Federal Bureau of Investigation, June 2015, https://info.publicintelligence.net/FBI-SPIN-ProtectingAcademicResearch.pdf.

94. "FBI has 1,000 investigations into Chinese intellectual property theft, director Christopher Wray says, calling China the most severe counter-intelligence threat to US," Agence France-Presse, July 24, 2019, https://www.scmp.com/news/china/article/3019829/fbi-has-1000-probes-chinese-intellectual-property-theft-director.

95. "National Security Strategy of the United States of America," the White House, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

96. U.S. Congress, "Title XVII - Review of Foreign Investment and Export Controls," in *John S. McCain National Defense Authorization Act for Fiscal Year 2019,* January 3, 2018, H.R. 5515, 115th Cong., 2nd sess., https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf.

97. Eric Rosenbaum, "1 in 5 corporations say China has stolen their IP within the last year: CNBC CFO survey," CNBC.com*,* March 1, 2019, https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html.

98. "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," update to the IP Commission Report, Commission on the Theft of American Intellectual Property, February 2017, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

99. "The Theft of American Intellectual Property."

100. Andrew Martins, "Cyberattacks and Your Small Business: A Primer for Cybersecurity," *Business News Daily,* August 21, 2019, https://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html.

101. "Protecting Critical Infrastructure," DHS.gov, https://www.dhs.gov/cisa/protecting-critical-infrastructure.

102. "DHS Needs to Improve Cybersecurity Workforce Planning," U.S. Department of Homeland Security Office of Inspector General, OIG-19-62, September 23, 2019, https://www.oig.dhs.gov/sites/default/files/assets/2019-09/OIG-19-62-Sep19.pdf.

103. "Open Hearing on Worldwide Threats," statement of Daniel Coats, Michael Pompeo, Admiral Michael Rogers, Robert Ashley, Christopher Wray, and Robert Cardillo, February 13, 2018, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0#; Jane Perlez, "F.B.I. Bars Some China Scholars From Visiting U.S. Over Spying Fears," *The New York Times,* April 14, 2019, https://www.nytimes.com/2019/04/14/world/asia/china-academics-fbi-visa-bans.html; Lee C. Bollinger, "No, I won't start spying on my foreign-born students," *The Washington Post*, August 30, 2019, https://www.washingtonpost.com/opinions/no-i-wont-start-spying-on-my-foreign-born-students/2019/08/29/01c80e84-c9b2-11e9-a1fe-ca46e8d573c0_story.html; Response from the UMich LSA Dean Andrew Martin, https://sites.lsa.umich.edu/indigo/wp-content/uploads/sites/529/2018/02/Response-from-the-LSA-Dean-Andrew-Martin.pdf; Wallace Loh, "UMD's commitment to international collaborations and the international community on campus," https://president.umd.edu/communications/statements/umds-commitment-international-collaborations-and-international-community; and Erin Doherty and Will Cassou, "Student Advocates Call for University Support in Response to Anti-China Rhetoric," TheHoya.com, February 23, 2018, https://www.thehoya.com/student-advocates-call-university-support-response-anti-china-rhetoric.

104. Bollinger, "No, I won't start spying on my foreign-born students."

105. Ma, "The AI Race Is Wide Open, If America Remains Open"; and Sheehan, "Chinese AI Talent in Six Charts."

106. Alex Joske, "Picking flowers, making honey: The Chinese military's collaboration with foreign universities," Australian Strategic Policy Institute, October 30, 2019, https://www.aspi.org.au/report/picking-flowers-making-honey.

107. Eggerton, "Senate Bill Limits Visas for Chinese Engineers, Scientists"; U.S. Congress, Senate, *People's Liberation Army (PLA) Visa Security Act*; and U.S. Congress, Senate, *Protect Our Universities Act of 2019*, S. 1879 116th Cong., 1st sess., introduced in Senate June 18, 2019, https://www.hawley.senate.gov/sites/default/files/2019-06/Bill%20Text%20-%20The%20Protect%20Our%20Universities%20Act%20of%202019.pdf.

108. Mary Sue Coleman and Peter McPherson, "Responding to Undue Foreign Influence and Security Concerns on Campus," memo, April 22, 2019, https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Science%20%26%20Security/AAU-APLU-Effective-Practices-Memo-and-Summary.pdf.

109. Eddie Johnson, Donald Beyer Jr., and Daniel Lipinski to Christopher Wray, May 10, 2018, https://www.whitehouse.gov/wp-content/uploads/2019/09/OSTP-letter-to-the-US-research-community-september-2019.pdf.

110. U.S. House of Representatives, *Securing American Science and Technology Act of 2019,* H.R.3038, 116th Cong., 1st sess, https://www.congress.gov/bill/116th-congress/house-bill/3038.

111. A survey of 40 universities from the AAU and APLU outlined existing measures at some universities to mitigate technology theft. Measures included improved data security, conflict of interest reporting, intellectual property and technology control plans, and faculty foreign travel assistance, among others. Researchers and students on travel abroad should adopt best practices such as using virtual private networks (VPN), encrypted email and text messaging apps, and receive pre-travel counterintelligence briefings. See https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Science%20%26%20Security/AAU-APLU-Effective-Practices-Memo-and-Summary.pdf.

112. Eddie Johnson, Donald Beyer Jr., and Daniel Lipinski to Christopher Wray, May 10, 2018.

113. Ted Mitchel to Christopher Wray, April 24, 2018, https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Letter-FBI-NSHEAB.pdf.

114. "Scholars or Spies: Foreign Plots Targeting America's Research and Development," Joint Statement of the American Council on Education, Association of American Universities, Association of Public and Land-grant Universities and the Council on Governmental Relations, April 11, 2018, https://www.acenet.edu/Documents/Community-Statement-House-SST-Committee-Hearing.pdf.

115. Eddie Johnson, Donald Beyer Jr., and Daniel Lipinski to Christopher Wray, May 10, 2018.

116. "FBI Director Appoints National Security Higher Education Advisory Board," Federal Bureau of Investigation press release, September 15, 2005, https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-appoints-national-security-higher-education-advisory-board; https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Letter-FBI-NSHEAB.pdf.

117. Jade Leung, Sophie-Charlotte Fischer, and Allan Dafoe, "Export Controls in the Age of AI," WarontheRocks.com, August 28, 2019, https://warontherocks.com/2019/08/export-controls-in-the-age-of-ai.

118. Stephen Chen, "Google denies link to China's military over touch-screen tools that may help PLA pilots," *South China Morning Post,* July 4, 2019, https://www.scmp.com/news/china/science/article/3017141/google-denies-link-chinas-military-over-touch-screen-tools-may.

119. Tim Hwang, "Computational Power and the Social Impact of Artificial Intelligence," available at SSRN, March 23, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3147971, 15.

120. President Donald J. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence," the White House, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

121. "Frontier: Center For Accelerated Application Readiness," Oak Ridge National Laboratory, https://www.olcf.ornl.gov/frontier-center-for-accelerated-application-readiness/.

122. "Designing Chips for Real Time Machine Learning," Darpa.mil, March 21, 2019, https://www.darpa.mil/news-events/2019-03-21.

123. "Trusted Accreditation," Dmea.osd.mil, https://www.dmea.osd.mil/trustedic.html; and Marie A. Mak, "Trusted Defense Microelectronics: Future Access and Capabilities Are Uncertain," Gao.gov, October 28, 2015, https://www.gao.gov/assets/680/673401.pdf.

124. Doug Cameron, "Pentagon Hires Foreign Chips Supplier," *The Wall Street Journal,* June 5, 2016, https://www.wsj.com/articles/pentagon-takes-foreign-chips-partner-1465159332.

125. Hwang, "Computational Power and the Social Impact of Artificial Intelligence," 25; https://www.gao.gov/assets/680/673401.pdf.

126. Cameron, "Pentagon Hires Foreign Chips Supplier."

127. Hwang, "Computational Power and the Social Impact of Artificial Intelligence," 26.

128. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update," Select Committee on Artificial Intelligence of the National Science & Technology Council, June 2019, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf; https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

129. "Frontier," Oak Ridge National Laboratory, https://www.olcf.ornl.gov/frontier.

130. Nick Pandolfo, "As some schools plunge into technology, poor schools are left behind," HechingerReport.org, January 24, 2012, https://hechingerreport.org/as-some-schools-plunge-into-technology-poor-schools-are-left-behind.

131. Dan H., "How much did AlphaGo Zero cost?" Yuzeh.com, https://www.yuzeh.com/data/agz-cost.html.

132. Jeffrey Shek, "Takeaways from OpenAI Five (2019)," Towards Data Science on Medium.com, April 23, 2019, https://towardsdatascience.com/takeaways-from-openai-five-2019-f90a612fe5d.

133. "Enabling Access to Cloud Computing Resources for CISE Research and Education (Cloud Access)," NSF 19-510, https://www.nsf.gov/pubs/2019/nsf19510/nsf19510.htm.; and "Exploring Clouds for Acceleration of Science (E-CAS)," Nsf.gov, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1904444&HistoricalAwards=false.

134. Dario Amodei and Danny Hernandez, "AI and Compute," OpenAI.com, May 16, 2018, https://openai.com/blog/ai-and-compute.

135. "MGHPCC Fact Sheet," The Massachusetts Green High Performance Computing Center, http://www.mghpcc.org/about/mghpcc-fact-sheet.

136. "New Markets Tax Credit Program," Community Development Financial Institutions Fund, U.S. Department of the Treasury, https://www.cdfifund.gov/programs-training/Programs/new-markets-tax-credit/Pages/default.aspx.

137. "The Potential Impacts of the Made in China 2025 Roadmap on the Integrated Circuit Industries in the U.S., EU and Japan," working paper, U.S. International Trade Commission, August 2019, https://www.usitc.gov/publications/332/working_papers/id_19_061_china_integrated_circuits_technology_roadmap_final_080519_kim_verwey-508_compliant.pdf; Addition of Entities to the Entity List and Revision of an Entry on the Entity List, 84 Fed. Reg. 121 (June 24, 2019), https://www.federalregister.gov/documents/2019/06/24/2019-13245/addition-of-entities-to-the-entity-list-and-revision-of-an-entry-on-the-entity-list; Ana Swanson, Paul Mozur, and Steve Lohr, "U.S. Blacklists More Chinese Tech Companies Over National Security Concerns," *The New York Times,* June 21, 2019, https://www.nytimes.com/2019/06/21/us/politics/us-china-trade-blacklist.html; Ana Swanson and Paul Mozur, "U.S. Blacklists 28 Chinese Entities Over Abuses in Xinjiang," *The New York Times,* October 7, 2019, https://www.nytimes.com/2019/10/07/us/politics/us-to-blacklist-28-chinese-entities-over-abuses-in-xinjiang.html; and Department of Commerce, "Addition of Certain Entities to the Entity List," Richard Ashooh, 15 CFR Part 744, October 7, 2019, https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-22210.pdf.

138. John VerWey, "What's Causing U.S. Semiconductor Equipment Production and Exports to Grow?" Usitc.gov, January 2019, https://www.usitc.gov/publications/332/executive_briefings/ebot_john_verwey_semi_manufacturing_equipment_pdf.pdf.

139. "The Health and Competitiveness of the U.S. Semiconductor Manufacturing Equipment Industry," working paper, U.S. International Trade Commission, July 2019, https://www.usitc.gov/publications/332/working_papers/id_058_the_health_and_competitiveness_of_the_sme_industry_final_070219checked.pdf.

140. "Photoresist," Science Direct, https://www.sciencedirect.com/topics/engineering/photoresist; and Kiran Pulidindi and Soumalya Chakraborty, "Photoresist and Photoresist Ancillaries Market Size By Product," Global Market Insights, https://www.gminsights.com/industry-analysis/photoresist-and-photoresist-ancillaries-market.

141. "The Health and Competitiveness of the U.S. Semiconductor Manufacturing Equipment Industry."

142. Hwang, "Computational Power and the Social Impact of Artificial Intelligence," 21.

143. "Beyond Borders: The Global Semiconductor Value Chain," Semiconductor Industry Association and Nathan Associates, May 2016, 22, https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Beyond-Borders-Report-FINAL-June-7.pdf.

144. Doug Cameron, "Pentagon Hires Foreign Chips Supplier," *The Wall Street Journal*, June 5, 2016, https://www.wsj.com/articles/pentagon-takes-foreign-chips-partner-1465159332.

145. *U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy*, Congressional Research Service, R44544, June 27, 2016, https://fas.org/sgp/crs/misc/R44544.pdf; Hwang, "Computational Power and the Social Impact of Artificial Intelligence"; and John VerWey, "Global Value Chains: Explaining U.S. Bilateral Trade Deficits in Semiconductors," March 2018, https://www.usitc.gov/publications/332/executive_briefings/ebot-semiconductor_gvc_final.pdf?source=govdelivery.

146. "America's Semiconductors Supply Chain Faces Big Cybersecurity Risks," Manufacture This on AmericanManufacturing.org, March 23, 2017, http://www.americanmanufacturing.org/blog/entry/americas-semiconductors-supply-chain-faces-big-cybersecurity-risks.

147. Sherisse Pham, "Computer virus cripples top Apple supplier TSMC," CNN.com, August 6, 2018, https://money.cnn.com/2018/08/06/technology/tsmc-chip-supplier-virus/index.html.

148. "Beyond Borders: The Global Semiconductor Value Chain."

149. Kathrin Hille, "Taiwan to share Chinese hacks data with private companies," *Financial Times*, October 22, 2018, https://www.ft.com/content/e3e39f54-d5fc-11e8-ab8e-6be0dcf18713.

150. Samson Ellis, Yuan Gao, and Cindy Wang, "TSMC Ready to Spend $20 Billion on its Most Advanced Chip Plant," Bloomberg.com, October 6, 2017, https://www.bloomberg.com/news/articles/2017-10-06/tsmc-ready-to-spend-20-billion-on-its-most-advanced-chip-plant.

151. Jon Harper, "China Threatens Microelectronics Supply Chain, DoD Official Says," National Defense, December 19, 2017, https://www.nationaldefensemagazine.org/articles/2017/12/19/china-threatens-microelectronics-supply-chain-dod-official-says.

152. Charles Rollet and Sofiya Voznaya, "Western Academia Helps Build China's Automated Racism," CodaStory.com, August 6, 2019, https://codastory.com/authoritarian-tech/western-academia-china-automated-racism; and Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *The New York Times,* February 21, 2019, https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

153. Remco Zwetsloot and Allan Dafoe, "Thinking About Risks From AI: Accidents, Misuse and Structure," LawfareBlog.com, February 11, 2019, https://www.lawfareblog.com/thinking-about-risks-ai-accidents-misuse-and-structure.

154. Zwetsloot and Dafoe, "Thinking About Risks From AI."

155. "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense," Defense Innovation Board, October 2019, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

156. "OECD Principles on AI," Organisation for Economic Cooperation and Development, https://www.oecd.org/going-digital/ai/principles.

157. Michael Kratsios, "White House OSTP's Michael Kratsios Keynote on AI Next Steps" OECD Forum and Ministerial Council Meeting, Paris, May 21, 2019, https://usoecd.usmission.gov/white-house-ostps-michael-kratsios-keynote-on-ai-next-steps.

158. "China: 'Where Are They?'" Amnesty International, ASA 17/9113/2018, 2018, https://www.amnesty.org/download/Documents/ASA1791132018ENGLISH.PDF.

159. Darren Byler, "China's hi-tech war on its Muslim minority," *The Guardian*, April 11, 2019, https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.

160. "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance; and Yi Shu Ng, "China forces its Muslim minority to install spyware on their phones," Mashable.com, July 21, 2017, https://mashable.com/2017/07/21/china-spyware-xinjiang/#p2_q.Fw.DOqd.

161. Megha Rajagopalan, "They Thought They'd Left The Surveillance State Behind. They Were Wrong," BuzzFeedNews.com, July 9, 2018, https://www.buzzfeednews.com/article/meghara/china-uighur-spies-surveillance; "China: Voice Biometric Collection Threatens Privacy," HRW.org, October 22, 2017, https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy; and China: Police DNA Database Threatens Privacy," HRW.org, May 15, 2017, https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy.

162. Josh Chin and Clement Burge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal,* December 19, 2017, https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.

163. "How Mass Surveillance Works in Xinjiang, China," HRW.org, May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang.

164. Edward Schwarck, "Behind the Golden Shield: China Reforms Public Security Intelligence, *China Brief*, 17 no. 16 (December 8, 2017), https://jamestown.org/program/behind-golden-shield-china-reforms-public-security-intelligence; Oiwan Lam, "With 'Sharp Eyes', smartphones and TV sets are watching Chinese citizens," HongKongFP.com, April 8, 2018, https://www.hongkongfp.com/2018/04/08/sharp-eyes-smartphones-tv-sets-watching-chinese-citizens; and "China: Voice Biometric Collection Threatens Privacy."

165. Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism,"(Freedom House, October 2018), 9, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf; Shazeda Ahmed, Natasha Bajema, and Samuel Bendett, "AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," 73, https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf; Andrei Soldatov and Irina Borogan, "Putin brings China's Great Firewall to Russia in cybersecurity pact," *The Guardian*, November 29, 2016, https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact; Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html; and Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Hellped African Governments Spy on Political Opponents," *The Wall Street Journal,* August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

166. Lindsay Gorman and Matt Schrader, "U.S. Firms Are Helping Build China's Orwellian State," ForeignPolicy.com, March 19, 201i, https://foreignpolicy.com/2019/03/19/962492-orwell-china-socialcredit-surveillance; and Loretta Chao and Don Clark, "Cisco Poised to Help China Keep an Eye on Its Citizens," *The Wall Street Journal,* July 5, 2011, https://www.wsj.com/articles/SB10001424052702304778304576377141077267316.

167. "Draft U.S. Government Guidance for the Export of Hardware, Software and Technology with Surveillance Capabilities and/or Parts/Know-How," U.S. Department of State, https://www.state.gov/wp-content/uploads/2019/09/draft-guidance-for-the-export-of-hardware-software-and-technology-with-surveillance-capabilities.pdf.

168. "China-U.S. Export Controls," China Country Commercial Guide, Export.gov, last modified July 30, 2019, https://www.export.gov/apex/article2?id=China-U-S-Export-Controls.

169. "Menendez, Rubio, Colleagues Urge Strong Sanctions, Export Controls & Financial Disclosures to Counter Chinese Human Rights Abuses in Xinjiang," U.S. Senate Committee on Foreign Relations press release, April 4, 2019, https://www.foreign.senate.gov/press/ranking/release/menendez-rubio-colleagues-urge-strong-sanctions-export-controls-and-financial-disclosures-to-counter-chinese-human-rights-abuses-in-xinjiang.

170. "Addition of Certain Entities to the Entity List," Richard Ashooh, 15 CFR Part 744, Department of Commerce, October 7, 2019, https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-22210.pdf; and Jacob Pramuk, "US puts visa restrictions on Chinese officials over abuses of Muslims in Xinjiang," CNBC.com, October 8, 2019, https://www.cnbc.com/2019/10/08/us-puts-visa-restrictions-on-chinese-officials-over-abuses-of-muslims-in-xinjiang.html.

171. Jon Russell, "China's SenseTime, the world's highest-valued AI startup, closes $620M follow-on round," TechCrunch.com, May 30, 2018, https://techcrunch.com/2018/05/30/even-more-money-for-senstime-ai-china.

172. "The US Global Magnitsky Act: Questions And Answers," HRW.org, September 13, 2017, https://www.hrw.org/news/2017/09/13/us-global-magnitsky-act.

173. Hannah Miller, Richard Stirling, Yaera Chung, Sriganesh Lokanathan, Emma Martinho-Truswell, Joshua New, Isaac Rutenberg, and Fabrizio Scrollini, "Government Artificial Intelligence Readiness Index 2019," Oxford Insights, 2019, https://www.oxfordinsights.com/ai-readiness2019.

174. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update," the White House, June 2019, https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf; and President Donald J. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence," the White House, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

175. U.S. House of Representatives, *Foundations for Evidence-Based Policymaking Act of 2018*, H.R.4174, 115th Cong., introduced in House October 31, 2017, https://www.congress.gov/bill/115th-congress/house-bill/4174.

176. U.S. Congress, Senate, OPEN Government Data Act, S.2852, 114th Cong., introduced in Senate April 26, 2016, https://www.congress.gov/bill/114th-congress/senate-bill/2852.

177. "United States Digital Service Press Sheet," U.S. Digital Service, Spring 2019, https://www.usds.gov/assets/files/USDS-Press-Sheet.pdf.

178. "NIH Strategic Plan for Data Science," National Institutes of Health, June 2018, https://datascience.nih.gov/sites/default/files/NIH_Strategic_Plan_for_Data_Science_Final_508.pdf.

179. Loren DeJonge Schulman, "Managing the National Security Workforce Crisis," CNAS, May 2019, https://s3.amazonaws.com/files.cnas.org/documents/Key-Issues-for-Congress-Schulman-1.pdf?mtime=20190509150436.

180. Max Stier, President and CEO of the Partnership for Public Service, testimony to the Committee on Homeland Security and Government Affairs, Subcommittee on Regulatory Affairs and Federal Management, U.S. Senate, April 12, 2016, https://www.hsgac.senate.gov/imo/media/doc/Stier%20Statement.pdf.

181. Jared Serbu, "New DoD personnel system hires cyber workers faster, but numbers still small," FederalNewsNetwork.com, March 19, 2019, https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2019/03/new-dod-personnel-system-hires-cyber-workers-faster-but-numbers-small; and "Careers: Find Your Future at the JAIC," Joint Artificial Intelligence Center, https://www.ai.mil/careers.html.

182. "Start your cybersecurity career with the U.S. government," Scholarship for Service, U.S. Office of Personnel Management, https://www.sfs.opm.gov.

183. C. Todd Lopez, "Defense Digital Service Delivers Mission-Aligned Tech for DOD," Defense.gov, May 29, 2019, https://www.defense.gov/explore/story/Article/1858615/defense-digital-service-delivers-mission-aligned-tech-for-dod.

184. "Our Work," Department of Defense Digital Service, https://dds.mil/#our-work.

185. Dan Ward, "Vignette 5 – Kessel Run: The Future of Defense Acquisitions Is #AgileAF," 3 May 2019, https://media.defense.gov/2019/May/01/2002126684/-1/-1/0/VIGNETTE%205%20-%20KESSEL%20RUN,%20THE%20FUTURE%20OF%20DEFENSE%20ACQUISITION%20IS%20#AGILEAF.PDF.

186. "Department of Energy Announces $20 Million to Develop Artificial Intelligence and Machine Learning Tools," Department of Energy,, April 5, 2019, https://www.energy.gov/articles/department-energy-announces-20-million-develop-artificial-intelligence-and-machine-learning.

187. Megan Lamberth, "The White House and Defense Department unveiled AI strategies. Now what?" C4ISRNET.com, February 27, 2019, https://www.c4isrnet.com/opinion/2019/02/27/the-white-house-and-defense-department-unveiled-ai-strategies-now-what.

188. "Improving the Management of IT Acquisitions and Operations," GAO.gov, https://www.gao.gov/highrisk/improving_management_it_acquisitions_operations/why_did_study#t=0.

189. Defense Innovation Board, "Software Acquisition and Practices (SWAP) Study," Defense.gov, https://innovation.defense.gov/software/.

190. Peter Modigliani, "6 Key Acquisition Provisions in the FY20 NDAA Bills," Mitre.org, July 9, 2019, https://aida.mitre.org/blog/2019/07/09/fy20-ndaa/.

191. "DoD Cloud Strategy," Department of Defense, December 2018, https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF.

192. "Data Center Optimization Initiative (DCOI)," White House memo August 1, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_19_1.pdf; "Improving the Management of IT Acquisitions and Operations"; and "DoD Cloud Strategy."

193. "Data Center Optimization Initiative (DCOI)," the White House, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_19_1.pdf.

194. "How America's 4g Leadership Propelled The U.S. Economy," *Recon Analytics*, April 16, 2018, https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.

195. "U.S. Leadership In AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools," National Institute of Standards and Technology, August 9, 2019,

https://www.nist.gov/sites/default/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

196. "NIST Releases Draft Plan for Federal Engagement in AI Standards Development," National Institute of Standards and Technology,, July 2, 2019, https://www.nist.gov/news-events/news/2019/07/nist-releases-draft-plan-federal-engagement-ai-standards-development.

197. ISO/IEC JTC 1/SC 42 Artificial intelligence, 2017, https://www.iso.org/committee/6794475.html.

198. Olga Russakovsky, Jia Deng, and Hao Su, "ImageNet Large Scale Visual Recognition Challenge," IJCV, 2015, http://image-net.org/challenges/LSVRC/.

199. SuperGLUE, https://super.gluebenchmark.com/.

200. The AI Index Report, 2018, https://aiindex.org/.

201. "Computational creativity," Wikipedia, https://en.wikipedia.org/wiki/Computational_creativity; Martin Mumford and Dan Ventura, "The man behind the curtain: Overcoming skepticism about creative computing," June 2015, http://axon.cs.byu.edu/ICCC2015proceedings/1.1Mumford.pdf; and Christian Guckelsberger, Christoph Salge, and Simon Colton, "Addressing the 'Why?' in Computational Creativity: A Non-Anthropocentric, Minimal Model of Intentional Creative Agency," http://ccg.doc.gold.ac.uk/wp-content/uploads/2017/05/iccc2017_guckelsberger.pdf.

202. Josua Batson, "Forget the Turing Test: Here's How We Could Actually Measure AI," Wired.com, June 12, 2014, https://www.wired.com/2014/06/beyond-the-turing-test/; and Skye Pathare, "How do you measure artificial intelligence?" Blog.bynder.com, May 25, 2018, https://blog.bynder.com/en/how-do-you-measure-artificial-intelligence/.

203. Keisuke Sakaguchi, Ronan Le Bras, and Chandra Bhagavatula, "WINOGRANDE: An Adversarial Winograd Schema Challenge at Scale," July 24, 2019, https://arxiv.org/pdf/1907.10641.pdf.

204. Office of Science and Technology Policy NSTC, https://www.whitehouse.gov/ostp/nstc/.

205. "Charter of the Subcommittee on Machine Learning and Artificial Intelligence," National Science and Technology Council, May 6, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/ostp/MLAI_Charter.pdf.

206. Congress also should appropriate money for representatives of U.S. government agencies to attend ANSI meetings, thereby encouraging increased engagement in the standards-setting process. U.S. government involvement in ANSI is necessary to maintain U.S. leadership on the international stage. Adequate agency representation in ANSI often is a challenge because of the organizational dues, travel costs, and staffing requirements necessary for membership.

207. "Assessing Trustworthy AI," European Commission, June 2018, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/2.

208. To include, but not limited to: Department of Commerce, Department of Transportation, Department of Energy, Department of Defense, Department of Education, Department of Health and Human Services, Department of Homeland Security, Department of Justice, Department of Labor, Department of State, Department of Treasury, Department of Veterans Affairs, U.S. Agency for International Development, Central Intelligence Agency, General Services Administration, National Science Foundation, National Security Agency.

209. National Research Council of the National Academies, *Avoiding Technology Surprise for Tomorrow's Warfighter: A Symposium Report (2009),* Chapter 2, "Current Technology Surprise Problems," pp.9–10, https://www.nap.edu/read/12735/chapter/3.

210. "AI and Compute", May 16, 2008, https://openai.com/blog/ai-and-compute/.

211. "Horizon scanning: What's next in digital technologies and how can this help?" Jisc.ac.uk, https://www.jisc.ac.uk/rd/projects/horizon-scanning; "Horizon-scanning and road-mapping," Leverhulme Centre for the Future of Intelligence, http://lcfi.ac.uk/projects/ai-futures-and-responsibility/horizon-scanning-and-road-mapping/; and "Horizon Scanning Series," Australian Council of Learned Academies, https://acola.org/programs/horizon-scanning-series/.

212. Yoav Shoham, et. al., *AI Index 2018 Annual Report*, http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf.

213. 2019 AIoT, https://www.leiphone.com/.

214. *Defense Threat Reduction Agency Strategic Plan FY 2018–2022*, p. 6, https://www.dtra.mil/Portals/61/Documents/STRAT%20Plan%202018-2022%2004022019.pdf?ver=2019-05-30-092929-907; "Technology Scouting and Horizon Scanning*," Department of Homeland Security Science and Technology Directorate,* https://www.dhs.gov/publication/st-technology-scouting-and-horizon-scanning-fact-sheet; and "Forecasting Science & Technology (ForeST)," Intelligence Advanced Research Projects Activity, https://www.iarpa.gov/index.php/research-programs/forest.

215. For additional information on ongoing AI initiatives across the U.S. government, go to www.whitehouse.gov/ai/.

216. President Donald J. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence," the White House, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

217. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence."

218. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence."

219. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update," Select Committee on Artificial Intelligence, National Science and Technology Council, June 2019, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf; and "Summary of the 2018 White House Summit on Artificial Intelligence for American Industry," Office of Science and Technology Policy, May 10, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf.

220. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update."

221. "The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update, p. III," Select Committee on Artificial Intelligence, National Science and Technology Council, June 2019, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

222. "2016-2019 Progress Report: Advancing Artificial Intelligence R&D," National Science and Technology Council, November 2019, https://www.whitehouse.gov/wp-content/uploads/2019/11/AI-Research-and-Development-Progress-Report-2016-2019.pdf.

223. President Donald J. Trump, "Presidential Memorandum for the Secretary of Education," the White House, September 25, 2017, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-secretary-education/.

224. "Charting a Course for Success: America's Strategy for STEM Education, Committee on STEM Education, National Science and Technology Council, December 2018, https://www.whitehouse.gov/wp-content/uploads/2018/12/STEM-Education-Strategic-Plan-2018.pdf.

225. 115th Congress, *John S. McCain National Defense Authorization Act for Fiscal Year 2019,* p. 329, July 25, 2018, https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf.

226 "Initial Report," National Security Commission on Artificial Intelligence," July 2019, https://drive.google.com/file/d/1wRGmHgKURwkTUeusOrHA4gAStFwFSAdE/view.

227. "Interim Report," National Security Commission on Artificial Intelligence," November 2019, https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view.

228. House AI Caucus Co-Chairs: Rep. Pete Olson (R-TX) and Rep. Jerry McNerney (D-CA). Additional members include: Rep. Don Beyer (D-VA), Rep. G. K. Butterfield (D-NC), Rep. André Carson (D-IN), Rep. Emanuel Cleaver II (D-MO), Rep. Suzan DelBene (D-WA), Rep. Mark DeSaulnier (D-MA), Rep. Nanette Diaz Barradán (D-CA), Rep. Debbie Dingell (D-MI), Rep. Anna G. Eshoo (D-CA), Rep. Bill Foster (D-IL), Rep. Josh Gottheimer (D-NJ), Rep. Pramila Jayapal (D-WA), Rep. Henry C. Johnson (D-GA), Rep. Ro Khanna (D-CA), Rep. Derek Kilmer (D-WA), Rep. Brenda Lawrence (D-MI), Rep. Ted Lieu (D-CA), Rep. Dan Lipinski (D-IL), Rep. Michael McCaul (R-TX), Rep. Bobby Rush (D-IL), Rep. Brad Sherman (D-CA), Rep. Darren Soto (D-FL), Rep. Elise Stefanik (R-NY), Rep. Steve Stivers (R-OH), and Rep. Marc Veasey (D-TX); Congressional Artificial Intelligence Caucus, "About," U.S. House of Representatives, https://artificialintelligencecaucus-olson.house.gov/about.

229. Senate AI Caucus Leaders: Sen. Martin Heinrich (D-NM) and Sen. Rob Portman (R-OH). Additional members include: Sen. Brian Schatz (D-HI), Sen. Cory Gardner (R-CO), Sen. Gary Peters (D-MI), and Sen. Joni Ernst (R-IA).

230. Tajha Chappellet-Lanier, "Senate's new AI caucus will work toward 'responsible policy,'" Fedscoop.com, March 13, 2009, https://www.fedscoop.com/artificial-intelligence-caucus-senate/.

231. To learn more about the Joint Artificial Intelligence Center's ongoing efforts, go to www.ai.mil.

232. Terri Moon Cronk, "DOD Unveils Its Artificial Intelligence Strategy," Department of Defense, February 12, 2019, https://dod.defense.gov/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

233. Billy Mitchell, "White House looks to fund DOD's Joint AI Center," Fedscoop.com, March 11, 2019, https://www.fedscoop.com/joint-ai-center-dod-fiscal-2020-budget/.

234. Adam Stone, "What's the best way for the Pentagon to invest in artificial intelligence?," C4isrnet.com, August 16, 2019, https://www.c4isrnet.com/artificial-intelligence/2019/08/16/whats-the-best-way-for-the-pentagon-to-invest-in-artificial-intelligence/; Billy Mitchell, "White House looks to fund DOD's Joint AI Center," Fedscoop.com, March 11, 2019, https://www.fedscoop.com/joint-ai-center-dod-fiscal-2020-budget/; and "June 2018 Prior Approval Request (Omnibus)," Department of Defense Comptroller, June 2018, https://comptroller.defense.gov/Portals/45/Documents/execution/reprogramming/fy2018/prior1415s/18-17_PA_June_2018_Omnibus_Request.pdf.

235. "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity," Department of Defense, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

236. Lamberth, "The White House and Defense Department unveiled AI strategies. Now what?"

237. "AI for American Industry," the White House, https://www.whitehouse.gov/ai/ai-american-industry/.

238. "Defense Innovations Board's AI Principles Project," Defense Innovation Board, https://innovation.defense.gov/ai/.

239. "Defense Innovations Board's AI Principles Project."

240. "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense," Defense Innovation Board, October 2019, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

241. "Defense Innovations Board's AI Principles Project.".

242. "AI Next Campaign," Defense Advanced Research Projects Agency, https://www.darpa.mil/work-with-us/ai-next-campaign.

243. "AI Next Campaign."

244. "Air Force Releases 2019 Artificial Intelligence Strategy," U.S. Air Force press release, https://www.af.mil/News/Article-Display/Article/1959225/air-force-releases-2019-artificial-intelligence-strategy/.

245. "The United States Air Force Artificial Intelligence Annex to The Department of Defense Artificial Intelligence Strategy," Department of the Air Force, 2019, https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf.

246. "CFIUS Reform: Our Analysis," Gibsondunn.com, August 14, 2018, https://www.gibsondunn.com/cfius-reform-our-analysis/.

247. Theodore Schleifer, "Silicon Valley is awash in Chinese and Saudi cash—and no one is paying attention (except Trump)," Vox.com, May 1, 2019, https://www.vox.com/recode/2019/5/1/18511540/silicon-valley-foreign-money-china-saudi-arabia-cfius-firrma-geopolitics-venture-capital.

248. "Review of Controls for Certain Emerging Technologies," *Federal Register*, 83 no. 223 (November 19, 2018), https://www.govinfo.gov/content/pkg/FR-2018-11-19/pdf/2018-25221.pdf.

249. "The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines," Office of the Director of National Intelligence, https://www.afcea.org/event/sites/default/files/files/AIM%20Strategy.pdf.

250. "The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines."

251. "Plan Outlines Priorities for Federal Agency Engagement in AI Standards Development," National Institute of Standards and Technology, August 12, 2019, https://www.nist.gov/news-events/news/2019/08/plan-outlines-priorities-federal-agency-engagement-ai-standards-development.

252. President Donald J. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence," the White House, February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

253. "Plan Outlines Priorities for Federal Agency Engagement in AI Standards Development.".

254. "About the Artificial Intelligence and Technology Office," Department of Energy, https://www.energy.gov/artificial-intelligence-and-technology-office.