DRAFT
FINAL REPORT

National Security Commission on Artificial Intelligence
January 2021

NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE

TABLE OF CONTENTS

Introduction

Artificial Intelligence (AI) technologies promise to be the most powerful tools in generations for expanding knowledge, increasing prosperity, and enriching the human experience. The technologies will be the foundation of the innovation economy and a source of enormous power for countries that harness them. AI will fuel competition between governments and companies racing to field it. And it will be employed by nation states to pursue their strategic ambitions.

Americans have not yet seriously grappled with how profoundly the AI revolution will impact society, the economy, and national security. Recent AI breakthroughs, such as a computer defeating a human in the popular strategy game of Go,[1] shocked other nations into action, but did not inspire the same response in the United States. Americans have not recognized the assertive role the government will have to play in ensuring the United States wins this innovation competition. And they have not contemplated the scale of public resources required to achieve it. Despite our private sector and university leadership in AI, the United States remains unprepared for the coming era.

The magnitude of the technological opportunity coincides with a moment of strategic vulnerability. China is a competitor possessing the might, talent, and ambition to challenge America's technological leadership, military superiority, and its broader position in the world. AI is deepening the threat posed by cyber attacks and disinformation campaigns that Russia, China, and other state and non-state actors use to infiltrate our society, steal our data, and interfere in our democracy. Global crises exemplified in the global pandemic and climate change are expanding the definition of national security and crying out for innovative solutions. AI can help us navigate many of these challenges.

We are fortunate. The AI revolution is not a strategic surprise. We are experiencing its impact in our daily lives and can anticipate how research progress will translate into real world applications before we have to confront the full national security ramifications. This commission can warn of national security challenges and articulate the benefits, rather than explain why previous warnings were ignored and opportunities were missed. We still have a window to make the changes to build a safer and better future.

This report is divided into two parts.

- Part I, "Defending America in the AI Era," (Chapters 1-8) outlines what the United States must do to defend against the spectrum of AI-related threats from state and non-state actors, and recommends how the U.S. government can responsibly use AI technologies to protect the American people and our interests.
- Part II, "Winning the Technology Competition," (Chapters 9-16) outlines AI's role in a broader technology competition, and recommends actions the government must take to promote AI innovation to improve all facets of national competitiveness and protect critical U.S. advantages.

Together the two parts represent the outline for a White House-led strategy to reorient the nation to meet the opportunities and challenges of the emerging era.

[1] *The Google DeepMind Challenge Match*, DeepMind (last accessed Jan. 7, 2021), https://deepmind.com/alphago-korea.

<u>Why Does AI Matter?</u> In 1901, Thomas Edison was asked to predict electricity’s impact on humanity. Two decades after the development of the light bulb, he foresaw a general purpose technology of unlimited possibilities. “[Electricity] is the field of fields,” he said. “It holds the secrets which will reorganize the life of the world.”[2] AI is a very different kind of general purpose technology, but we are standing at a similar juncture and see a similarly wide-ranging impact.[3] The rapidly improving ability of computer systems to solve problems and to perform tasks that would otherwise require human intelligence is transforming many aspects of human life and every field of science. It will be incorporated into virtually all future technology. The entire innovation base supporting our economy and security will leverage AI. How this “field of fields” is used—for good and for ill—will reorganize the world.

The Commission’s assessment is rooted in a realistic understanding of AI’s current state of development and a projection of how the technology will evolve.

AI is ubiquitous in everyday life. We take for granted the ways that AI already shapes our lives in ways small and big. A “smartphone” has multiple AI-enabled features including voice assistants, photo tagging, facial recognition security, search apps, recommendation and advertising engines, and less obvious AI enhancements in its operating system. AI is helping predict the spread and escalation of a pandemic outbreak, planning and optimizing the distribution of goods and services, monitoring traffic flow and safety, speeding up drug and therapeutic discovery, and automating routine office functions. AI is compressing innovation timescales in other disciplines, turning once fantastical ideas in areas like biotechnology into realities.

Deploying and adopting AI remains a hard problem. AI cannot magically solve problems. As AI moves from an elite niche science to a mainstream tool, engineering will be as important as scientific breakthroughs. Early adopters across sectors have learned similar lessons: trying to employ AI is a slog even after the science is settled. Many of the most important real world impacts will come from figuring out how to employ existing AI algorithms and systems, some more than a decade old. The integration challenge is immense. Harnessing data, hardening and packaging laboratory algorithms so they are ready for use in the field, and adapting AI software to legacy equipment and rigid organizations all require time, effort, and patience. Integrating AI often necessitates overcoming substantial organizational and cultural barriers, and it demands top-down leadership.

AI tools are diffusing broadly and rapidly. Cutting-edge deep learning techniques are often prohibitively expensive, requiring vast amounts of data, computing power, and specialized knowledge. However, AI will not be the provenance of only big states and big tech. Many machine learning tools that fuel AI applications are publicly available and usable even for non-experts. Open-source applications and development tools combined with inexpensive cloud computing and less data-intensive approaches are expanding AI opportunities across the world.

[2] Quoted in Orison Swett Marden, *How They Succeeded: Life Stories of Successful Men Told by Themselves*, Lothrop Publishing Co. at 238 (1901).

[3] Andrew Ng is widely credited with making this comparison. See e.g., Shana Lynch, *Andrew Ng: Why AI Is the New Electricity*, Insights by Stanford Business (Mar. 11, 2017), https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity.

AI is changing relationships between humans and machines. In modern society, we already rely much more on machines and automation than we may be aware. The U.S. military, for instance, has used autonomous systems for decades. However, as AI capabilities improve, the dynamics within human-machine "teams" will change. In the past, computers could only perform tasks that fell within a clearly defined set of parameters or rules programmed by a human. As AI becomes more capable, computers will be able to learn and perform tasks based on parameters that humans do not explicitly program, creating choices and taking actions at a volume and speed never before possible. Across many fields of human activity, AI innovations are raising important questions about what choices to delegate to intelligent machines, in what circumstances, and for what reasons. In the national security sphere, these questions will take on greater significance as AI is integrated into defense and intelligence systems. Across our entire society, we will need to address these new complexities with nuanced approaches, intellectual curiosity, and care that recognizes the increasing ubiquity of AI.

Part I - Defending America in the AI-Era. Technology so ubiquitous in other facets of society will have an equivalent impact on international competition and conflict.[4] We must adopt AI to change the way we defend America, deter adversaries, use intelligence to make sense of the world, and fight and win wars.

AI is the quintessential "dual use" technology—it can be used for civilian and military purposes. The AI promise—that a machine can perceive, decide, and act more quickly, in a more complex environment, with more accuracy than a human—represents a competitive advantage in any field. It will be employed for military ends, by governments and non-state groups.

We can expect the large-scale proliferation of AI-enabled capabilities. Many national security applications of AI will require only modest resources and good, but not great, expertise to use. AI algorithms are often accessible. The hardware is "off-the-shelf" and in most cases generally available to consumers (as with graphics processing units, for example). Deep-fake capabilities can be easily downloaded and used by anyone.[5] AI-enabled tools and mutating malware are in the hands of hackers.[6] Cheap, lethal drones will be common. Azerbaijan's use of Turkish drones and Israeli loitering munitions in combat against Armenia in October 2020 confirmed that autonomous military capabilities are spreading.[7] Many states are watching and learning from these experiences. The likelihood of reckless or unethical uses of AI-enabled technologies by rogue states, criminals, or terrorists is increasing.

[4] For an overview of AI and international relations see Michael Horowitz, *Artificial Intelligence, International Competition, and the Balance of Power*, Texas National Security Review (May, 2018), https://doi.org/10.15781/T2639KP49.

[5] Karen Hao & Will Douglas Heaven, *The Year Deep Fakes Went Mainstream*, MIT Technology Review (Dec. 24, 2020). https://www.technologyreview.com/2020/12/24/1015380/best-ai-deepfakes-of-2020/.

[6] Nicholas Duran, et al., *2018 Webroot Threat Report*, Webroot (2018), https://www-cdn.webroot.com/9315/2354/6488/2018-Webroot-Threat-Report_US-ONLINE.pdf; *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, & Medicine (2019), https://www.nap.edu/catalog/25488/implications-of-artificial-intelligence-for-cybersecurity-proceedings-of-a-workshop; Ben Buchanan, et al., *Automating Cyber Attacks: Hype and Reality*, Center for Security and Emerging Technology (Nov. 2020), https://cset.georgetown.edu/research/automating-cyber-attacks/; *Deep Exploit: Fully Automatic Penetration Test Tool Using Deep Reinforcement Learning*, GitHub (last accessed Jan. 9, 2021), https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit.

[7] Robyn Dixon, *Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare*, Washington Post (Nov. 11, 2020), https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html.

AI-enabled capabilities will be tools of first resort in a new era of conflict. State and non-state actors determined to challenge the United States, but avoid direct military confrontation, will use AI to amplify existing tools and develop new ones. Adversaries are exploiting our digital openness through AI-accelerated information operations and cyber attacks. Ad-tech will become natsec-tech as adversaries recognize what advertising and technology firms have recognized for years—that machine learning is a powerful tool for harvesting and analyzing data, and targeting activities. Using espionage and publicly available data, adversaries will gather information, and use AI to identify vulnerabilities in individuals, society, and critical infrastructure. They will model how best to manipulate behavior, and then act.

AI will transform all aspects of military affairs. AI applications will help militaries prepare, sense and understand, decide, and execute faster and more efficiently. Numerous weapons systems will leverage one or more AI technologies. AI-systems will generate options for commanders and create battle networks connecting systems across all domains. It will transform logistics, procurement, training, and the design and development of new hardware. Adopting AI will demand the development of new tactics and operational concepts. In the future, warfare will pit algorithm against algorithm. The sources of battlefield advantage will shift from traditional factors like force size and levels of armaments, to factors like superior data collection and assimilation, connectivity, computing power, algorithms, and system security.

Competitors are actively developing AI concepts and technologies for military use. Russia has plans to automate a substantial portion of its military systems.[8] It has irresponsibly deployed autonomous systems in Syria for testing on the battlefield.[9] China sees AI as the path to offset U.S. conventional military superiority by "leapfrogging" to a new generation of technology. Its military has embraced "intelligentized war" —investing, for example, in swarming drones to contest U.S. naval supremacy.[10] China's military leaders talk openly about using AI systems for "reconnaissance, electromagnetic countermeasures and coordinated firepower strikes."[11] China is testing and training AI algorithms in military games designed around real-world scenarios. As these authoritarian states field new AI-enabled military systems, we are concerned that they will not be constrained by the same rigorous testing and ethical code that guide the U.S. military.

AI will revolutionize the practice of intelligence. There may be no national security function better suited for AI adoption than intelligence tradecraft and analysis. Machines will sift troves of data amassed from all sources, locate critical information, translate languages, fuse data sets from different domains, identify correlations and connections, redirect assets, and inform analysts and decision-makers. To protect the American people, perhaps the most urgent and compelling reason to accelerate the use of AI for national security is the possibility that more advanced machine analysis

[8] Vadim Kozyulin, *Militarization of AI*, Stanley Center for Peace and Security (July 2019), https://stanleycenter.org/wp-content/uploads/2020/05/MilitarizationofAI-Russia.pdf.

[9] Dylan Malyasov, *Combat Tests in Syria Brought to Light Deficiencies of Russian Unmanned Mini-tank*, Defence Blog (June 18, 2018), https://defence-blog.com/news/army/combat-tests-syria-brought-light-deficiencies-russian-unmanned-mini-tank.html.

[10] Testimony of Elsa Kania before the U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion* (June 7, 2019), https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence_0.pdf; Elsa Kania, *"AI Weapons" in China's Military Innovation*, Brookings at 1 (Apr. 20, 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf.

[11] Marcus Clay, *The PLA's AI Competitions*, The Diplomat (Nov. 5, 2020), https://thediplomat.com/2020/11/the-plas-ai-competitions/.

could find and connect the dots before the next attack, when human analysis alone may not see the full picture as clearly.

Defending against AI-capable adversaries without employing AI is an invitation to disaster. AI will compress decision time frames from minutes to seconds, expand the scale of attacks, and demand responses that will tax the limits of human cognition. Human operators will not be able to defend against AI-enabled cyber or disinformation attacks, drone swarms, or missile attacks without the assistance of AI-enabled machines. The best human operator cannot defend against multiple machines making thousands of maneuvers per second potentially moving at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can.

Compelling logic dictates quick, but careful and responsible AI adoption. The government should adopt AI following the principle of legendary basketball coach John Wooden: "be quick, but don't hurry."[12] Like other "safety critical" applications of AI, military and intelligence functions require deliberation and caution before they are developed and fielded. Some current AI systems are narrow and brittle. All require rigorous testing, safeguards, and an understanding of how they might operate differently in the real world than in a testbed. AI-enabled autonomous weapon systems could be more precise, and as a result, reduce inadvertent civilian casualties. But they also raise important ethical questions about the role of human judgment in employing lethal force. If improperly designed or used, they could also increase the risk of military escalation.

There is an emerging consensus on principles for using AI responsibly in the defense and intelligence communities.[13] If an AI-powered machine does not work as designed with predictability and guided by clear principles then operators will not use it, organizations will not embrace it, and the American people will not support it. Hurrying would be counterproductive and dangerous if it caused Americans to lose confidence in the benefits AI could confer. Risk, however, is inescapable. Failing to use AI to solve real national security challenges risks putting the United States at a disadvantage, leaving American service members more vulnerable, and spending taxpayer money unwisely on antiquated and inefficient equipment. Delaying AI adoption will push all of the risk onto the next generation of Americans—who will have to defend against, and perhaps fight, a 21st century adversary with 20th century tools.

The U.S. government still operates at human speed not machine speed. Adopting AI requires profound adjustments in national security business practices, organizational cultures, and mindsets. The government lags behind the commercial state of the art in most AI categories—including basic business automation. It suffers from technical deficits that range from digital workforce shortages to inadequate acquisition policies, insufficient network architecture, and weak data practices. Bureaucracy is thwarting better partnerships with the AI leaders in the private sector that could help. The government must become a better customer and a better partner. National security innovation, in the absence of an impetus like a major war or terrorist attack, will require strong leadership.

[12] Andrew Hill & John Wooden, *Be Quick - But Don't Hurry: Finding Success in the Teachings of a Lifetime*, Simon & Schuster at 69 (2001).

[13] Press Release, U.S. Department of Defense, *DoD Adopts Ethical Principles for Artificial Intelligence* (Feb. 24, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/; *Principles of Artificial Intelligence Ethics for the Intelligence Community*, ODNI (last accessed Jan. 11, 2021), https://www.dni.gov/index.php/features/2763-principles-of-artificial-intelligence-ethics-for-the-intelligence-community.

Part II - Winning The Technology Competition. In addition to AI's narrow national security and defense applications, AI is the fulcrum of a broader technology competition in the world. AI will be leveraged to advance all dimensions of national power from healthcare to food production to environmental sustainability. The successful adoption of AI in adjacent fields and technologies will drive economies, shape societies, and determine which states exert influence and exercise power in the world. Many countries have national AI strategies. But only the United States and China have the resources, commercial might, talent pool, and innovation ecosystem to lead the world in AI. In some areas of research and applications, China is already an AI peer, and it is more technically advanced in some applications.[14] Within the next decade, China could surpass the United States as the world's AI superpower.[15]

On a level playing field, the United States is capable of out innovating any competitor. However, today, there is a fundamental difference in the U.S. and China's approaches to AI innovation that puts American AI leadership in peril. For decades, the U.S. innovation model has been the envy of the world. The open exchange of ideas, free markets, and limited government involvement to support basic research are pillars of the American way of innovation and reflect American values. In America, tech firms compete for market share. They are not instruments of state power. Researchers collaborate in an open research environment in competition with their peers to make AI breakthroughs without regard for borders. The international flow of venture capital and AI-related commerce is encouraged as firms compete for profits and the next big idea.

Most AI progress in the United States should remain with the private sector and universities. We must not lose an innovation culture that is bottom-up, and infused with a garage startup mentality. However, a fully-distributed approach is not a winning strategy in this strategic competition. Even large tech firms cannot be expected to compete with the resources of China or make the big investments the U.S. will need to stay ahead. We will need a hybrid approach meshing government and private sector efforts to win.

China is organized, resourced, and determined to win the technology competition. AI is central to China's global expansion and domestic stability. It has a head start on executing a national AI plan as part of larger plans encompassing several critical technology fields. Beginning in 2017, China established AI goals, objectives, and strategies tied to specific timelines with resources backed by committed leadership to lead the world in AI by 2030.[16] China is executing a centrally-directed systematic plan to extract AI knowledge from abroad through espionage, talent recruitment, technology transfer, and investments. It has ambitious plans to build and train a new generation of AI engineers in new AI hubs. It supports "national champion" firms (including Huawei, Baidu, Alibaba, Tencent, iFlytek, and SenseTime) to lead development of AI technologies at home, advance state-directed priorities that feed military and security programs, and capture markets abroad.[17] It funds

[14] Graham Allison & Eric Schmidt, *Is China Beating the U.S. to AI Supremacy?*, Belfer Center for Science and International Affairs (Aug. 2020), https://www.belfercenter.org/publication/china-beating-us-ai-supremacy;

[15] See e.g., Alexandra Mousavizadeh, et al., *The Global AI Index*, Tortoise Media (Dec. 3, 2019), https://www.tortoisemedia.com/2019/12/03/global-ai-index/.

[16] See Graham Webster, et al., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan'*, New America (Aug. 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ (translating China's State Council Notice on the Issuance of the New Generation Artificial Intelligence Development Plan, date July 20, 2017).

[17] Benjamin Larsen, *Drafting China's National AI Team for Governance*, New America (Nov. 18, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/drafting-chinas-national-ai-team-governance/ (originally

massive digital infrastructure projects across several continents. China developed an intellectual property (IP) strategy and is trying to set global technical standards for AI development.[18] And its laws make it all but impossible for a company in China to shield its data from the authorities.[19]

Advancements in AI are contributing to a broad platform technology competition in e-commerce, search engines, social media, and much else. The countries, companies, and researchers that win the AI competition—in computing, data, talent, and commercialization—will be positioned to win a much larger game. In essence, more and better data, fed by a larger consumer/participant base, produce better algorithms which produce better results, which in turn produces more users, more data, and better performance—until, ultimately, fewer companies will become entrenched as the dominant platforms. If China's firms win these competitions, it will not just disadvantage U.S. commercial firms. It will create the digital foundation for a geopolitical challenge to the United States and its allies. Platform domination abroad allows China to harvest the data of its users, and permits China to extend aspects of its domestic system of control. Wherever China controls the digital infrastructure, social media platforms, and e-commerce, it would possess greater leverage and power to coerce, propagandize, and shape the world to conform to its goals.

The AI competition is complicated by deep interconnections. The United States and China are not operating in parallel lanes like the Soviets and Americans did in the space race, with disconnected research and development (R&D) enterprises and minimal commercial contacts. The research ecosystems in China and the United States are deeply connected through shared research projects, talent circulation (particularly from China to the United States), and commercial linkages that include supply chains, markets, and joint research ventures. It would be counterproductive to sever the technology ties to China that benefit basic research and U.S. companies. However, the United States must protect the integrity of open research, prevent the theft of American IP, and employ targeted tools like export controls and investment screening to protect technology industries critical to national security.

The United States retains advantages in critical areas, but trends are worrisome. For the first time in our lifetime, the world's best scientific talent may be staying home or migrating elsewhere.[20] The

published in Graham Webster, ed., *AI Policy and China: Realities of State-Led Developmen*t, Stanford-New America DigiChina Project (Oct. 29, 2019), https://d1y8sb8igg2f8e.cloudfront.net/documents/DigiChina-AI-report-20191029.pdf); Meng Jing, *China to Boost its 'National Team' to Meet Goal of Global AI Leadership by 2030*, South China Morning Post (Nov. 15, 2018), https://www.scmp.com/tech/innovation/article/2173345/china-boost-its-national-team-meet-goal-global-ai-leadership-2030; Gregory C. Allen, *Understanding China's AI Strategy*, Center for a New American Security (Feb. 6, 2019), https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy, ("The price of SenseTime and the other AI Champions being allowed to dominate these technologies is the Champions' extensive cooperation with China's national security community. Even beyond direct cooperation, China's success in commercial AI and semiconductor markets brings funding, talent, and economies of scale that both reduce China's vulnerability from losing access to international markets and offer useful technology for the development of weaponry and espionage capabilities.").

[18] Emily de La Bruyère & Nathan Picarsic, *China Standards 2035*, Horizon Advisory (Apr. 2020), https://www.horizonadvisory.org/china-standards-2035-first-report.

[19] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[20] Remco Zwetsloot, *China's Approach to Tech Talent Competition: Policies, Results, and the Developing Global Response*, Brookings Institution (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_china_talent_policy_zwetsloot.pdf. According to a Center for Security and Emerging Technology report, in 2016, 14 percent of international students declined offers to study at U.S. universities to study at home, and 19 percent decided to study in another country. In 2018, these numbers rose, with 39 percent staying at home and 59 percent studying in another country. Remco Zwetsloot, et al., *Keeping Top AI Talent in the United States*, Center for Security and Emerging Technology at 26 (Dec. 2019), https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

U.S. lead in microelectronics—the hardware on which all AI runs—has diminished, and for cutting-edge chips it is dependent on foreign supply chains and manufacturers in Asia that are vulnerable to coercion or disruption.[21] While many machine learning tools are widely available and per-unit computing costs have declined, the computing power and data access needed for cutting-edge deep learning research breakthroughs are making it harder for university-based researchers and smaller companies to compete.[22] The geography of innovation remains concentrated in only some parts of the country.[23]

The U.S. government must take a hands-on approach to national technology competitiveness. Promoting a diverse and resilient research and development ecosystem and commercial sector is a government responsibility. Expanding talent pipelines to attract the world's best and redoubling efforts to educate AI-ready Americans are public policy choices. Judiciously, but aggressively, protecting critical AI intellectual property and thwarting the systemic campaign of illicit knowledge transfer being conducted by competitors is a government obligation. Protecting hardware advantages and building resiliency into supply chains necessitates legislation and federal incentives. Bringing together like-minded allies and partners to build a digital coalition that ensures a democratic vision for AI that will shape the digital future requires U.S.-led diplomacy.

The AI competition will require White House leadership. The critical elements of the strategy are too complicated for any one department or agency to lead because they cut across national security, economic, and technology policy. Only strong executive leadership from the White House can drive policy, force tradeoffs, and mobilize the country to make the necessary investments.

AI for What Ends? Technology and Values. The widespread adoption of AI by governments around the world is impacting not only the international order among states but also the political order within them. The stakes of the AI future are intimately connected to the enduring contest between authoritarian and democratic political systems and ideologies.

Technology itself does not possess an ideology, but how it is designed, where it is employed, and which laws govern its use, reflect the priorities and values of those who design and employ it. More AI-enabled surveillance and analysis capabilities will soon be in the hands of most or all governments. As the technology diffuses, the main difference between states will have less to do with the quality or sophistication of the technology and more to do with the way it is used—for what purpose, and under what rules.

[21] "90% of all high-volume, leading-edge [semiconductor] production will soon be based in Taiwan, China, and South Korea." The Department of Defense estimates that by 2022 only 8% of all semiconductor fabrication will occur in the United States, "down from 40% in the 1990s." Michaela D. Platzer, et al., *Semiconductors: U.S. Industry, Global Competition, and Federal Policy,* Congressional Research Service at 12 (Oct. 26, 2020), https://fas.org/sgp/crs/misc/R46581.pdf (quoting Rick Switzer, *U.S. National Security Implications of Microelectronics Supply Chain Concentration in Taiwan, South Korea, and the People's Republic of China*, U.S. Air Force (Sept. 2019)).

[22] For example, non-elite universities and AI startups have difficulty affording the cost of compute resources and data for training sophisticated machine learning (ML) models. Nur Ahmed & Muntasir Wahed, *The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research*, arXiv (Oct. 22, 2020), https://arxiv.org/abs/2010.15581.

[23] More than 90 percent of U.S. innovation sector job creation occurred in just five major coastal cities between 2005 and 2017. Robert D. Atkinson, et al., *The Case for Growth Centers: How to Spread Tech Innovation Across America*, Brookings (Dec. 9, 2019), https://www.brookings.edu/research/growth-centers-how-to-spread-tech-innovation-across-america/.

Authoritarian regimes will continue to use AI-powered face recognition, biometrics, predictive analytics, and data fusion as instruments of surveillance, influence, and political control. China's use of AI-powered surveillance technologies to repress its Uyghur minority and monitor all of its citizens foreshadows how authoritarian regimes will use AI-systems to facilitate censorship, track the physical movements and digital activities of their citizens, and stifle dissent.[24] The global circulation of these digital systems creates the prospect of a wider adoption of authoritarian governance. But liberal democracies also employ AI for internal security and public safety purposes. Over half of the world's advanced democracies use AI-enabled surveillance systems.[25] Such technologies have legitimate public purposes and are compatible with the rule of law. Yet in states edging toward illiberal practices, utilizing digital tools in ways that undermine the rule of law could tip the scales toward further democratic backsliding. The preservation of individual liberties calls for continued vigilance. A responsible democracy must ensure that the use of AI by the government is limited by wise restraints to comport with the rights and liberties that define a free and open society.

The U.S. government should develop and field AI-enabled technologies with adequate transparency, strong oversight, and accountability to protect against misuse. Merely stating U.S. opposition to the authoritarian use of AI is not enough. The United States must also demonstrate how a democracy should use AI to protect the security of its citizens in ways that uphold liberal democratic values. There is an urgent need to field AI for national security purposes against, for instance, foreign and domestic terrorists operating within our borders; there is also an enduring need to ensure that security applications of AI conform to core values of individual liberty and equal protection under law.

The United States must lead a coalition of democracies. As we ensure AI is developed and used in ways that are safe for democracy at home, we must also promote global norms to make its use safe for democracy abroad. While the U.S. government's ability to influence the governance practices of other states is limited, a strong plank of the U.S. foreign policy agenda with respect to AI must be to promote human rights and counter techno-authoritarian trends. The United States can use diplomacy and leverage its global partnerships to advocate for establishing privacy protecting technical standards and norms in international bodies, and work with like-minded nations to ensure other nations have an alternative to embracing China's technology and methods of social control, and access to technologies that protect democratic values like privacy. We do not seek a fragmented digital world. We want the United States and its allies to exist in a world with a diverse set of choices in digital infrastructure, e-commerce, and social media that will not be vulnerable to authoritarian coercion and that supports free speech, individual rights, privacy, and tolerance for differing views.

Conclusion: We are at the beginning of the beginning of this new era of competition. We now know the uses of AI in all aspects of life will grow. We know adversaries are determined to turn AI capabilities against us. We know a competitor is determined to surpass us in AI leadership. We know

[24] See, e.g., Patrice Taddonio, *How China's Government Is Using AI on Its Uighur Muslim Population*, PBS Frontline (Nov. 21, 2019), https://www.pbs.org/wgbh/frontline/article/how-chinas-government-is-using-ai-on-its-uighur-muslim-population/; Bethany Allen-Ebrahimian, *Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm*, International Consortium of Investigative Journalists (Nov. 24, 2019), https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/.

[25] See Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace (Sept. 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

AI is accelerating breakthroughs in a wide array of fields. We know that whoever translates AI developments into applications first will have the advantage. Now we must act. The principles we establish, the federal investments we make, the national security applications we field, the organizations we redesign, the partnerships we forge, the coalitions we build, and the talent we cultivate will set America's strategic course. The United States should invest what it takes to maintain its innovation leadership, to responsibly use AI to defend free people and free societies, and to advance the frontiers of science for the benefit of all humanity. AI is going to reorganize the world. America must lead the charge.

Artificial Intelligence in Context

Artificial intelligence (AI) is not a single piece of hardware or software, but rather a constellation of technologies. To address such a broad topic, the Commission's legislative mandate provided guidance on how to scope its work to include technologies that solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action; and technologies that may learn and act autonomously whether in the form of software agents or embodied robots.[26]

Successful development and fielding of AI technologies depends on a number of interrelated elements that can be envisioned as a stack.[27] AI requires talent, data, hardware, algorithms, applications, and integration. We regard talent as the most essential requirement because it drives the creation and management of all the other elements. Data is critical for most AI systems.[28] Labeled and curated data enables much of current machine learning (ML) used to create new applications and improve the performance of existing AI applications. The underlying hardware provides the computing power to analyze ever-growing data pools and run applications. This hardware layer includes cloud-based compute and storage, supported by a networking and communications backbone, instrumental for connecting smart sensors and devices at the network edge. Algorithms are the mathematical operations that tell the system how to navigate the data to provide answers in response to specific questions. An application makes the answers useful for specific tasks. Integration of these elements is critical to fielding a successful end-to-end AI system. This requires significant engineering talent and investment to integrate existing data flows, decision pipelines, legacy equipment, testing designs, etc. This task of integration can be daunting and historically has been underestimated.[29]

AI technologies and applications such as pattern recognition, machine learning, computer vision, natural language understanding, and speech recognition have evolved for many decades. In the early years of AI, the period the Defense Advanced Research Projects Agency (DARPA) describes as the "first wave," researchers explored many approaches, including symbolic logic, expert systems, and planning. Some of the most effective results were based on "handcrafted knowledge" defined by humans and then used by the machine for reasoning and interacting.[30]

[26] The John S. McCain National Defense Authorization Act for Fiscal Year 2019 includes the following definition to guide the Commission's work: 1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. 2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. 3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks. 4. A set of techniques, including machine learning that is designed to approximate a cognitive task. 5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting. Pub. L. 115-232, 132 Stat. 1636, 1965 (2018).

[27] Dave Martinez, et al., *Artificial Intelligence: Short History, Present Developments, and Future Outlook*, MIT Lincoln Laboratory at 27 (Jan. 2019), https://www.ll.mit.edu/media/9526.

[28] Note that model-based AI requires data for the manual construction of the model(s). Typically, this involves less data than statistical machine learning, but more human effort.

[29] Saleema Amershi, et al., *Software Engineering for Machine Learning: A Case Study*, CSE-SEIP '10 Proceedings of the 41st International Conference on Software Engineering at 291-300 (2019), https://2019.icse-conferences.org/details/icse-2019-Software-Engineering-in-Practice/30/Software-Engineering-for-Machine-Learning-A-Case-Study; D. Sculley, et al., *Machine Learning: The High Interest Credit Card of Technical Debt*, SE4ML: Software Engineering for Machine Learning (NIPS 2014 Workshop) (2014), https://ai.google/research/pubs/pub43146.

[30] John Launchbury, *A DARPA Perspective on Artificial Intelligence*, DARPA, 4-7 (Feb. 2017), https://www.darpa.mil/attachments/AIFull.pdf.

Within the past ten years, we have witnessed a "second wave" of AI, propelled by large-scale statistical machine learning that enables engineers to create models that can be trained to specific problem domains if given exemplar data or simulated interactions. Learning from data, these systems are designed to solve specific tasks and achieve particular goals with competencies that, in some respects, parallel the cognitive processes of humans: perceiving, reasoning, learning, communicating, deciding, and acting. Today most fielded large-scale AI systems employ elements of both first and second wave AI approaches.

Age of Deployed AI. Today, we have reached an inflection point. Global digital transformation has led to an overwhelming supply of data. Statistical ML algorithms, particularly deep neural networks, have matured as problem solvers—albeit with limitations.[31] The powerful and networked computing that fuels ML capabilities has become widely available. The convergence of these factors now places this capable technology in the hands of the technical and non-technical alike. The fundamental "question is no longer how this technology works, but what it can do for you."[32]

While the current technology still has significant limitations, it is well-suited for certain use cases. We have entered the age of deployed AI. AI is now ubiquitous, embedded in devices we use and interact with on a daily basis—take, for example, our smartphones, wireless routers, and cars. We routinely rely on AI-enriched applications, whether searching for a new restaurant, navigating traffic, selecting a movie, or getting customer service over the phone or online.

Forecasting the future of AI is difficult. Five years ago, few would have predicted the recent breakthroughs in natural language understanding that have resulted in systems that can generate full text almost indistinguishable from human prose.[33] With a remarkable increase of investments in the global AI industry over the past five years[34] and an unprecedented amount of general research and development (R&D) dollars being invested worldwide,[35] there is no AI slowdown in sight—only new horizons for deployed AI.

Frontiers of AI Technology. The next decade of AI research will likely be defined by efforts to incorporate existing knowledge, push forward novel ways of learning, and make systems more robust, generalizable, and trustworthy.[36] Research on advancing human-machine teaming will be at the forefront, as will improvements in hybrid AI techniques, enhanced training methods, and explainable AI.

[31] The limitations of today's statistical machine learning, as an example, include: the vulnerability of unknowingly learning and amplifying biases in the training data; the fact that they are often complex models composed of a very large number of learned parameters making them opaque and difficult to interpret; the fact that they are trained to solve narrow tasks and lack generalization to other related problems (such as when operationally encountered data fundamentally changes characteristic from the training data); and the fact that they require large amounts of labeled training data.

[32] Andrew Moore, *When AI Becomes an Everyday Technology*, Harvard Business Review (June 7, 2019), https://hbr.org/2019/06/when-ai-becomes-an-everyday-technology.

[33] Tom B. Brown, et. al, *Language Models are Few-Shot Learners*, arXiv (July 22, 2020), https://arxiv.org/abs/2005.14165.

[34] Zachary Arnold, et al., *Tracking AI Investment: Initial Findings from the Private Markets*, Center for Security and Emerging Technology (Sept. 2020). https://cset.georgetown.edu/wp-content/uploads/CSET-Tracking-AI-Investment.pdf.

[35] According to UNESCO, global spending on R&D has reached a record high of almost US$ 1.7 trillion. See *How Much Does Your Country Invest in R&D?*, UNESCO Institute for Statistics (last accessed Jan. 7, 2021), http://uis.unesco.org/apps/visualisations/research-and-development-spending/.

[36] For a recent debate from AI experts see *AI DEBATE 2: Moving AI Forward: An Interdisciplinary Approach*, Montreal Artificial Intelligence (Dec. 23, 2020), https://montrealartificialintelligence.com/aidebate2.html.

Human-AI Teaming. Mastering human-AI collaboration and teaming is a foundational element for future application of AI. Synergy between humans and AI holds the promise of a whole greater than the sum of its parts. Researchers are addressing this challenge by studying issues of delegated authority, observability, predictability, directability, and trust.[37] Gaining greater understanding of how humans will learn to work with AI will provide insights for creating effective training programs for humans. Advances in language understanding are being pursued to create systems that can summarize complex inputs and engage through human-like conversation, a critical component of next-generation teaming. The frontier of teaming includes the need for collaborative intelligence among cohorts of agents, whether mixed groups of humans and machines, or teams of coordinating machines.

Novel Ways of Learning. New learning methods are allowing for greater efficiency in both training and inference from data.[38] This decreases dependence on vast data sets and widens the aperture of systems to handle tasks beyond their original scope, building pathways towards contextual learning and common sense reasoning. Hybrid AI techniques combine different AI approaches to capitalize on their complementary strengths.[39] For example, neuro-symbolic research is combining symbolic manipulation with neural networks.[40] Model-based and data-based approaches may also be combined, for example, leveraging physics knowledge within statistical machine learning frameworks.[41] Researchers are also advancing supervised learning techniques with low supplies of labeled data,[42] while others have devised more efficient methods of labeling data.[43] Synthetic data generation through simulation is one such promising approach.[44] It allows a model to see conditions

[37] See e.g., Bryan Wilder, et al., *Learning to Complement Humans*, International Joint Conferences on Artificial Intelligence Organization (2020), https://doi.org/10.24963/ijcai.2020/212; Ece Kamar, et al., *Combining Human and Machine Intelligence in Large-scale Crowdsourcing*, Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012) (June 4-8, 2012), https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/galaxyZoo.pdf; Ramya Ramakrishnan, et al., *Overcoming Blind Spots in the Real World: Leveraging Complementary Abilities for Joint Execution*, Proceedings of the AAAI Conference on Artificial Intelligence (July 17, 2019), https://doi.org/10.1609/aaai.v33i01.33016137; Gagan Bansal, et al., *Updates in Human-AI Teams: Understanding and Addressing the Performance/Compatibility Tradeoff*, AAAI Conference on Artificial Intelligence (Jan. 2019), https://www.microsoft.com/en-us/research/uploads/prod/2019/01/Backward_Compatibility_in_AI.pdf; Saleema Amershi, et al.; *Guidelines for Human-AI Interaction*, CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (May 2019), https://doi.org/10.1145/3290605.3300233; Eric Horvitz, *Reflections on Challenges and Promises of Mixed-Initiative Interaction*, AI Magazine (June 15, 2007), https://doi.org/10.1609/aimag.v28i2.2036.

[38] A goal of these new methods is to eliminate the need for many complex calculations that make traditional training very slow. Vincent Dutordoir, *Sparse Gaussian Processes with Spherical Harmonic Features*, arXiv (June 30, 2020), https://arxiv.org/abs/2006.16649.

[39] For a discussion on hybrid intelligence architectures that combine symbolic manipulation with deep learning see Gary Marcus, *The Next Decade in AI: Four Steps Towards Robust Artificial Intelligence*, arXiv at 14-19 (Feb. 19, 2020), https://arxiv.org/abs/2002.06177.

[40] See *Neuro-symbolic AI*, MIT-IBM Watson AI Lab (last accessed Jan. 16, 2021), https://mitibmwatsonailab.mit.edu/category/neuro-symbolic-ai/.

[41] Anuj Karpatne, et al., *Physics-guided Neural Networks (PGNN): An Application in Lake Temperature Modeling*, Association for Computing Machinery's Special Interest Group on Knowledge Discovery and Data Mining (ACM SIGKDD) 2018 (Feb. 20, 2018), https://arxiv.org/pdf/1710.11431.pdf.

[42] Rajat Raina, et al., *Self-Taught Learning: Transfer Learning from Unlabeled Data*, Proceedings of the 24th International Conference of Machine Learning (June 2007), https://dl.acm.org/doi/abs/10.1145/1273496.1273592; Dr. Bruce Draper, *Learning with Less Labeling*, DARPA (last accessed Dec. 19, 2020), https://www.darpa.mil/program/learning-with-less-labeling.

[43] Rahul Dixit, et al., *Artificial Intelligence and Machine Learning in Sparse/Inaccurate Data Situations*, IEEE (Aug. 21, 2020), https://ieeexplore.ieee.org/document/9172612.

[44] See Cem Dilmegani, *The Ultimate Guide to Synthetic Data in 2021*, AI Multiple (Jan. 12, 2021), https://research.aimultiple.com/synthetic-data/.

and scenarios it may not have encountered with a real data set, while preserving relationships between important variables in the original data and privacy of sensitive data.[45]

Edge Computing. Breaking size, weight, and power barriers also increases the ubiquity of AI and aids privacy protection. Companies are working to pack more computational power into tighter, specialized chips that use less energy to train and run the same models. Such chips allow consumer devices to run complex models locally, rather than transmit data externally and wait for models to run remotely. Retaining data entirely on the device where a model is being trained or run is an advancement that could potentially enhance individual privacy in AI-powered systems.[46]

Advances in Reasoning. In comparison to humans, even our most capable current AI systems lack what one might think of as "commonsense reasoning." Efforts are underway to create systems that can generalize knowledge and translate learning across domains. An AI system endowed with commonsense reasoning could effectively model the human ability to make and exploit presumptions about the physical properties, purpose, intentions, and behavior of people and objects and thereby characterize the probable consequences of an action or interaction. Advancements in categorization, creating generalized structured ontologies, and in language understanding will drive the ability for machines to learn while understanding context and content, and allow people to discover rapid solutions to problems that would historically take years to examine.[47] This research promises to pave the way for more explainable AI along with greater ability to detect and mitigate bias, which will be essential to improving trustworthiness of these more general AI technologies.[48]

Toward More General Artificial Intelligence. AI solutions to date have demonstrated narrow and deep competencies, but with fundamental distinction from capabilities demonstrated by humans. Humans perform tasks by learning without explicit supervised signals; they generalize skills required for one task and apply them to other tasks; and they accrue, manipulate, and reason with large amounts of commonsense knowledge. Some researchers have used the phrase "artificial general intelligence" (AGI) to refer to a goal of extending AI beyond narrow, vertical wedges of expertise. Debates have focused on whether there might be specific breakthroughs that would lead to more general, human-like capabilities or whether the field will more likely continue to push more general AI along one or more dimensions of skills. No matter what the perspective, significant progress across the research areas mentioned in this section will be required to create more general AI systems. There are some efforts to pursue more general AI.[49] If achieved, more general AI methods would have an enormous impact economically, socially, and in terms of security. While breakthroughs are decades away and in no way guaranteed, the United States should not shy away

[45] *The Real Promise of Synthetic Data*, MIT News (Oct. 16, 2020), https://news.mit.edu/2020/real-promise-synthetic-data-1016.

[46] *10 Breakthrough Technologies 2020*, MIT Technology Review (Feb. 26, 2020), https://www.technologyreview.com/10-breakthrough-technologies/2020/#tiny-ai.

[47] *The World's Largest and Most Complete Common-Sense Knowledge Base*, Cycorp (last accessed Dec. 19, 2020), https://www.cyc.com/the-cyc-platform/the-knowledge-base; John Pavlus, *Common Sense Comes Closer to Computers*, Quanta Magazine (Apr. 30, 2020), https://www.quantamagazine.org/common-sense-comes-to-computers-20200430/; Antoine Bosselut, et al., *COMET: Commonsense Transformers for Automatic Knowledge Graph Construction*, Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics (2019), https://homes.cs.washington.edu/~msap/pdfs/bosselut2019comet.pdf.

[48] Amy Blumenthal, *How to Make AI Trustworthy*, Science Daily (Aug. 31, 2020), https://www.sciencedaily.com/releases/2020/08/200827105937.htm.

[49] See Benedict Neo, *Top 4 AI companies leading in the race towards Artificial General Intelligence*, Towards Data Science (Apr. 13, 2020), https://towardsdatascience.com/four-ai-companies-on-the-bleeding-edge-of-artificial-general-intelligence-b17227a0b64a; Srishti Deoras, *9 Companies Doing Exceptional Work In AGI, Just Like OpenAI*, Analytics India Magazine (Jul. 25, 2019), https://analyticsindiamag.com/9-companies-doing-exceptional-work-in-agi-just-like-openai/.

from studying, analyzing, and working to achieve the long-term goals of creating systems with more human-like capabilities.

<u>Looking to an AI-enabled Future.</u> Following the trajectories of the research threads outlined above sketches a future in which AI empowers humanity in unprecedented ways, unlocking capabilities across science, education, space technology, healthcare, infrastructure, manufacturing, agriculture, entertainment, and countless other sectors. For example, advances in natural language understanding could enable real-time, ubiquitous translation for more obscure languages for which written and spoken training data is limited.[50] This would transform the way we communicate across geographic and cultural barriers, enabling business, diplomacy, and free exchange of ideas.

Breakthroughs in integration of multi-modal, multi-source data could enable real-time AI-driven modeling and simulation for federal responses to crises including pandemics and natural disasters.[51] Drone feeds augmented with maps, building layouts, and other visual data layers could empower first responders with life-saving emergency scene understanding,[52] and AI could help build response plans, expedite command and control, and optimize logistics for a range of disaster response scenarios.[53]

Table 1. Current Application of AI in Key Areas.

Key Areas	Description	Example(s)
Prediction	Event forecasting and pattern analysis has impacted nearly all industries (e.g., finance, farming, and transportation).	**Preventative Vehicle Maintenance.** Sensor technology is allowing automakers to develop safer vehicles that can detect and communicate service needs early.[54] **Precision Agriculture.** Farmers are increasing crop yield and field usage through image analysis of crop health and predicting effects of fertilizers and weather conditions.[55]

[50] Envisioned translation systems will leverage feedback to the system by actively correcting translation and recognition errors the software makes, improving performance as the interaction between translating parties goes on. A major goal is rapid deployment to new languages that have not been seen before. For example, Carnegie Mellon's DIPLOMAT Project makes interactive speech translation possible through a new architecture called Multi Engine Machine Translation (MEMT). DIPLOMAT gives users the ability to provide translation corrections to support rapid development to new languages that have not been seen before. Robert Frederking, *Interactive Speech Translation in the DIPLOMAT Project*, Carnegie Mellon University Language Technologies Institute (last accessed Dec. 19, 2020), http://www.cs.cmu.edu/~air/papers/acl97-workshop.pdf.

[51] Modeling and simulation can also help prepare for effective pandemic supply chain responses orchestrated by the government. Madhav Marathe, *High Performance Simulations to Support Real-time COVID19 Response*, SIGSIM-PADS '20 (June 2020), https://dl.acm.org/doi/pdf/10.1145/3384441.3395993.

[52] Edgybees (last accessed Dec. 19, 2020), https://edgybees.com/.

[53] *Department of Energy Announces the First Five Consortium*, U.S. Department of Energy (Aug. 18, 2020), ttps://www.energy.gov/articles/department-energy-announces-first-five-consortium.

[54] Alex Kwanten, *Big Data Lets OEMs, Dealers Predict When Vehicles Will Need Service*, Automotive News (Apr. 14, 2019), https://www.autonews.com/fixed-ops-journal/big-data-lets-oems-dealers-predict-when-vehicles-will-need-service.

[55] Climate Fieldview (last accessed Dec. 19, 2020), https://climate.com/features/crop-performance-analysis.

Natural Language Understanding (NLU)	Machines are able to process, analyze, understand, and mimic human language, either spoken or written.	**Richer Human-Computer Interaction.** Recent advances in NLU are producing human-like text for complex tasks, such as answering questions, generating meaningful writing based on context clues, or generating code from verbal descriptions.[56]
Planning and Optimization	Determining necessary steps to complete a series of tasks can save time, money, and improve safety.	**Transportation Planning in Cities.** AI is helping track traffic conditions and pedestrian movements, supporting real-time decision-making to reduce traffic congestion and aid in accident response (e.g., self-adjusting traffic lights, traffic rerouting, adjusting speed limits, smart toll pricing).[57]
Computer Vision	Perceiving and learning visual tasks from the world through cameras and sensors.	**Livestock Monitoring.** Computer vision algorithms applied to video of livestock can track decreases in daily motion, preemptively detecting muscle weakness or infection in livestock on farms. This reduces spread of infection and saves farmers money on treating ill livestock.[58]
Modeling and Simulation	Modeling our physical, economical, and social world to support the study, optimization, and testing of operations through simulation without interfering or interrupting ongoing processes.	**COVID-19 Research.** High performance computing, modeling and simulations are accelerating antiviral drug discovery by reducing the pool of potential drug candidates for testing and elucidating viral mechanisms of COVID-19.[59] **Tracking Space Debris.** AI is being used to predict when physical modeling is in error, helping track space debris, enhancing situational awareness of potential collisions that threaten the International Space Station and essential satellite systems (e.g., Global Positioning System (GPS), internet, and communications).[60]
Robotic Process Automation (RPA)	Software robotics to help organizations automate tedious and repetitive tasks.	**RPA Platforms.** Businesses have access to automation tools to create scalable software bots that harness NLP, computer vision, and prediction.[61]

[56] Tom Brown, et al., *Language Models are Few-Shot Learners*, arXiv (July 22, 2020), https://arxiv.org/abs/2005.14165; OpenAI (last accessed Dec. 19, 2020), https://openai.com/; Rosalie Chan, *A Developer Used a Tool from the AI Company Elon Musk Cofounded to Create an App that Lets You Build Websites Simply by Describing How They Work*, Business Insider (Sep. 7, 2020), https://www.businessinsider.com/developer-sharif-shameem-openai-gpt-3-debuild-2020-9.

[57] *One Hundred Year Study on AI: Transportation Planning*, Stanford University (2016), https://ai100.stanford.edu/2016-report/section-ii-ai-domain/transportation/transportation-planning (and references therein).

[58] Gaudenz Boesch, *Animal Monitoring: How to Use Visual AI to Automate Inspection?*, viso.ai (Sept. 21, 2020), https://viso.ai/applications/animal-monitoring-how-to-use-visual-ai-to-automate-inspection/; Mohammad Sadegh Norouzzadeh, et al., *Automatically Identifying, Counting, and Describing Wild Animals in Camera-Trap Images with Deep Learning*, PNAS (June 19, 2018), https://www.pnas.org/content/115/25/E5716.

[59] COVID-19 HPC Consortium (last accessed Dec. 19, 2020), https://covid19-hpc-consortium.org/; *AI Fast Tracks Drug Discovery to Fight COVID-19*, EurekAlert! (Apr. 22, 2020), https://www.eurekalert.org/pub_releases/2020-04/uota-afd042220.php.

[60] Daniel Nelson, *Open Source AI Models Tackle Space Junk Problem*, Unite.AI (Oct. 8, 2020), https://www.unite.ai/open-source-ai-models-tackle-space-junk-problem/; *Space Situational Awareness in Low Earth Orbit*, GitHub (last accessed Dec. 19, 2020), https://github.com/IBM/spacetech-ssa. GPS is a major component of PNT (Positioning, Navigation, and Timing) services enabled by satellites. Users of PNT services include countless military, governmental, and commercial entities, so preserving them is important. *What is Positioning, Navigation and Timing (PNT)?*, U.S. Department of Transportation (last accessed Jan. 9, 2021), https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt.

[61] *Robotic Process Automation*, Microsoft (last accessed Dec. 2019, 2020), https://flow.microsoft.com/en-us/robotic-process-automation/.

Table 2. AI as the Engine of Invention: Transformational Benefits Due to the Application of AI to Other Fields.

Future Impact	Example(s)
Science: Accelerating Discovery & Technology Innovation	
Expediting the discovery and effective utilization of materials.	***Accelerating Materials Development and Resilience.*** New high temperature superconductors, thermoelectrics, piezoelectrics, catalysts, etc. that can revolutionize society across many areas including energy, transportation, medicine, and carbon capture.[62] ***Expediting Drug and Vaccine Discovery.*** Predicting the structures and understanding the interaction of biological proteins and molecules to help reduce disease burden.[63]
Education: Transforming Learning and High-Skilled Training	
Optimizing curricula for individual students.	***Curriculum Augmentation.*** Enhancing teachers' capabilities through AI-based assistants that curate methods and materials, optimize to each students' needs and personal achievement.[64]
Increasing the effectiveness and safety in training using digital technologies.	***Utilizing a Mixture of Digital Technologies for Field Training.*** Remote digital tutors that use virtual and augmented reality to provide expert guidance in a shared environment, augmenting specialized training in informational technologies, utilities services, medicine, and hazardous environments.[65]
Space: Facilitating Advanced Autonomy with Minimal Communications	
Enabling extended and flexible space exploration.	***Autonomous Spacecraft & Smart Habitats.*** Autonomous and semi-autonomous facilities that are situationally aware, capable of identifying and solving problems with or without the need of human intervention, will advance frontiers in space exploration.[66]

[62] Elizabeth Gibney, *AI Helps Unlock 'Dark Matter' of Bizarre Superconductors*, Nature (Sept. 14, 2018), https://www.nature.com/articles/d41586-018-06144-3; Ivan A. Sadovskyy, et al., *Targeted Evolution of Pinning Landscapes for Large Superconducting Critical Currents*, PNAS, https://www.pnas.org/content/116/21/10291; Miao Zhong, et al., *Accelerated Discovery of CO2 Electrocatalysts Using Active Machine Learning*, Nature (May 13, 2020), https://www.nature.com/articles/s41586-020-2242-8; Miguel A. Bessa, *Bayesian Machine Learning in Metamaterial Design: Fragile Becomes Supercompressible*, Advanced Materials (Oct. 14, 2019), https://onlinelibrary.wiley.com/doi/full/10.1002/adma.201904845.

[63] Andrew W. Senior, et al., *Improved Protein Structure Prediction Using Potentials from Deep Learning* Nature (Jan. 15, 2020), https://www.nature.com/articles/s41586-019-1923-7.

[64] Ron Schmelzer, *AI Applications in Education*, Forbes (July 12, 2019), https://www.forbes.com/sites/cognitiveworld/2019/07/12/ai-applications-in-education/?sh=2ef2086e62a3.

[65] FactualVR (last accessed Dec. 19, 2020), https://factualvr.com/press/; J.D. Fletcher, *DARPA Education Dominance Program: April 2010 and November 2010 Digital Tutor Assessments*, IDA (Feb. 2011), https://pdfs.semanticscholar.org/91d8/0183c405b6aa7d238ab932fd23afe07460e8.pdf.

[66] Dr. Stephen K. Robinson, *Habitats Optimized for Missions of Exploration*, NASA (Oct. 3, 2019), https://www.nasa.gov/directorates/spacetech/strg/stri/stri_2018/Habitats_Optimized_for_Missions_of_Exploration_HOME/; *CIMON-*

Healthcare: Revolutionizing Treatment and Care with Sensors and Smart Systems	
Advancing AI assisted disease prevention.	***Averting Cardiovascular Disease (CD) & Stroke.*** Identifying subtle changes in the retina, indicative of early risk factors of CD and potential stroke, while still preventable.[67]
Aiding in early disease detection and disease monitoring.	**Biological Sensors.** Smart biosensors for early detection of COVID-19-releated disease[68] or monitoring of disease progress (e.g., infections, neurological disorders, therapeutic response, etc.)[69]
Mitigating the effects of disabilities.	***Assisting the Visually Impaired.*** Platforms and novel wearable devices that use automatic object recognition for identifying specific personal items for blind or low-vision individuals.[70]
Supporting health care providers in patient care.	***Telehealth Robots.*** Autonomous interfaces that navigate to patients in hospital rooms, allowing multiple patients to interact with nurses, remote specialists or physicians on rounds, while reducing the spread of COVID-19 infection at the same time.[71]
Enhancing the daily lives and care of elders.	***Companion Robots.*** Intelligent companions aiding in eldercare; capable of recognizing emotions and responding empathetically, [72] that can reduce stress in those suffering from dementia,[73] or aid in daily chores and medical care.[74]

2, European Space Agency (Nov. 12, 2019), https://www.esa.int/ESA_Multimedia/Images/2019/12/CIMON-2; *What is Astrobee?*, NASA (Nov. 24, 2020), https://www.nasa.gov/astrobee; Steve Chien & Kiri L. Wagstaff, *Robotic Space Exploration Agents*, Science Robotics (June 21, 2017), https://robotics.sciencemag.org/content/2/7/eaan4831; Raymond Francis, et al., *AEGIS Autonomous Targeting for ChemCam on Mars Science Laboratory: Deployment and Results of Initial Science Team Use*, Science Robotics, (June 21, 2017), https://robotics.sciencemag.org/content/2/7/eaan4582.

[67] Ryan Poplin, et al., *Prediction of Cardiovascular Risk Factors from Retinal Fundus Photographs via Deep Learning*, Nature (Feb. 19, 2018), https://www.nature.com/articles/s41551-018-0195-0.

[68] *Profusa and Partners Receive DARPA Award to Speed Detection of Disease Outbreaks*, Cision (Aug. 8, 2019), https://www.prnewswire.com/news-releases/profusa-and-partners-receive-darpa-award-to-speed-detection-of-disease-outbreaks-300898518.html.

[69] Taavi Saviauk, et al., *Electronic Nose in the Detection of Wound Infection Bacteria from Bacterial Cultures: A Proof-of-Principle Study*, Eur Surg Res (Jan. 10, 2018), https://pubmed.ncbi.nlm.nih.gov/29320769/; R de Vries, et al., *Prediction of Response to Anti-PD-1 Therapy in Patients with Non-Small-Cell Lung Cancer by Electronic Nose Analysis of Exhaled Breath*, Ann Oncol. (Oct. 1, 2019), https://pubmed.ncbi.nlm.nih.gov/31529107/; *Engineering with the Brain*, NeuralLink (last accessed Dec. 19, 2020), https://neuralink.com/applications/.

[70] Simone Strumph, et al., *Where's My Stuff? Developing AI with Help from People who are Blind or Low Vision to Meet Their Needs*, Microsoft Research Blog (May 12, 2020), https://www.microsoft.com/en-us/research/blog/wheres-my-stuff-developing-ai-with-help-from-people-who-are-blind-or-low-vision-to-meet-their-needs/.

[71] Evan Ackerman, *Telepresence Robots are Helping Take Pressure Off Hospital Staff*, IEEE (Apr. 15, 2020), https://spectrum.ieee.org/automaton/robotics/medical-robots/telepresence-robots-are-helping-take-pressure-off-hospital-staff.

[72] *Pepper*, SoftBank Robotics (last accessed Dec. 19, 2020), https://www.softbankrobotics.com/emea/en/pepper.

[73] *PARO Therapeutic Robot*, PARO Robots (last accessed Dec. 19, 2020), http://www.parorobots.com/.

[74] *Moonshot Goal 3*, Japan Science and Technology Agency (last accessed Jan. 9, 2021), https://www.jst.go.jp/moonshot/en/program/goal3/index.html.

Smart Cities: Driving Operational Efficiency, Reducing Costs, and Ensuring Environmental Sustainability	
Improving safety and the environment in cities.	***Smart City Sensor Technologies.*** Intelligent sensing, high performance computer modeling, edge computing, and distributed systems to manage sustainable use of energy and resources, monitor air quality, and prevent urban flooding.[75] ***Environmental Sustainability***. Data-driven analytics for environmental planning and decision-making; supporting low-carbon energy systems; improving the health and biodiversity of ecosystems by monitoring for changes from overuse and pollution.[76]
Optimizing complex transportation hubs.	***Improve Efficiency in Transportation Hubs.*** Advanced modeling and computing to provide decision support guidance for the coordination of passenger movement, goods, and services at airports making travel more efficient and affordable.[77]
Enabling smart infrastructure.	***Smart Roads.*** Allow vehicles to recharge while driving, reducing the need for large car batteries.[78]

[75] *Building a Hyperconnected City*, ESI Thought Lab (last accessed Jan. 9, 2020), https://econsultsolutions.com/wp-content/uploads/2019/11/ESITL_Building-a-Hyperconnected-City_Report.pdf; Array of Things (last accessed Dec. 19, 2020), https://arrayofthings.github.io/.

[76] Ricardo Vinuesa, et al., *The Role of Artificial Intelligence in Achieving the Sustainable Development Goals*, Nature Communications (Jan. 13, 2020), https://www.nature.com/articles/s41467-019-14108-y.

[77] Athena (last accessed Dec. 19, 2020), https://www.athena-mobility.org/.

[78] ElectReon (last accessed Dec. 19, 2020), https://www.electreon.com/.

PART I: DEFENDING AMERICA IN THE AI ERA

Chapter 1: Emerging Threats in the Artificial Intelligence Era

The U.S. government is not prepared to defend the United States in the coming AI era. AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state adversaries to exploit vulnerabilities in our open society.[79] AI systems will extend the range and reach of adversaries into the United States just as the missile age and terrorism brought threats closer to home. Because of AI, adversaries will be able to act with micro-precision, but at macro-scale and greater speed. They will use AI to enhance cyber attacks and digital disinformation campaigns, and to target individuals in new ways. AI will help create precisely engineered biological agents. Adversaries will manipulate AI systems for malign purposes.

AI technologies exacerbate two existing national security challenges.

- First, digital dependence in all walks of life increases vulnerabilities to cyber intrusion across every segment of our society: corporations, universities, government, private organizations, and the homes of individual citizens. In parallel, new sensors have flooded the modern world. The internet of things, cars, phones, homes, and social media platforms collect streams of data, which can then be fed into AI systems that can identify, target, and coerce our citizens.[80]

- Second, state and non-state adversaries are challenging the United States below the threshold of direct military confrontation using cyber attacks, espionage, psychological and political warfare, and financial instruments. Adversaries do not need AI to conduct widespread cyber attacks, exfiltrate troves of sensitive data about American citizens, interfere in our elections, or bombard us with malign information on digital platforms. However, AI is starting to change these attacks in kind and in degree, creating new threats to the U.S. economy, critical infrastructure, and societal cohesion.[81] Moreover, these AI-enabled capabilities will be used across the spectrum of conflict. They will be used as tools of first resort in non-military conflicts, as a prelude to military actions, or in concert with military actions in war.

Americans are waking to some of the privacy implications of their digital dependence and the potential threats from AI-powered malign information like "deep fakes." However, debate in the United States has not yet accounted for the full scope and danger of the AI-enabled threats and the overall security risks to the AI systems all around us. The prospect of adversaries using machine learning, planning, and optimization to create systems to manipulate citizens' beliefs and behavior in

[79] A threat can be understood as an adversary capability paired with a vulnerability that can create a harmful consequence. See Terry L. Deibel, *Foreign Affairs Strategy: Logic for American Statecraft*, Cambridge University Press at 142-150 (2007). Threats can be further graded by their seriousness, likelihood, imminence, and tractability.

[80] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. For example, the internet of things and AI-powered applications can turn your new robotic vacuum into a listening device. See Sriram Sami, et al., *Spying with Your Robot Vacuum Cleaner*, Proceedings of the 18th Conference on Embedded Networked Sensor Systems (Nov. 2020), https://dl.acm.org/doi/10.1145/3384419.3430781.

[81] This is in some ways analogous to what Cold War strategists called "counter-value targeting." See Lawrence Freedman, *The Evolution of Nuclear Strategy*, Palgrave Macmillan Vol. 20 at 119-122 (1989). In the realm of nuclear strategy, this was also known as counter-city or counter-economy targeting.

undetectable ways is a gathering storm.[82] Most concerning is the prospect that adversaries will use AI to create weapons of mass influence to use as leverage during future wars, in which every citizen and organization becomes a potential target.

Five AI-related threats have already been, or soon will be, developed and used against the United States:

AI-Enabled Information Operations. AI and associated technologies will increase the magnitude, precision, and persistence of adversarial information operations. AI exacerbates the problem of malign information in three ways:

- *Message*: AI can produce original text-based content and manipulate images, audio, and video, including through generative adversarial network (GAN)-enabled and Reinforced Learning deep fakes that will be very difficult to distinguish from authentic messages.

- *Audience*: AI can construct profiles of individuals' preferences, behaviors, and beliefs to target specific audiences with specific messages.

- *Medium*: AI can be embedded within platforms, such as through ranking algorithms, to proliferate malign information.

AI-enabled malign information campaigns will not just send one powerful message to one million people like 20th century propaganda. They also will send a million individualized messages—configured on the basis of a detailed understanding of the targets' digital lives, emotional state, and social network.[83] Rival states are already using AI-powered malign information. For example, according to Taiwanese officials, China's government tested its AI-powered malign information capacities during the 2020 Taiwanese elections.[84] An National Basketball Association (NBA) General Manager was harassed on social media for supporting protesters in Hong Kong, in an effort that may have involved autonomous bots.[85] Other techniques rely on AI-generated fake personas.[86] The control and manipulation of digital information has become central to the Kremlin's strategy,

[82] Some observers have used the concept of "sharp power" to describe such efforts to wield influence in open societies. These uses of power are sharp "in the sense that [authoritarian states aim to] pierce, penetrate, or perforate the information environments in the targeted countries." *Sharp Power: Rising Authoritarian Influence*, National Endowment for Democracy at 13 (Dec. 5, 2017), https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/. See also Testimony of Dr. Eric Horvitz, Microsoft, before the U.S. Senate Committee on Commerce, Science, & Transportation, Subcommittee on Space, Science, & Competitiveness, *Hearing on the Dawn of Artificial Intelligence* at 13 (Nov. 30, 2016), http://erichorvitz.com/Senate_Testimony_Eric_Horvitz.pdf.

[83] Some have characterized AI-driven information operations as "computational propaganda." See Matt Chessen, *The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy… and What Can Be Done About It*, Atlantic Council (Sept. 2017), https://www.atlanticcouncil.org/wp-content/uploads/2017/09/The_MADCOM_Future_RW_0926.pdf.

[84] Philip Sherwell, *China Uses Taiwan for AI Target Practice to Influence Elections,* The Australian (Jan. 5, 2020), https://www.theaustralian.com.au/world/the-times/china-uses-taiwan-for-ai-target-practice-to-influence-elections/news-story/57499d2650d4d359a3857688d416d1e5.

[85] Ben Cohen, et al., *How One Tweet Turned Pro-China Trolls Against the NBA*, Wall Street Journal (Oct. 16, 2019), https://www.wsj.com/articles/how-one-tweet-turned-pro-china-trolls-against-the-nba-11571238943. On automated bots, see, e.g., Sarah Kreps & Miles McCain, *Not Your Father's Bots*, Foreign Affairs (Aug. 2, 2019), https://www.foreignaffairs.com/articles/2019-08-02/not-your-fathers-bots.

[86] James Vincent, *An Online Propaganda Campaign Used AI-Generated Headshots to Create Fake Journalists*, The Verge (July 7, 2020), https://www.theverge.com/2020/7/7/21315861/ai-generated-headshots-profile-pictures-fake-journalists-daily-beast-investigation.

including in efforts to undermine the integrity of the democratic process in the United States and elsewhere.[87]

In the United States, the private sector has taken the leading role in combating foreign malign information. Social media companies in particular have extensive operations to track and manage information on their platforms. But coordination between the government and the social media firms remains ad hoc. We need a more integrated public-private response to the problem of foreign-generated disinformation. Moreover, the government needs to devote greater attention and resources to the technical challenges of detection, attribution, and media authentication. The government should:

✦ **Create a Joint Interagency Task Force (JIATF) and Operations Center.** Congress has authorized a Foreign Malign Influence Response Center to be established within ODNI.[88] The government should use this authority to create a technologically advanced, 24-hour task force and operations center to lead and integrate government efforts to counter foreign-sourced malign information. It would survey the landscape of relevant public and private actors, coordinate among them, and act in real time to counter foreign information campaigns. To expose, attribute, and respond effectively, the center must be equipped with modern AI-enabled digital tools and staff with specialized expertise.

✦ **Coordinate government-wide challenges to detect and attribute AI-enabled malign information campaigns and to authenticate digital media.** Congress should create a fund that would be used to incentivize more companies and investors to make technical advances in these areas. A Grand Challenge would amplify ongoing Defense Advanced Research Projects Agency (DARPA) research programs, and would build upon a Deepfake Detection Challenge launched by private companies.[89] However promising some of these detection technologies may prove to be, they may ultimately fail. Some research suggests that AI-enabled detection of AI-generated deep fakes will not be able to authenticate reality. We will need to develop alternative technologies to authenticate the provenance and products of the digital media we consume.[90]

Data Harvesting and Targeting of Individuals. Data security is a national security problem. "AdTech" has become "NatSecTech." Potential adversaries will recognize what every advertiser and social media company knows: AI is a powerful targeting tool. Just as AI-powered analytics

[87] For recent studies on technical aspects of Russia's interference in the 2016 election, see Alexander Spangher, et al., *Characterizing Search-Engine Traffic to Internet Research Agency Web Properties*, Web Conference (2020), https://www.microsoft.com/en-us/research/publication/characterizing-search-engine-traffic-to-internet-research-agency-web-properties/; Ryan Boyd, et al., *Characterizing the Internet Research Agency's Social Media Operations During the 2016 U.S. Presidential Election using Linguistic Analyses*, PsyArXiv Preprints (2018), https://psyarxiv.com/ajh2q/.Alina Polyakova, *Weapons of the Weak: Russian and AI-driven Asymmetric Warfare*, Brookings Institution (Nov. 15, 2018), https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

[88] Pub. L. 116-92, National Defense Authorization Act for Fiscal Year 2020, 133 Stat. 1198, 2129 (2019).

[89] These include the Media Forensics (MediFor) and Semantic Forensics (SemaFor) programs. See Dr. Matt Turek, *Media Forensics*, DARPA (last accessed Jan.10, 2021), https://www.darpa.mil/program/media-forensics; Dr. Matt Turek, *Semantic Forensics*, DARPA (last accessed Jan.10, 2021),https://www.darpa.mil/program/semantic-forensics; . see also Cristian Canton Ferrer, et al., *Deepfake Detection Challenge Results: An Open Initiative to Advance AI*, Facebook AI (June 12, 2020), https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/; Kyle Wiggers, *Facebook, Microsoft, and Others Launch Deepfake Detection Challenge*, VentureBeat (Dec. 11, 2019), https://venturebeat.com/2019/12/11/facebook-microsoft-and-others-launch-deepfake-detection-challenge/.

[90] See, e.g., Paul England, et al., *AMP: Authentication of Media via Provenance*, arXiv (June 20, 2020), https://arxiv.org/abs/2001.07886.

transformed the relationship between companies and customers, now they are transforming the relationship between governments and individuals. The broad circulation of personal data drives commercial innovation but also creates vulnerabilities.[91] We fear that adversaries' systematic efforts to harvest data on U.S. companies, individuals, and the government is about more than traditional espionage.[92] Adversaries will combine widely available commercial data with data acquired illicitly—like in the 2015 Office of Personnel Management hack—to track, manipulate, and coerce individuals.[93] The reach of tools that China, for instance, uses to monitor, control, and coerce its own citizens—big data analytics, surveillance, and propaganda—can be extended beyond its borders and directed at foreigners.[94] Without adequate data protection, AI makes it harder for anyone to hide his or her financial situation, patterns of daily life, relationships, health, and even emotions. Personal and commercial vulnerabilities become national security weaknesses as adversaries map individuals, networks, and social fissures in society; predict responses to different stimuli; and model how best to manipulate behavior or cause harm. The rise and spread of these techniques represent a major counterintelligence challenge.

For the government to treat the data of its citizens and businesses as a national security asset, substantial changes are required in the way we think about data security and in our policies and laws to strengthen it. We need to identify categories and combinations of personal and commercial data that are most sensitive. Early efforts to limit foreign adversaries' data harvesting—such as the government's decision to force a Chinese company to relinquish ownership of a popular dating application for fear of what a hostile adversary could do with sensitive private data[95]—represent important initial steps. However, the government lacks a broad approach with clear policies, criteria, or authorities to confront this multifaceted problem. The government should:

✦ **Develop policies that treat data security as national security, including in these areas:**

- *First, from a technical standpoint, the government must ensure that a security development lifecycle approach is in place for its own AI systems (including commercial systems it*

[91] Robert Williams has described how policy makers face an "innovation-security conundrum," one aspect of which is "the worry that data privacy and national security are increasingly interconnected. Data (and data networks) can be exploited in ways that threaten security, but they also form the lifeblood of technological innovation on which both economic growth and national security depend." Robert D. Williams, *Crafting a Multilateral Technology and Cybersecurity Policy*, Brookings at 1 (Nov. 2020), https://www.brookings.edu/wp-content/uploads/2020/11/Robert-D-Williams.pdf.

[92] Ellen Nakashima, *With a Series of Major Hacks, China Builds a Database on Americans*, Washington Post (June 5, 2015), https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html.

[93] Another example of an adversary acquiring significant data on U.S. individuals is the hack of the credit reporting agency, Equifax. Press Release, Department of Justice, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax* (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking; Aruna Viswanatha, et al., *Four Members of China's Military Indicted Over Massive Equifax Breach*, Wall Street Journal (Feb. 11, 2020), https://www.wsj.com/articles/four-members-of-china-s-military-indicted-for-massive-equifax-breach-11581346824.

[94] Paul Mozur, *One Month, 500,000 Face Scans: How China is Using AI to Profile a Minority*, New York Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Yingzhi Yang & Julie Zhu, *Coronavirus Brings China's Surveillance State Out of the Shadows*, Reuters (Feb. 7, 2020), https://www.reuters.com/article/us-china-health-surveillance/coronavirus-brings-chinas-surveillance-state-out-of-the-shadows-idUSKBN2011HO; Ross Anderson, *The Panopticon Is Already Here*, The Atlantic (Sept. 2020), https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

[95] Yuan Yang & James Fontanella-Khan, *Grindr Sold by Chinese Owner After US National Security Concerns*, Financial Times (Mar. 7, 2020), https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98.

acquires), which should include a focus on potential privacy attacks.[96] Red teaming must include privacy expertise. Government databases should be federated and anonymized whenever possible, and personal data retained no longer than is necessary, in order to make it more difficult for adversaries to utilize information for malicious purposes.

- *Second, the government should ensure that data privacy and security are priority considerations* as part of larger efforts to strengthen foreign investment screening and supply chain risk management.

- *Third, national efforts to legislate and regulate data protection and privacy must integrate national security considerations*, such as limiting the ability of hostile foreign actors to acquire sensitive data on Americans on the commercial market.

Accelerated Cyber Attacks. Malware in the AI era will be able to mutate into thousands of different forms once it is lodged on a computer system. Such mutating polymorphic malware already accounts for over 90 percent of malicious executable files.[97] Deep reinforcement learning tools can already find vulnerabilities, conceal malware, and attack selectively.[98] While it is uncertain which methods will dominate, there is a clear path for U.S. adversaries to transform the effectiveness of cyber attack and espionage campaigns, with an ensemble of new and old algorithmic means to automate, optimize, and inform attacks.[99] Machine learning has current and potential applications across all the phases of cyber attack campaigns and will change the nature of cyber warfare and cyber crime.[100] The expanding application of existing AI cyber capabilities will make cyber attacks more precise and tailored; further accelerate and automate cyber warfare; enable stealthier and more persistent cyberweapons; and make cyber campaigns more effective on a larger scale.

U.S. defenses have proven incapable of handling even more elementary cyber challenges. Vulnerabilities remain open in outdated infrastructure and medical devices, while new vulnerabilities are proliferating in 5G networks, billions of Internet of Things (IoT) devices, and in software supply chains.[101] The multi-billion dollar global damage caused by Russia's 2017 NotPetya attack concretely demonstrates the power of even basic automated malware, the risk tolerance of capable

[96] On privacy attacks, see Maria Rigaki & Sebastian Garcia, *A Survey of Privacy Attacks in Machine Learning*, arXiv (July 15, 2020), https://arxiv.org/abs/2007.07646.

[97] Nicholas Duran, et al., *2018 Webroot Threat Report*, Webroot at 6 (2018), https://www-cdn.webroot.com/9315/2354/6488/2018-Webroot-Threat-Report_US-ONLINE.pdf.

[98] Gary J. Saavedra, et al., *A Review of Machine Learning Applications in Fuzzing*, arXiv (Oct. 9, 2019), https://arxiv.org/pdf/1906.11133.pdf; Isao Takaesu, *Machine Learning Security: DeepExploit*, GitHub (Aug. 29, 2019), https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit.

[99] *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine (2019), https://doi.org/10.17226/25488; Nektaria Kaloudi & Jingyue Li, *The AI-Based Cyber Threat Landscape*, ACM Computing Surveys at 1-34 (Feb. 2020), https://dl.acm.org/doi/abs/10.1145/3372823; Ben Buchanan, et al., *Automating Cyber Attacks*, Center for Security and Emerging Technology (Nov. 2020), https://cset.georgetown.edu/research/automating-cyber-attacks/; Dakota Cary & Daniel Cebul, *Destructive Cyber Operations and Machine Learning*, Center for Security and Emerging Technology at 5-23 (Nov. 2020), https://cset.georgetown.edu/research/destructive-cyber-operations-and-machine-learning/.

[100] *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine (2019), https://doi.org/10.17226/25488.

[101] The recent SolarWinds attack demonstrates deep vulnerabilities in our software supply chains. See *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI)*, Office of the Director of National Intelligence (Dec. 16, 2020), https://www.dni.gov/index.php/newsroom/press-releases/item/2175-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-and-the-office-of-the-director-of-national-intelligence-odni.

state actors, and the consequences of such capabilities proliferating.[102] Though defensive applications of AI bring the promise to improve our national cyber defenses, AI can't defend inherently vulnerable digital infrastructure. To address the present threat, Congress must continue implementing the Cyberspace Solarium Commission's recommendations.[103] With this foundation for cyber defense, the U.S. can prepare for expanding threats via testing and building the instrumented infrastructure required for AI-enabled cyber defenses, establishing better incentives for security, properly organizing to meet the challenge, and keeping attackers off balance. Pervasive cyber-enabled espionage and attacks on U.S. computer networks and critical infrastructure will continue—and become more damaging with AI—unless urgent federal action is taken. The government should:

✦ **Develop and deploy AI-enabled defenses against cyber attacks.** National security agencies need to acquire the sensors and instrumentation needed to train AI systems to detect and respond to threats on their networks. AI-enable cyber defenses will also need large-scale, instrumented, and realistic testing, and must be robust enough to withstand adversarial attacks. The defenses should be employed to expand machine speed information sharing, behavior-based anomaly detection, and malware mitigation across government networks. To capitalize on these capabilities, the government should accelerate the establishment of a Joint Cyber Planning and Operations Center, modeled after the National Counterterrorism Center.[104] The Center would serve as a centralized cyber intelligence sharing and collaboration unit with multi-agency jurisdiction and authorities to investigate threats, proactively support defensive mitigations, and coordinate responses.

Adversarial AI. AI systems represent a new target for attack. While we are on the front edge of this phenomenon, commercial firms and researchers have documented attacks that involve evasion, data poisoning, model replication, and exploiting traditional software flaws to deceive, manipulate, compromise, and render AI systems ineffective.[105] This threat is related to, but distinct from, traditional cyber activities, because AI systems will be vulnerable to adversarial attacks from any domain where AI augments action—civilian or military.[106] Given the reliance of AI systems on large data sets and algorithms, even small manipulations of these data sets or algorithms can lead to consequential changes for how AI systems operate. The threat is not hypothetical: adversarial attacks are happening and already impacting commercial machine learning (ML) systems.[107] With rare exceptions, the idea of protecting AI systems has been an afterthought in engineering and fielding AI systems, with inadequate investment in research and development.[108] Only three of 28 organizations

[102] *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine (2019), https://doi.org/10.17226/25488; Ben Buchanan, et al., *Automating Cyber Attacks*, Center for Security and Emerging Technology at 3 (Nov. 2020), https://cset.georgetown.edu/research/automating-cyber-attacks/.

[103] *Cyberspace Solarium Commission Report*, U.S. Cyberspace Solarium Commission (Mar. 2020), https://www.solarium.gov/report.

[104] See recommendation 5.4 in *Cyberspace Solarium Commission Report*, U.S. Cyberspace Solarium Commission at 87 (Mar. 2020), https://www.solarium.gov/report.

[105] *Adversarial AI Threat Matrix: Case Studies*, GitHub (last accessed Jan. 10, 2021), https://github.com/mitre/advmlthreatmatrix/blob/master/pages/case-studies-page.md. For more on applications of adversarial AI, see Naveed Akhtar & Ajmal Mian, *Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey*, IEEE (Mar. 28, 2018), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8294186.

[106] Adversarial AI is about what can be done *to* AI systems. The defensive science of protecting AI applications for attacks is called "AI Assurance." The offensive science of attacking each technological component of AI is called "Counter-AI."

[107] Ram Shankar Siva Kumar & Ann Johnson, *Cyberattacks Against Machine Learning Systems Are More Common than You Think*, Microsoft Security (Oct. 22, 2020), https://www.microsoft.com/security/blog/2020/10/22/cyberattacks-against-machine-learning-systems-are-more-common-than-you-think/.

[108] It has been estimated that less than 1 percent of AI R&D funding is directed toward the security of AI systems. See Nathan Strout, *The Three Major Security Threats to AI*, Center for Security and Emerging Technology (Sept. 10, 2019), https://cset.georgetown.edu/article/the-three-major-security-threats-to-ai/.

recently surveyed have "the right tools in place to secure their ML systems."[109] There has not yet been a uniform effort to integrate AI assurance across the entire U.S. national security enterprise. To improve AI "assurance" the government should:

✦ **Create a National AI Assurance Framework.** All government agencies will need to develop and apply an adversarial machine learning threat framework to address how key AI systems could be attacked and should be defended. An analytical framework can help to categorize threats to government AI systems, and assist analysts with detecting, responding to, and remediating threats and vulnerabilities.[110]

✦ **Create dedicated red teams for adversarial testing.** Red teams should assume an offensive posture, trying to break systems and make them violate rules for appropriate behavior. Because of the scarcity of required expertise and experience for AI red teams, DoD and the Office of the Director of National Intelligence (ODNI) should consider establishing government-wide communities of AI red teaming capabilities that could be applied to multiple AI developments.[111]

AI-Enabled Biotechnology. Biology is now programmable. New technologies such as the gene editing tool CRISPR ushered in an era where humans are able to edit DNA. Combined with massive computing power and AI, innovations in biotechnology may provide novel solutions for mankind's most vexing challenges including in health, food production, and environmental sustainability. Like other powerful technologies, however, applications of biotechnology can have a dark side. The COVID-19 pandemic reminded the world of the dangers of a highly contagious pathogen. AI may enable a pathogen to be specifically engineered for lethality or to target a genetic profile—the ultimate range and reach weapon. Also, AI, when applied to biology, could optimize for the physiological enhancement of human beings, including intelligence and physical attributes. To the extent that brain waves can be represented as a machine vision challenge for AI, the mysteries of the brain may be unlocked and programmed.

Individuals, societies, and states will have different moral and ethical views and accept different degrees of risk in the name of progress, and U.S. competitors are comparatively likely to take more risk-tolerant actions and conform less rigidly to bioethical norms and standards. China understands the tremendous upside associated with leading the bio revolution. Massive genomic data sets at places like BGI Group (formerly known as the Beijing Genomics Institute), coupled with China's now global genetic data collection platform and "all-of-nation" approach to AI, will make them a

[109] Ram Shankar Siva Kumar, et al., *Adversarial - Industry Perspectives*, arXiv at 2 (May 21, 2020), https://arxiv.org/pdf/2002.05646.pdf.

[110] There are various ongoing public and private efforts including, for instance, the MITRE-Microsoft adversarial ML framework. See Ram Shankar Siva Kumar & Ann Johnson, *Cyberattacks against Machine Learning Systems Are More Common than You Think*, Microsoft Security (Oct. 22, 2020), https://www.microsoft.com/security/blog/2020/10/22/cyberattacks-against-machine-learning-systems-are-more-common-than-you-think/; *Adversarial AI Threat Matrix: Case Studies*, MITRE (last accessed Jan. 10, 2021), https://github.com/mitre/advmlthreatmatrix/blob/master/pages/case-studies-page.md.

[111] For a similar recommendation, see Michele Flournoy, et al., *Building Trust Through Testing*, WestExec Advisors at 27 (Oct. 2020), https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf (Flournoy, et al., argue for "a national AI and ML red team as a central hub to test against adversarial attacks, pulling together DoD operators and analysts, AI researchers, T&E, [Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Security Agency (NSA)], and other IC components, as appropriate. This would be an independent red-teaming organization that would have both the technical and intelligence expertise to mimic realistic adversary attacks in a simulated operational environment.").

formidable competitor in the bio realm.[112] The United States cannot afford to look back in ten years and be "surprised" by the biotechnology equivalent of Huawei. Additionally, Russia's long-standing disregard for scientific norms and bioethical principles, demonstrated by Russia's development and employment of novel nerve agents such as Novichok for assassination attempts and U.S. government concerns over Russia's compliance with the Biological Weapons Convention, could presage a willingness to utilize advanced biotechnology abilities for nefarious purposes.[113] The government should:

✦ **Increase the profile of biosecurity and biotechnology issues within U.S. national security agencies.** Given how AI will substantially increase the rate of technical advancement in biotechnology, the government should update the National Biodefense Strategy to include a wider vision of biological threats, such as human enhancement, exploitation of genetic data for malicious ends, and ways U.S. competitors could utilize biotechnology or biodata advantages for novel purposes.

[112] BGI built and operates China National GeneBank, the Chinese government's national genetic database. It also is a major global supplier of COVID-19 testing, which potentially provides access to large international genetic data sets; by June 30, 2020 it had supplied over 35 million test kits to 180 countries, including the United States, and built 58 testing labs in 18 countries. See Kristy Needham, *Special Report: COVID Opens New Doors for China's Gene Giant*, Reuters (Aug. 5, 2020), https://www.reuters.com/article/us-health-coronavirus-bgi-specialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE.

[113] See Richard Perez-Pena, *What is Novichok, the Russian Nerve Agent Tied to Navalny Poisoning?*, New York Times (Sept. 2, 2020), https://www.nytimes.com/2020/09/02/world/europe/novichok-skripal.html; *2020 Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments (Compliance Report)*, U.S. Department of State (2020), https://www.state.gov/2020-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments-compliance-report-2/#_Toc43298166.

Chapter 2: Foundations of Future Defense

The U.S. military has enjoyed military-technical superiority over all potential adversaries since the end of the Cold War. Now, its technical prowess is being challenged, especially by China and Russia. Senior military leaders have warned that if current trend lines are not altered, the U.S. military will lose its military-technical superiority within the next five years. Artificial intelligence (AI) is a key aspect of this challenge, as both of our great power competitors believe they will be able to "leapfrog" over our armed forces using AI, AI-enabled systems, and AI-enabled autonomy. In the coming decades, the U.S. will only win against technically sophisticated adversaries if it accelerates adoption of AI-enabled sensors and command and control, weapon and logistics systems.

The Department of Defense (DoD) must set an ambitious goal. By 2025, the foundations for widespread integration of AI across DoD must be in place. Those foundations include a common digital infrastructure that is accessible to internal AI development teams and critical industry partners, a technically literate workforce, and modern AI-enabled business practices that improve efficiency. All are prerequisites to achieving a state of military AI readiness, which is discussed in the next chapter.

DoD lags far behind the commercial sector in integrating new and disruptive technologies such as AI into its operations. Pockets of excellence started to emerge in 2017 when Project Maven was launched with the aim to simplify work for intelligence analysts by recognizing objects in video footage captured by drones and other platforms.[114] Other promising initiatives are occurring in defense labs and agencies, and proof of concept demonstrations are ongoing in service-level tests.[115] However, visionary technologists and warfighters largely remain stymied by antiquated technology, cumbersome processes, and incentive structures that are designed for outdated or competing aims.[116] Successes are usually based on workarounds—in spite of the system.

The obstacles to integrating AI are many. DoD has long been hardware-oriented toward ships, planes, and tanks. It is now trying to make the leap to a software-intensive enterprise. Spending remains concentrated on legacy systems designed for the industrial age and Cold War.[117] Many

[114] *Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare*, Modern War Institute (Aug. 25, 2020), https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/; Cheryl Pellerin, *Project Maven to Deploy Computer Algorithms to War Zone by Year's End*, DoD (July 21, 2017), https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/. Project Maven now includes detecting, classifying, and tracking objects within full motion video images (e.g., person, vehicle, and weapon) and other AI algorithms for text based projects. *PE 0305245D8Z: Intelligence Capabilities and Innovation*, Office of the Secretary of Defense (Feb. 2019), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/D/0305245D8Z_187.pdf.

[115] For example, the Army's Project Convergence exercise in September 2020 demonstrated use of AI at multiple stages of the targeting process. Jen Judson & Nathan Strout, *At Project Convergence, the US Army Experienced Success and Failure — and It's Happy About Both*, Defense News (Oct. 12, 2020), https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/at-project-convergence-the-us-army-experienced-success-and-failure-and-its-happy-about-both/. The Air Force has held similar exercises, most notably as part of its efforts associated with the Advanced Battle Management System–the technical infrastructure which will support the DoD's Joint All Domain Command and Control concept. Theresa Hitchens, *ABMS Demo Proves AI Chops For C2*, Breaking Defense (Sept. 3, 2020), https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/.

[116] This includes the traditional process by which concepts of operation interact with technology development. Chapter 3 offers recommendations to adapt this approach and ensure technological advancements inform concepts as much as concepts drive technology development.

[117] As one observer has noted: "While DoD's investment accounts have grown substantially in the last three years, this growth has been highly concentrated in buying systems from existing production lines and doing prototypes of military systems." Testimony of Andrew Hunter, Director, Defense-Industrial Initiatives Group, CSIS before the U.S. House of Representatives Armed Services

Departmental processes still rely too much on PowerPoint and manually-driven work streams. The data that is needed to fuel machine learning is currently stovepiped, messy, or often discarded. Platforms are disconnected. Acquisition, development, and fielding practices still largely follow rigid, sequential processes, inhibiting early and continuous experimentation and testing critical for AI. Even promising AI programs have not yet delivered as hoped and often remain bound to proprietary software and data storage of commercial vendors. Steps such as building the cloud infrastructure necessary to scale AI applications proceed slowly. Data-sharing agreements and software updates that take hours or days in industry turn into months-long delays. Service members at every level lack the technical education and experience to employ AI.

Meanwhile, bureaucracy hinders partnerships with technology firms and critical efforts to expand the National Security Innovation Base.[118] The prospect of bureaucratic snarls deters companies from working with DoD. It is economically irrational for many startups to even try. Traditional defense companies will continue to play a central role in building and integrating large systems for AI-enabled warfare.[119] However, even these contractors, who have the resources and expertise to navigate the system, face process and technical roadblocks that slow efforts to build and integrate AI systems.

As a result, change will not be easy. It will require a Secretary of Defense who focuses the Department on speeding the adoption of new technologies. The Secretary should direct action in five areas:

✦ **Build the technical backbone.** DoD should make foundational investments to support a Department-wide technical infrastructure for ubiquitous development and fielding of AI. It took a promising first step in 2020 with the issuance of a DoD Data Strategy.[120] However, the Department lacks the modern digital ecosystem, collaborative tools and environments, and broad on-demand access to shared AI resources it needs to integrate AI across the organization. The Department should avoid reinventing core infrastructure for each new AI-driven program or capability, and it should look to leverage and interoperate with proven solutions from the IC wherever possible. A broader platform that could be used across the Department would enable more dynamic development and employment of AI, and would more efficiently utilize scarce technical expertise.[121]

Committee, *Hearing on DoD's Role in Competing with China* at 6 (Jan. 15, 2020), https://armedservices.house.gov/_cache/files/5/8/5818cc1f-b86f-4dca-8aee-10ca788e6f43/9F4A03ABF1DEAB747AF2D1302087A426.20200115-hasc-andrew-hunter-statement-vfinal.pdf.

[118] The National Defense Strategy highlights the importance of the National Security Innovation Base in maintaining the Department's technological advantage. *Summary of the 2018 National Defense Strategy*, U.S. Department of Defense at 3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. The Center for Strategic and International Studies offers a useful definition of the term, noting the "[National Security Innovation Base] is a significant expansion in scope [. . .] compared to the traditional concept of the defense industrial base," and includes tech firms out of innovation hubs such as Silicon Valley, Boston, and Austin. See Andrew Hunter, A Strategic Approach to Defense Investment, CSIS (Mar. 26, 2018), https://www.csis.org/analysis/strategic-approach-defense-investment.

[119] "The largest six prime defense suppliers (Lockheed Martin, Boeing, Northrop Grumman, Raytheon, General Dynamics, and BAE Systems) . . . represented 32 percent of all DoD prime obligations in 2019." *Fiscal Year 2020: Industrial Capabilities*, U.S. Department of Defense at 40 (Dec. 23, 2020), https://www.businessdefense.gov/Portals/51/USA002573-20%20ICR_2020_Web.pdf?ver=o3D76uGwxcg0n0Yxvd5k-Q%3d%3d.

[120] The strategy lays the foundation for the Department to treat data as a strategic asset, and details the goals to make DoD data visible, accessible, understandable, linked, trustworthy, interoperable, and secure. *Executive Summary: DoD Data Strategy*, U.S. Department of Defense (Sept. 30, 2020), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

[121] Components of this platform are underway as a result of the Joint AI Center's Joint Common Foundation initiative—particularly the marketplace of shared AI resources including data, algorithms, and trained AI models.

- *The Secretary of Defense should direct the establishment of a DoD-wide digital ecosystem.* The Secretary should require that all new joint and service programs adhere to the design of this ecosystem, and that, wherever possible, existing programs become interoperable with it by 2025.[122] Key elements should include:
    - Data architecture composed of a secure federated system of distributed repositories linked by a data catalog and appropriate access controls[123] that facilitates finding, accessing, and moving desired data across the DoD.[124]
    - Packaged AI environments[125] that enable agile and iterative AI capabilities development,[126] testing, fielding, and updating in support of a diverse set of stakeholders.[127]
    - Marketplace of shared AI resources[128] that builds upon federated repositories of data, software, and trained models,[129] along with pre-negotiated computing and storage services from a pool of vetted cloud providers.
    - Bolstered network and communications backbone to provide bandwidth to support transport and data fusion, secure processing, continuous development and fielding of AI applications, and software system integration at all levels.
    - Common standard interfaces that allow swift integration of mission-oriented investments.

✦ **Train and educate warfighters.** Warfighters cannot change the way they fight without also changing the way they think. Most service members only use the powerful computers they have to create PowerPoints, build spreadsheets, or send emails. Our service members need to develop core competencies in building, using, and responsibly teaming with machine systems to recognize AI's potential for building a faster and more effective force. In particular, they need to know:

- How to use data in decision-making in ways that complement intuition and experience.

[122] Use of a common technical infrastructure will vastly improve DoD's ability to ensure interoperability and increase the effectiveness of the joint force. However, it is important to note that even without such critical technical infrastructure, the Department is taking important policy steps to drive interoperability and AI-readiness for programs designed to meet joint capability needs. See Aaron Mehta, *Hyten to Issue New Joint Requirements on Handling Data*, Defense News (Sept. 23, 2020), https://www.defensenews.com/pentagon/2020/09/23/hyten-to-issue-new-joint-requirements-on-handling-data/. Chapter 3 outlines additional recommendations for achieving a state of military AI-readiness by 2025.

[123] Secured access to data sets as well as other shared building blocks should be managed by user- and role-based authentication facilitated by an end-to-end identity, credential, and access management infrastructure.

[124] This hinges on implementation of the DoD's new data strategy. *Executive Summary: DoD Data Strategy*, U.S. Department of Defense (Sept. 30, 2020), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

[125] These are platform environments with readymade workflows that can be tailored and launched depending on user-type (e.g., researcher, industry partner, operator) and use case (e.g., development, TEVV, fielding).

[126] In other words, the DevSecOps application lifecycle.

[127] Stakeholders could include embedded development teams working at the tactical edge; AI company partners contributing pre-trained models; academic researchers working on open, relevant challenge problems; government S&T researchers working within a Service lab; or international partners co-developing interoperable AI capabilities.

[128] Shared AI resources should be managed with continuous Authorization to Operate (ATO) frameworks and with mandated default ATO reciprocity across the Department.

[129] Similar to or relying upon the platform delivery and features of Git (https://git-scm.com), GitHub (https://github.com), and GitLab (https://about.gitlab.com).

- How to use information processing agents, and how to get a computer to perform calculations and analytics that could not be done efficiently by a human.
- How to develop and thrive in a "maker" culture that encourages continuous contact and regular experimentation with and development of new tools.
- How to move toward a "teammate model" for interacting with autonomous systems, and navigate issues of delegated authority, observability, predictability, directability, and trust.
- How to bring organizations into the AI era—including when and how to integrate AI-related tasks into priority missions, allocate resources to build and maintain the AI stack, oversee new systems, and support the careers of technical experts.

To improve training and education along these lines, DoD should:

- *Identify service members who excel at computational thinking during the accession process;*
- *Invest in upskilling its workforce through self-guided education courses and coding language incentives;*
- *Teach junior leaders about problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making as part of their pre-commissioning requirements and initial training;*
- *Integrate emerging and disruptive technology training into professional military education courses; and*
- *Create emerging technology coded billets and an emerging technology certification program comparable to the joint billet and qualification system.*

✦ **Accelerate the adoption of existing digital technologies.** DoD has largely relied on workarounds to adopt new technologies, while the core acquisition processes remain sclerotic. There are some bright spots, including the release of the Department's tailorable acquisition framework, contracting resources,[130] and approaches taken by certain programs within the Air Force.[131] The Department must scale these innovative practices and take further steps to align acquisition workforce training, program incentives, budget, and organizational structures to better support the delivery of digitally-enabled capabilities.

[130] The Pentagon's acquisition office's Adaptive Acquisition Framework and Contracting Cone mark important steps by the Department to promote the use of alternate authorities for acquisitions and contracting. These include, for example, other transaction authorities, middle-tier acquisitions, rapid prototyping and rapid fielding, and specialized pathways for software acquisition.

[131] For example, the Air Force's Advanced Battle Management System (ABMS), which is managing systems intended to support the new Joint All Domain Command and Control concept as a portfolio and based heavily on experimentation to drive innovation and an iterative approach to requirements. Notably, the Fiscal Year 2021 defense appropriations bill expresses concern with various aspects of the Air Force's approach, including the "absence of firm requirements, acquisition strategy, or cost estimate" and system of systems integration. See H.R. Rep. No. 116-453, at 294-295 (July 16, 2020), https://www.congress.gov/116/crpt/hrpt453/CRPT-116hrpt453.pdf.

A number of the Department's "innovation" organizations have delivered results. But they are uncoordinated and under-resourced. DoD signaling of technology priorities is ad hoc and is not supported by a track record of significant DoD investments in digital technology with non-traditional vendors. As a result, national security AI applications attract less private-market investment. The Department should focus on four actions:

- *Integrate commercial AI to optimize core business processes.* DoD should embrace proven commercial AI applications and incentivize their use to generate labor and cost savings, speed administrative actions, and inform decision-making. As a critical first step, DoD should prioritize construction of enterprise data sets across core administration areas.

- *Network digital innovation initiatives to scale impact.* Pockets of bottom-up innovation need to be married with top-down leadership. The Department should harmonize its innovation initiatives[132] to carry out a coordinated go-to-market strategy for commercial technology solutions. The Under Secretary of Defense for Research and Engineering, working closely with the Under Secretary of Defense for Acquisition and Sustainment, the military services and other headquarters counterparts, should provide strategic direction for this effort.

- *Expand use of specialized acquisition pathways and contracting approaches.* DoD should accelerate efforts to train acquisition professionals on the full range of available options for acquisition and contracting and incentivize their use for AI and digital technologies.

- *Update the budget and oversight processes.* DoD's resource allocation process is nearly identical to what was put in place in 1961. It is incompatible with AI and other digital technologies. DoD and Congress should institute reforms that enable the advancement of software and digital technologies by accounting for speed, uncertainty, experimentation, and continuous upgrades.

✦ **Democratize AI development.** The Department must promote bottom-up AI development.[133] At every level, technologists, operators, and domain experts should function as integrated teams.[134] This would facilitate user feedback and improve trust and confidence in AI systems. DoD should:

- *Designate the Joint AI Center (JAIC) as the Department's AI Accelerator.* The JAIC cannot identify every potential use for AI in the Department, but it can and should serve as a central hub of AI expertise. In this "accelerator" model, JAIC would coordinate with relevant acquisition, technology, and governance offices to inform strategy; develop AI applications that address shared challenges at the Combatant Commands; deploy Department-wide

[132] Defense Innovation Unit (DIU), Army Applications Laboratory (AAL), AFWERX, SOFWERX, etc.

[133] The Department-wide digital infrastructure described above is critical to enabling this approach, but structural changes are also required to maximize its utility.

[134] There are notable examples of warfighter-technologist pairings within DoD such as the Air Force's software factories and the forward-deployed tactical data teams used by Special Operations and Army Futures Command. They found that partnering technologists (such as data scientists) with operators or analysts at the tactical edge: 1) significantly reduces the time it typically takes a contractor to understand the problem set and deploy a solution; 2) incentivizes iterative development techniques and fast-fielding of minimum viable products eventually yielding higher-impact solutions on an accelerated timeline; and 3) generates increased buy-in to data and AI technologies as critical mission enablers. NSCAI Engagements (Nov. 2020). However, to ensure U.S. forces maintain overmatch in the long-term, DoD must scale this user-centered development.

business AI applications; and provide resources that enable distributed AI development across the Department and the military services.[135]

- *Establish software teams at each Combatant Command.* These commands have specific operational needs that routinely outpace centralized software development. Software teams should be embedded at each Combatant Command to locate, tailor, and field AI applications in support of operational units.[136] Software teams should also include smaller development teams that are forward-deployed to act as the local interface with operational units.[137]

✦ **Invest in next generation capabilities.** DoD leaders anticipate flat or declining defense budgets for the coming years.[138] Despite potential budgetary pressures, DoD must continue accelerating its modernization programs by prioritizing emerging and disruptive technologies such as AI.[139]

- *Fund AI research and development (R&D).* The Department should commit to spending at least 3.4% of its budget on science and technology, and allocate at least $8 billion toward AI R&D annually.[140] Additional resources should be focused on organizations with significant AI expertise, such as Defense Advanced Research Projects Agency, the Office of Naval Research, the Air Force Office of Scientific Research, the Army Research Office, and the service laboratories.

- *Retire legacy systems ill-equipped to compete in AI-enabled warfare.* To make AI ubiquitous throughout its business processes and military systems, DoD must make tough budget tradeoffs and prioritize modernization.[141] DoD should pursue a balanced approach to update existing systems with leading-edge technologies to buy time for investments in longer-term bets. Further, to guard against bias in favor of defending the status quo, DoD should require an evaluation of AI alternatives prior to funding new programs.[142]

[135] Important offices for coordination with the JAIC include but are not limited to USD(R&E), USD Acquisition & Sustainment (USD(A&S)), Director Operational Test & Evaluation (DOT&E), DoD Chief Information Officer (CIO) and the DoD Chief Data Officer (CDO). The JAIC currently serves the Combatant Commands through its Component Mission Initiatives (CMIs), including a Mission Initiative for Joint Warfighting Operations. See *Mission Initiatives*, JAIC (last accessed Dec. 28, 2020), https://www.ai.mil/mi_joint_warfighting_operations.html.

[136] Such applications could be developed by other Combatant Commands, Service software factories, or the JAIC and discoverable via the recommended digital ecosystem

[137]As an example, both Army Futures Command (AFC) and Army Special Operations Command (USASOC) use a model known as "tactical data teams." This model brings AI/ML expertise forward to the field in the form of 3 to 6 person teams to build AI solutions for real-time operational problems. Executed by a small business, Striveworks, under contract with AFC and USASOC, they are currently supporting efforts in Central Command and Indo-Pacific Command Areas of Responsibility.

[138] Jim Garamone, *Chairman Discusses Future Defense Budgets*, U.S. Department of Defense (Dec. 3, 2020), https://www.defense.gov/Explore/News/Article/Article/2433856/chairman-discusses-future-defense-budgets/.

[139] *Summary of the 2018 National Defense Strategy*, U.S. Department of Defense at 6 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[140] The Defense Science Board has proposed the level of 3.4% in the past to mirror typical practices in the private sector. See *Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure*, Congressional Research Service at 12 (Oct. 7, 2020), https://fas.org/sgp/crs/natsec/R44711.pdf.

[141] The Future of Defense Task Force report similarly stated that "policy makers, industry, and the Pentagon must work together to identify trade-offs within the defense apparatus to include legacy systems and operations, which will allow for investment in technology and operational concepts to address future challenges." *Future of Defense Task Force Report 2020* at 18, House Armed Services Committee (Sept. 23, 2020), https://armedservices.house.gov/_cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/424EB2008281A3C79BA8C7EA71890AE9.future-of-defense-task-force-report.pdf.

[142] Using wargaming, experimentation, and live-virtual-constructive environments wherever feasible and mandating interoperability with the digital ecosystem. Of note, the Future of Defense Task Force also recommended every Major Defense Acquisition Program be required "to evaluate at least one AI or autonomous alternative prior to funding." *Id.* at 7.

- *Produce a technology annex to the National Defense Strategy (NDS).* To link DoD's technology investment strategy to future operational needs, the annex should include roadmaps for designing, developing, fielding, and sustaining critical technologies that are needed to address the operational challenges identified in the NDS.

Chapter 3: AI and Warfare

Even with the right AI-ready technology foundations in place, the U.S. military will still be at a battlefield disadvantage if it fails to adopt the right concepts and operations to integrate AI technologies. Throughout history, the best adopters and integrators rather than the best technologists have reaped the military rewards of new technology.[143] The Department of Defense (DoD) should not be a witness to the AI revolution in military affairs, but deliver it with leadership from the top, new operating concepts, relentless experimentation, and a system that rewards agility and risk.

A new warfighting paradigm is emerging because of artificial intelligence (AI). Our competitors are making substantial investments to take advantage of it. This idea has been called "algorithmic" or "mosaic" warfare;[144] China's theorists have called it "intelligentized" war.[145] All of these terms capture, in various ways, how a new era of conflict will be dominated by AI and pit algorithms against algorithms. Advantage will be determined by the amount and quality of a military's data, the algorithms it develops, the AI-enabled networks it connects, the AI-enabled weapons it fields, and the AI-enabled operating concepts it embraces to create new ways of war.

Today's DoD is trying to execute an AI pivot, but without urgency. Despite pockets of imaginative reform and a few farsighted leaders, DoD remains locked in an industrial age mentality in which great-power conflict is seen as a contest of massed forces and monolithic platforms and systems. The emerging ubiquity of AI in the commercial realm and the speed of digital transformation punctuates the risk of not pivoting fast enough. The Department must act now to integrate AI into critical functions, existing systems, exercises and wargames to become an AI-ready force by 2025. Simultaneously, DoD must develop more creative warfighting concepts that are paired with investments in future AI-enabled technologies to set conditions to continuously out-innovate the adversary. If our forces are not equipped with AI-enabled systems guided by new concepts that exceed those of their adversaries, they will be outmatched and paralyzed by the complexity of battle.

> **An AI-Ready DoD by 2025:** Warfighters enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in training, exercises, and operations.

To compete, deter, and, if necessary, fight and win in future conflicts requires wholesale adjustments to operational concepts, technologies, organizational structures, and how we integrate allies and

[143] On military adoption, see for instance, Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010).

[144] The Defense Advanced Research Projects Agency's Mosaic warfare central concept is built around the "adaptability for U.S. forces and complexity or uncertainty for the enemy through the rapid composition and recomposition of a more disaggregated U.S. military force using human command and machine control." Bryan Clark, et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations*, CSBA at vi (Feb. 11, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations/publication/1.

[145] The People's Liberation Army has developed a warfighting concept for what it calls "intelligentized operations" with AI at its core. Within this construct, China theorizes that in future conflict, the central contest will be between adversarial battle networks rather than traditional weapons platforms, and that information advantage and algorithmic superiority will be a determinant of victory. See Elsa Kania, *Chinese Military Innovation in Artificial Intelligence*, CNAS at 1 (June 7, 2019), https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence (testimony before the U.S.-China Economic Security Review Commission).

partners into operations. It will also require risk-based assessments of both the benefits and drawbacks of widespread integration of AI-enabled capabilities, to include future autonomous weapon systems. Lastly, it will require a willingness to engage in bilateral and multilateral dialogues with our allies and partners to urge them to make similar AI pivots to ensure future interoperability.

How AI Will Change Warfare. AI-enabled warfare will not hinge on a single new weapon, technology, or operational concept; rather, it will center on the application and integration of AI-enabled technologies into every facet of warfighting. AI will transform the way war is conducted in every domain—from undersea to outer space, as well as in cyberspace and along the electromagnetic spectrum. It will impact strategic decision-making, operational concepts and planning, tactical maneuvers in the field, and back-office support. In this new kind of warfare, traditional confines of the battlefield will be expanded through AI-enabled micro-targeting, disinformation, and cyber operations, as described in Chapter 1. AI will reshape many attributes of war—such as its speed, tempo, and scale; the relationships service members have with machines; the persistence with which the battlefield can be monitored; and the discrimination and precision with which targets can be attacked. There will be a premium on speed and accuracy in developing knowledge, acting, and reacting as the conflict unfolds.

AI will make the process of finding and hitting targets of military value faster and more efficient. It will also increase accuracy of target identification and minimize collateral damage. Currently, this process generally involves passing data in a serial fashion from a sensor, through a series of humans, to a platform that can shoot at the target. AI will help automate some of the intermediate stages of the decision process. AI will also create opportunities for more advanced processes that would operate more akin to a web, fusing multiple sensors and platforms to manage complex data flows, and transmitting actionable information to human operators and machines across all domains.[146]

In war, many of the military uses of AI will complement rather than supplant the role of humans. AI tools will improve the way service members perceive, understand, decide, adapt, and act in the course of their missions. However, new concepts for military operations will also need to account for the changing ways in which humans will be able to delegate increasingly complex tasks to AI-enabled systems. In the near term, this will be managed through the military's principle of "mission command"—which stresses decentralized execution and disciplined initiative by subordinates who follow a commander's intent. This human-centric approach to fighting should remain the standard for the foreseeable future. But as AI continues to advance into the cognitive and neuromorphic domain, and human-machine teaming becomes more sophisticated, the military will need to develop more imaginative concepts and organizational constructs that take full advantage of AI technologies without relinquishing the principles that undergird mission command.

Mastery of Military AI. The United States must master military AI in the following areas:

Prepare: Transform business and force management processes to enhance efficiency, adaptability, and readiness.

[146] See *Creating Cross-Domain Kill Webs in Real Time*, DARPA (Sept. 18, 2020), https://www.darpa.mil/news-events/2020-09-18a. See also Shane Shaneman, *AI Fusion: Enabling Distributed Artificial Intelligence to Enhance Multi-Domain Operations & Real-time Situational Awareness*, Carnegie Mellon University (2020), http://www.cs.cmu.edu/~ai-fusion/overview.

- *Business processes*. Robotic Process Automation (RPA) and AI-enabled analysis can generate significant savings, speed administrative actions, and provide decision-makers with superior insights into core business processes such as finance, budget, contracting, travel, and human resources.

- *Design.* AI will support a holistic system-of-systems approach to developmental force design via digital engineering, digital twins, and modeling and simulation to enable a more comprehensive understanding of system vulnerabilities and adjacent capabilities, concepts, and technologies.

- *Readiness*. AI will enhance training by relieving the cognitive burden of doing repetitive tasks that can be performed better by the machine. AI will be prevalent in all exercises and wargames and will enhance the military's ability to train in live, virtual, and constructive environments.

<u>Sense and Understand:</u> Enhance awareness and visibility of the battlespace.

- *Plan and task*. Through automation, AI-enabled systems will optimize tasking and collection for platforms, sensors, and assets in near-real time in response to dynamic intelligence requirements or changes in the environment.

- *Collect.* At the tactical edge, "smart" sensors will be capable of pre-processing raw intelligence and prioritizing the data to transmit and store, which will be especially helpful in degraded or low bandwidth environments.

- *Analyze and warn*. AI-enabled tools have potential to augment filtering, flagging, and triage across multiple data sets. Such tools can identify connections and correlations more efficiently and at a greater scale than human analysts, and can flag those findings and the most important content for human analysis. AI will improve indications and warnings for military leaders.
  - AI can fuse data from multiple sources, types of intelligence, and classification levels to produce accurate predictive analysis in a way that is not currently possible.
  - Advances in speech to text transcription and language analytics now enable reading comprehension, question answering, and automated summarization of large quantities of text.

- *Process and exploit*. AI-enabled natural language processing, computer vision, and audiovisual analysis can vastly reduce manual processing of data. AI can also be used to automate data conversion such as translations and decryptions, accelerating the ability to derive actionable insights.

- *Disseminate*. AI will be able to automatically generate machine readable versions of intelligence products and disseminate them at machine speed so that computer systems across the Intelligence Community (IC) and the military can ingest and use them in real time without manual intervention.

Decide: Increase decision speed, clarify options, and enable forward operations.

- *Planning*. AI decision-support applications will utilize modeling and simulation algorithms and real-time data sets to optimize planning options.

- *Deciding.* AI will integrate command and control networks and compress the speed of finding and attacking targets of military value.

- *Tasking, Delegation, and Distribution*. Edge processing enhanced by delegated authorities will allow front-line units to operate in a coordinated manner with minimal to no communications. AI techniques like machine learning (ML) and rule-based models will support network resiliency.

Execute: Improve and reimagine force sustainment, movement, and application of force.

- *Logistics and Sustainment*. AI-enabled predictive analytics, optimization, and tracking will improve efficiency and effectiveness across all facets of logistics. Intelligent systems will aid in the development of courses of action for routine and contingency logistics and sustainment operations. Robotic process automation will streamline human-centric maintenance and supply chain workflows.

- *Movement*. AI will enhance the ability of commanders to maneuver, position, and protect units and forces. AI will help network and coordinate movements of autonomous swarms via human-machine and machine-machine teaming.

- *Targeting*. AI-enabled systems will expand a single targeting chain into a complex targeting web that considers numerous variables across units and domains.

- *Precision and accuracy*. Through AI-enabled smart weapons and autonomous platforms, AI will enable the military to be more precise and discern friendly forces, non-combatants, and adversary targets with greater accuracy.

This list of how AI might transform warfighting principles and capabilities—as well as others like it—is by no means exhaustive. Innovation will lead to future capabilities that are unknowable at present and will only become clearer in time.

Stronger Together. If the United States wants to fight with AI, it will need allies and partners with AI-enabled militaries. Uneven adoption of AI will threaten military interoperability, and the political cohesion and resiliency of U.S. alliances.[147] As it deepens and expands conventional defense arrangements across the globe—especially in Europe and the Indo-Pacific—the United States should incorporate AI and emerging technology into coordinated defense and intelligence activities. Given the dual use nature of many software based capabilities, DoD will need more flexibility to work with civilian agencies, companies, and research institutions in partner nations.

[147] On military interoperability challenges related to AI, see Erik Lin-Greenberg, *Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making*, Texas National Security Review (Spring 2020), https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/.

✦ **Promote AI interoperability and the adoption of critical emerging technologies among allies and partners,** including the Five Eyes, the North Atlantic Treaty Organization (NATO), and across the Indo-Pacific. This should include:

- Supporting NATO efforts to accelerate agreements on architectures and standards, develop allied technical expertise, and pursue coalition AI use cases for exercises and wargames.
- Developing JAIC's international AI Partnership for Defense as a critical vehicle to further AI defense and security cooperation.
- Creating an Atlantic-Pacific Security Technology Partnership to improve military capability and interoperability across European and Indo-Pacific allies and partners.

Achieving a state of military AI readiness by 2025. To reach this goal, the DoD should:

✦ **Drive organizational reforms through innovative leadership.** Senior civilian and military officials should set clear priorities and direction, empower subordinates, and accept higher uncertainty and risk in pursuing new technologies. Specifically, DoD should:

- Establish a high-level Steering Committee on Emerging Technology, tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence;[148]
- Ensure the JAIC Director remains a three-star general or flag officer with significant operational experience who reports directly to the Secretary of Defense or Deputy Secretary of Defense; and
- Appoint the Under Secretary of Defense for Research and Engineering as the co-chair and chief science advisor to the Joint Requirements Oversight Council.
- Assign an AI Operational Advocate on the staff of every Combatant Command. This officer would perform a similar role to that played by the Staff Judge Advocate. He or she would be an expert in AI systems, advise the commander and staff on the capabilities and limitations of AI systems, and identify when AI-enabled systems are being used inappropriately.

✦ **Design imaginative warfighting concepts to inform the development of AI-enabled capabilities.**[149] These concepts should strive for seamless interoperability across the military services

[148] The Commission acknowledges Section 236 of the Fiscal Year 2021 National Defense Authorization Act, which permits the Secretary of Defense to establish a steering committee on emerging technology and national security threats composed of the The Deputy Secretary of Defense; The Vice Chairman of the Joint Chiefs of Staff; The Under Secretary of Defense for Intelligence and Security; The Under Secretary of Defense for Research and Engineering; The Under Secretary of Defense for Personnel and Readiness; The Under Secretary of Defense for Acquisition and Sustainment; The Chief Information Officer; and such other officials of the Department of Defense as the Secretary determines appropriate. However, the structure described in Sec. 236 does not include leadership from the Intelligence Community and will thus not drive the intended action. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

[149] Notably, the National Defense Strategy emphasizes the need to "evolve innovative operational concepts" and "foster a culture of experimentation and calculated risk-taking." Tighter coordination between concept writers and technologists would create a more

and across operational domains. The concept developers should work closely with technologists to articulate how the military could fight most effectively in future scenarios, and should assume that AI-enabled capabilities will be ubiquitous on future battlefields. These concepts can also drive future investments

✦**By the end of 2021, establish AI-readiness performance goals.** To achieve more substantial integration of AI across DoD, the Secretary of Defense should:

- Direct DoD components to assess military AI-readiness through existing readiness management forums and processes. The Tri-Chaired Steering Committee should work closely with the Under Secretary of Defense for Personnel and Readiness and the Joint Staff to ensure the identified AI readiness criteria are incorporated into the military services' readiness recovery frameworks and resourcing strategies.

- Direct the military services to accelerate review of specific skill gaps in AI, in order to inform recruitment and talent management strategies.[150]

- Direct the military services to accelerate use of AI in predictive analytics for maintenance and supply chain to optimize equipment and parts.

- Direct the military services, in coordination with the Defense Logistics Agency and Joint Staff J-4, to prioritize integration of AI into logistics systems wherever possible.

- Integrate AI into major wargames and exercises to promote field-to-learn approaches to technology adoption. Operators need persistent interaction with AI-enabled capabilities early in the development cycle to generate critical feedback on how they function and how they impact the mission. Widespread experimentation will advance both concept development and the performance of the technology.[151]

- Incentivize experimentation with AI-enabled applications through the Warfighting Lab Incentive Fund, which could be overseen by the proposed Tri-Chaired Steering Committee.[152]

✦ **Set the conditions to continuously out-innovate competitors.** The military services should inculcate a culture of experimentation and innovation in operational units to support the rapid integration of AI-enabled applications in current and future weapon systems. DoD should also apply the DevSecOps-style approach of pairing users and technologists more widely and across all aspects of readiness, with particular attention to training environments. Training with AI systems will help to develop the applications themselves as well as the trust needed to use them effectively.

dynamic cycle of technology development and integration. *Summary of the 2018 National Defense Strategy*, U.S. Department of Defense at 7 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[150] As noted in Chapter 6, there is already an identified need for the creation of digital corps, civilian and military AI and AI-related career fields, an expansion of recruiting pathways, and the creation of recruiting offices. The military services need to assess the number of personnel in those fields and structures, not the need to establish them.

[151] Although AI will be ubiquitous across all domains, the high-data volumes associated with the space, cyber, and information operations domains make use cases in those domains particularly well-suited for prioritized integration of AI-enabled applications in wargames, exercises, and experimentation.

[152] The Warfighting Lab Incentive Fund is intended to spur field experiments and demonstrations to "evaluate, analyze and provide insight into more effective ways of using current capabilities, and to identify new ways to incorporate technologies into future operations and organizations." See Memorandum from the Deputy Secretary of Defense, *Warfighting Lab Incentive Fund and Governance Structure*, U.S. Department of Defense (May 6, 2016), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/DSD_memo.pdf.

✦ **Define a joint warfighting network architecture by the end of 2021.** The key objective of this joint warfighting network should be a secure, open-standards systems network that supports the integration of AI applications at operational levels and across domains.[153] It should be accessible by all of the military services and encompass several elements, including command and control networks; data transport, storage, and secure processing; and weapon system integration. The technical infrastructure for the network should be supported by best practices in digital engineering. It should also be interoperable with the digital ecosystem described in Chapter 2.

✦ **Invest in priority AI research and development (R&D) areas that could support future military capabilities,** including the following:

Table 3. AI Research and Development Areas that Could Support Future Military Capabilities.

Category	Research Area	Time Horizon		Key Challenges
		Near	Long	
Work with Humans	**Future of Teaming**	Increased safety through proximity sensing and spatial coordination	Trusted collaboration between mixed cohorts of humans and machines	Dynamic planning, machines' ability to understand human interaction
Sense & Perceive	**Advanced Scene Understanding**	Ability to sense fundamental changes in the operating environment and alert the human operator while switching to a better-suited, environmentally-tuned perceptual model, if one exists	Maintaining a perceptual model that supports actionable awareness and insight across a range of complex, dynamic environments and scenarios	Incorporating multi-source and multi-modal information from complex and changing environments
Hardware, Devices, & Robotics	**Intelligent Edge Devices, Computing & Networking**	Narrow AI applications within edge sensors, such as remote cameras positioned to monitor a highly contested space	Autonomous edge devices that dynamically learn, share, and team with other devices, while exercising intelligent data collection, exploitation, and retention; mastery of domain-specific physical manipulation	Network limitation; size, weight, and power (SWaP)
Integrate & Assure	**Robust & Resilient AI**	Standard practice for exchanging trained AI models with tamper resistance and non-repudiation	AI systems that are resilient on attack surfaces and able to learn securely via privacy-centric machine learning, including use of encryption	Many attack surfaces; addressing rise of adversarial machine learning methods with robust learning; applying security techniques while maintaining high accuracy

[153] The network envisioned is well-aligned with ongoing DoD efforts to embrace standards-driven interoperability, system adaptability, and data-sharing. See *Memorandum for Service Acquisition Executives and Program Officers*, U.S. Department of Defense (Jan. 7, 2019), https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular_Open_Systems_Approach.pdf.

	Test and Evaluation, Verification and Validation (TEVV)	Common framework for AI TEVV	TEVV for fully autonomous AI systems that employ dynamic learning along with self-awareness and monitoring, and autonomous AI test ranges involving cohorts of humans and machines	Knowing how much and what types of testing is sufficient to determine an acceptable level of risk for a given use case
Learn & Reason	**Integrated AI, Modeling & Simulation for Decision Support**	Decision support for highly constrained scenarios and environments	Real-time decision support and course of action development for open-world environments with longer time horizons	Multi-modal data integration; assessing the predictive fidelity of simulation models
	Autonomous AI Systems	Operate for relatively short periods of delegated autonomy from human operators in relatively unchanging and predictable environments while carrying out simple, independent tasks	Longer periods of independent mission engagement with awareness and understanding of a dynamically changing operational environment, requiring continual assurance and self-monitoring, while carrying out complex mission sets involving multi-agent collaboration	Independent accomplishment of goals in environments that are complex, changing, and unpredictable; understanding how and when to engage with human operators
	Toward More General Artificial Intelligence	Growth in interpretability and explainability for narrow AI; methods for performing transfer learning; fine-tuning of models	AI systems able to learn by engaging with the operational environment, make decisions based on contextual knowledge, and amass experiential knowledge	Unlocking multiple mysteries of human learning and reasoning; more general situational awareness and problem-solving

Chapter 4: Autonomous Weapon Systems and Risks Associated with AI-Enabled Warfare

World military powers both large and small are pursuing AI-enabled and autonomous weapon systems. Such systems have the potential to help commanders make faster, better, and more relevant decisions. They will enable weapon systems to be capable of levels of performance, speed, and discrimination that exceed human capabilities. And they will enable hitherto impossible complex tasks. If properly designed, they could improve compliance with International Humanitarian Law (IHL)[154] by reducing the risk of accidental engagements, decreasing civilian casualties, minimizing collateral infrastructure damage, and auditing the decisions and actions of operators and their command chain. Although U.S. weapons platforms have utilized autonomous functionalities for over eight decades,[155] AI technologies have the potential to enable novel, sophisticated offensive and defensive autonomous capabilities.

The increasing use of AI technologies in weapon systems has generated important questions regarding whether such systems are lawful, safe, and ethical. Those critical of using AI technologies in weapons argue that states should negotiate limits or restrictions on such systems and their use. There is also concern that autonomous weapon systems may make conflict escalation more likely, and debate continues over what steps are needed to ensure that such systems minimize the risk of unintended military engagements or inadvertent and uncontrollable conflict escalation. Since 2014, the United Nations Convention on Certain Conventional Weapons (CCW) has held meetings among states parties to discuss the technological, military, legal and ethical dimensions of "emerging technologies in the area of lethal autonomous weapon systems (LAWS)."[156] Specifically, it is examining whether autonomous technologies will be capable of complying with IHL, and whether additional measures are necessary to ensure that humans maintain an appropriate degree of control over the use of force.

The Commission has consulted with civil society, academic organizations, and government agencies in studying the legal, ethical, and strategic questions which surround AI-enabled and autonomous weapon systems, including their potential military benefits and risks, possible ethical issues coming to the fore, international efforts to regulate them, as well as their compliance with IHL. The Commission offers the following four judgments to reflect its conclusions on these discussions:

Judgment 1. Provided their use is authorized by a human commander or operator, properly designed and tested AI-enabled and autonomous weapon systems have been and can continue to be used in ways which are consistent with IHL. This judgment is grounded in several elements of IHL:

- *Distinction*: The principle of distinction holds that parties to an armed conflict must distinguish between civilians and combatants.[157] Weapons with increasingly accurate AI-enabled target recognition systems can reduce cases of target misidentification, the leading

[154] IHL is also referred to as the law of armed conflict (LOAC) and the law of war.
[155] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, W. W. Norton & Company at 39 (Apr. 24, 2018).
[156] *Background on Lethal Autonomous Weapons Systems in the CCW*, United Nations (last accessed Jan. 11, 2021), https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument.
[157] *Distinction*, International Committee of the Red Cross (last accessed Jan. 15, 2021), https://casebook.icrc.org/glossary/distinction.

cause of inadvertent engagements during combat operations, and thus reduce civilian casualties and collateral infrastructure damage.[158]

- *Proportionality*: The principle of proportionality prohibits attacks which would cause incidental loss of civilian life excessive to the anticipated military advantage.[159] AI-enabled and autonomous systems can and should also be designed to carry out operations in accordance with human judgments and directions regarding the proportionality of an attack. The moral reasoning involved in this calculus—weighing anticipated military advantage against potential civilian harm—ultimately must fall to a human commander.[160]

- *Accountability*: Ensuring accountability and command responsibility is essential to compliance with IHL. A human can and should be held accountable for the development, testing, use and behavior of any autonomous system, AI-enabled or otherwise. Autonomous systems will operate within the same general parameters as those used for human command and control systems, which are specifically designed to ensure accountability for actions and compliance with IHL. This is no different than for any other weapon system.[161]

The Commission endorses the Department of Defense (DoD)'s body of policy that states that human judgment must be involved in decisions to take human life in armed conflict. The kind of involvement necessary for humans to remain accountable for the use of autonomous systems will vary depending on the time criticality of the situation as well as the operational context, circumstance, and type of weapon systems involved.[162] It is incumbent upon states to establish processes which ensure that appropriate levels of human judgment are relied upon in the use of AI-enabled and autonomous weapon systems and that human operators of such systems remain accountable for the results of their employment.

Human accountability for the results of lethal engagements does not necessarily require human oversight of every step of an engagement process. Once a human authorizes an engagement against a target or group of targets, subsequent steps in the attack sequence can be completed autonomously without relinquishing human accountability. The exact number of steps in this sequence is dependent on the system's technical capabilities and the context, and must consider factors such as the uncertainty associated with the system's behavior and potential outcomes, the magnitude of the threat, and the time available for action. For instance, a system located in a rapidly-changing environment, such as an urban setting, for an extended period, may require more frequent human authorization to ensure sufficient human accountability over autonomous actions than an equivalent

[158] There is room for improvement in reducing target misidentification in U.S. military operations. In the Afghanistan war, for example, a study indicated that about half of all civilian casualty incidents caused by U.S. forces resulted from target misidentification. The use of AI-enabled systems to make more accurate targeting decisions is perhaps the principal way in which the proper employment of AI could make warfare more humane. Larry Lewis, *Redefining Human Control: Lessons from the Battlefield for Autonomous Control*, CNA at 4 (Mar. 2018), https://www.cna.org/cna_files/pdf/DRM-2017-U-016281-Final.pdf.

[159] *Proportionality*, International Committee of the Red Cross (last accessed Jan. 15, 2021), https://casebook.icrc.org/glossary/proportionality.

[160] See Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, W.W. Norton & Co. at 255-257 (2018).

[161] For a properly designed autonomous system which correctly carries out the commander's intent, the commander is clearly accountable for the actions of that system. It is incumbent on states to properly design such systems and also put in place rigorous procedures ensuring any weapon use complies with IHL including by ensuring individual accountability.

[162] The Commission believes DoD's existing formulation of "appropriate human judgment," discussed in the following Judgment, captures that necessary variation, and ensures that any decision to employ lethal force begins with and is under the control of human judgment, and that a human ultimately will remain accountable for any decision to employ force.

system, operated for a similar amount of time, in a highly predictable and less populated environment—such as underwater or in space. This logic can and should be incorporated into the system's design, testing, and operational planning. Taking these factors into consideration, when feasible and deemed necessary operation designs should include points of required human guidance amid a sequence of automated actions. At such points, a human must review the system's status and authorize its next actions before the system's mission can continue. A blanket decision to compel every discrete step in an engagement involving lethal force to be subject to explicit authorization by a human is neither realistic nor desirable. Indeed, such a policy could instead spur commanders to use less precise, unguided weapon systems that might result in greater levels of collateral damage.

Judgment 2. Existing DoD procedures are capable of ensuring that the United States will field safe and reliable AI-enabled and autonomous weapon systems and use them in a manner that is consistent with IHL. DoD's commitment to rigorous procedures for the development and use of autonomous systems—as well as its commitment to strong AI ethical principles[163]—instills confidence that it will be able to field AI-enabled and autonomous systems that are used lawfully. DoD has comprehensive processes for ensuring that the use of *any* weapon it fields is compliant with IHL and has a demonstrated commitment to operating within IHL, minimizing civilian casualties, and learning from its mistakes.[164] DoD has established a cross-department legal group, the DoD Law of War Working Group, to "develop and coordinate law of war initiatives and issues, such as analysis regarding the legality of new means or methods of warfare under consideration by DoD components."[165] This standing body is well positioned to examine implications for IHL as technology evolves over time. The International Committee on the Red Cross (ICRC) has lauded the strength and transparency of this system, listing the United States as one of eight countries which has "national mechanisms to review the legality of weapons and that have made the instruments setting up these mechanisms available to the ICRC."[166]

In addition to baseline legal review, the Department has taken special precautions for autonomous weapon systems to ensure these systems undergo sufficient TEVV. In 2012, DoD added to an extensive list of guiding directives and instructions regarding weapons development within the Department by publishing Directive (DoDD) 3000.09, *Autonomy in Weapon Systems*, which establishes DoD policy for the development and use of autonomous weapon systems. It requires that all systems be designed "to allow commanders and operators to exercise appropriate levels of human judgment over the use of force," and requires senior DoD leaders to approve any autonomous

[163] Press Release, U.S. Department of Defense, *DoD Adopts Ethical Principles for Artificial Intelligence* (Feb. 24, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[164] DoDD 5000.01 requires any weapon fielded by DoD to undergo a legal review to ensure compliance with LOAC, adhering to the requirements set out in Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949. DoDD 3000.09 and the DoD AI Ethics Principles build on top of this baseline. See *Department of Defense Directive 5000.01: The Defense Acquisition System*, U.S. Department of Defense at 9 (Sept. 9, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf?ver=2020-09-09-160307-310; *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, International Committee of the Red Cross (last accessed Jan. 5, 2021), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/WebART/470-750045.

[165] *Department of Defense Directive No. 2311.01: DoD Law of War Program*, U.S. Department of Defense at 11 (July 2, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101p.pdf?ver=2020-07-02-143157-007.

[166] *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, International Committee of the Red Cross at 5, n. 8 (Jan. 2006), https://www.icrc.org/en/doc/assets/files/other/icrc_002_0902.pdf.

weapon with lethal capabilities first when development begins, and again before fielding.[167] It also mandates any autonomous or semi-autonomous weapon that undergoes a revision to its operating state to undergo additional testing and evaluation.[168] DoDD 3000.09 provides important baseline requirements for such systems, and should be reviewed and updated over time as technology evolves.

In addition, DoD's command and control procedures to authorize target selection and employment of munitions are rigorous and designed to ensure compliance with IHL. Operational commanders in the field are directly supported by lawyers embedded at multiple levels to advise on decisions about the use of force. The U.S. commitment to IHL is longstanding, and AI-enabled and autonomous weapon systems will not change this commitment.[169] These same principles will be ingrained into the design of those weapons, demonstrated in TEVV, and maintained by commanders overseeing their deployment. The DoD's policy for autonomy in weapon systems and the Department's adoption of ethical principles for AI in 2019 resonates with and reinforces this commitment.[170]

Judgment 3. There is little evidence that U.S. competitors have equivalent rigorous procedures to ensure their AI-enabled and autonomous weapon systems will be responsibly designed and lawfully used. Battlefield success may become increasingly dependent on AI performance, and AI-enabled weapons are likely to proliferate given the open-source and dual-use nature of AI. This could cause pressure to mount on states to rapidly field new and untested systems and algorithms. Pressures could also tilt designs toward systems that react more quickly—leading to shorter periods of time for effective human oversight on engagement decisions. U.S. competitors, particularly Russia and China, likely do not have equivalent operational and targeting procedures to ensure the use of such systems is compliant with IHL and to preserve human accountability over the use of lethal force. Russia and China also have not published anything equivalent to DoDD 3000.09, outlining their policies and processes governing the acquisition, development, testing, and deployment of autonomous weapon systems. Unlike in the United States, in Russia and China these processes are secret, if they exist at all.

U.S. competitors have demonstrated that they are unlikely to adhere to the same ethical and legal standards in developing and utilizing AI-enabled weapon systems. Russia in particular has historically demonstrated a willingness to deploy risky and under-tested weapon systems, and has reportedly deployed poorly-performing unmanned ground vehicles with limited autonomous functionalities in combat in Syria.[171] China has not only developed autonomous weapon systems but is actively proliferating them to other nations. The Chinese government is currently exporting

[167] *Department of Defense Directive 3000.09: Autonomy in Weapon Systems*, U.S. Department of Defense at 2 (Nov. 21, 2012, incorp. change 1 May 8, 2017), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf. The weapons review processes established in DoDD 3000.09 are designed specifically to ensure that any U.S. autonomous weapon system complies with IHL principles such as discrimination and proportionality, while also maintaining appropriate levels of human judgement and ensuring accountability.

[168] See Chapter 7 for recommendations regarding the need for continued U.S. investments in TEVV.

[169] The DoD Law of War manual serves as a detailed resource for all DoD personnel responsible for implementing the law of war and executing military operations. See *Department of Defense Law of War Manual*, U.S. Department of Defense (Dec. 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

[170] Press Release, U.S. Department of Defense, *DoD Adopts Ethical Principles for Artificial Intelligence*, (Feb. 24, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[171] David Axe, *Don't Panic, But Russia is Training its Robot Tanks to Understand Human Speech*, Forbes (June 30, 2020), https://www.forbes.com/sites/davidaxe/2020/06/30/dont-panic-but-russia-is-training-its-robot-tanks-to-understand-human-speech/?sh=7373377914f2.

autonomous armed drones to the Middle East, including systems which companies based in China such as Ziyan advertise as capable of conducting autonomous, lethal, targeted strikes.[172]

Judgment 4. The Commission does not support a global prohibition of AI-enabled and autonomous weapon systems. A global treaty prohibiting the development, deployment, or use of AI-enabled and autonomous weapon systems is not in the interest of U.S. or international security, and would be inadvisable to pursue for several reasons:

- First is the basic definitional problem. Although the UN discussions about LAWS date back to 2014, states have yet to agree on a definition for them. This makes any treaty negotiation problematic, as it may be impossible to define the category of systems to be restricted in such a way that provides adequate clarity while not overly constraining existing U.S. military capabilities.

- Even if the definitional problem could be overcome, we judge that, at present, implementation of such an agreement would be impractical because compliance could not be verified. There is no feasible technical manner in which states could demonstrate to one another that specific weapon systems are or are not autonomous, or that they possess or lack certain capabilities. Doing so would require foreign inspectors to have short-notice access to the underlying code in weapon systems of concern. States are unlikely to agree to such an intrusive verification regime because revealing that information would create unacceptable risks to the security of their systems.

- Additionally, the effects of a prohibition agreement likely would run counter to U.S. strategic interests. Commitments from states such as Russia or China likely would be empty ones. Such an agreement would not serve the goal of putting political pressure on the states that are most likely to deploy autonomous systems in unsafe and ethically concerning ways. Rather, the primary impact of an agreement would be to increase pressure on those countries that abide by international law, including the United States and its democratic allies and partners. Moreover, differing views on a prohibition among U.S. allies could deepen divisions among them on the employment of AI-enabled autonomous systems. If U.S. allies joined an agreement while the United States did not, that divergence would likely hinder allied military interoperability.[173]

For these reasons, we believe the practical and strategic problems with a prohibition treaty outweigh potential benefits for the United States and its allies and partners, and therefore support the current U.S. policy in opposition to such an agreement. However, this does not preclude other agreements or policies to address strategic risks associated with AI-enabled and autonomous weapon systems, or the future possibility of regulating specific types of technologies in AI-enabled and autonomous weapons technologies when such an agreement could be verifiable.

[172] Patrick Tucker, *SecDef: China Is Exporting Killer Robots to the Mideast*, Defense One (Nov. 5, 2019), https://www.defenseone.com/technology/2019/11/secdef-china-exporting-killer-robots-mideast/161100/.

[173] The United States has expressed similar concerns with respect to treaties banning cluster munitions and nuclear weapons. See *Q&A: Convention on Cluster Munitions*, HRW (Nov. 6, 2010), https://www.hrw.org/news/2010/11/06/qa-convention-cluster-munitions#; Heather Williams, *What the Nuclear Ban Treaty Means for America's Allies*, War on the Rocks (Nov. 5, 2020), https://warontherocks.com/2020/11/what-the-nuclear-ban-treaty-means-for-americas-allies/. As of March 2021, no ally with which the United States has a mutual defense agreement has expressed support for a treaty banning LAWS.

Recommendations to Mitigate Strategic Risks of AI. While the Commission believes that well-designed AI-enabled and autonomous weapon systems will bring substantial military and even humanitarian benefit, the unchecked global use of such systems potentially risks unintended conflict escalation and crisis instability. The United States cannot assume that AI-enabled and autonomous systems fielded by other countries will be developed, acquired, and fielded with the appropriate testing and verification to enable them to act as intended. Unintended escalations may occur for numerous reasons, including when systems fail to perform as intended, because of challenging and untested complexities of interaction between AI-enabled and autonomous systems on the battlefield, and, more generally, as the result of machines or humans misperceiving signals or actions. AI-enabled systems will likely increase the pace and automation of warfare across the board, reducing the time and space available for de-escalatory measures. Beyond testing and robustness, we cannot assume that AI-enabled and autonomous weapons developed by other nations will be designed to behave in accordance with IHL. Thus, AI-enabled and autonomous systems may perform inconsistently with IHL, for example by bypassing considerations of proportionality and disregarding threats to civilian populations.

Therefore, countries must take actions which focus on reducing risks associated with AI-enabled and autonomous weapon systems, and encourage safety and compliance with IHL when discussing their development, deployment, and use. Such efforts should and must be led by the United States, which is uniquely situated to lead them given its technical expertise, military prowess, and clear and transparent policies and ethical principles governing the deployment and use of AI-enabled and autonomous weapon systems. The Commission presents the following four recommendations regarding actions the United States should take to mitigate risks associated with AI-enabled and autonomous weapon systems.

✦ **Clearly and publicly affirm existing U.S. policy that only human beings can authorize employment of nuclear weapons, and seek similar commitments from Russia and China.** The United States should make a clear, public statement that decisions to authorize nuclear weapons employment must only be made by humans, not by an AI-enabled or autonomous system, and should include such an affirmation in the DoD's next Nuclear Posture Review.[174] This would cement and highlight existing U.S. policy, which states that "[t]he decision to employ nuclear weapons requires the explicit authorization of the President of the United States."[175] It would also demonstrate a practical U.S. commitment to employing AI and autonomous functions in a responsible manner, limiting irresponsible capabilities, and preventing AI systems from escalating conflicts in dangerous ways. It could also have a stabilizing effect, as it would reduce competitors' fears of an AI-enabled, bolt-from-the-blue strike from the United States, and could incentivize other countries to make equivalent pledges.

The United States should also actively press Russia and China, as well as other states that possess nuclear weapons, to issue similar statements. Although joint political commitments that only humans will authorize employment of nuclear weapons would not be verifiable, they could still be stabilizing,

[174] The Commission recognizes that AI should assist in some aspects of the nuclear command and control apparatus, such as early warning, early launch detection, and multi-sensor fusion to validate single sensor detections and potentially eliminate false detections.
[175] *Nuclear Matters Handbook 2020*, Office of the Deputy Assistant Secretary of Defense for Nuclear Matters at 18 (2020), https://fas.org/man/eprint/nmhb2020.pdf.

responding to a classic prisoner's dilemma: as long as countries have confidence that others are not building risky command and control structures that have the potential to inadvertently trigger massive nuclear escalation, they would have less incentive to develop such systems themselves.[176] While this norm is widely accepted in the United States, it is unclear if Russia and China share the same strategic concerns. Public reports indicate that Russia previously installed a "dead hand" system to automate nuclear launch authorization,[177] and China's representatives in Track II dialogues with the United States have been hesitant to state that China would make an equivalent commitment. If neither Russia nor China are willing to agree to such a proposal, the United States should mount a strong international pressure campaign to condemn this decision and highlight how Russia and China refuse to commit to responsible military uses of AI.

✦ **Discuss AI's impact on crisis stability in the existing U.S.-Russia Strategic Security Dialogue and create an equivalent dialogue with China.** The Departments of State and Defense should discuss AI's impact on crisis stability within the existing U.S.-Russia Strategic Security Dialogue (SSD) and create an equivalent dialogue with China. The SSD is an interagency bilateral dialogue focused on reducing misunderstandings and misperceptions on key strategic issues and threats, as well as reducing the likelihood of inadvertent escalation. Although the dialogue has traditionally focused on nuclear arms control and doctrine, it has recently been used to also discuss emerging technologies and space security.[178] The United States has no equivalent dialogue with China, as China has resisted U.S. attempts to establish one for nearly a decade. However, within the last year there has been increasing evidence that China is interested in formal talks with the United States concerning AI-enabled military systems.[179] This interest should be cultivated, and leveraged into establishing the U.S.-China SSD.

Given that the United States, Russia, and China are all aggressively pursuing AI-enabled capabilities, and that Russia and China are likely to field AI-enabled systems which have undergone less rigorous TEVV than comparable U.S. systems and may be unsafe or unreliable, it is crucial to improve mutual understanding of each other's military doctrines with respect to AI. The United States should use this channel to highlight how deploying unsafe systems could risk inadvertent conflict escalation, emphasize the need to conduct rigorous TEVV, and discuss where each side sees risks of a conventional conflict rapidly escalating in order to better anticipate future responses in a crisis.

These dialogues could also plant the seeds for a future, standing dialogue exclusively focused on establishing more concrete confidence building measures surrounding AI-enabled and autonomous weapon systems. For instance, the United States, Russia, and China could work to develop an "international autonomous incidents agreement," modeled after the 1972 Incidents at Sea Agreement,

[176] There could be other reasons countries may delegate nuclear weapons launch authority to autonomous systems, particularly if leadership trusts machines to execute launch orders more than humans. A political agreement is unlikely to be able to address these concerns, although offering it would highlight how other nations are engaging in irresponsible and dangerous behavior.

[177] Michael Peck, *Russia's 'Dead Hand' Nuclear Doomsday Weapon is Back*, The National Interest (Dec. 12, 2018), https://nationalinterest.org/blog/buzz/russias-dead-hand-nuclear-doomsday-weapon-back-38492.

[178] Press Release, U.S. Department of State, *Deputy Secretary Sullivan's Participation in Strategic Dialogue with Russian Deputy Foreign Minister Sergey Ryabkov* (July 17, 2019), https://www.state.gov/deputy-secretary-sullivans-participation-in-strategic-security-dialogue-with-russian-deputy-foreign-minister-sergey-ryabkov/; Press Release, U.S. Department of State, *The United States and Russia Hold Space Security Exchange* (July 28, 2020), https://www.state.gov/the-united-states-and-russia-hold-space-security-exchange/.

[179] Over the last year, Chinese experts have participated actively in several Track II dialogues with U.S. experts on the safety of military AI systems, potentially signaling a desire for formal government-to-government communication on these issues.

which would seek to define the "rules of the road" for behavior of autonomous military systems to create a more predictable operating environment and avoid accidents and miscalculations.[180] They could also agree to integrate "automated escalation tripwires" into systems that would prevent the automated escalation of conflict in specific scenarios without human intervention, to include nuclear weapons employment as noted above.

✦ **Work with allies to develop international standards of practice for the development, testing, and use of AI-enabled and autonomous weapon systems.** The United States must work closely with its allies to develop standards of practice regarding how states should responsibly develop, test, and employ AI-enabled and autonomous weapon systems. This could build off of existing work, to include the 11 Guiding Principles agreed to by the LAWS GGE in 2019,[181] DoDD 3000.09, the DoD Ethical Principles for AI, and the NSCAI Key Considerations for Responsible Development and Fielding of AI.[182] As part of this effort, the DoD Law of War Working Group should meet regularly to review any future technical developments that pertain to autonomous systems and IHL, and the Tri-Chaired Steering Committee on Emerging Technology (separately recommended by the Commission in Chapter 3 of this report) should advise on how such future technical developments impact policy and national defense.

The outputs of both groups should inform future DoD engagements with both allies and competitors on AI-enabled and autonomous systems. Obtaining allied consensus regarding standards for the development, testing, and use of such systems will set important norms regarding these systems, help to ensure they are developed and used safely, and further highlight the commitment of the United States and its allies to ethical and responsible uses of AI. The United States should also use these consultations to highlight the ways in which AI will become a crucial part of future military operations, and develop common frameworks guiding the appropriate and responsible use of AI-enabled and autonomous systems on the battlefield. This should seek to incentivize allies to invest in the digital modernization of their own forces, while also highlighting the risks to military interoperability should any ally agree to join a treaty prohibiting LAWS.

✦ **Pursue technical means to verify compliance with future AI arms control agreements.** The United States should actively pursue the development of technologies and strategies that could enable effective and secure verification of future arms control agreements involving uses of AI technologies. Although arms control of AI-enabled weapon systems is currently technically unverifiable, effective verification will likely be necessary to achieve future legally binding restrictions on AI capabilities. DoD and the Department of Energy (DoE) should spearhead efforts to design and implement technologies which could provide other countries confidence that an AI-enabled and autonomous system is working as intended without revealing sensitive operational details. For instance, it could examine ways for AI-enabled weapons platforms to produce authenticatable records of operation, which could be spot-checked via international challenge inspections if noncompliant activity is

[180] See Michael C. Horowitz and Paul Scharre, *AI and International Stability: Risks and Confidence-Building Measures*, Center for a New American Security (Jan. 2021), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AI-and-International-Stability-Risks-and-Confidence-Building-Measures.pdf?mtime=20210112103229&focal=none.

[181] *Final Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effect*, CCW/MSP/2019/CRP.2/Rev.1, (Nov. 13-15, 2019), https://undocs.org/CCW/MSP/2019/9.

[182] See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI (July 2020), https://www.nscai.gov/reports.

suspected. Technical creativity will be necessary to enable any future international restrictions on AI capabilities without revealing sensitive information.

✦ **Fund research on technical means to prevent proliferation of AI-enabled and autonomous weapon systems.** Controlling the proliferation of AI-enabled and autonomous weapon systems poses significant challenges given the open-source, dual-use, and inherently transmissible nature of AI algorithms.[183] The proliferation of makeshift autonomous weapon systems which primarily utilize commercial components will be particularly difficult to control via regulation, and will necessitate capable intelligence sharing and domestic law enforcement efforts to prevent their use by terrorists and other non-state actors. Regarding more sophisticated autonomous weapon systems, the United States should double down on efforts to design and incorporate proliferation-resistant features, such as standardized ways to prevent unauthorized users from utilizing such weapons, or reprogramming a system's functionality by changing key system parameters. DoD and DoE should fund technical research on such methods, and if appropriate, these methods could be shared with Russia and China, or potentially other countries, to prevent the proliferation or loss of control of certain AI-enabled autonomous weapon systems.[184]

[183] See Chapter 14 of this report for additional information on the difficulty of using export controls to prevent the transfer of AI algorithms.

[184] Along these lines, the United States shared the technology for Permissive Action Links (PALs), which prevent the unauthorized arming of a nuclear weapon, with the Soviet Union in the 1970s. It is not clear if there is an equivalent technology to PALs for AI - one which would reduce the risk of unauthorized or accidental escalation by an AI system without simultaneously significantly increasing the military performance of that system. If equivalent technologies are developed, cooperation would have to be considered on a case-by-case basis.

Chapter 5: AI and the Future of National Intelligence

Intelligence will benefit from rapid adoption of artificial intelligence (AI)-enabled technologies more than any other national security mission. As every possible platform—both machine and human—contributes to the global information grid and as the number of sensors grows exponentially, the volume, velocity, and variety of data threaten to overwhelm intelligence analysis. Ascertaining the veracity and value of information will be harder. Analysts will be challenged to provide the context crucial for turning information into actionable intelligence.

AI will help intelligence professionals find needles in haystacks, connect the dots, and disrupt dangerous plots by discerning trends and discovering previously hidden or masked indications and warnings. AI-enabled capabilities will improve every stage of the intelligence cycle from tasking through collection, processing, exploitation, analysis, and dissemination. AI algorithms can sift through vast amounts of data to find patterns, detect threats, identify correlations, and make predictions. AI tools can make satellite imagery, communications signals, economic indicators, social media data, and other large sources of information more intelligible. AI can find correlations between open-source data and other sources of intelligence, and help the Intelligence Community (IC) be more precise, efficient, and effective in its targeting and collections activities. The constellation of current and emerging AI technologies applicable to intelligence missions includes computer vision for imagery analysis, biometric technologies (such as face, voice, and gait recognition), natural language processing, and algorithmic search and query functions for large databases, among others. Most importantly, AI enables data fusion from dissimilar data streams to create a composite picture.[185]

In military scenarios—against technologically advanced adversaries, rogue states, or terrorist organizations—AI-enabled intelligence, surveillance, and reconnaissance platforms and AI-enabled indication and warning (I&W) systems will be critical for the kind of advanced warfighting capabilities discussed in Chapter 3 of this report. Through automation, AI-enabled systems will optimize tasking and collection for platforms, sensors, and assets in near-real time in response to dynamic intelligence requirements or changes in the environment. At the tactical edge, "smart" sensors will be capable of pre-processing raw intelligence and prioritizing the data to transmit and store, which will be especially helpful in degraded or low bandwidth environments. Once collected, intelligent processing systems can triage information, identify trends and patterns, summarize key implications, and prepare the highest priority information for human review (or flag items of particular interest, based on analyst-defined conditions). This includes advanced I&W systems which will enable warfighters to anticipate and understand emerging threats earlier, allowing them to proactively shape the environment, as well as systems close to the tactical edge identifying adversarial denial and deception efforts. When paired with human judgment, these capabilities will enhance all-domain awareness, lead to tighter and more informed decision cycles, offer recommendations for different courses of action, and allow rapid counter-actions to adversary actions.

[185] For additional information on AI-enabled use cases throughout the intelligence cycle, see the discussion on "Applications" in *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation,* CSIS Technology and Intelligence Task Force at 8-22 (Jan. 13, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

The need to adapt is made urgent by the quickening diffusion of these new technologies. Once exquisite IC capabilities are now in wide use around the world.[186] Our adversaries' ability to quickly adopt AI tools means that the IC may be more vulnerable to deception, information operations, sources and methods exposure, cyber operations, and counterintelligence activities. The IC has been an early mover within the government in establishing some of the underlying infrastructure to enable the adoption of AI, such as contracting an IC-wide commercial cloud service in 2013.[187] In addition, the IC's 2019 Augmenting Intelligence with Machines (AIM) Initiative provided direction and a framework for broader adoption, and some intelligence agencies have made great strides in AI adoption, putting them ahead of others in government. Still, critical barriers in authorities, policies, budgets, data sharing, and technical standards keep the IC from fully realizing its potential, and none of these recommendations will be effective without substantial reforms of the security clearance process.

An Ambitious Agenda: AI-Ready by 2025. To build on the progress that individual agencies have made, the IC should set the ambitious goal of adopting and integrating AI-enabled capabilities across every possible aspect of the intelligence enterprise as part of a larger vision for the future of intelligence.

> **An AI-Ready IC by 2025:** Intelligence professionals enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in each stage of the intelligence cycle.

Starting immediately, the IC should prioritize automating each stage of the intelligence cycle to the greatest extent possible and processing all available data and information through AI-enabled analytic systems before human analyst review. Products should also be disseminated at machine speed—which means they must be in machine readable formats—and systems across the IC must be able to ingest and use them without manual intervention. Optimizing AI-enabled systems in this way will require an entirely different approach to the creation and review of finished intelligence products. The IC should require that all intelligence products include both a human-readable version and, as importantly, an automated machine-readable version that can be ingested into other analytic systems throughout the IC. All future intelligence systems should be optimized for AI-oriented data collection and processing.

Preparing for an AI-ready 2025 demands the following actions:

✦ **Change risk management practices to accelerate new technology adoption.** The IC needs to balance the technical risks involved in bringing new technologies on line and quickly updating them with the substantial operational risks that result from not keeping pace, similar to the Department of Defense (DoD). Regular software upgrades should be automated to the extent possible. To share software tools more easily among agencies, reciprocal accreditation of information technology (IT)

[186] *AIM Initiative: A Strategy for Augmenting Intelligence Using Machines*, Office of the Director of National Intelligence (2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf (foreword by the Honorable Sue Gordon, Principal Deputy Director of National Intelligence).
[187] Frank Konkel, *The Details about the CIA's Deal with Amazon*, The Atlantic (July 14, 2014), https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

systems should be the standard.[188]

To coordinate these changes, the Office of the Director of National Intelligence (ODNI) should establish a Senior Risk Management Council focused on technology modernization.[189] Its task should be to weigh the risks of adopting new technologies with the opportunity costs of not doing so. Its goal should be to ensure that analysts have access to the tools they need to do their jobs.

The IC will need support from the intelligence committees in Congress—for example, in the flexible use of funds within a more agile software development framework. To support the argument for greater flexibility, the IC should develop data-driven ways of communicating operational gains, as well as credible assessments of the risk of inaction.

✦ **Empower the IC's science and technology leadership.** The DNI should designate the Director of Science and Technology (S&T) within ODNI as the IC's Chief Technology Officer (CTO) and task and empower this position to drive the IC's adoption of AI-enabled applications to solve operational intelligence requirements. To do so, the IC CTO should oversee the AIM Strategy, establish and enforce common technical standards and policies necessary to rapidly and responsibly scale AI-enabled applications across the IC, and lead acquisition reform to ensure the IC can rapidly procure and field systems to its intelligence professionals. The IC CTO should be granted additional authorities for establishing policies on and supervising IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.

✦ **Improve coordination and interoperability between the IC and DoD.** The IC must aggressively pursue automated interoperability with the DoD for intelligence operations conducted at machine speeds.[190] To do this, security managers and network administrators must build greater confidence in fast and secure data exchanges. ODNI, the Under Secretary of Defense for Intelligence & Security, and the Joint Artificial Intelligence Center (JAIC) should coordinate more on intelligence-related AI projects to minimize duplication of effort, while maximizing common approaches to AI capability development, testing and evaluation, deployment, international engagement, and policies and authorities. They should work together to create interoperable and sharable resources and tools—such as those envisioned in the AI R&D ecosystem described in Chapter 2—and should establish a culture of sharing all AI-enabled capabilities whenever feasible.[191]

✦ **Capitalize on AI-enabled analysis of open source and publicly available information.** The IC should develop a coordinated and federated approach to applying AI-enabled applications to open

[188] In adopting new software systems, the IC follows a risk management framework developed by the National Institute of Standards and Technology. While it is a useful framework overall, it can also create delays or prevent the IC from keeping up with cutting-edge AI tools that are commercially available. For more information, see *FISMA Implementation Project*, National Institute of Standards and Technology (Dec. 3, 2020), https://csrc.nist.gov/projects/risk-management/rmf-overview.

[189] The Senior Risk Management Council would help the IC implement guidance from the proposed Tri-Chair Committee on Emerging Technology and function similarly to the role this commission recommended for the Under Secretary of Defense for Research and Engineering as a co-chair on the Joint Requirements Oversight Council in DoD.

[190] For more information, see Kent Linnebur, et al., *Intelligence After Next: The Future of the IC Workplace*, MITRE Center for Technology and National Security (Nov. 1, 2020), https://www.mitre.org/sites/default/files/publications/pr-20-1891-intelligence-after-next-the-future-of-the-ic-workplace.pdf.

[191] These efforts should leverage the JAIC's Joint Common Foundation (JCF).

source intelligence, and should strive to integrate open source analysis into existing intelligence processes wherever possible.[192]

✦ **Prioritize and accelerate collection of scientific and technical intelligence to better understand adversary capabilities and intentions.** Such collection requires the IC to significantly increase the technical sophistication, capabilities, and capacity of its analytic workforce. That must involve aggressive efforts to train, recruit, and retain analysts who have the requisite skills. These analysts must guide collection requirements and provide timely, accurate assessments. To better coordinate intelligence on these topics, the DNI should appoint an Emerging Technology Collection Executive within the National Intelligence Council.[193]

✦ **To recruit more science and technology experts into the IC, aggressively pursue security clearance reform for clearances at the Top Secret level and above, and enforce security clearance reciprocity among members of the IC.** ODNI should develop and implement an AI-enabled data and science-based approach to security clearance adjudication that significantly shortens investigation timelines.[194]

The Goal: AI-Enabled Intelligence by 2030. By 2030, the IC should rely on a continuous pipeline of all-domain/all-source intelligence analysis processed through a federated architecture of continually-learning analytic engines. This could lead to insights arising from human-machine teaming that are beyond the current limits of unaided human cognition. Such a system would bring greater clarity to ongoing developments and also enable more accurate and reliable predictive analysis of emerging threats. As analysts gain more trust in AI-enabled systems, the ratio of human- to machine-led analysis will tip more heavily toward machines. To achieve this vision the IC should take several steps:

✦ **Advance and continue to build out a purpose-built IC Information Technology Environment that can fuse intelligence from different domains and sources.** An AI-enabled technical architecture of this kind could help autonomously integrate intelligence across stove-piped intelligence domains which currently often require manual intervention to share raw data or finished analysis.[195] Doing so would help the IC blend insights from different streams of information to create a composite picture. For example, signals intelligence often depends upon human intelligence or geospatial intelligence. Likewise, the value of human intelligence can almost always be enhanced by layering signals intelligence or open source information on top of it.

[192] It is important to note that open source intelligence (OSINT) is not limited to traditional media sources (newspapers, radio broadcasts, etc.) and social media. OSINT also includes publicly available information such as public government data sources (official reports, budget documents, hearing testimonies, etc.), professional and academic publications, commercial data sources (industry reports, financial statements, commercial imagery, etc.), and more.

[193] For additional information, see the discussion on "Elevating Technical Intelligence" in *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation,* CSIS Technology and Intelligence Task Force at 12 (Jan. 13, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

[194] For more information on the need for an academic and scientific review of behavioral approaches to security clearance adjudication, see David Luckey, et. al., *Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?*, RAND Corporation at 28-34 (2019), https://www.rand.org/pubs/research_reports/RR2684.html.

[195] The technical aspects of such an environment are covered in more detail in Chapter 2 of this report.

✦ **Embrace fused, predictive analysis as the new standard.** Successfully fusing all-source/all-domain intelligence will enable accurate predictive analysis in a way that is not currently possible. The government's response to COVID-19 has offered glimpses into the potential for fused data sets to inform such analysis. For example, U.S. Northern Command (working with the JAIC and the National Guard Bureau) built predictive models from dozens of different data sets that helped to identify COVID-19 hotspots and reconcile demands for critical supplies.[196]

✦ **Develop innovative human-centric approaches to human-machine teaming.** The kind of data fusion envisioned here through autonomous machine-to-machine integration will require new concepts for human-machine teaming that optimize the strengths of each. The IC will need new approaches that amplify and extend human cognition to effectively handle the scale and complexity of the information generated by an all-intelligence analytic engine.[197] When developing these systems, the IC must understand and make deliberate decisions on when and under what conditions the human or machine should act alone—and under what conditions human-machine collaboration is desirable.

[196] Air Force General Terrence J. O'Shaughnessy, Commander, U.S. Northern Command & Army Lieutenant General Laura J. Richardson, Commander, U.S. Army North, *Transcript: US NORTHCOM and ARNORTH Commanders Discuss Ongoing COVID-19 Efforts*, U.S. Department of Defense (Apr. 21, 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2160070/us-northcom-and-arnorth-commanders-discuss-ongoing-covid-19-efforts/.

[197] Kenneth M. Ford, et al., *Cognitive Orthoses: Toward Human-Centered AI*, AI Magazine at 7 (Winter 2015), https://doi.org/10.1609/aimag.v36i4.2629.

Chapter 6: Technical Talent in Government

The artificial intelligence (AI) competition will not be won by the side with the best technology. It will be won by the side with the best, most diverse and tech-savvy talent. The Department of Defense (DoD) and the Intelligence Community both face an alarming talent deficit. This problem is the greatest impediment to being AI-ready by 2025. National security agencies need more digital experts now or they will remain unprepared to buy, build, and use AI and its associated technologies. Digital expertise is the most important requirement for government modernization, but few parts of government have adequately invested in building a digital workforce.[198]

To expand its digital and AI workforce, the government needs to:

- *Organize* technologists within government through a talent management system designed to house highly skilled specialists;

- *Recruit* people that already have the skills the government needs, such as industry experts, academics, and recent college graduates;

- *Build* its own workforce by training and educating current government employees; and

- *Employ* its digital workforce more effectively to ensure digital talent can perform meaningful work once they are in government.

The Current Model. Government organizations responsible for creating AI solutions are struggling to build their digital workforce. Real obstacles impede recruiting and retaining AI practitioners and broader digital talent. The government does not compete with private sector salaries and suffers from a cumbersome hiring process, and all reforms are hindered by a slow security clearance process.

We should not accept an undesirable status quo as the inevitable future. The government can compete with the private sector for talent. The government may not match private sector salaries, but it does offer the opportunity to tackle national security challenges and to make a substantial contribution to society. The biggest obstacle hindering the recruitment of digital talent is not compensation. It is the perception, and too often the reality, that it is difficult for digital talent in government to perform meaningful work, with modern computing tools, at the forefront of a rapidly changing field.[199]

The Commission is not persuaded by the argument that the government should focus on project management and data collection and management, and outsource all development. We have heard this argument from leaders who do not believe it is feasible for the government to hire or train its own AI experts. Interestingly, we have not heard this argument from industry.

[198] There are pockets of excellence in several parts of the government—such as in the United States Digital Service, Kessel Run, the Army Artificial Intelligence Task Force, the USAF-MIT AI Accelerator, components of the Intelligence Community, and the national labs—but there are too few, and they have not spread across government enough. Agencies' requirements for the size and type of AI workforce vary, but every agency NSCAI has engaged has expressed a need to expand its AI workforce, and the below recommendations are broadly applicable.

[199] NSCAI staff discussions with the Defense Innovation Board and Defense Digital Service (May 2019).

Government strategies that do not develop a government technical workforce are short-sighted. Government agencies that rely solely on contractors for digital expertise will become incapable of understanding the underlying technology well enough to make successful acquisition decisions independent of contractors.[200] This situation creates national security risks. While contractors should continue to play a critical role, they are incentivized, and in some sense required, to fulfill the terms of their contract, not to pursue overall system improvements, or to disagree with poorly thought out requirements or ineffective strategies. As a result, agencies that rely on contractors force their digital experts to have a secondary voice in key decisions, even those related to their field of expertise. The government will always have contractors. But the government can and should grow its own digital workforce.

Organize. How a digital workforce is organized is as important as the workforce's level of expertise. To generate and manage a proficient digital workforce at the scale required by the national security enterprise, the government needs to establish a talent management framework tailored to the task.

✦ **Create a Digital Corps.** We propose agencies create Digital Corps that would recruit, train, and educate personnel; place personnel in and remove personnel from digital workforce billets; manage digital careers; and set standards for digital workforce qualifications. Agencies would create billets for members of the digital corps, and provide guidance to members of the Digital Corps about the work they perform for the agencies.

The Digital Corps model is inspired by the Army's Medical Corps, which organizes experts with specialized healthcare skills that do not fit into the Army's traditional talent management framework. Like the Medical Corps, the Digital Corps should have specialized personnel policies, guidelines for promotion, training resources, and certifications for personnel to demonstrate proficiency in new digital areas.

Recruit. To create digital corps or improve its digital workforce, the government needs to improve recruiting and the hiring process, accelerate security clearances, use temporary hiring vehicles such as the IPA, and build mechanisms for part-time civilian service. Many AI and other digital practitioners are interested in working with the government as either full-time employees or part-time employees. Of those desiring full-time employment, some seek an entire career as a government civilian or in the military. Others are less willing to make long-term commitments and instead desire to become temporary, full-time employees, fellows, talent exchange participants, or military reservists. A third group is willing to work with or for the government part-time, but they are unwilling to become full-time civilian employees and have no desire to serve as part of the military.

✦ **Establish a Civilian National Reserve Digital Corps.** The government must tap into the pool of technologists willing to contribute part of their time to public service by creating a mechanism to hire them. While part-time employees are not a substitute for full-time employees, they can help improve AI education, perform data triage and acquisition, help guide projects and frame digital solutions, build bridges between the public and private sectors, and accomplish other important tasks.

[200] William A. LaPlante, *Owning the Technical Baseline*, Defense AT&L at 18-20 (July-Aug. 2015), https://apps.dtic.mil/dtic/tr/fulltext/u2/1016084.pdf.

To eliminate this recruitment gap, the government should establish a civilian National Reserve Digital Corps (NRDC) modeled after the military reserve's commitments and incentive structure. Members of the NRDC would become civilian government employees in the Digital Corps, and work at least 38 days each year as advisors, instructors, or developers across the government.

✦ **Streamline the hiring process and expand digital talent pipelines.** The government's hiring system's problems are well known: it moves too slowly, struggles to attract experts in a competitive market, and makes it difficult for experts that are young or do not have a degree to be hired, especially at a pay grade matching their level of expertise. These challenges are not caused by a lack of hiring authorities or an inherently slow hiring process. The Commission has been unable to identify a gap in hiring authorities for the digital workforce.

To clear this recruiting bottleneck, the government needs to expand science, technology, engineering, and mathematics (STEM) and AI talent pipelines from universities to government service, streamline the hiring process, and create agency and military service specific digital talent recruiting offices either for digital corps or agencies. The recruiting offices would monitor their corps, agency, or service's need for specific types of digital talent and be empowered to recruit technologists virtually, by attending conferences and career fairs, recruiting on college campuses, hosting prize competitions, and offering scholarships, recruiting bonuses, and referral bonuses.

Standing Digital Corps will oversee government-wide progress and make recommendations to expand and improve digital talent hiring and pipelines. They should also be able to experiment with new authorities.

Build. The government will not be able to recruit its way out of its technology workforce deficit. AI and digital talent are simply too scarce in the United States. In 2020, there were more than 430,000 open computer science jobs in the United States, while only 71,000 new computer scientists graduate from American universities each year.[201] The government should also make a new commitment to building its workforce from the ground up with a major initiative.

✦ **Establish a United States Digital Service Academy.** The United States needs to establish a new service academy to train future civil servants in digital skills to create a digitally skilled civil service prepared to modernize the government. The United States Digital Service Academy (USDSA) would be an accredited, degree-granting university that receives both government and private funding, is managed by a purpose-built independent agency within the federal government, and meets the government's needs for digital expertise as determined by an interagency board assisted by a Federal Advisory Committee composed of private sector and academic technology leaders. The USDSA should be modeled off of the five U.S. military service academies, but produce trained and educated government civilians for all federal government departments and agencies.

Employ. Digitally talented people should be able to reasonably expect to spend a career performing meaningful work focused on their field of expertise in government. Without such an expectation, they are unlikely to join the government workforce, and without their experience matching

[201] Code.org (last accessed Jan. 11, 2021), https://code.org/promote. See also Oren Etzioni, *What Trump's Executive Order on AI Is Missing: America Needs a Special Visa Program Aimed at Attracting More AI Experts and Specialists*, Wired (Feb. 13, 2019), https://www.wired.com/story/what-trumps-executive-order-on-ai-is-missing/.

expectations, they are unlikely to stay for long. Aligning expectations and experience for the digital workforce requires three changes:

- Opportunity for technologists to spend an entire career focused on the field they are passionate about;
- Well-informed leaders, some of whom are digitally proficient themselves; and
- Access to tools, data sets, and infrastructure.

These changes are more tactical than those described above, but no less impactful. Strategic initiatives succeed or fail at the tactical level, and many digital initiatives that might otherwise have strategic impact are struggling or failing tactically in part because the government does not employ its technologists effectively.

✦ **Establish new digital career fields.** New career fields challenge an organization's definition of its necessary competencies and, potentially, the nature of its identity. If the military services create career fields for software developers and data scientists, this will almost inevitably change what it means to be a soldier, sailor, airman, or marine, much as the introduction of aviation did generations ago. The government should create civilian occupational series for software development, software engineering, knowledge management, data science, and artificial intelligence. The military services should create career fields in software development, data science, and artificial intelligence, with both management and specialist tracks. Digital corps will need additional career fields as they develop, but the above described will establish a strong foundation.

✦ **Expand access to tools, data sets, and infrastructure.** Highly skilled technologists working in government are regularly denied access to software engineering tools. The digital workforce needs access to enterprise-level software capabilities on par with those found in the private sector. Capabilities include software engineering tools, access to software libraries, vetted open-source support, curated data sets, and infrastructure for large-scale collaboration.

All career fields need improved access to the latest open-source libraries and tools.[202] Most advanced AI and machine learning libraries need vast amounts of data available to train models on. Providing AI practitioners with rich data sets across the physical and biological sciences, economics, and behavioral studies will let them focus on their areas of expertise rather than scraping obscure sources for data.

[202] For the AI career field in particular, TensorFlow is one of the world's most popular libraries for training neural networks and other machine learning algorithms. PyTorch is another open-source library that aids in transforming research prototypes to production-ready machine learning models. These two libraries were implemented by Google Brain and Facebook AI Research (FAIR) respectively, and are must-have tools in any AI developer's arsenal.

Chapter 7: Establishing Justified Confidence in AI Systems

Artificial intelligence (AI) systems must be developed and fielded with justified confidence.[203] If AI systems routinely do not work as designed or if an AI system is unpredictable in ways that can have significant negative consequences, then leaders will not adopt it, operators will not use it, Congress will not fund it, and the American people will not support it.

Achieving acceptable AI performance often is linked to the decision to accept some level of risk. No technology works perfectly under all conditions. Risk calculus changes with circumstances. The variables and considerations that inform judgments to rely on AI will vary significantly across military, intelligence, homeland security, or law enforcement missions. In a high threat environment like combat, in some cases it may be reasonable to employ a system offering some immediate military advantage, while recognizing that it might fail; in other cases, however, a reasonable commander might want the highest assurances of AI reliability before fielding when lives are at risk.

As departments and agencies rely more heavily on machines, a central guiding principle across national security scenarios is the continued centrality of human judgment. Those charged with utilizing AI need an informed understanding of risks, opportunities, and tradeoffs. They need awareness of the possibilities and limitations in a system's expected performance. Ultimately, they need to formulate an educated answer to this question: In the given circumstance, how much confidence in the machine is enough confidence? These issues bear on the full lifecycle of an AI system—from acquisition or system development, to the thresholds for justified confidence to deploy a specific AI-intensive system, to the performance of the system in the field.

While there is no absolute assurance or perfection, there are policies and best practices that support making these decisions responsibly. Agencies are broadly aware of the principal challenges in employing AI systems and the necessity of incorporating best practices in the engineering and management of AI systems.

The Commission has produced a detailed framework to guide the responsible development and fielding of AI across the national security community. It contains key considerations for policymakers and technical practitioners covering the full breadth of the AI lifecycle and can be found in an Appendix to this report. The framework includes recommended practices that should be integrated and updated as the technology advances. The Commission is heartened that some departments have already taken actions to integrate recommendations from our framework, Key Considerations for the Responsible Development and Fielding of AI.[204]

[203] The term "justified confidence," taken from a widely used international standard, uses a specific definition of assurance as being "grounds for justified confidence." It notes that "stakeholders need grounds for justifiable confidence prior to depending on a system," and that "the greater the degree of dependence, the greater the need for strong grounds for confidence." IEEE Standard Adoption of ISO/IEC 15026-1, Systems and Software Engineering - Systems and Software Assurance, https://standards.ieee.org/standard/15026-1-2014.html.

[204] The Department of Defense's Joint Artificial Intelligence Center (JAIC) Subcommittees on Responsible AI and Test & Evaluation have both conducted substantial mapping exercises to determine which existing practices correspond to recommendations found in the Key Considerations. Recommendations from the Key Considerations are also reinforced by inclusions in the Department of Homeland Security (DHS)'s AI Strategy. See *Department of Homeland Security Artificial Intelligence Strategy*, DHS (Dec. 2020), https://www.dhs.gov/publication/us-department-homeland-security-artificial-intelligence-strategy?topic=intelligence-and-analysis.

To assist agencies in meeting baseline criteria for responsible AI, we highlight the main challenges and key recommendations in our framework across five issue areas:

Robust and Reliable AI. Current AI systems, such as those used for perception and classification, have different kinds of failure—characterized as rates of false positives and false negatives. They are often brittle when operating at the edges of their performance competence, and it is difficult to anticipate their competence boundaries. They are also vulnerable to attack, and they can exhibit unwanted bias in operation. For national security missions, these can be serious problems. U.S. government agencies should:

✦ **Focus more federal research and development (R&D) investments on advancing AI security and robustness.** These investments should also advance the interpretability and explainability of AI systems, so users can better understand whether the systems are operating as intended.

✦ **Consult interdisciplinary groups of experts to conduct risk assessments, improve documentation practices, and build overall system architectures to limit the worst-case consequences of system failure.**[205] Such architectures should securely monitor component performance and handle errors when anomalies are detected;[206] contain AI components that are self-protecting (validating input data) and self-checking (validating data passed to the rest of the system); and include aggressive stress testing.

Human-AI Interaction and Teaming. The government needs AI systems that augment and complement human understanding and decision-making so that the complementary strengths of humans and AI can be leveraged as an optimal team. Achieving this remains a challenge. For instance, humans are prone both to over-trusting and to under-trusting machines depending on context. Challenges also exist for measuring the performance of human-AI teams, conveying enough information while avoiding cognitive overload, enabling humans and machines to understand the circumstances in which they should pass control between each other, and maintaining appropriate human engagement to preserve situational awareness and meaningfully take action when needed. Agencies will also need to determine machine performance standards and expectations as compared with humans. The government should:

✦ **Pursue a sustained, multi-disciplinary initiative through national security research labs to enhance human-AI teaming.** This initiative should focus on maximizing the benefits of human-AI interaction; better measuring human performance and capabilities when working with AI systems, including testing through continuous contact and experimentation with end users; and helping AI systems better understand contextual nuances of a situation.

✦ **Clarify policies on human roles and functions, develop designs that optimize human-machine interaction, and provide ongoing and organization-wide AI training.**

[205] Such interdisciplinary teams should explore the possibility of documentation/labels specifying the narrow task/mission for which a system was designed and tested. As noted in the Annex (Key Considerations for Responsible Development & Fielding of AI), documentation of the AI lifecycle should include information about the data used to train and test a model and the methods used to test a model, both based on the context in which it will be used. It also should include requirements for re-testing, retraining, and tuning when a system is used in a different scenario or setting.

[206] Monitoring can add a layer of robustness, but must itself also be guarded to prevent new openings for external espionage or tampering with AI systems.

Testing and Evaluation, Verification and Validation. Having justified confidence in AI systems requires assurances that they will perform as intended, including when interacting with humans and other systems. The TEVV of traditional legacy systems is not sufficient at providing these assurances. As a result, agencies lack common metrics to assess trustworthiness that AI systems will perform as intended. To minimize performance problems and unanticipated outcomes, an entirely new type of TEVV will be needed. This is a priority task, and a challenging one. The federal government will need to increase R&D investments to improve our understanding of how to conduct AI and software-related TEVV. Toward this end:

✦ **DoD should adopt a sweeping package of testing and evaluation processes, methods, and resources for AI systems.** This should include establishing a TEVV framework and culture that integrates continuous testing; making TEVV tools and capabilities more readily available across the Department of Defense (DoD); and updating or creating live, virtual, and constructive test ranges for AI-enabled systems.[207]

✦ **National Institute of Standards and Technology (NIST) should provide and regularly refresh a set of standards, performance metrics, and tools for qualified confidence in AI models, data, and training environments, and predicted outcomes.** NIST should lead the AI community in establishing these resources, closely engaging with experts and users from industry, academia, and government to ensure their efficacy.

Leadership. Responsible development and fielding of AI requires end users and senior leaders to be aware of system capabilities and limitations so that they are not misused. It also requires subject matter experts to support training, acquisition, risk assessment, and adoption of best practices as they evolve. Today, only the DoD has a dedicated lead for responsible AI; employees in national security agencies taking on these roles typically do so on a voluntary, part-time basis. Without full-time dedicated staff, agencies will not succeed in fully adopting and implementing these recommended practices. The government should:

✦ **Appoint a full-time, senior-level responsible AI lead in each national security agency and each branch of the armed services.** Such an official should drive Responsible AI training, provide expertise on Responsible AI policies and practices, lead interagency coordination, and shape procurement policies.

✦ **Create a standing body of multi-disciplinary experts in the National AI Initiative Office.** The standing body would provide advice to agencies as needed on responsible AI issues. The group should include people with expertise at the intersection of AI and other fields such as ethics, law, policy, economics, cognitive science, and technology including adversarial AI techniques.

Accountability and Governance. Congress and the public need to see that the government is equipped to catch and fix critical flaws in systems, in time to prevent inadvertent disasters, and hold humans accountable, including for misuse. Agencies need the ability to monitor AI performance as systems run (to assess if they are performing as intended) and to build systems with the necessary

[207] Upgrades to digital infrastructure, as outlined in Chapter 2, will be required to augment physical test ranges to create digital testing environments that can leverage digital twins.

instrumentation to do so.[208] Departments and agencies critical to national security and oversight entities have all expressed challenges with having visibility into their systems, while vendors are calling for clarity on instrumentation/auditability requirements. Government agencies should:

✦ **Adapt and extend existing accountability policies to cover the full lifecycle of AI systems and their components.**

✦ **Establish policies that allow individuals to raise concerns about irresponsible AI development, and institute comprehensive oversight and enforcement practices.** These should include auditing and reporting requirements, a review mechanism for the most sensitive or high-risk AI systems, and appeals and grievance processes for those affected by the actions of AI systems.

[208] Cases where new sensors and instrumentation are added can also introduce new vulnerabilities. It is especially important to ensure the overall architecture of such systems are secure against external espionage and tampering.

Chapter 8: Upholding Democratic Values: Privacy, Civil Liberties, and Civil Rights in Uses of AI for National Security

The basic purpose of the American government is to protect the security and liberty of the American people. Americans have a long tradition of debating how best to achieve these twin goals when tensions arise between them. The two decades following 9/11 saw intensive efforts to calibrate the government's powers to stop another terrorist attack with its obligations to respect individual rights and liberties. AI is ushering in the next era of this debate because new technologies offer government agencies more powerful ways to collect and process information, track individuals' behavior and movements, and act on the basis of computer-generated analyses.

In addition to supporting military and intelligence missions abroad, these tools are promising for national security purposes closer to home—whether to examine foreign intelligence to find signs of danger to the United States, to screen for threats at the borders, to protect against cyber attacks and information operations, or to identify domestic terrorism plots. Americans have concerns that AI applications used for these security and public safety purposes—especially those involving biometric technologies or the analysis of aggregated personal data—will invade their privacy, restrict their freedoms of speech and assembly, and reinforce bias and discrimination. At the same time, if applied effectively, AI can help improve protections for privacy and civil liberties. Machine analysis could be more precise, and AI systems potentially could enhance oversight through real-time monitoring.

For the United States, as for other democratic countries, official use of AI must comport with principles of limited government and individual liberty. These principles do not uphold themselves. In a democratic society, any empowerment of the state must be accompanied by wise restraints to make that power legitimate in the eyes of its citizens.

As this report argues, the promise of emerging AI technologies to enhance national security is real and significant. The ability of U.S. intelligence, homeland security, and law enforcement agencies to develop and use them for national security purposes must be preserved. To do so, however, the government must ensure that their use is effective, legitimate, and lawful. Public trust will hinge on justified assurance about compliance with privacy, civil liberties, and civil rights.

Democratic AI Governance and Novel Challenges for Privacy, Civil Liberties, and Civil Rights. With new models of techno-authoritarian governance gaining traction abroad, the United States must continue to serve as a beacon of democratic values. The democratic model must prove its resilience in the face of emerging technological changes that could challenge it. Fundamentally, we are confident that the American system—and the rules, norms, and institutions that uphold it—can adapt to uphold the dual imperatives of security and liberty in the AI era.

For the IC, core features of that system include laws, rules, and procedures to minimize the collection, retention, and dissemination of U.S. persons' data, as well as oversight from all three branches of government.[209] Homeland security and law enforcement agencies likewise operate within

[209] For a compilation of Attorney General guidelines from the IC components, see *Status of Attorney General Approved U.S. Person Procedure under E.O. 12333*, ODNI (July 14, 2016), https://www.dni.gov/files/documents/Table_of_EO12333_AG_Guidelines%20for%20PCLOB_%20Updated%20July_2016.pdf. Elements of the IC oversight system include counsels and privacy officials within intelligence agencies, the Department of Justice,

frameworks of policy, oversight, and judicial review that guide border protection and criminal investigations. Ultimately, the actions of all federal agencies are subject to the Constitution's guarantees.

Within this context, the advent of modern AI—and the novel capabilities it can bring to intelligence, homeland security, and law enforcement missions—raises a number of concerns and difficult questions and challenges with respect to the privacy, civil liberties, and civil rights of U.S. persons. For example:

- AI-powered analytics can help officials process and make sense of huge amounts of information, which can be aggregated to form a revealing "mosaic" picture of a person's activities, whereabouts, and patterns of behavior.[210] Combining disparate data streams involving geolocation, web browsing, financial transactions, and other data sources creates the possibility of new insights for analysts or investigators. This could be highly useful to identify threats, but has also raised questions about the proper scope and authorization for border or law enforcement searches.[211]

- Much of this personal information is held by private companies. This fact of modern digital life has raised constitutional questions about whether and when individuals should have a "reasonable expectation of privacy" in the information they provide to third parties like technology firms—and questions about the circumstances in which that information may be accessed and utilized by intelligence, homeland security, or law enforcement agencies for a legitimate national security purpose.[212]

- AI can help automate aspects of data collection and analysis. Such methods can augment the ability of analysts or investigators to sift through and triage masses of information to establish patterns or pinpoint threats. But they also raise questions about the proper roles of machine and human analysis in these processes, including for making predictive judgments. To the extent that an AI system's functions are opaque, it may be difficult to trace and justify the computational process that led the system to make a recommendation. Determining when and how to rely on algorithms is especially pertinent to minimization and querying procedures in the IC, and to building cases for law enforcement action.[213]

independent bodies such as the Privacy and Civil Liberties Oversight Board, Federal courts including the Foreign Intelligence Surveillance Court, and the House and Senate intelligence committees.

[210] On the mosaic concept, see, for example, Steven M. Bellovin, et al., *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, NYU Journal of Law & Liberty, Vol. 8 (Sept. 3, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320019.

[211] For an informative discussion of evolving debates over Fourth Amendment regulation of government searches in the context of AI, see James E. Baker, *The Centaur's Dilemma: National Security Law for the Coming AI Revolution*, Ch. 6 (Brookings, 2020).

[212] Congress and the Judiciary will need to assess the adequacy of current legal constraints over the federal government's obtainment and use of third party data, including data acquired from data brokers. Either through evolving case law or legislation, agencies would benefit from clarity surrounding the Fourth Amendment's application with respect to third party data. On third-party doctrine, see Richard M. Thompson II, *The Fourth Amendment Third-Party Doctrine*, Congressional Research Service (June 5, 2014), https://fas.org/sgp/crs/misc/R43586.pdf.

[213] For a discussion and different views on the implications of human and machine analysis in the intelligence context, see Robert Litt, *The Fourth Amendment in the Information Age*, Yale Law Journal Vol. 126 (Apr. 27, 2016), https://www.yalelawjournal.org/forum/fourth-amendment-information-age; Cindy Cohn, *Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt*, Yale Law Journal (July 27, 2016), https://www.yalelawjournal.org/forum/protecting-the-fourth-amendment-in-the-information-age.

- AI models can evolve based on changing data and interaction with other models, leading to unexpected outcomes. As a result, AI systems require more continuous testing and evaluation than prior generations of technology.

- Unintended bias can be introduced during many stages of the machine learning (ML) process, which can lead to disparate impacts in American society, a problem that has been documented in law enforcement contexts.[214]

Tenets for Managing AI Challenges. This Commission will not endeavor to draw all of the lines for what may be permissible or wise in particular circumstances. However, important principles to follow in different national security contexts include the following:

- *Foreign Intelligence Collection and Analysis*: The Office of the Director of National Intelligence (ODNI) AI Ethics Guidance to the Intelligence Community is an encouraging step, as it places strong emphasis on utilizing AI for foreign intelligence missions in ways that uphold the privacy and civil liberties of Americans.[215] *As these guidelines are implemented, it will be important to pay close attention to ensuring that data minimization, retention, and querying procedures are adequate and rigorously enforced.*

- *Border Security*: AI surveillance and analysis capabilities can make the government's operations more efficient and effective at the borders and ports of entry. But to sustain public support for these uses, *the Department of Homeland Security (DHS) must take care to ensure that automated screening processes lead agents only to the information they need and are authorized to access, and do not impermissibly single out individuals based on characteristics such as race or religion.*

- *Domestic Security and Public Safety*: Rapid advances in AI-enabled technologies for law enforcement purposes, including biometric surveillance techniques such as facial recognition, may be outpacing rules for their proper use. *The government must exercise special caution in managing risks to bedrock constitutional principles including equal protection, due process, freedom from unreasonable searches and seizures, and freedoms of speech and assembly.*[216]

In carrying out these missions, it will be important to maintain clear distinctions between appropriate authorities in these different national security contexts. It is also important to gain greater public confidence by enhancing transparency, improving the performance and reliability of AI technologies, ensuring due process, and strengthening oversight. With these tenets in mind, the government should take the following steps:

[214] Concerns about algorithmic error rates and disparate performance across age, skin tones, and genders are especially pronounced for facial recognition. See Patrick Grother, et al., *Face Recognition Vendor Test: Part 3 Demographic Effects*, NIST (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. The Gender Shades Project found that various facial recognition systems were very accurate for white men, but significantly less accurate for women and people of color (and worst for women of color). See Gender Shades (last accessed Jan. 11, 2021), http://gendershades.org/.

[215] See *Principles of Artificial Intelligence Ethics for the Intelligence Community*, ODNI (last accessed Jan. 11, 2021), https://www.dni.gov/index.php/features/2763-principles-of-artificial-intelligence-ethics-for-the-intelligence-community.

[216] Some observers have found a "chilling effect" that impacts the degree to which individuals exercise freedoms of expression, association, and assembly. See, for example, Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, Emory Law Journal Vol. 66 (2017), https://scholarlycommons.law.emory.edu/elj/vol66/iss3/4/.

✦ **Invest in and adopt AI tools to enhance oversight and auditing in support of privacy and civil liberties.** Agencies should assess near-term opportunities and research gaps in applications of AI to address privacy and civil liberties challenges, such as ML techniques for classification, recommendation, anomaly detection and other applications.[217] Examples of advances in AI to improve auditing include tools that support financial audits and model risk management. Agencies should examine the utility of these and other current or emerging practices.[218]

✦ **Improve public transparency about how the government uses AI.** There is a lack of transparency into agency policies and procedures, and into the accuracy of AI systems that may impact civil liberties.[219] The "black box" nature of some ML systems only adds to this opacity.[220] More transparency could help to ease public concerns. Of course, in certain operational contexts, especially for intelligence and law enforcement agencies, secrecy is essential to the mission. However, existing transparency mechanisms could be utilized more effectively, and in some cases, revised. New agency reporting requirements would also be beneficial. In particular, Congress should amend impact assessment and disclosure reporting requirements to require the DHS and the Federal Bureau of Investigation (FBI) to publish civil rights and civil liberties reports for each new AI system or significant system refresh. DHS and the FBI should also improve practices for issuing system of record notices and privacy impact assessments to provide a more holistic view of the role of AI systems before they are fielded.

✦ **Develop and test systems with the goal of advancing privacy preservation and fairness.** ML systems in particular require ongoing assessments of privacy and fairness assurances, including the specific definition of fairness being assumed. Although an ML system may meet requirements at a static point in time, ongoing compliance is not a given once the system is operational. This is in large part due to changing data, the introduction of unintended bias, and potential re-identification of anonymized data.[221] This is a complex technical area, and continued work in the technical, legal, and

[217] Xuning (Mike) Tang & Yihua Astle, *The Impact of Deep Learning on Anomaly Detection*, Law.com (Aug. 10, 2020), https://www.law.com/legaltechnews/2020/08/10/the-impact-of-deep-learning-on-anomaly-detection/.

[218] See e.g., Bernhard Babel, et al., *Derisking Machine Learning and Artificial Intelligence*, McKinsey & Company (Feb. 19, 2019), https://www.mckinsey.com/business-functions/risk/our-insights/derisking-machine-learning-and-artificial-intelligence; Saqib Aziz & Michael Dowling, *Machine Learning and AI for Risk Management*, Disrupting Finance at 33-50 (Dec. 7, 2018), https://link.springer.com/chapter/10.1007/978-3-030-02330-0_3.

[219] For instance, disclosure by U.S. Customs and Border Protection (CBP) when using facial recognition at airports has been inconsistent, and claims exist that the FBI failed to provide information about its Next Generation Identification database and use of facial recognition as required by law. In 2020, the U.S. Government Accountability Office (GAO) found that "CPB's privacy notices—which informs the public about its use of this technology—were not always current or available [at airports] where this technology is being used or on CBP's website." *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO (Sept. 2, 2020), https://www.gao.gov/products/GAO-20-568; see also *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016), https://www.perpetuallineup.org/.

[220] In a 2018 report, GAO has raised concerns about lack of transparency from tech companies that build algorithms and "limited testing on the systems for accuracy." *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications*, GAO (Mar. 2018), https://www.gao.gov/assets/700/690910.pdf.

[221] For example, pseudonymized data can be linked with other data to uncover a cell phone owner's identity. See Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall Street Journal (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=breakingnews.

policy domains is required to find greater consensus on technical approaches to preserving privacy, civil liberties, and civil rights.[222] Meanwhile, agencies should take several steps:

- *Assess risks in the design, development, and testing of AI systems.* IC agencies, DHS, and the FBI should assess risks to the privacy, civil liberties and civil rights of U.S. persons, take measures to mitigate those risks, and document remaining risks that are accepted. In doing so, they should adopt practices from the Key Considerations, including conducting privacy, civil liberties and civil rights risk assessments; using privacy protections such as robust anonymization, and when possible, privacy-preserving technology; taking steps to bias in development and testing; and assessing model performance on an ongoing basis.[223]

- *Identify an office, committee, or team in each agency that will conduct a pre-deployment review of AI technologies that will impact privacy, civil liberties, and civil rights.* This should include review in advance of their deployment and for compliance over the lifespan of the system. An office in each IC agency, DHS, and the FBI should be equipped to assess data, document models and systems, and test the degree to which results fit their intended use.

- *Establish third-party testing centers for national security-related AI systems that could impact U.S. persons.* Such independent, third-party testing could be done by a national laboratory, a University Affiliated Research Center, or a Federally Funded Research and Development Center. Such testing should be mandatory for high-stakes systems[224] but otherwise voluntary. It would provide agencies with additional expertise to help overcome in-house limitations.

✦ **Strengthen the ability of those impacted by government actions involving AI to seek redress and have due process.** AI systems will make errors.[225] Agencies have to accept non-zero false positive and false negative rates in order to deploy any AI system. It is important to ensure opportunities for redress, consistent with the constitutional principle of due process—for example, when a system error leads to a benefit being denied (e.g., visa approval); restrictions on movement (e.g., being placed on a no-fly list); or an arrest. There are also due process concerns in cases where AI contributes to building a case to press criminal charges.[226] We recommend two steps to start addressing these issues:

[222] Investments to better test and evaluate systems, as outlined in Chapter 7, will be required to continually advance capabilities in this domain. "The National Institute of Standards and Technology (NIST) should provide and regularly refresh a set of standards, performance metrics, and tools for qualified confidence in AI models, data, and training environments, and predicted outcomes."

[223] *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI (July 2020), https://www.nscai.gov/reports.

[224] To provide agencies guidance on when such a test mechanism should be leveraged, an organization should establish guidance on thresholds by which agencies would be required to conduct third-party testing. This should include criteria for when an AI system may pose high enough risk for privacy, civil liberties, and civil rights that it would trigger a testing requirement by a third-party auditor.

[225] See, e.g., Kashmir Hill, *Wrongfully Accused by an Algorithm*, New York Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[226] Due process rights require that individuals have the ability to meaningfully challenge a decision made against them. In federal criminal trials, this includes the government explaining how an unfavorable decision was reached, so it can be contested. In cases where AI-assisted or AI-enabled decisions are made, certain AI techniques will be less conducive to due process. See Danielle Keats Citron, *Technological Due Process*, Washington University Law Review Vol. 85 (2008), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview and Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, Emory Law Journal (Mar. 9, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3553590. Early cases in which an AI system's predictions, classifications, or recommendations have been challenged in court illustrate that defendants encounter substantial impediments in seeking to exercise

- *Review DHS and FBI policies and practices that may impact due process and the ability to seek redress.* DHS and the FBI should review agency policies and practices to ensure that parties aggrieved by government action involving AI technology, including through system actions or misuse, can seek redress and clearly know how to do so. This review should include whether adequate notice of AI use in decision-making is provided to impacted parties, as well as the degree to which AI systems can be audited to trace the process by which a system arrived at a recommendation, if it is contested.

- *Issue Attorney General guidance on AI and due process.* The guidance should describe how relevant agencies should safeguard the due process rights of U.S. persons when AI use may lead to a deprivation of life or liberty.

✦ **Strengthen oversight mechanisms to address current and evolving concerns.** The advancement of AI requires a forward-looking approach to oversight that anticipates the continued evolution and adoption of new technologies, and better positions the government to responsibly manage their employment well into the future. The government should:

- *Establish a task force to assess the privacy and civil liberties implications of AI and emerging technologies.* The goal of the task force would be to identify gaps and make recommendations to ensure that uses of AI in U.S. government operations comport with U.S. law and values, and to study organizational reforms that would support this goal. Specifically, it should assess existing policy and legal gaps for current AI applications and emerging technologies, and make recommendations for:
    - legislative and regulatory reforms on the development and use of AI and emerging technologies[227]; and
    - institutional changes to ensure sustained assessment and recurring guidance on privacy and civil liberties implications of AI applications and emerging technologies.

- *Strengthen the ability of the Privacy and Civil Liberties Oversight Board (PCLOB) to provide meaningful oversight and advice on AI use for national security.* Since its creation in 2007, following a recommendation of the 9/11 Commission, PCLOB has had an especially important role in overseeing, and advising the government on, U.S. counterterrorism missions. In recent years, it has started turning attention to the use of new technologies in foreign intelligence collection and analysis.[228] The board should be given visibility into AI systems before they are fielded, including at a more granular technical level, and should be resourced and staffed to fulfill the more technically sophisticated mission that the AI era now requires.[229]

their rights. See *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems*, AI Now Institute (Sept. 2018), https://ainowinstitute.org/litigatingalgorithms.pdf. There are also open questions including federal rules of evidence and criminal procedure as they relate to AI. For instance, evidentiary standards for admitting AI evidence in court have yet to be developed and are not encompassed in current Daubert standards.

[227] Examples include baseline AI standards and policy guidance for biometric identification technologies; for government procurement of commercial AI products; and for federal data privacy standards.

[228] See *Projects*, PCLOB (last accessed Jan. 9, 2021), https://www.pclob.gov/Projects.

[229] PCLOB works alongside multiple oversight organizations to conduct oversight. It will also be important for PCLOB and such organizations to better align and coordinate to conduct complementary AI oversight and auditing with respect to privacy, civil liberties and civil rights.

- *Empower DHS Offices of Privacy and Civil Rights and Civil Liberties (CRCL).* The Chief CRCL Officer, in coordination with the Privacy Officer, must play an integral role in the legal and approval processes for the procurement and use of AI-enabled systems, including for associated data used in DHS ML systems.

- *Require stronger coordination and alignment among federal oversight and audit organizations.* Compliance by agencies with AI documentation and testing requirements should be supported by rigorous, technically informed oversight. To achieve this and overcome current audit and oversight impediments, a standing body should align and coordinate to enhance AI oversight and audit with respect to privacy, civil liberties and civil rights.[230]

[230] For examples of impediments, see Taka Ariga & Stephen Sanford, *A is for Accountability - Oversight in the Age of Artificial Intelligence,* ECA Journal at 88-91 (Jan. 2020), https://www.eca.europa.eu/Lists/ECADocuments/JOURNAL20_01/JOURNAL20_01.pdf; see also Press Release, Office of the Inspector General of the Intelligence Community, *The Inspector General of the Intelligence Community Issues Statement on Artificial Intelligence* (May 30, 2019), https://www.dni.gov/files/ICIG/Documents/News/ICIG%20News/2019/May%2030%20-%20AI/Press%20Release%20-%20AI.pdf; Michael K. Atkinson, *Semiannual Report: October 2018 - March 2019*, Office of the Inspector General of the Intelligence Community (2019), https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2019/ICIG%20Semiannual.

PART II: WINNING THE TECHNOLOGY COMPETITION

Chapter 9: A Strategy for Competition and Cooperation

AI's impact on the world will extend far beyond narrow national security applications. The development of AI constitutes a new pillar of strategic competition, and heightens the competition in existing pillars. The nation with the most resilient and productive economic base will be best positioned to seize the mantle of world leadership. That base increasingly depends on the strength of the innovation economy, which in turn will depend on AI. AI technologies will drive waves of advancement in critical infrastructure, commerce, transportation, health, education, financial markets, food production and environmental sustainability.

The race to research, develop and deploy AI and associated technologies is already intensifying strategic competition. The U.S. government must embrace the AI competition and organize to win it. The American approach to innovation, which has served the country well for decades, must be recalibrated to account for the centrality of the competition involving AI and associated technologies to the emerging US-China rivalry. To retain its innovation leadership and position in the world, the United States needs a stronger government-led technology strategy that integrates promotion and protection policies and links investments in AI to a larger constellation of related emerging technologies.[231]

The U.S.-China AI Competition is Serious and Complex. The leading indexes that measure progress in AI development generally place the United States ahead of China.[232] However, the gap is closing quickly. China stands a reasonable chance of overtaking the United States as the leading center of AI innovation in the coming decade.[233] In recent years, technology firms in China have produced pathfinding advances in natural language processing,[234] facial recognition technology,[235] and other AI-enabled domains. China's businesses, investors, technologists, and academics are integral to global AI development. China's social media and e-commerce companies compete for users around the world. Its telecoms build global 5G infrastructure. Its venture capitalists and large

[231] While the U.S. government has released a number of documents emphasizing the importance of artificial intelligence research and development—see, for example, President Trump's executive order on AI—the U.S. lacks a comprehensive, whole of government plan to guide policymakers, researchers, and businesses toward a more secure U.S. future. *Artificial Intelligence for the American People*, The White House (last accessed Jan. 5, 2021), https://www.whitehouse.gov/ai/.

[232] See e.g., Alexandra Mousavizadeh, et al., *The Global AI Index*, Tortoise Media (Dec. 3, 2019), https://www.tortoisemedia.com/2019/12/03/global-ai-index/; Jean François Gagné, et al., *Global AI Talent Report 2020* (last accessed Dec. 29, 2020), https://jfgagne.ai/global-ai-talent-report-2020/; *The Global AI Talent Tracker*, MacroPolo (last accessed Dec. 29, 2020), (https://macropolo.org/digital-projects/the-global-ai-talent-tracker/; Jeffrey Ding, et al., *MERICS Web Seminar: China as an AI Superpower? Quantifying China's AI progress against the US and Europe*, MERICS (July 1, 2020), https://merics.org/en/video/merics-web-seminar-china-ai-superpower-quantifying-chinas-ai-progress-against-us-and-europe.

[233] Audrey Cher, *'Superpower Marathon': U.S. May Lead China in Tech Right Now — But Beijing Has the Strength to Catch Up*, CNBC (May 17, 2020), https://www.cnbc.com/2020/05/18/us-china-tech-race-beijing-has-strength-to-catch-up-with-us-lead.html; Graham Allison & Eric Schmidt, *Is China Beating the U.S. to AI Supremacy?*, Belfer Center for Science and International Affairs (Aug. 2020), https://www.belfercenter.org/publication/china-beating-us-ai-supremacy; Will Knight, *China May Overtake the US with the Best AI Research in Just Two Year*s, MIT Technology Review (Mar. 13, 2019), https://www.technologyreview.com/2019/03/13/136642/china-may-overtake-the-us-with-the-best-ai-research-in-just-two-years/.

[234] Karen Hao, *Three Charts Show How China's AI Industry is Propped up by Three Companies*, MIT Technology Review (Jan. 22, 2019), https://www.technologyreview.com/2019/01/22/137760/the-future-of-chinas-ai-industry-is-in-the-hands-of-just-three-companies/.

[235] James Kynge & Nian Liu, *From AI to Facial Recognition: How China is Setting the Rules in New Tech*, Financial Times (Oct. 7, 2020), https://www.ft.com/content/188d86df-6e82-47eb-a134-2e1e45c777b6.

technology firms invest huge sums in new startups.[236] Its leading AI companies have research labs in the United States[237] and elsewhere.[238] Its researchers produce a trove of respected AI papers that advance the field.[239] None of this would concern us from a national security perspective, but for the fact that China is led by a single-party authoritarian regime that threatens American interests.

China has moved more quickly and with more determination than the United States, guided by a constellation of AI plans for government ministries, universities, and companies.[240] These strategic documents reflect Beijing's view that advances in AI will fundamentally reshape military and economic competition in the coming decades.[241] China has backed up its strategic plans with significant state subsidies to technology firms and academic institutions that engage in cutting edge AI research.[242] China preserves its capital by taking advantage of basic research done by the West so that it can focus more on applications. It pours significant sums of money into research and talent in relevant fields,[243] and promotes "national champion" companies to win markets abroad.[244] Through its military-civil fusion programs, China has sought to integrate advances in AI from the commercial and academic worlds into military power.[245] Using espionage, technology transfer programs, and targeted investment, Beijing seeks to acquire sensitive intellectual property (IP) and data from the United States and other countries.[246]

[236] Yusho Chao, *Chinese Venture Capitalists Take a Shine to Startups Again*, Nikkei (Sept. 13, 2020), https://asia.nikkei.com/Business/Finance/Chinese-venture-capitalists-take-a-shine-to-startups-again. See also, *Visualizing Chinese Tech Giants Billion-dollar Acquisitions*, CB Insights (May 28, 2020); https://www.cbinsights.com/research/bat-billion-dollar-acquisitions-infographic/.

[237] See, e.g., *A Chinese Tech Giant is Setting Up an A.I. Research Lab on Amazon's Home Turf*, CNBC (May 2, 2017), https://www.cnbc.com/2017/05/02/tencent-ai-research-lab-seattle.html.

[238] See, e.g., Saheli Roy Choudhury, *Alibaba Sets up Joint A.I. Research Center Outside China to Focus on AI*, CNBC (Feb. 28, 2018), https://www.cnbc.com/2018/02/28/alibaba-sets-up-joint-a-i-research-lab-in-singapore.html.

[239] In 2019, China had the largest number of submitted and accepted papers to the Association for the Advancement of AI (AAAI), one of the longest running AI conferences. See *Artificial Intelligence Index: 2019 Annual Report*, Stanford Institute for Human-Centered AI at 41 (2019), https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf. The Allen Institute for AI also predicts that China is poised to overtake the U.S. in the share of top cited, breakthrough papers in AI by 2025. See Field Cady & Oren Etzioni, *China May Overtake US in AI Research*, Allen Institute for Artificial Intelligence (Mar. 13, 2019), https://medium.com/ai2-blog/china-to-overtake-us-in-ai-research-8b6b1fe30595.

[240] For a selection of such strategic documents, see *AI Policy—China*, Future of Life Institute (last accessed Dec. 30, 2020), https://futureoflife.org/ai-policy-china/; Graham Webster, et al., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan'*, New America (Aug. 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ (translating China's State Council Notice on the Issuance of the New Generation Artificial Intelligence Development Plan, date July 20, 2017).

[241] Gregory C. Allen, *Understanding China's AI Strategy*, Center for a New American Security (Feb. 6, 2019), https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

[242] Ashwin Acharya & Zachary Arnold, *Chinese Public AI R&D Spending: Provisional Findings*, Center for Security and Emerging Technology (Dec. 2019), https://cset.georgetown.edu/wp-content/uploads/Chinese-Public-AI-RD-Spending-Provisional-Findings-1.pdf; see also Emily Weinstein, *Mapping China's Sprawling Efforts to Recruit Scientists*, Defense One (Nov. 30, 2020), https://www.defenseone.com/ideas/2020/11/mapping-chinas-sprawling-efforts-recruit-scientists/170373/; David Cyranoski, *China Joins the Battle for AI Talent*, Nature (Jan. 17, 2018), https://www.nature.com/articles/d41586-018-00604-6.

[243] Id.

[244] U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy* at 46, 115-116 (June 7, 2019), https://www.uscc.gov/sites/default/files/2019-10/June%207,%202019%20Hearing%20Transcript.pdf.

[245] U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy* (June 7, 2019), https://www.uscc.gov/sites/default/files/2019-10/June%207,%202019%20Hearing%20Transcript.pdf.

[246] U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy* (June 7, 2019), https://www.uscc.gov/sites/default/files/2019-10/June%207,%202019%20Hearing%20Transcript.pdf.

The U.S.-China competition is complicated by the complex web of supply chains, research partnerships, and business relationships that link the world's two AI leaders. Dramatic steps to sever these ties could be costly for Americans and reverberate across the world. The relationships between American and Chinese academics, innovators, and markets are deep, often mutually beneficial, and help advance the field of AI.[247] Moreover, it remains in the U.S. national interest to leverage formal diplomatic dialogue about AI and other emerging technologies and to explore areas for cooperative AI projects that will benefit humanity.

The United States can compete against China without ending collaborative AI research and severing all technology commerce. Broad-based technological decoupling with China could deprive U.S. universities and companies of scarce AI and science, technology, engineering, and mathematics (STEM) talent,[248] sever American companies' efficient supply chains,[249] and cut off access to markets and capital for innovative firms.[250] Instead, the United States should conceive of targeted disentanglement as just one element of its overall approach, which if applied judiciously to key sectors can help build U.S. technological resilience, reduce threats from illicit technology transfer, and protect national security-critical sectors.

The Policy Challenges. China's competitive approach should not define the U.S. approach to innovation, but it does present an alternative model of AI development, frame the stakes of competition, and expose the sheer breadth of public policy choices the U.S. government must make to preserve American advantages.

The United States will need to reexamine its immigration policies to ensure that America wins the competition for AI talent. It will need to consider AI and broader STEM education initiatives through the lens of global competitiveness. It will have to consider how to diversify the AI research agenda and expand access to the data and tools necessary to conduct AI research in the face of costs for compute and data that are consolidating AI in fewer locations and shifting the balance from universities to the private sector. The United States will have to consider whether the long-standing approaches to intellectual property (IP) are best suited to an era in which IP theft is pervasive and the U.S. IP regime has not yet fully accounted for AI and other emerging technologies. The United States will need to protect its leadership in the design of microelectronics, which may include encouraging the domestic reshoring of critical manufacturing on which our national security depends. And the United States will have to ensure its tools and policies designed to prevent illicit technology transfer are postured to address the national security challenges presented by dual-use emerging technologies.

[247] As Eric Schmidt noted in *Building a New Technological Relationship and Rivalry*. See Hal Brands & Francis J. Gavin, *COVID-19 and World Order: The Future of Conflict, Competition, and Cooperation*, Johns Hopkins University Press 406-418 (Aug. 31, 2020), https://muse.jhu.edu/chapter/2696578.

[248] Ishan Banerjee & Matt Sheehan, *America's Got AI Talent: US' Big Lead in AI Research Is Built on Importing Researchers*, MacroPolo (June 9, 2020), https://macropolo.org/americas-got-ai-talent-us-big-lead-in-ai-research-is-built-on-importing-researchers/?rp=m.

[249] *U.S. Dependence on China's Rare Earth: Trade War Vulnerability*, Reuters (June 27, 2019), https://www.reuters.com/article/us-usa-trade-china-rareearth-explainer/u-s-dependence-on-chinas-rare-earth-trade-war-vulnerability-idUSKCN1TS3AQ.

[250] *Member Survey*, US-China Business Council (Aug. 2019), https://www.uschina.org/sites/default/files/member_survey_2019_-_en_0.pdf.

These AI-specific challenges, in turn, expose even more fundamental questions spanning technology, economic, and national security spheres:

- How to compete with a rival without compromising U.S. values—including free market principles, individual liberty, and limited government.
- How to ensure the proper balance between defense and economic priorities.
- How to preserve hardware advantages without suffocating the domestic designers and producers that rely on foreign competitors' markets.
- How to capitalize on and shape private sector developments for national security ends without stifling private sector-led and free market innovation.
- How to draw on the best global talent without enabling damaging technology and knowledge transfer to competitors.
- How to foster an open collaborative research environment while closing licit and illicit loopholes exploited by foreign competitors.
- How to sustain long-term strategies for research and development that are nevertheless responsive to rapidly shifting geopolitical and technology developments.
- How to ensure the free flow of investment/capital without allowing strategic competitors to buy strategic advantage.
- How to engage with our allies and other partners to reduce their dependence on China's digital technologies, build more resilient supply chains, and develop technology standards and norms that reflect democratic values.

The Need for a Stronger Government Role in Technology Strategy

The Commission is not calling for a state-directed economy, a five-year plan, or China-style "military-civil fusion." It is instead urging a government-led process to restore a more balanced equilibrium between government, industry, and academia that ensures a diverse research environment, competitive economy, and the sustainment of a research agenda that supports the needs of the nation. The government has a long-history of mobilizing industry and academia and making huge investments when it is challenged.[251] Against the backdrop of a declared and committed competitor like China, and given AI's transformative potential, the United States is confronting such a moment.

[251] For instance, adjusted for inflation, the Manhattan Project cost an estimated $27 billion and the Apollo program totaled roughly $121 billion. Deborah Stine, *The Manhattan Project, the Apollo Program, and Federal Energy Technology R&D Programs: A Comparative Analysis*, Congressional Research Service (June 30, 2009), https://fas.org/sgp/crs/misc/RL34645.pdf (conversion of totals into 2020 dollars was calculated using the U.S. Bureau of Labor Statistics' CPI Inflation Calculator, available at https://www.bls.gov/data/inflation_calculator.htm).

Today, the U.S. government champions AI leadership in speeches and memorandums, but deploys few resources relative to commercial investment and historic funding benchmarks, and relies on a decentralized governance structure for achieving it.[252] There is talk of a global talent competition, but in recent years the United States has tightened restrictions on visas for highly skilled workers[253] and U.S. students at the kindergarten to 12th grade (K-12) level have lagged behind East Asian and European competitors in exams designed to measure competency in STEM fields.[254] Tech leaders and government officials talk about the importance of "public-private partnership," but there is little action in either direction to deepen it in concrete ways. U.S. experts warn of the danger of AI being used for techno-authoritarian ends,[255] but Washington has not led any new enduring coalition to create democratic alternatives. Current policies amount to a compilation of disparate AI-related activities underway in the federal government. Nowhere can one find a strategy coupled with the organization and resources to win an AI competition and preserve the United States' AI leadership.

The government will have to orchestrate policies to promote innovation; protect industries and sectors critical to national security; recruit and train talent; incentivize domestic research, development, and production across a range of technologies deemed essential for national security and economic prosperity; and marshal coalitions of allies and partners to support democratic norms. Some elements of a national strategy will need to be coordinated and replicated at the state level, through state-specific strategies to support AI research, commerce, and education. This will require a complex sequencing of promotion and protection actions to minimize costs and risks of punitive actions; ensure basic and applied research agendas are mutually reinforcing; coordinate approaches with international partners; and align executive priorities with legislative powers. It will require identifying technology trends and assessing the relative strengths of the United States and its competitors. It will require, above all, strong and consistent White House leadership.

The following Chapters (10-16) enumerate the core elements of a competitive strategy and prescribe the actions that will ensure the United States wins the AI competition and sets the foundation to win the broader technology competition. It is foremost an affirmative agenda. Protection of research, intellectual property, and investments will be necessary, but only to complement an effort to invigorate AI competitiveness at home and build a coalition of like-minded partners in the world.

The strategy begins with two prerequisites: organizing for technology competition under White House leadership, and establishing the principles for continued cooperation with competitors.

The Case for White House Leadership. The government will require a center of power that can exert gravitational pull on domestic economic, national security, and science and technology policies. We have no such organization today. Several separate Executive Office of the President (EOP)

[252] In 2018, U.S. federal research & development funding amounted to 0.7 percent of GDP, down from its peak at above 2 percent in the 1970s. See James Manyika & William H. McRaven, *Innovation and National Security: Keeping our Edge*, Council on Foreign Relations (Sept. 2019), https://www.cfr.org/report/keeping-our-edge/recommendations/.

[253] Zolan Kanno-Youngs & Miriam Jordan, *Trump Moves to Tighten Visa Access for High-Skilled Foreign Workers*, New York Times (Oct. 6, 2020), https://www.nytimes.com/2020/10/06/us/politics/h1b-visas-foreign-workers-trump.html.

[254] Moriah Balingit & Andrew Van Dam, *U.S. Students Continue to Lag Behind Peers in East Asia and Europe in Reading, Math and Science, Exams Show*, Washington Post (Dec. 3, 2019), https://www.washingtonpost.com/local/education/us-students-continue-to-lag-behind-peers-in-east-asia-and-europe-in-reading-math-and-science-exams-show/2019/12/02/e9e3b37c-153d-11ea-9110-3b34ce1d92b1_story.html.

[255] Alina Polyakova & Chris Meserole, *Exporting Digital Authoritarianism*, Brookings (Aug. 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.

entities possess some responsibility and capacity to fulfill the basic organizational requirements: the National Security Council (NSC),[256] the Office of Science and Technology Policy (OSTP)[257] and its associated National Science and Technology Council (NSTC),[258] and the National Economic Council (NEC).[259] The Domestic Policy Council (DPC) also has critical related responsibilities and a similar mandate with leadership in the realm of immigration policy, education policy, and regulatory policy.[260] An additional entity—the Office of Management and Budget (OMB)—oversees related budgets and government reform efforts.

In the absence of an overarching structure, it is left to the President and Vice President to identify, adjudicate, and reconcile the positions that emerge from parallel interagency processes, while leaving endless room for gadflies to run the gaps and influence the President. The President needs a tool to help decide and drive a new technology strategy down through the necessary but not sufficient existing councils, and into the rest of the government. The White House should:

✦ **Create a Technology Competitiveness Council.** The United States must strengthen executive leadership in technology policy in the White House by empowering a single entity to implement a comprehensive technology strategy. The Commission proposes creating a new Technology Competitiveness Council (TCC), which would include the same amalgamation of EOP leaders and Cabinet secretaries as other White House forums for convening the interagency, and be chaired by the Vice President with a newly appointed Assistant to the President for Technology Competitiveness serving as the day-to-day leader. The TCC would ensure that the gaps between NEC, OSTP, and NSC responsibilities are filled and linked to OMB. It would not replace the NSC, NEC, or OSTP-led NSTC structures, but would provide a forum for reconciling competing security, economic, and scientific priorities, and elevate technology policy and concerns from technical to strategic. To coordinate the council's work it is necessary to create a new principal, the Assistant to the President for Technology Competitiveness responsible for ensuring policies pertaining to emerging technologies receive sufficient Presidential-level attention.

✦ **Develop a National Technology Strategy.** The TCC should create a National Technology Strategy, building on the elements we present below, which can guide U.S. policy across all key emerging technologies starting with AI. The strategy should weigh the difficult tradeoffs between competing policy interests and priorities, identify critical technologies where competitors have sought to match or overtake U.S. leadership, and facilitate an integrated policy approach to emerging

[256] The National Security Council has a statutory mandate to "advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the Armed Forces and the other departments and agencies of the United States Government to cooperate more effectively in matters involving the national security." 50 U.S.C. § 3021(b)(1).

[257] Pub. L. 94-282, National Science and Technology Policy, Organization, and Priorities Act of 1976, 90 Stat. 459 (1976), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_organic_statute.pdf.

[258] The function of the NSTC under the supervision of the Director of OSTP is to: "(1) to coordinate the science and technology policy-making process; (2) to ensure science and technology policy decisions and programs are consistent with the President's stated goals; (3) to help integrate the President's science and technology policy agenda across the Federal Government; (4) to ensure science and technology are considered in development and implementation of Federal policies and programs; and (5) to further international cooperation in science and technology. The Assistant may take such actions, including drafting a Charter, as may be necessary or appropriate to implement such functions." William J. Clinton, *Executive Order 12881: Establishment of the National Science and Technology Council* (Nov. 23, 1993), https://www.govinfo.gov/content/pkg/WCPD-1993-11-29/pdf/WCPD-1993-11-29-Pg2450.pdf.

[259] William J. Clinton, *Executive Order 12835: Establishment of the National Economic Council* (Jan. 25, 1993), https://www.govinfo.gov/content/pkg/WCPD-1993-02-01/pdf/WCPD-1993-02-01-Pg95.pdf.

[260] William J. Clinton, *Executive Order 12859: Establishment of the Domestic Policy Council* (Aug. 16, 1993), https://www.archives.gov/files/federal-register/executive-orders/pdf/12859.pdf.

technologies. As a starting point, the strategy should build on the following pillars: 1) winning the AI talent competition; 2) promoting American AI innovation; 3) protecting U.S. AI advantages; and 4) leading a favorable international AI order.

✦ Establish a high-level U.S.-China Comprehensive Science & Technology Dialogue (CSTD). The United States should establish a regular, high-level diplomatic dialogue with China that benefits the American people, remains faithful to our allies, and presses China to abide by international norms. The dialogue should focus on challenges presented by emerging technologies—to include AI, biotechnology, and other technologies as agreed by both sides. The CSTD should have two overarching objectives:

- *Identify targeted areas of cooperation on emerging technologies* to solve global challenges such as climate change and natural disaster relief; and

- *Provide a forum to air a discrete set of concerns around specific uses of emerging technologies* while building relationships and establishing processes between the two nations.

Chapter 10: The Talent Competition

The United States is in a global competition for scarce artificial intelligence (AI) and science, technology, engineering, and mathematics (STEM) talent.[261] The Commission is very concerned with current talent trends. The number of domestic-born students participating in AI doctorate programs has not increased since 1990, and competition for international students has accelerated, endangering the United States' ability to retain international students.[262] For the first time in our lifetime, the United States risks losing the competition for talent on the scientific frontiers. Cultivating more potential talent at home and recruiting and retaining more existing talent from foreign countries are the only two options to sustain the U.S. lead.

Competitors and allies recognize the importance of implementing AI talent strategies. Between 2000 and 2014, China's university system increased STEM graduates by 360 percent, producing 1.7 million in 2014 alone..[263] The United States' university system rose by 54 percent during the same time period, and many were international students.[264] In some important AI research areas, China's researchers now represent roughly 29 percent of top-tier deep learning talent in the world.[265] China and other states have also taken steps to attract international talent with flexible immigration policies and incentives for tech talent.[266]

The United States needs to invest in all AI talent pipelines in order to remain at the forefront of AI now and into the future. A passive strategy will not work in the face of the AI talent competition.

<u>The Promise and Limits of Expanding STEM.</u> Investments in STEM education are a necessary part of increasing American national power and improving national security. The United States ranks well overall on international measures of talent because of our ability to attract international talent, in spite of our uneven kindergarten to 12th grade (K-12) education system.[267] It is critical that the

[261] Estimates to the gap of talent necessary to fill AI slots vary greatly, but it is agreed upon that the gap in talent currently is and will continue to be significant as nations compete for scarce resources. See Remco Zwetsloot, et al., *Strengthening the U.S. AI Workforce: A Policy and Research Agenda*, Center for Security and Emerging Technology at 2 (Sept. 2019), https://cset.georgetown.edu/wp-content/uploads/CSET-Strengthening-the-U.S.-AI-Workforce.pdf ("The Research Institute at Tencent, a major Chinese technology company, asserts there are roughly 300,000 AI researchers and practitioners worldwide, with market demand for millions of roles. Element AI, a leading Canadian AI company, estimated in 2018 that there are roughly 22,000 PhD-educated researchers globally who are able to work on AI research, with only about 25 percent of those "well-versed enough in the technology to work with teams to take it from research to application." AI firm Diffbot estimates that there are over 700,000 people skilled in machine learning worldwide.").

[262] Remco Zwetsloot, et al., *Keeping Top AI Talent in the United States*, Center for Security and Emerging Technology at iii-vi (Dec. 2019), https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

[263] *The Rise of China in Science and Engineering*, NSF National Science Board (2018), https://www.nsf.gov/nsb/sei/one-pagers/China-2018.pdf (China also passed the United States in the global share in numbers of peer reviewed S&E articles).

[264] *Science & Engineering Indicators 2018*, NSF National Science Board (2018), https://www.nsf.gov/statistics/2018/nsb20181/assets/561/higher-education-in-science-and-engineering.pdf.

[265] For these purposes "top tier" talent was defined by accepted papers at the prestigious AI deep learning conference Neural Information Processing Systems in 2019. This approximately reflected the top 20% of researchers in the field. *The Global AI Talent Tracker*, MacroPolo (last accessed Dec. 28, 2020), https://macropolo.org/digital-projects/the-global-ai-talent-tracker/. China has placed a strong emphasis on deep learning, just one of the important components of AI.

[266] For example, China's Thousand Talents Plan is a state-organized blueprint to be a global leader in science and technology by 2050. Staff Report, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans*, U.S. Senate Permanent Subcommittee on Investigations at 14 (Nov. 2019), https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf.

[267] *The Global AI Talent Tracker*, MacroPolo (last accessed Dec. 28, 2020), https://macropolo.org/digital-projects/the-global-ai-talent-tracker/. See also Gordon Hanson & Matthew Slaughter, *High-Skilled Immigration and the Rise of STEM Occupations in U.S.*

United States invest significantly in STEM education as an engine to drive the growth of AI talent in America. Investments in STEM education alone, however, will not be enough for the United States to win the international competition for AI and STEM talent. China is producing large numbers of computer scientists, engineers, and other STEM graduates.[268] For the foreseeable future, the United States' STEM education system does not have the capacity nor quality to produce sufficient STEM or AI talent to supply the United States' markets or national security enterprise.[269] To compete, the United States must reform our education system to produce both a higher quality and quantity of graduates.

✦ **Pass the National Defense Education Act II.** Motivated by fear that America had fallen behind in education and innovation after the Soviets launched Sputnik in 1957, Congress passed the National Defense Education Act (NDEA) the following year. The NDEA promoted the importance of science, mathematics, and foreign languages for students, authorizing over one billion dollars toward decreasing student loans, funding for education at all levels, and funding for graduate fellowships. Many students were able to attend college because of this legislation. In 1960, 3.6 million students attended college; by 1970 it was 7.5 million.[270] This act helped America win the Space Race, helped power the microelectronics industry, accelerated the U.S. capacity to innovate, and ultimately, played an important role in America's victory in the Cold War.

The Commission believes the time is right for a second NDEA, one that mirrors the first legislation, but with important distinctions. NDEA II would focus on funding students acquiring digital skills, like mathematics, computer science, information science, data science, and statistics. NDEA II should include K-12 education and reskilling programs that address deficiencies across the spectrum of the American educational system, purposefully targeting under resourced school districts. If the United States does not invest in domestic digital talent, there will be a shortage of qualified practitioners to fill digital roles, now and in the future. Ultimately, the goal of NDEA II is to widen the digital talent pool by incentivizing programs for underrepresented Americans.

✦ **Strengthen AI talent through immigration.** Immigration is a national security imperative. Nations that can successfully attract and retain highly skilled individuals gain strategic and economic advantage over competitors. The advantages granted by human capital are particularly strong in the field of AI, where demand for talent far exceeds supply.[271] Highly skilled immigrants accelerate

Employment, National Bureau of Economic Research at 1 (Sept. 2016), https://www.nber.org/system/files/working_papers/w22623/w22623.pdf. Id.

[268] *The Rise of China in Science and Engineering*, NSF National Science Board (2018), https://www.nsf.gov/nsb/sei/one-pagers/China-2018.pdf.

[269] As noted in Chapter 6, there were 433,116 open computer science jobs in the United States in 2019, while only 71,226 new computer scientists graduate from American universities each year. Code.org (last accessed Jan. 11, 2021), https://code.org/promote. See also Oren Etzioni, *What Trump's Executive Order on AI Is Missing: America Needs a Special Visa Program Aimed at Attracting More AI Experts and Specialists*, Wired (Feb. 13, 2019), https://www.wired.com/story/what-trumps-executive-order-on-ai-is-missing/.

[270] *Sputnik Spurs Passage of the National Defense Education Act*, U.S. Senate (last accessed Dec. 28, 2020), https://www.senate.gov/artandhistory/history/minute/Sputnik_Spurs_Passage_of_National_Defense_Education_Act.htm#:~:text=The%20National%20Defense%20Education%20Act%20of%201958%20became%20one%20of,and%20private%20colleges%20and%20universities.

[271] According to a Center for Security and Emerging Technology report, job listings for AI on one popular job website "increased more than five-fold between 2015 and 2017 and demand for 'deep learning' skills increased by a factor of more than 30," while the number of people looking for jobs in the field grew much more slowly. This mismatch is slowing the adoption of AI. Most firms report that skills gaps are one of the top obstacles preventing them from adopting AI. Remco Zwetsloot, et al., *Strengthening the U.S. AI Workforce: A Policy and Research Agenda*, Center for Security and Emerging Technology at 1 (Sept. 2019), https://cset.georgetown.edu/wp-content/uploads/CSET-Strengthening-the-U.S.-AI-Workforce.pdf.

American innovation, improve entrepreneurship, and create jobs.[272] The United States benefits far more from the immigration of highly skilled foreign workers than other countries. In 2013, the United States had fifteen times as many immigrant inventors as there were American inventors living abroad.[273] By contrast, Canada, Germany, and the United Kingdom all maintain a net negative inventor immigration rate.[274] Compared to other U.S. advantages in the AI competition—such as financial resources or hardware capacity—this immigration advantage is harder for other countries to replicate.

Unfortunately, international students in the United States are increasingly choosing to study in other countries or return home.[275] One reason is the growing backlog of green card petitions.[276] Indian immigrants face a particularly long wait. Many will spend decades on constrictive work visas waiting to receive their green cards, hindering both the technology sector's ability to recruit talent and Indian immigrants' quality of life. At the same time, other countries are increasing their efforts to attract and retain AI talent, including immigrants in Silicon Valley.[277]

While immigration benefits the United States, policy makers must also bear in mind the threat of unwanted technology transfer. However, restricting immigration is far too blunt a tool to solve this problem.[278] Restrictions harm U.S. innovation and economic growth and only help our competitors by enabling their human capital to grow. They also incentivize U.S. technology companies to move to where talent resides, whether right across our borders or overseas.[279] Technology transfer would only get worse if significant components of the U.S. technology sector moved their research and development to China or other countries more vulnerable than the United States to technology transfer efforts.[280] A more effective strategic approach would pair actions to improve the United

[272] William S. Kerr, *High-Skilled Immigration, Innovation, and Entrepreneurship: Empirical Approaches and Evidence*, National Bureau of Economic Research at 7-8 (Aug. 2013), https://www.nber.org/papers/w19377; Gordon Hanson & Matthew Slaughter, *Strengthening the U.S. AI Workforce, High-Skilled Immigration and the Rise of STEM Occupations in U.S. Employment*, National Bureau of Economic Research at 23 (Sept. 2016), https://www.nber.org/system/files/working_papers/w22623/w22623.pdf; Remco Zwetsloot, et al., *Strengthening the U.S. AI Workforce: A Policy and Research Agenda*, Center for Security and Emerging Technology at 5 (Sept. 2019), https://cset.georgetown.edu/wp-content/uploads/CSET-Strengthening-the-U.S.-AI-Workforce.pdf.

[273] Carsten Fink, *What Leads Inventors to Migrate?*, World Economic Forum (July 17, 2013), https://www.weforum.org/agenda/2013/07/what-leads-inventors-to-migrate/.

[274] Ernest Miguelez & Carsten Fink, *Measuring the International Mobility of Inventors: A New Database*, World Intellectual Property Organization at 16 (May 2013), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_econstat_wp_8.pdf.

[275] According to the Brookings Institution's *China's Approach to Tech Talent Competition: Policies, Results, and the Developing Global Response*, in 2016, 14 percent of international students declined offers to study at U.S. universities to study at home, and 19 percent decided to study in another country. In 2018, these numbers rose, with 39 percent staying at home and 59 percent studying in another country. Remco Zwetsloot, et al., *Keeping Top AI Talent in the United States: Findings and Policy Options for International Graduate Student Retention*, Center for Security and Emerging Technology (Dec. 2019), https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

[276] Shulamit Kahn & Megan MacGarvie, *The Impact of Permanent Residency Delays for STEM PhDs: Who Leaves and Why*, Research Policy (Nov. 2020), https://www.sciencedirect.com/science/article/abs/pii/S0048733319301982.

[277] Tina Huang & Zachary Arnold, *Immigration Policy and the Global Competition for AI Talent*, Center for Security and Emerging Technology at 8 (June 2020), https://cset.georgetown.edu/research/immigration-policy-and-the-global-competition-for-ai-talent/.

[278] Zachary Arnold, et al., *Immigration Policy and the U.S. AI Sector: A Preliminary Assessment*, Center for Security and Emerging Technology at 22 (Sept. 2019), https://cset.georgetown.edu/research/immigration-policy-and-the-u-s-ai-sector/.

[279] Remco Zwetsloot, et al., *Strengthening the U.S. AI Workforce: A Policy and Research Agenda*, Center for Security and Emerging Technology at 5 (Sept. 2019), https://cset.georgetown.edu/wp-content/uploads/CSET-Strengthening-the-U.S.-AI-Workforce.pdf.

[280] China is the world's largest single source of AI talent. Leading U.S. technology companies such as Google and Microsoft have established cutting edge research centers in China, in part to access that talent. This increases China's AI research and development capacity, potential for technology transfer, and, if the companies remain American, reduces the American Intelligence Communities' legal authorization to collect information about Chinese technology development. See *The Global AI Talent Tracker*, MacroPolo (last accessed Jan 17, 2020), https://macropolo.org/digital-projects/the-global-ai-talent-tracker/; Roxanne Heeston & Reemco Zwetsloot,

States' ability to attract top global talent with targeted efforts to combat technology transfer vectors.[281]

Immigration policy can also slow China's progress. China's government takes the threat of brain drain seriously, noting that the United States' ability to attract and retain China's talent is an obstacle to the Chinese Communist Party's (CCP) ambitions.[282] Increasing China's brain drain will create a dilemma for the CCP—which will be forced to choose between losing even more human capital—further slowing their economic growth and threatening their advancement in AI, or denying Chinese nationals opportunities to study and work in the United States. Notably, the United States should avoid increasing brain drain from its friends and allies.

✦ **Broaden the scope of "extraordinary" talent to make the O-1 visa more accessible and emphasize AI talent.** The O-1 temporary worker visa is for people with extraordinary ability or achievement. Currently adjudicators determine an applicant's eligibility through a subjective assessment. For the sciences and technology, this aligns largely with academic criteria such as publications in major outlets, and is not well suited for people who excel in industry.

✦ **Implement and advertise the international entrepreneur rule.** The International Entrepreneur Rule (IER) allows U.S. Citizenship and Immigration Services (USCIS) to grant a period of authorized stay to international entrepreneurs who demonstrate that "their stay in the United States would provide a significant public benefit through their business venture."[283] An executive action could announce the administration's intention to use the IER to boost immigrant entrepreneurship, job creation for Americans, and economic growth. USCIS could also be directed to announce that it will give priority to entrepreneurs active in high-priority STEM fields such as AI, or in fields that use AI for other applications, such as agriculture. Entrepreneurs' ability to attract investors should be used as a screening criterion for entrepreneurs.

✦ **Expand and clarify job portability for highly skilled workers.** The criteria for workers with H-1B, O-1, and other temporary work visas to obtain open market work permits for a one-year renewable period are too limited and ambiguous. Changes should clarify when highly skilled, nonimmigrant workers are permitted to change jobs or employers, increase job flexibility when an employer either withdraws their petition or goes out of business, and increase flexibility for H-1B workers seeking other H-1B employment.

Mapping U.S. Multinationals' Global AI R&D Activity, Center for Security and Emerging Technology at 20 (Dec. 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Mapping-U.S.-Multinationals-Global-AI-RD-Activity-1.pdf.

[281] Recommendations for such countermeasures are described in Chapter 11.

[282] Remco Zwetsloot, *US-China STEM Talent "Decoupling": Background, Policy, and Impact*, Johns Hopkins Applied Physics Laboratory at 19 (2020), https://www.jhuapl.edu/assessing-us-china-technology-connections/dist/407b0211ec49299608551326041488d4.pdf ("[T]he head of the [Chinese Communist Party's (CCP)] Central Talent Work Coordination Small Group . . . complained that 'the number of top talents lost in China ranks first in the world.'"); see also Joy Dantong Ma, *China's AI Talent Base Is Growing, and then Leaving*, Macro Polo (July 30, 2019), https://macropolo.org/chinas-ai-talent-base-is-growing-and-then-leaving/?rp=m (noting that of the 2,800 Chinese NeurIPS participants between 2009 and 2018, about three-quarters of them were currently working outside of China).

[283] *International Entrepreneur Parole*, USCIS (May 25, 2018), https://www.uscis.gov/humanitarian/humanitarian-parole/international-entrepreneur-parole. There is currently no visa category well-suited to entrepreneurship in immigration statute. The IER, which relies on parole authority, was initiated after legislative avenues were exhausted. Legislative fixes would be preferable, but have so far proven politically infeasible.

✦ **Recapture green cards lost to bureaucratic error.** Federal agencies generally issue fewer green cards than they are allowed. As of 2009, the federal government had failed to issue over 326,000 green cards based on cumulative bureaucratic error.[284] The Departments of State and Homeland Security (DHS) should publish an up-to-date report on the number of green cards lost due to bureaucratic error. The Departments of State and Homeland Security, using available authorities, should grant lost green cards to applicants waiting in line. Congress should support the Departments of State and Homeland Security by passing legislation to recapture lost green cards.[285]

✦ **Grant green cards to students graduating with STEM PhDs from accredited American universities.** Congress should amend the Immigration and Nationality Act[286] to grant lawful permanent residence to any vetted (not posing a national security risk) foreign national who graduates from an accredited United States institution of higher education with a doctoral degree in a field related to science, technology, engineering, or mathematics in a residential or mixed residential and distance program; and has a job offer in a field related to science, technology, engineering, or mathematics. They should not be counted towards permanent residency caps.

✦ **Double the number of employment based green cards.** Under the current system, employment-based green cards are unduly scarce: 140,000 per year, fewer than half of which go to the principal worker.[287] This leaves many highly skilled workers unable to gain permanent residency, and unable to transfer jobs or negotiate with employers as effectively as domestic workers. This decreases the appeal of joining the American workforce. To reduce the backlog of highly skilled workers, the United States should double the number of employment based green cards, with an emphasis on permanent residency for STEM and AI-related fields.

✦ **Create an entrepreneur visa.** International doctoral students are more likely to want to found a company or become an employee at a startup than their native peers, but are less likely to pursue those paths.[288] One reason is the constraints of the H-1B visa system.[289] Similarly, immigrant entrepreneurs without the capital to use the EB-5 route to permanent residency are forced to use other visas that are designed for academics and workers in existing companies, not entrepreneurs.[290] All of these issues make the United States less attractive for international talent, and, perhaps as importantly, reduce the ability of startups and other small companies—the main source of new jobs for Americans—to hire highly skilled immigrants that have been shown to improve the odds the business will succeed. Congress should create an entrepreneur visa for those that would provide a

[284] A 2009 report to Congress indicates that some 242,000 unused family-based green cards were ultimately applied to the employment-based backlog, while Congress recaptured some 180,000 green cards via special legislation, leaving over 326,000 green card numbers wasted. *Citizenship and Immigration Services Ombudsman: Annual Report 2010*, U.S. Department of Homeland Security (June 30, 2010), https://www.dhs.gov/xlibrary/assets/cisomb_2010_annual_report_to_congress.pdf. The number today is likely higher, but DHS has not published updated statistics.

[285] Prior examples of congressional action include provisions in the American Competitiveness in the 21st Century Act of 2000 and REAL ID Act of 2005. *See* Pub. L. 106-313, 114 Stat. 1251, 1254 (2000) and Pub. L. No. 109-013, 119 Stat. 231, 322 (2005).

[286] Specifically, 8 U.S.C. § 1151(b)(1).

[287] William Kandel, *The Employment-Based Immigrant Backlog*, Congressional Research Service at 4-5 (Mar. 26, 2020), https://fas.org/sgp/crs/homesec/R46291.pdf.

[288] Michael Roach, et al., *Are Foreign STEM PhDs More Entrepreneurial? Entrepreneurial Characteristics, Preferences and Employment Outcomes of Native and Foreign Science & Engineering PhD Students*, National Bureau of Economic Research at 1 (Sept. 2019), https://www.nber.org/system/files/working_papers/w26225/w26225.pdf.

[289] Id. at 12.

[290] EB-5 visas require a minimum of $900,000 of investment in a business in the United States. William R. Kerr, *Global Talent and U.S. Immigration Policy: Working Paper 20-107*, Harvard Business School at 14 (2020), https://www.hbs.edu/faculty/Publication%20Files/20-107_0967f1ab-1d23-4d54-b5a1-c884234d9b31.pdf.

"significant public benefit" to the United States if allowed to stay in the country for a limited trial period to grow their companies.[291] This visa should serve as an alternative to employee-sponsored, investor, or student visas, and should instead target promising potential founders.

✦ **Create an emerging and disruptive technology visa.** The National Science Foundation (NSF) should identify critical emerging technologies every three years. DHS would then allow students, researchers, entrepreneurs, and technologists in applicable fields to apply for emerging and disruptive technology visas. This would provide much needed talent research and development and strengthen our economy.[292]

[291] 83 Fed. Reg. 24415, *Removal of International Entrepreneur Parole Program*, U.S. Department of Homeland Security (May 29, 2018), https://www.federalregister.gov/documents/2018/05/29/2018-11348/removal-of-international-entrepreneur-parole-program.
[292] Oren Etzioni, *What Trump's Executive Order on AI Is Missing: America Needs a Special Visa Program Aimed at Attracting more AI Experts and Specialists*, Wired (Feb. 13, 2019), https://www.wired.com/story/what-trumps-executive-order-on-ai-is-missing/.

Chapter 11: Accelerating AI Innovation

To remain the world's leader in artificial intelligence (AI), the U.S. government must renew its commitment to investing in America's national strength—innovation. This will require building incentives and making substantial new investments in AI research and development (R&D). Members of Congress must come to terms with the reality that tens of billions of dollars will be needed over the next several years. The return on these investments will transform America's economy, society, and national security.

A lack of national urgency is dangerous at a time when underlying weaknesses have emerged in our AI ecosystem that impair innovation, and when viewed against the backdrop of China's state-directed AI progress. The development of AI in the United States is concentrated in fewer organizations in fewer geographic regions pursuing fewer research pathways. The center of AI gravity—even for research—has shifted from academia and government labs to the private sector. Commercial agendas are dictating the future of AI and investing heavily in one discipline, machine learning (ML).[293] Despite promising moves, government funding has lagged behind the transformative potential of the field, limiting its ability to shape research towards the public good.[294] As a result, the long-term health of the AI innovation environment rests on a narrowing foundation.

Much of this consolidation comes as a result of resources. Declining per-unit costs of cloud-based computing and availability of open source platforms have lowered barriers of access to core ML. However, those same conditions have enabled pursuit of sophisticated models that require extensive training data, often held in privately controlled data sets or knowledge graphs, enormous computing power, and substantial hardware and software engineering.[295] These prerequisites now define the cutting edge of AI research and effectively limit the number of Americans researchers able to contribute to the field. For efforts that involve robotics or real-world applications, development requires complex modeling and simulation capabilities for training algorithms as well as specialized facilities for experimentation.

[293] A 2020 analysis of arXiv papers on AI found private sector basic AI research to be thematically narrower than the broader corpus of AI publications, focusing on deep learning and computational infrastructure to support deep learning. Furthermore, the study found that elite academic institutions who collaborate more closely with industry had a similar narrowing of thematic concentration, leading to a tilting of the U.S. AI research environment away from the diversity still preserved in other countries. See Joel Klinger, et al., *A Narrowing of AI Research?*, ArXiv (Nov. 18, 2020), https://arxiv.org/pdf/2009.10385.pdf. Increasing specialization of hardware achieved through industry investments has further prioritized commercial use cases, making it costly to pursue approaches outside the mainstream. See Sara Hooker, *The Hardware Lottery*, ArXiv (Sept. 21, 2020), https://arxiv.org/pdf/2009.06489.pdf.

[294] The Administration's proposed budget for non-defense AI R&D in Fiscal Year 2021 was $1.5 billion, a growth from the just under $1 billion spent in Fiscal Year 2020. *The Networking & Information Technology Research & Development Program, Supplement to The President's FY2021 Budget*, National Science & Technology Council at 4, 12 (Aug. 14, 2020), https://www.nitrd.gov/pubs/FY2021-NITRD-Supplement.pdf. The National AI Initiative Act of 2020 included in the National Defense Authorization Act for 2020 included additional investments in AI R&D at the National Science Foundation (NSF), Department of Energy, NIST, and the National Oceanic and Atmospheric Administration (NOAA). Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

[295] Based on projections by OpenAI, at the current rate of increasing costs of model training, "in 4 years, training the largest model will cost more than launching a rocket into orbit." See Yaroslav Bulatov, *Large-scale AI and Sharing of Models*, Medium (July 20, 2019), https://yaroslavvb.medium.com/large-scale-ai-and-sharing-of-models-4622ba59ec18.

This high barrier to entry has benefited large private sector efforts concentrated in select regions such as Silicon Valley and hampered AI R&D in academia and small businesses.[296] This sets the conditions for the future of AI technology to be shaped by a limited group of stakeholders.

The consolidation of the AI industry threatens U.S. technological competitiveness in five ways:

- *Brain Drain.* Brain drain from academic institutions to the private sector threatens to hollow out the foundations of the United States' advantage in basic AI research—its universities.[297] Federal funding that has not kept pace with the growth of the field has led to low grant application success rates and amplified time spent on the bureaucracy of pursuing and completing proposals.[298] However, academic experts and their students are not just lured to big tech by the promise of less bureaucracy and higher financial incentives. Increasingly, the private sector is the best place to conduct cutting-edge research with access to the best computing and data resources. The result is the weakening of the teaching base for the next generation of AI leaders in industry and academia, and the narrowing of the overall AI research agenda.[299]

- *Diversity.* The growing divide between "haves" and "have nots" in AI will exacerbate the well-documented lack of diversity in the field,[300] limiting the field's collective ability to build equitable, inclusive systems.

- *Research Focus.* American technology firms are accountable to their shareholders, and will logically not invest in areas of national security importance or make uncertain bets on fundamental research that do not hold commercial or economic benefit for the company.[301] While return-focused investments can lead to applications that contribute to the public good or benefit government work, there are gaps. ML and the underlying algorithms were in exactly this position two decades ago—seemingly without commercial promise—only to be

[296] Joel Klinger, et al., *A Narrowing of AI Research?*, ArXiv (Nov. 18, 2020), https://arxiv.org/pdf/2009.10385.pdf.

[297] A recent study found that from 2004-2018, 131 AI professors left universities for industry and 90 adopted a dual affiliation while maintaining part-time positions at a university, and documented the adverse effect departures had on AI startups of students from these universities. Michael Gofman & Zhao Jin, *Artificial Intelligence, Education, and Entrepreneurship*, SSRN at 2 (Oct. 26, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3449440. High salaries in the commercial sector pull researchers from academic tracks—in 2019, 57% of AI/ML PhD graduates in North America went to industry versus staying in academia for post-doc, research, or faculty appointments. Stuart Zweben & Betsy Bizot, *2019 Taulbee Survey,* Computing Research Association at 11 (May 2020), https://cra.org/wp-content/uploads/2020/05/2019-Taulbee-Survey.pdf.

[298] For example, in 2018, NSF, which provides 85% of federal funding for computer science, funded $165 million in core AI research, but did not have room in the budget to fund another $185 million worth of well-rated proposals. In 2017, the numbers were $122 million funded, $174 million unfunded. NSF presentation to NSCAI (June 2019).

[299] Time computer science faculty can spend holding concurrent appointments in industry increased from 20% to up to 50-80%, which has implications on their academic responsibilities including recruitment of students, development of coursework and seminars, as well as the possible consequence of aligning graduate student work on industry's needs over high impact basic research. Shwetak Patel, et al., *Evolving Academia/Industry Relations in Computing Research*, Computing Community Consortium at 3 (June 2019), https://cra.org/ccc/wp-content/uploads/sites/2/2019/06/Evolving-AcademiaIndustry-Relations-in-Computing-Research.pdf.

[300] The annual Taulbee study that tracks the field of computer science (CS) found that women make up 21.0 percent of CS bachelors graduates and 20.3 percent of CS doctoral graduates, and domestic underrepresented minorities make up 14.7 percent of CS bachelor degrees awarded and only 3.1 percent of doctoral graduates. Stuart Zweben & Betsy Bizot, *2019 Taulbee Survey,* Computing Research Association at 4, 5, 22 (May 2020), https://cra.org/wp-content/uploads/2020/05/2019-Taulbee-Survey.pdf. A trend toward narrowing participation in the field holds the potential to worsen this state. See Nur Ahmed & Muntasir Wahed, *The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research*, ArXiv (Oct. 22, 2020), https://arxiv.org/abs/2010.15581.

[301] See, e.g., Joel Klinger, et al., *A Narrowing of AI Research?*, ArXiv (Nov. 18, 2020), https://arxiv.org/pdf/2009.10385.pdf; Sara Hooker, *The Hardware Lottery*, ArXiv (Sept. 21, 2020), https://arxiv.org/pdf/2009.06489.pdf.

sustained by federal research dollars until computing power and an overabundance of data transformed the discipline.[302] A recent study found that 82 percent of the algorithms in use today originated from federally-funded non-profits and universities, compared to just 18 percent from private companies.[303]

- *Competition.* The rising cost of developing cutting-edge ML models and high likelihood of acquisition by leading technology companies means AI startups have narrowing paths to growth in the United States.[304] Lack of competition undermines the industry's ability to innovate and be globally competitive in the research and development of AI.

- *Regional Divergence.* The clustering of technology firms in regions like Silicon Valley drives innovation by expediting knowledge sharing and sharpening domestic rivalry.[305] However, this trend has benefitted some regions and demographics more than others.[306] More than 90 percent of U.S. innovation sector job creation occurred in just five major coastal cities between 2005 and 2017.[307] This divergence concentrates gains from technological progress in just a few regions and misses out on latent innovation potential in the rest of the country.

Ingenuity not access should be the key to AI innovation in America. The federal government holds the responsibility to reverse these trends. It must step in and step up to provide strategic direction and sustained resources, as both a funder and consumer of technology.[308] It must break the

[302] From the very outset of the field, the federal government had a hand in fostering research. The Air Force via RAND supported the work of Herbert Simon and Allen Newell, who in 1956 created the first successful artificial intelligence computer program, the Logic Theorist. Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, Anthem Press (2013). Defense Advanced Research Projects Agency (DARPA) (then ARPA) funded the work of Charles Rosen, who developed the first self-navigating robot, "Shakey," in 1972. *Shakey the Robot*, DARPA (last accessed Dec. 30, 2020), https://www.darpa.mil/about-us/timeline/shakey-the-robot. Reinforcement learning, the approach on which many of today's commercial applications are based, was sustained through the "AI Winter" of the 1990s by NSF's support of Andrew Barto. NSCAI staff engagement with NSF (Aug. 8, 2019). DARPA's 30 years of funding for research on image understanding created the foundation for autonomous driving capabilities. DARPAtv, *DARPA Artificial Intelligence Colloquium Opening Video*, YouTube (Mar. 12, 2019), https://www.youtube.com/watch?v=FTaW6ZJ9oyQ. The PAL program run by DARPA in the mid-2000s led to the development of the first artificially-intelligent assistant, which eventually became SIRI. DARPAtv, *DARPA and AI: Visionary Pioneer and Advocate*, YouTube (Dec. 7, 2018), https://www.youtube.com/watch?v=ri5gOjYgLns.

[303] Neil C. Thompson, et al., *Building the Algorithm Commons: Who Discovered the Algorithms that Underpin Computing in the Modern Enterprise?*, Global Strategy Journal at 4 (2020), https://onlinelibrary.wiley.com/doi/epdf/10.1002/gsj.1393.

[304] For example, non-elite universities and AI startups have difficulty affording the cost of compute resources and data for training sophisticated ML models. See Nur Ahmed & Muntasir Wahed, *The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research*, arXiv (Oct. 22, 2020), https://arxiv.org/abs/2010.15581. Ninety percent of Silicon Valley AI startups were purchased by large technology companies between 2013 and 2018. See Ryan Kottenstette, *Silicon Valley Companies Are Undermining the Impact of Artificial Intelligence*, TechCrunch (Mar. 15, 2018), https://techcrunch.com/2018/03/15/silicon-valley-companies-are-undermining-the-impact-of-artificial-intelligence/. These same companies dominate U.S. patent lists, excluding adoption patents. See Al AuYeung, *Who is Winning the AI Race?*, IP Watch Dog (Feb. 1, 2020), https://www.ipwatchdog.com/2020/02/01/winning-ai-race/id=118431/.

[305] Michael Porter, *Clusters and the New Economics of Competition*, Harvard Business Review (Nov.-Dec. 1998), https://hbr.org/1998/11/clusters-and-the-new-economics-of-competition.

[306] William R. Kerr & Frederic Robert-Nicoud, *Tech Clusters*, Journal of Economic Perspectives at 63 (Summer 2020), https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.34.3.50.

[307] Specifically, Seattle, Boston, San Francisco, San Diego, and San Jose. See Robert D. Atkinson, et al., *The Case for Growth Centers: How to Spread Tech Innovation Across America*, Brookings (Dec. 9, 2019), https://www.brookings.edu/research/growth-centers-how-to-spread-tech-innovation-across-america/.

[308] NSF and other government agencies are doing admirable work, with the resources available, to encourage diverse research and create economies of scale for AI innovation, but they will not produce a strategic effect at the current level of effort, which is set against the backdrop of an overall decline in federal investment in R&D. Other notable recent federal initiatives include DARPA's Artificial Intelligence Exploration Program, which fast tracks funding for awards up to $1 million to explore feasibility of new AI concepts within an 18-month timeframe; and NSF's National AI Research Institute effort, which in 2020 funded seven multi-

mold of standard scientific research funding. The outcomes of technology innovation, which generate greatest value when translated into fieldable solutions, are driven by multi-sector contributions and a culture of risk acceptance. The status quo at federal agencies and research entities is insufficient for making these big bets and propelling promising technology concepts from laboratory to field.

A passive national approach that relies too heavily on the private sector to drive innovation and determine research agendas—and that presumes commercial innovation can simply "spin-in" to become government applications—will not win this strategic competition. The United States—through government leadership in partnership with industry and academia—must increase the diversity, competitiveness, and accessibility of its AI innovation environment. That begins with a substantial infusion of new R&D dollars.

✦ **Scale and coordinate federal AI R&D funding.** A bold, integrated push for long-term investments in AI R&D will foster nationwide AI innovation and drive breakthroughs in AI technologies. An infusion of sustained resources, guided by a comprehensive strategy and distributed through a diversity of mechanisms, will enable U.S. researchers to stay at the forefront of the field. Specifically, the United States should:

- *Establish a National Technology Foundation (NTF).* A new, independent organization would complement successful existing organizations, such as the National Science Foundation (NSF). An emerging technology-focused organization would fund academic and small business research, coordinate and support a network of AI infrastructure assets, and create transition pipelines for commercialization or government use of technology advancements.

- *Increase federal funding for AI R&D at compounding levels, doubling annually to reach $32 billion per year by Fiscal Year 2026.* This would bring AI spending to a level near to federal spending on biomedical research.[309] Overall, the government should spend at least 1% of GDP on R&D to reinforce a base of innovation across scientific fields.[310] Additional funding should strengthen basic and applied research, expand fellowship programs, support research infrastructure, and cover several agencies, with an emphasis on:

    ○ National Technology Foundation (proposed)
    ○ Department of Energy
    ○ National Science Foundation
    ○ National Institutes of Health
    ○ National Institute of Standards and Technology
    ○ National Aeronautics and Space Administration

institution, university-based research institutes at $4 million per year for five years, and plans to launch another eight in 2021. *Artificial Intelligence at NSF*, NSF (Aug. 26, 2020), https://www.nsf.gov/cise/ai.jsp.

[309] Funding for the National Institutes of Health (NIH) has grown from $30 billion in 2010 to $41 billion in 2020. *NIH Budget History: NIH Budget Mechanism Detail*, NIH Data Book(Oct. 2019), https://report.nih.gov/nihdatabook/category/1; *Budget*, NIH (June 29, 2020), https://www.nih.gov/about-nih/what-we-do/budget.

[310] In 1953, the U.S. spent 0.72 percent of its GDP on R&D. In 1957, when the then-Soviet Union launched Sputnik, it had grown to 1.3 percent. R&D spending peaked at 1.86 percent in 1964. In 2017, it declined below 1953 levels to 0.61 percent. *Federal R&D Budget Dashboard*, American Association for the Advancement of Science (last accessed Jan. 14, 2021), https://www.aaas.org/programs/r-d-budget-and-policy/federal-rd-budget-dashboard.

- *Prioritize funding for key areas of AI R&D.* Amplified federal funding should prioritize AI R&D investments in areas critical to advance technology that will underpin future national security and economic stability, supporting areas that may not receive significant private sector investment. Coordinated through the newly established National AI Initiative,[311] investments should reflect a portfolio approach, focused on advancing basic science, solving specific challenge problems and facilitating commercialization breakthroughs.

Table 4. Priority Areas for AI Research Investment

Research Area	Goal
Novel machine learning directions	To further non-traditional approaches to supervised machine learning in an unsupervised or semi-supervised manner as well as the transfer of learning from one task or domain to another.
Test and evaluation, verification and validation (TEVV) of AI systems	To develop a better understanding of how to conduct TEVV and build checks and balances into an AI system, including improved methods to explore, predict and control individual AI system behavior so that when AI systems are composed into systems-of-systems their interaction does not lead to unexpected negative outcomes. Understand context-specificity and degradation of performance in new and unseen environments.
Robust machine learning	To cultivate more robust methods that can overcome adverse conditions, and advance approaches that enable assessment of types and levels of vulnerability and immunity. Addressing challenges of multiple classes of adversarial machine learning attacks. Includes research on fairness.
Complex multi-agent scenarios	To advance the understanding of interacting cohorts of AI systems, including research into adversarial vulnerabilities and mitigations, along with the application of game theory to varied and complex scenarios.
Integrating AI, modeling, simulation, and design	To progress the use of rich simulations as a source of data and scenarios for training and testing AI systems, and to use AI to solve complex analytical problems and to serve as a generative design engine in scientific discovery and engineering.
Advanced scene understanding	To evolve perceptual models to incorporate multi-source and multi-modal information to support enhanced actionable awareness and insight across a range of complex, dynamic environments and scenarios.
Preserving personal privacy	To assure personal privacy of individuals is protected in the acquisition and use of data for AI system development and operation through advancements in anonymity techniques and privacy-preserving technologies such as homomorphic encryption, differential privacy techniques, and multi-party federated learning.
AI system risk assessment	Advance capabilities to support risk assessment including standard methods and metrics for evaluating degrees of auditability, traceability, interpretability, explainability, and reliability.

[311] The National AI Initiative Act of 2020 included in the National Defense Authorization Act for Fiscal Year 2021 creates a structure for a more strategic approach to harnessing AI through establishment of a National AI Initiative Office within the Office of Science and Technology Policy and associated advisory group and interagency construct. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

Enhanced human-AI interaction and teaming	To advance the understanding of human-AI teaming, including human-AI complementarity, methods for augmenting human reasoning abilities, fluid handoffs in mixed-initiative systems. Also includes bolstering AI technologies to better perceive and understand human intention and communications, including comprehension of spoken speech, written text, and gestures. Advances in human-machine teaming will enable human interactions with AI-enabled systems to move from the current model of interaction where the human is the "operator" to a future in which humans have a "teammate" relationship with machines.
AI autonomous systems	To advance a system's ability to accomplish goals independently, or with minimal supervision from human operators in environments that are complex and unpredictable.
Toward more general artificial intelligence	Research persistent challenging problems, and mysteries of human intellect, including ability to learn efficiently in an unsupervised manner; amass and apply commonsense knowledge; build causal models that provide robust explanations; exercise self-awareness, assessment, and control; and generalize and leverage knowledge learned about specific tasks to become proficient at another task.

- *Triple the number of National AI Research Institutes.* The government should triple the current number of federally-funded national AI research institutes across a range of regions and research areas.[312] This would increase training and research opportunities for students and academic faculty, national lab researchers, and non-profit research organizations.

- *Invest in talent that will transform the field.* In parallel, NSF or the proposed NTF should invest in top AI researchers and interdisciplinary teams, launching grant awards that make big bets on the people and the out of the box ideas that could lead to unexpected breakthroughs.

✦ **Expand access to AI resources through a National AI Research Infrastructure.** Democratized access to AI R&D will support more equitable growth of the field, an expansion of AI expertise across the country, application of AI to a broader range of fields, and new innovations. This national infrastructure should have five main elements:

- *A National AI Research Resource (NAIRR).*[313] To bridge the "compute divide,"[314] the NAIRR should be created as a public-private partnership, leveraging a federation of cloud platforms. This construct would provide verified researchers and students subsidized access to compute resources, co-located with AI-ready government and non-government data sets, educational tools, and user support.

[312] NSF awarded grants for the first national AI research institutes in 2020, supporting seven university-based, multi-institution consortia organized around fundamental and applied areas of AI research, and plans to fund a second round of institutes in 2021, coordinating support not only with interagency partners but also with private sector stakeholders to launch eight additional institutes. *Artificial Intelligence at NSF*, NSF (Aug. 26, 2020), https://www.nsf.gov/cise/ai.jsp.

[313] Acting on a recommendation NSCAI issued in our *First Quarter Recommendations*, Congress has taken the first step to establish the NAIRR in the Fiscal Year 2021 National Defense Authorization Act, creating a task force to develop a roadmap for a future NAIRR. The result of this effort will be due to Congress 18 months after appointment of task force members. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

[314] Since the explosion of deep learning in 2012 and accompanying growth in use of specialized hardware for AI computing, there has arisen what some have termed the "compute divide"—a disparity in access between large technology companies and elite universities and mid- and lower-tier universities to the resources necessary for cutting-edge AI research. Nur Ahmed & Muntasir Wahed, *The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research*, ArXiv (Oct. 22, 2020), https://arxiv.org/abs/2010.15581.

- *A set of domain-specific AI R&D test beds.* Sponsored by various federal agencies, these would provide accessible facilities, establish benchmarking standards, and build communities of discovery around AI application areas that are in the public interest.

- *Pipelines for the curation, hosting, and maintenance of complex data sets.* This should include creation of large scale, open source training data, and funding for teams of data engineers and scientists to unlock public data currently held by the government for use by the AI research community.

- *An open knowledge network.* Coordinated by the Office of Science and Technology Policy, such a resource would enable use of constructed and organized world knowledge to develop AI systems that operate effectively and efficiently.[315]

- *A Multilateral AI Research Institute* to foster collaborative R&D with researchers from key allies and partners (described further in Chapter 15).

These resources would work in complement to each other, providing a virtuous cycle of data, experimentation, testing, and knowledge building that would fuel innovation and application of AI to a wide range of challenge problems and fields of study.

✦ **Leverage both sides of the public-private partnership.** U.S. leadership in technologies like AI depends upon closer public-private collaboration and a shared sense of responsibility for U.S. global competitiveness. To promote innovation and accelerate the growth of globally competitive firms in strategic emerging sectors, the government should:

- *Create markets for AI and other strategic technologies.* The application of AI across government agencies can save taxpayer dollars and improve the quality of public services. Some applications can be adopted directly from the private sector, while others are unique to the government mission. By accelerating AI adoption across federal agencies, the government can drive additional commercial investment in AI applications that benefit national security and the public good.

- *Form a network of regional innovation clusters focused on strategic emerging technologies.* The government should designate regional innovation clusters focused on strategic emerging technologies like AI to foster the growth of small companies in sectors that are critical to overall U.S. competitiveness. Established through a competitive bid process, the clusters would offer participants from industry and academia tax incentives, research grants, and access to federal R&D resources.

[315] This would build on prior work undertaken by the Networking and Information Technology Research and Development (NITRD) Program Big Data Interagency Working Group. See *Open Knowledge Network: Summary of the Big Data IWG Workshop*, National Science & Technology Council (Nov. 2018), https://www.nitrd.gov/pubs/Open-Knowledge-Network-Workshop-Report-2018.pdf.

The private sector should:

- *Privately fund an AI competitiveness consortium.* Private firms should establish a non-profit organization with $1 billion in funding over five years to broaden AI research opportunities and support AI skills and education. This donation-funded organization would focus on fostering economic opportunity through resources for AI research and AI skills training. Such corporate social responsibility spending to promote AI education and entrepreneurship would help bridge the gap between digital “haves” and “have nots.”

✦ **Tackle Some of Humanity’s Biggest Challenges.** By focusing on solving real human problems that impact the lives of millions of people, we can build a new raison d’etre for the triangular alliance of government, academia, and industry; sustain public support for ambitious AI research; and extend America’s AI innovation leadership. Examples of promising initiatives that could improve societal well-being and advance scientific frontiers include:

- *Enable long term quality of life.* AI technology that can help the elderly live independently longer, assisting in managing health and daily tasks, and improving the quality of life. This can include application of AI to biomedicine to address acute and chronic illnesses and enhance healthy aging.

- *Revolutionize education and life-long learning.* AI tools that personalize education, training, and retraining at appropriate challenge levels and intuitively evaluate development to optimize standard curricula to promote individual learning success.

- *Transform energy management.* Smart infrastructure for cities that can effectively respond to surges in energy demand and emergencies (both man-made or natural disasters).

- *Effectively predict, model, prepare for and respond to disasters.* Accurate, near real time weather, earthquake, and fire line detection and prediction of escalation to aid in emergency response and planning for optimized deployment of limited resources. Autonomous robots for search, rescue, and clean up in the wake of natural or man-made disaster, providing force-multiplying support to first responders and hazardous materials professionals.

- *Reach new frontiers in space.* Autonomous AI spacecraft, habitats, and facilities capable of identifying and solving problems with or without the need of human intervention, enabling extended and more flexible space exploration.

Chapter 12: Intellectual Property

China is both leveraging and exploiting intellectual property (IP) policies as a critical tool within its national strategies for emerging technologies. The United States has failed to similarly recognize the importance of IP in securing its own national security, economic interests, and technology competitiveness. The U.S. has not developed comprehensive IP policies to incentivize investments[316] in and protect the creation of AI and other emerging technologies.[317] The consequence of this policy void—which includes legal uncertainties created by current U.S. patent eligibility and patentability doctrine, the lack of an effective response to China's domestic and geopolitical strategies centered on its IP institutions,[318] and the lack of effective data protection policies—is that the U.S. could lose its prime position in IP global leadership. At the same time, by strengthening its IP regimes,[319] China is posed to "fill the void" left by weakened U.S. IP protections, particularly for patents, as the U.S. has lost its "comparative advantage in securing stable and effective property rights in new technological innovation."[320] This stark policy asymmetry has multiple significant domestic and international implications for the U.S.

First, U.S. courts have severely restricted what types of computer-implemented and biotech-related inventions can be protected under U.S. patent law.[321] Critical AI and biotech-related inventions have been denied patent protection since 2010.[322] Facing uncertainty in obtaining and retaining patent

[316] Advances in emerging technologies require significant investments. These investments are partly public, but also require extensive private investments.

[317] Technologies critical to national security interests include AI and biotechnology. NSCAI proposes an initial list of emerging technologies key to U.S. national competitiveness in Chapter 16: Associated Technologies.

[318] CSET translation of *National 13th Five-Year Plan for the Development of Strategic Emerging Industries*, Central People's Government of the People's Republic of China at 59 (Nov. 29, 2016) (translation by CSET on Dec. 9, 2019), https://cset.georgetown.edu/research/national-13th-five-year-plan-for-the-development-of-strategic-emerging-industries/. China continues to make extensive reforms to its IP regimes in furtherance of its innovation and industrial competitiveness goals. See Mark Cohen, *IPO's Comments on Recent Patent Legislation: Untangling a Complex Web*, China IPR blog (Dec. 15, 2020), https://chinaipr.com/2020/12/15/ipos-comments-on-recent-patent-legislation-untangling-a-complex-web/.

[319] China's actions include ensuring that AI and associated technologies are eligible for patent protection, increasing damages awards for patent infringement, continuing to issue preliminary injunctions for infringement of valid patents, and creating specialized IP courts with more efficient resolution of IP cases. See Kevin Madigan & Adam Mossoff, *Turning Gold into Lead: How Patent Eligibility Doctrine is Undermining U.S. Leadership in Innovation*, George Mason Law Review at 943–46 (Apr. 13, 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2943431 [hereinafter Turning Gold Into Lead]; Ryan Davis, *4 Things to Know About China's Revised Patent Law,* Law 360 (Nov. 5, 2020), https://www.law360.com/articles/1326419/; Liaoteng Wang et. al., *A Comparative Look at Patent Subject Matter Eligibility Standards: China Versus the United States* (June 12, 2020), https://www.ipwatchdog.com/2020/06/12/comparative-look-patent-subject-matter-eligibility-standards-china-versus-united-states/id=122339/; Erick Robinson, *Everything You Need to Know about China's New Preliminary Injunction Rules,* IAM (Dec. 21, 2018), https://www.iam-media.com/designs/everything-you-need-know-about-chinas-new-preliminary-injunction-rule; Justice Tao Kaiyuan, *China's Commitment to Strengthening IP Judicial Protection and Creating a Bright Future for IP Rights,* WIPO Magazine (June 2019), https://www.wipo.int/wipo_magazine/en/2019/03/article_0004.html.

[320] See Turning Gold Into Lead, at 955.

[321] See Turning Gold Into Lead. In January 2019, the United States Patent & Trademark Office (USPTO) published initial patent eligibility guidance that applies during examination of patent applications at the USPTO, which arguably decreased uncertainty as to patent eligibility determinations during the patent application examination and granting process. However, the United States Court of Appeals for the Federal Circuit, the appellate court with jurisdiction of appeals from patent cases, held that it is not bound by the Guidance. *See Cleveland Clinic Found. v. True Health Diagnostics LLC*, 760 F. App'x 1013, 1020 (Fed. Cir. 2019) (non-precedential); *In re Rudy*, 956 F.3d 1379, 1383 (Fed. Cir. 2020) (precedential) (citing *Cleveland Clinic Found.*, 760 F. App'x at 1021).

[322] *Athena Diagnostics v. Mayo Collaborative Services,* 915 F.3d 743 (Fed. Cir. 2019), rehearing en banc denied 927 F.3d 1333 (Fed. Cir. 2019) (method of diagnosing certain, previously undiagnosable, patients suffering from the neurological disorder myasthenia gravis using MuSK autoantibodies); *The Cleveland Clinic Found. v. True Health Diagnostics LLC*, 760 F. App'x 1013 (Fed. Cir. 2019) (method of assessing the risk a patient has cardiovascular disease by analyzing the level of a certain enzyme in a patient's blood); *Roche Molecular Systems, Inc. v. Cepheid*, 905 F.3d 1363 (Fed. Cir. 2018) (DNA primers used in a method to detect the pathogenic bacterium Mycobacterium tuberculosis); *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371 (Fed. Cir. 2015), *cert. denied*, 136

protection, inventors pursue trade secret protection. Trade secrets do not readily promote innovation markets, because trade secrets, unlike patents, do not contribute to accessible technical knowledge in the public domain.[323] While these impacts might not be immediate, the long-term effects on AI and other emerging technology development and competitiveness are concerning.[324]

Second, China has met its strategic policy goal of increasing the quantity of its patent applications and issued patents, creating the narrative that it has "won" the innovation race. In 2019, the total number of "invention" patent applications filed at the China National Intellectual Property Administration (CNIPA) was approximately three times as many as utility patent applications filed at the U.S. Patent and Trademark Office (USPTO).[325] China also led the world in international patent applications under the Patent Cooperation Treaty (PCT) system of the World Intellectual Property Organization.[326] Critically, China is now frequently identified as the current leader in domestic patent application filings for AI inventions.[327] Globally, AI patent applications originating from China outnumber those originating from the United States, especially in recent years.[328]

Third, regardless of quality concerns,[329] China's prolific patent application filings may further hurt U.S. innovators by creating a vast reservoir of "prior art" (the term in patent law for the worldwide scientific and technical knowledge by which an invention is evaluated to determine if it is new). This dramatically increases the quantity of prior art that must be reviewed in examining a patent application. As a result, the patent examination process at the USPTO will become increasingly difficult, if not onerous. At the same time, U.S. inventors may find it more difficult to obtain patents

S. Ct. 2511 (2016) (method of diagnosing fetal characteristics based on paternally inherited DNA found in a mother's bloodstream without creating a major health risk for the fetus); *PUREPREDICTIVE, Inc. v. H20.AI, Inc.*, No. 17-cv-03049-WHO, 2017 WL 3721480 (N.D. Cal. Aug. 29, 2017) (predictive analytics); *Power Analytics Corp. v. Operation Tech., Inc.*, No. 16-cv-01955 JAK (FFMx), 2017 WL 5468179 (C.D. Cal. July 13, 2017) ("computer simulation techniques with real-time system monitoring and prediction of electrical system performance").

[323] See *Crash Course on Patents: What is a Patent and Why is it Useful*, Ius mentis (last accessed Dec. 30, 2020), https://www.iusmentis.com/patents/crashcourse/whatis/ (because patents openly publish details of the invention, other inventors can license this invention or think of enhancements or design around the disclosure); Steven Hoffman & Calla Simeone, *Trade Secret Protection & the COVID-19 Cure: Observations on Federal Policy-Making & Potential Impact on Biomedical Advances*, JDSupra (Sept. 15, 2020), https://www.jdsupra.com/legalnews/trade-secret-protection-the-covid-19-37383/ (discussing implications of uncertainty in patent eligibility on use of trade secrets for biomedical advances).

[324] Surveys and industry reports demonstrate that investment has already shifted away from patent-intensive industries. See Mark F. Schultz, *The Importance of an Effective and Reliable Patent System to Investment in Critical Technologies*, Alliance for U.S. Startups and Investors for Jobs at 24–37 (July 2020), https://static1.squarespace.com/static/5746149f86db43995675b6bb/t/5f2829980ddf0c536e7132a4/1596467617939/USIJ+Full+Report_Final_2020.pdf.

[325] Patrick Thomas & Dewey Murdick, *Patents and Artificial Intelligence: A Primer*, Center for Security and Emerging Technology at 10 (Sept. 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Patents-and-Artificial-Intelligence.pdf [hereinafter CSET, A Primer]; *U.S. Patent Statistics Chart Calendar Years 1963-2019*, USPTO (Apr. 2020), https://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.htm.

[326] See CSET, A Primer at 11; Aaron Wininger, *China Surpasses U.S. to Become Top Filer of PCT International Patent Applications in 2019*, National Law Review (Apr. 7, 2020), https://www.natlawreview.com/article/china-surpasses-us-to-become-top-filer-pct-international-patent-applications-2019. China is on pace to continue being the top PCT filer in 2020. See Aaron Wininger, *China 2020 H1 Patent Data Indicates China Likely to Remain Top International Filer in 2020*, National Law Review (July 11, 2020), https://www.natlawreview.com/article/china-2020-h1-patent-data-indicates-china-likely-to-remain-top-international-filer.

[327] *AI Innovators,* RS (last accessed Dec. 30, 2020), https://uk.rs-online.com/web/generalDisplay.html?id=did-you-know/ai-innovators; George Leopold, *China Dominates AI Patent Filings*, Enterprise AI (Aug. 31, 2020), https://www.enterpriseai.news/2020/08/31/china-dominates-ai-patent-filings/; CSET, A Primer.

[328] CSET, A Primer at 9, 12, n. 23.

[329] *Trademarks and Patents in China: The Impact of Non-Market Factors on Filing Trends and IP Systems*, USPTO at 1 (Jan. 2021), https://www.uspto.gov/sites/default/files/documents/USPTO-TrademarkPatentsInChina.pdf; Jonathan Putnam, et al., *Innovative Output in China*, SSRN at 32 (Aug. 2020) (pending revision), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3760816.

because they must show that their inventions are not disclosed in the prior art publications anywhere in the world, including in the Chinese-language patent applications filed in China and internationally.[330] As Chinese patents come to dominate prior art searches by patent offices throughout the world, the current dominance of U.S. patents in worldwide prior art searches will erode.[331]

Fourth, and consistent with China's extensive patent application filings, China's companies have been identifying too many patents as "standard essential" in standard development organizations, i.e., alleging that these patents must be practiced to comply with a technical standard.[332] Although standard development organizations require patent owners to self-identify patents that may be deemed essential in future standards, these organizations leave final essentiality determinations to private companies negotiating licenses or, if there is a dispute, to courts.[333] This practice of "over declaring" standard essential patents furthers China's global narrative that it has "won" the race to such standardized technologies as 5G, prompting other countries to adopt China's technologies in their own communications infrastructures.[334] A worrisome result may be that U.S. companies pay billions in royalties to China's companies or face claims and resulting litigation that they willfully infringed on Chinese company patent rights.[335]

Fifth, the lack of explicit legal protections for data or express policies on data ownership may hinder innovation and collaboration.[336] The absence of data protection regimes may disincentivize parties from making necessary investments to develop data sets that are critical for machine learning and AI

[330] Jeanne Suchodolski, et al., *Innovation Warfare*, North Carolina Journal of Law & Technology at 201 (Dec. 7, 2020), https://ncjolt.org/articles/volume-22/volume-22-issue-2/innovation-warfare/ [hereinafter Innovation Warfare].

[331] Rob Sterne, *How China Will Fundamentally Change the Global IP System*, IP Watchdog (July 24, 2019), https://www.ipwatchdog.com/2019/07/24/china-changing-global-ip-system/id=111613/.

[332] Over declaration is already present in 5G. See Matthew Noble, et al., *Determining Which Companies Are Leading the 5G Race*, IAM (July/August 2019), https://www.twobirds.com/~/media/pdfs/news/articles/2019/determining-which-companies-are-leading-the-5g-race.pdf?la=en&hash=8ABA5A7173EEE8FFA612E070C0EA4B4F53CC50DE; *Meeting the China Challenge: A New American Strategy for Technology Competition,* Working Group on Science and Technology in U.S.-China Relations at 27, 29 (Nov. 16, 2020), https://china.ucsd.edu/_files/meeting-the-china-challenge_2020_report.pdf [hereinafter Meeting the China Challenge].

[333] *IEEE SA Standards Board Bylaws*, IEEE SA (last accessed Jan. 15, 2020), https://standards.ieee.org/about/policies/bylaws/sect6-7.html#loa.

[334] Adam Mossoff & Urška Petrovčič, *5G Technological Leadership,* Hudson Institute (Dec. 5, 2020), https://www.hudson.org/research/16547-5-g-technological-leadership; *Innovation Warfare*, at 201, n.130 (China's firms recognize the strategic importance of standard setting activities and that participation in those forums provides the legal means to both access and influence developing technologies).

[335] Because SEPs may reach into the hundreds of thousands for technologies, licensing fees carry significant economic repercussions. See Adam Mossoff & Urška Petrovčič, *5G Technological Leadership,* Hudson Institute at 3 (Dec. 5, 2020), https://www.hudson.org/research/16547-5-g-technological-leadership ("[P]atent counting might have negative consequences on firms working in the US innovation economy . . . if judges or regulators rely on simple counts of total patents as a metric for determining the value of patent portfolios. The failure to account for differences in patent quality risks overcompensating some patent holders, namely those with less valuable technologies, but undercompensating those that have developed breakthrough innovation."); Andrei Iancu, Director of USPTO, Remarks at the Center for The Protection of Intellectual Property 2020 Fall Conference (Oct. 7, 2020), https://cpip.gmu.edu/2020/10/20/cpip-2020-fall-conference-day-one-recap/; Muzammil Hassan, et al., *Who Owns Core 5G Patents? - A Detailed Analysis of 5G SEPs*, GreyB (2020), https://www.greyb.com/5g-patents/#The-State-of-Declared-5G-Patents; Cody M. Akins, *Overdeclaration of Standard-Essential Patents*, Texas Law Review (2020), https://texaslawreview.org/wp-content/uploads/2020/02/Akins.Printer.pdf.

[336] Mitchell Smith, *A Comparison of the Legal Protection of Databases in the United States and EU: Implications for Scientific Research*, SSRN (May 23, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1613451; Daniel J. Gervais, *Exploring the Interfaces Between Big Data and Intellectual Property Law*, Journal of Intellectual Property, Information Technology and Electronic Commerce Law (2019), https://scholarship.law.vanderbilt.edu/faculty-publications/1095.

systems.[337] Additionally, the absence of data governance policies (such as contracting best practices) for IP-type protections or ownership rules, could undermine the willingness of companies to enter into the public-private partnerships that are crucial for creating cutting-edge technological innovations.[338] This could also create challenges for U.S. collaboration with allies and other partners in vital AI research and development (R&D) where data rights or ownership claims come into question.

Lastly, as further evidence that China views IP as essential in its domestic economic development, China continues to pervasively steal American IP-protected technological advances through varied means like cyber hacking of businesses and research institutes, technological espionage, blackmail, and illicit technology transfer.[339]

The Intellectual Property Policy Void. The U.S. government needs to address these vulnerabilities, resulting from the lack of comprehensive IP policies. Currently, the U.S. government does not efficiently utilize IP policy as a tool to support national strategies for national security, economic interests, and technology competitiveness in AI and emerging technologies. The majority of the United States government's coordinated IP policy efforts are focused on IP enforcement and preventing IP theft.[340] The U.S., however, lacks an agency or interagency entity that is empowered to both develop and execute national IP policies that support and integrate with national strategies. As a result, the United States lacks cohesive, legislatively mandated AI and emerging technology IP policies that are integrated into national strategy frameworks to address, for example, global competition from countries like China.

America's IP laws and institutions must be considered as critical components for safeguarding U.S. national security interests, including advancing economic prosperity and technology competitiveness. The United States must, at minimum, articulate and develop national IP reforms and policies with the goal of incentivizing, expanding and protecting AI and emerging technologies, at home and abroad. Such policies should be developed and proposed via the Executive Branch with a process that integrates the disparate departments and agencies that serve important roles in promoting U.S. innovation.

✦ **Develop and implement national intellectual property policies to incentivize, expand, and protect AI and emerging technologies.** The President should issue an executive order to recognize IP as a national priority and require the development of a comprehensive plan to reform and create IP policies and regimes that further national security, economic, and technology competitiveness strategies. The Commission recommends that the executive order direct the Vice President, as Chair of the Technology Competitiveness Council (TCC), or otherwise as chair of an interagency task

[337] In the USPTO report surveying stakeholders for perspectives on IP policy for AI, the majority of opinions supporting the creation of "new IP rights focused on the need to protect the data associated with AI, particularly ML." *Public Views on Artificial Intelligence and Intellectual Property Policy*, USPTO at 15 (Oct. 2020), https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf.

[338] Thomas E. Ayers, *Changing How We Buy Weapons Will Benefit Industry, Government and Taxpayers*, Defense News (Nov. 20, 2019), https://www.defensenews.com/opinion/commentary/2019/11/20/changing-how-we-buy-weapons-will-benefit-industry-government-and-taxpayers/ (discussing the tension between Air Force and vendors over IP protection).

[339] Meeting the China Challenge, at 4, 16.

[340] *Annual Intellectual Property Report to Congress*, U.S. Intellectual Property Enforcement Coordinator (Mar. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/04/IPEC-2019-Annual-Intellectual-Property-Report.pdf (providing an overview of IP responsibilities across the United States government).

force, to oversee this effort. The executive order should direct the Secretary of Commerce—in coordination with the Under Secretary for Intellectual Property and Director of the United States Patent and Trademark Office[341]—to develop proposals to reform and establish new IP policies and regimes, as needed, to incentivize, expand, and protect AI and emerging technologies. The plan should include proposals for executive and legislative actions for IP policy changes to achieve these objectives and should be accompanied by an assessment of a non-exhaustive list of "IP considerations."[342] The executive order should direct the TCC or Vice President to assess which IP policies, regimes, and reform proposals from the Secretary of Commerce should be elevated for implementation and integration as part of national security, economic interests, and technology competitiveness strategies.

[341] Other Executive Branch departments and agencies, and the U.S. Copyright Office, should resource and support the Secretary of Commerce in these efforts.

[342] A non-exhaustive list of IP considerations should include patent eligibility doctrine, countering China's narrative on "winning" AI innovation based on patent application filings, the impact of China's patent application filings on USPTO's examination process and U.S. inventors, impediments to IP contractual system to partnerships & collaboration, IP protections for data, IP theft, metrics & data to Inform IP policy, global IP alignment, democratizing innovation & IP ecosystems, and over declaration of "standard-essential" patents.

Chapter 13: Microelectronics

U.S. leadership in microelectronics is critical to overall U.S. leadership in artificial intelligence (AI). Several assessments underpin this argument:

- Hardware is a foundational element of the AI stack alongside data, algorithms, and talent.[343]
- Exponential increases in computational power have driven the last decade of progress in machine learning.[344]
- After decades leading the microelectronics industry, the United States will soon source roughly 90 percent of all high-volume, leading-edge integrated circuit production from countries in East Asia.[345] This means the United States is almost entirely reliant on foreign sources for production of the cutting-edge semiconductors critical for defense systems and industry more broadly, leaving the U.S. supply chain vulnerable to disruption by foreign government action or natural disaster.
- Specialized hardware, novel packaging techniques such as heterogeneous integration and 3D stacking, and new types of devices will drive future AI developments as traditional architectures of silicon-based chipsets encounter diminishing marginal performance improvements.[346]
- Demand for trusted microelectronics will only grow as the military and Intelligence Community continue to incorporate AI into mission-critical systems.[347]

U.S. leadership in semiconductors has long been taken for granted based on America's advantage as a pioneer of the microelectronics industry. Gradually, however, the United States has been losing its edge. Although American universities and firms remain global leaders in the key areas of semiconductor research and development (R&D) and chip design, the semiconductor industry is now highly globalized and competitive. Taiwan Semiconductor Manufacturing Corporation (TSMC) leads the world in semiconductor contract manufacturing and Samsung in South Korea is also producing state-of-the-art logic chips.[348] TSMC also leads in the production of ARM-based chips, which is

[343] Dave Martinez, et al., *Artificial Intelligence: Short History, Present Developments, and Future Outlook*, MIT at 27, n. 10 (Jan. 2019), https://www.ll.mit.edu/sites/default/files/publication/doc/2019-09/Artificial%20Intelligence%20Short%20History%2C%20Present%20Developments%2C%20and%20Future%20Outlook%20-%20Final%20Report%20-%20Martinez.pdf (citing Andrew Moore, et al., *The AI Stack: A Blueprint for Developing and Deploying Artificial Intelligence*, International Society for Optics and Photonics, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IX (2018)).

[344] Recent machine learning breakthroughs have relied heavily on computing power and the amount of compute used in the largest AI training runs has been increasing exponentially since 2012. Girish Sastry, et al., *Addendum: Compute Used in Older Headline Results*, OpenAI (Nov. 7, 2019), https://openai.com/blog/ai-and-compute/#addendum.

[345] Michaela Platzer, et al., *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, Congressional Research Service at 12 (Oct. 26, 2020), https://crsreports.congress.gov/product/pdf/R/R46581.

[346] Sara Hooker, *The Hardware Lottery*, arXiv (Sept. 21, 2020), https://arxiv.org/pdf/2009.06489.pdf.

[347] Gaurav Batra, et al., *Artificial Intelligence Hardware: New Opportunities for Semiconductor Companies*, McKinsey & Company (Jan. 2, 2019), https://www.mckinsey.com/industries/semiconductors/our-insights/artificial-intelligence-hardware-new-opportunities-for-semiconductor-companies.

[348] Taiwan Semiconductor Manufacturing Corporation (TSMC) has already begun producing 5nm state-of-the-art logic chips and aims to produce 3nm chips by the end of 2021. Samsung is also producing 5nm chips. Intel does not anticipate producing 7nm chips in-

becoming the predominant chip architecture for mobile devices, servers, and other key applications of emerging technologies.[349] In a bid to catch up and achieve chip self-sufficiency, China is pursuing unprecedented state-funded efforts to forge a world-leading semiconductor industry by 2030. Although China is behind firms headquartered in Taiwan, South Korea, and the U.S. in terms of chip manufacturing, it is advancing quickly.[350] Meanwhile, Intel, the leading U.S. manufacturer, remains competitive in chip design but has faced manufacturing setbacks for leading-edge chips and may fall further behind its Taiwanese and South Korean rivals. Current projections put the firm two generations or more behind the cutting-edge node by 2022.[351] These and other concerning trends indicate that America's leadership in microelectronics is eroding, especially in manufacturing, assembly, testing, and packaging.[352]

The dependency of the United States on semiconductor imports, particularly from Taiwan, creates a strategic vulnerability for both its economy and military to adverse foreign government action, natural disaster, and other events that can disrupt the supply chains for electronics. Despite tremendous expertise in microelectronics research, development, and innovation across the country, the United States is limited by a lack of domestically located semiconductor fabrication facilities, especially for state-of-the-art semiconductors. This limitation is compounding the risk that the United States may be outpaced in microelectronics design and fabrication. If a potential adversary bests the United States in semiconductors, it could gain the upper hand in every domain of warfare. Focusing the efforts of the U.S. Government, industry, and academia to develop domestic microelectronics fabrication facilities will reduce dependence on imports, preserve leadership in technological innovation, support job creation, improve national security and balance of trade, and enhance the technological superiority and readiness of the military, which is an important consumer of advanced microelectronics.

To regain U.S. leadership in microelectronics, the Executive Branch should finalize and implement a national microelectronics leadership strategy. Additionally, Congress should create a 40 percent refundable tax credit for domestic fabrication investments by firms from the United States and its allies, and appropriate an additional $12 billion over the next five years for microelectronics research, development, and infrastructure. Together these efforts will enable the U.S. government, private sector, and academia to rise to the challenge of rebuilding U.S. semiconductor superiority.

house until at least 2022 and may outsource manufacturing to TSMC. Firms in China are producing 12 nm chips. Richard Waters, *Intel Looks to New Chief's Technical Skills to Plot Rebound*, Financial Times (Jan. 14, 2021), https://www.ft.com/content/51f63b07-aeb8-4961-9ce9-c1f7a4e326f0; Mark Lapedus, *China Speeds Up Advanced Chip Development*, Semiconductor Engineering (June 22, 2020), https://semiengineering.com/china-speeds-up-advanced-chip-development/; *5nm Technology*, TSMC (last accessed Jan. 16, 2021), https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_5nm; Debby Wu, *TSMC's $28 Billion Spending Blitz Ignites a Global Chip Rally*, Bloomberg (Jan. 14, 2021), https://www.bloomberg.com/news/articles/2021-01-14/tsmc-profit-beats-expectations-as-chipmaker-widens-tech-lead; Anton Shilov, *Samsung Foundry Update: 5nm SoCs in Production, HPC Shipments to Expand in Q4*, Tom's Hardware (Nov. 1, 2020), https://www.tomshardware.com/news/samsung-foundry-update-5nm-socs-in-production-hpc-shipments-to-expand-in-q4.

[349] *ARM and TSMC Announce Multi-Year Agreement to Collaborate on 7nm FinFET Process Technology for High-Performance Compute*, Design & Reuse (Mar. 15, 2016), https://www.design-reuse.com/news/39433/arm-tsmc-7nm-finfet.html.

[350] Michaela D. Platzer, et al., *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, Congressional Research Service at 2, 25, 27 (Oct. 26, 2020), https://crsreports.congress.gov/product/pdf/R/R46581.

[351] Ian King, *Intel 'Stunning Failure' Heralds End of Era for U.S. Chip Sector*, Bloomberg (July 24, 2020), https://www.bloomberg.com/news/articles/2020-07-25/intel-stunning-failure-heralds-end-of-era-for-u-s-chip-sector.

[352] Michaela D. Platzer, et al., *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, Congressional Research Service (Oct. 26, 2020), https://crsreports.congress.gov/product/pdf/R/R46581.

Stay two generations ahead of China in state-of-the-art microelectronics and maintain multiple sources of cutting-edge microelectronics fabrication in the United States. The United States should focus the attention and resources necessary for long-term competition in microelectronics by adopting an overarching national objective: to stay two generations ahead of potential adversaries in state-of-the-art microelectronics while also maintaining multiple sources of cutting-edge microelectronics fabrication inside the United States.[353] While the United States has historically led China by at least two generations in semiconductor design and fabrication, this has not been an explicit policy goal. And while China has not been able to surpass the United States, other nations such as Taiwan and South Korea now clearly lead the U.S. in state-of-the-art semiconductor manufacturing. This leaves the U.S. reliant on foreign sources for critical inputs to defense systems and U.S. industry more broadly. An objective to rebuild microelectronics leadership should be stated plainly to concentrate the necessary national support across government, industry, and academia, and also to track progress over time against a clear yardstick. To achieve this objective, the Commission recommends focusing action along three fronts:

- Implementing a national microelectronics strategy.
- Revitalizing domestic microelectronics fabrication by incentivizing multiple cutting-edge domestic fabrication facilities; and
- Ramping up microelectronics research.

In addition to these efforts to promote U.S. microelectronics leadership, discussed below, the United States and its allies should utilize targeted export controls on high-end semiconductor manufacturing equipment, described in Chapter 14, to protect existing technical advantages and slow the advancement of China's semiconductor industry.

✦ **Implement the National Microelectronics Strategy.** The United States lacks a national microelectronics strategy to coordinate semiconductor policy, funding, and incentives within the Executive Branch and externally with industry and academia. A truly national strategy would build on this Commission's work, as well as previous studies conducted by the United States government or on its behalf. It would also integrate the disparate approaches of the Departments of State, Defense, Energy, Commerce, Treasury, and other relevant agencies to promote domestic R&D while preventing the illicit transfer of technology to competitors. Finally, it would be updated on a consistent basis to foster a coordinated approach and adapt to shifting challenges to microelectronics innovation, competitiveness, and supply chain integrity.

In line with the Commission's recommendations, the Fiscal Year 2021 National Defense Authorization Act (NDAA) creates a subcommittee of the National Science and Technology Council (NSTC), consisting of senior government officials, to develop a National Strategy on Microelectronics Research and oversee its implementation.[354] However, for this key effort to be

[353] The Commission's previous reports offered a range of initial recommendations to expand access to trusted semiconductors, increase microelectronics R&D funding, control the export of high-end semiconductor manufacturing equipment to adversaries, and reshore leading-edge fabrication facilities.

[354] Pub. L. 116-283, sec. 9906, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

successful, it should be prioritized by the White House by requiring the NSTC subcommittee to submit the Strategy to the President within 270 days.

✦ **Revitalize domestic microelectronics fabrication.** The Commission previously concluded that the United States is overly dependent upon globally diversified supply chains for microelectronics, including imports from potential adversaries. Furthermore, as a result of gaps in the U.S. industrial base, the risks are increasing that the United States could lose access to trusted, assured, and state-of-the-art semiconductors for national security use cases. Despite these concerns, the Commission has been encouraged by a number of developments over the past year to revitalize the domestic fabrication of state-of-the-art microelectronics. Examples include TSMC's decision to develop an advanced facility in the United States and Intel's publicly stated interest in working with the United States government to develop a commercial U.S. foundry.[355] However, these are only initial steps and more must be done by the U.S. government to reach an end-state where multiple firms are fabricating state-of-the-art chips domestically. Without several U.S.-based fabrication facilities, both U.S. industry and U.S. national security face risks from competitive pressures and supply chain shortages. The most significant development has been the inclusion of several semiconductor provisions from the "CHIPS for America Act" in the Fiscal Year 2021 NDAA.[356] However, these programs require sufficient appropriations to succeed and they did not receive appropriated funding in Fiscal Year 2021, which leaves congressional priorities unclear. Further congressional action to establish refundable investment tax credits and set the conditions for the domestic production of advanced microelectronics will be important to enable the United States to remain two generations ahead of China. Specifically, the U.S. government should:

- *Incentivize Domestic Leading-Edge Merchant Fabrication Through Refundable Investment Tax Credits.* Although introduced as part of the CHIPS for America Act, Congress has not yet passed legislation establishing a 40 percent refundable investment tax credit for semiconductor facilities and equipment.[357] Existing U.S. incentives reduce the cost of foundry construction attributable to capital expenses, operating expenses, and taxes by just 10 to 15 percent. A credit of this magnitude is needed to make the United States a competitive market for semiconductor manufacturing, as other leading semiconductor manufacturing nations such as South Korea, Taiwan, and Singapore offer 25 to 30 percent cost reduction, roughly double what the United States currently offers.[358] This gap in incentives is one driving factor behind the lack of an advanced logic merchant foundry in the United States. Closing the incentive gap and broadening it to include companies from allied countries will

[355] Stephen Nellis, *Phoenix Okays Development Deal with TSMC for $12 Billion Chip Factory* Reuters (Nov. 18, 2020), https://www.reuters.com/article/us-tsmc-arizona/phoenix-okays-development-deal-with-tsmc-for-12-billion-chip-factory-idUSKBN27Y30E; Asa Fitch, et al., *Trump and Chip Makers Including Intel Seek Semiconductor Self-Sufficiency*, Wall Street Journal (May 11, 2020), https://www.wsj.com/articles/trump-and-chip-makers-including-intel-seek-semiconductor-self-sufficiency-11589103002.

[356] Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021). These provisions authorize several programs the Commission has previously identified as essential to U.S. microelectronics leadership. In particular, the provisions would require drafting a national microelectronics leadership strategy; establish a national semiconductor technology center; and create an incubator for semiconductor startup firms, and an Advanced Packaging National Manufacturing Institute, all of which align with previous recommendations from the Commission.

[357] This incentive would reduce a semiconductor firm's tax bill by 40 percent on semiconductor manufacturing equipment and facilities through 2024, followed by reduced tax credit rates of 30 percent and 20 percent, respectively, through 2025 and 2026

[358] Antonio Varas, et al., *Government Incentives and US Competitiveness in Semiconductor Manufacturing*, BCG and SIA (Sept. 2020), https://web-assets.bcg.com/27/cf/9fa28eeb43649ef8674fe764726d/bcg-government-incentives-and-us-competitiveness-in-semiconductor-manufacturing-sep-2020.pdf.

incentivize U.S. firms to construct facilities domestically while also attracting foreign firms such as TSMC and Samsung. Additionally, increasing demand in the United States for high-end semiconductor manufacturing equipment (SME) will create new business opportunities for SME manufacturers from allied countries, particularly Japan and the Netherlands, which could increase their governments' willingness to align their export control policies with strict U.S. policies prohibiting the export of such equipment to China.[359]

✦ **Double-down on federally funded microelectronics research.** Each succeeding generation of chips using traditional architectures of silicon-based transistors faces diminishing marginal gains to performance as they reach the limits imposed by the laws of physics. As a result, the relative advantage the United States has enjoyed by staying roughly two generations ahead of potential adversaries in the design phase of developing cutting-edge hardware could decrease over time as the gap between hardware generations narrows. Therefore, the United States must look to heterogeneous integration and other novel hardware improvements in the medium-term to continue out-innovating competitors. Over the longer term, the United States must also continue its portfolio approach to future microelectronics pathways by investing in new materials and entirely new hardware approaches, such as quantum and neuromorphic computing.

The four primary research arms of the United States government focused on both medium- and long-term microelectronics breakthroughs are the Department of Energy, Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (NSF), and the Department of Commerce primarily through engagement with industry. Their suite of existing programs, such as DARPA's Electronics Resurgence Initiative, are targeting the right research areas but must expand by an order of magnitude to achieve the necessary breakthroughs and maintain U.S. competitiveness. Additional funding should support not only research projects but also the capital-intensive underlying infrastructure for microelectronics development, including the National Semiconductor Technology Center and advanced packaging prototyping activities authorized in the Fiscal Year 2021 NDAA. In particular, advances in packaging will be critical to future improvements in semiconductor capabilities as firms reach physical limits for two-dimensional transistor density.[360] The government should:

- *Double down on Federal Research Funding to Lead the Next Generation of Microelectronics.* The Commission recommends substantially increasing the United States government's full range of research efforts focused on microelectronics. Congress should appropriate an additional $1.1 billion for semiconductor research and $1 billion for the Advanced Packaging National Manufacturing Program in Fiscal Year 2022. Building on these investments, these funding levels should continue for five years for a total investment of roughly $12 billion. These amounts are consistent with the funding levels introduced, but not yet appropriated, in the CHIPS for America Act[361] and the American Foundries Act of 2020.[362] In line with the existing focus areas of these programs and the Commission's prior recommendations, the funding should be applied to developing infrastructure and pursuing breakthroughs in promising areas such as 3D chip stacking, photonics, carbon nanotubes,

[359] See Chapter 14 for additional details on export controls on SME.

[360] *Heterogeneous Integration Roadmap: Chapter 1: HIR Overview and Executive Summary*, IEEE Electronics Packaging Society (Oct. 2019), https://eps.ieee.org/images/files/HIR_2019/HIR1_ch01_overview.pdf.

[361] S. 3933 and H.R. 7178, 116th Cong. (2020).

[362] S. 4130, American Foundries Act of 2020 (2020).

gallium nitride transistors, domain specific hardware architectures, electronic design automation, and cryogenic computing.

Chapter 14: Technology Protection

America's ability to out-innovate competitors is the dominant component of any U.S. strategy for technology leadership. Promoting research, entrepreneurship, and talent development remain the key ingredients of success. However, as the margin of U.S. technological advantage narrows and foreign efforts to acquire American know-how and technology increase, the United States must also reexamine how it can protect ideas, hardware, companies, and its values.

The United States confronts sustained threats from state-directed technology transfer and theft targeting artificial intelligence (AI) and other cutting-edge, dual-use technologies and basic research. China poses the most significant challenge. The Chinese Communist Party (CCP) has embarked on a multi-pronged campaign of licit and illicit technology transfer to become a "science and technology superpower" by 2050.[363] The campaign deliberately targets U.S. critical sectors, companies, and research institutions.[364] China's theft of U.S. technology—be it through circumventing export controls, commercial deals with U.S. companies to access intellectual property, or espionage—costs the United States $300-$600 billion per year.[365] And that only captures immediate losses, not the ongoing damage to the U.S. economy over time. China simultaneously exploits open research environments through cyber-enabled intrusion, talent recruitment programs, and manipulated research partnerships.[366] In effect, China is using American taxpayers' dollars to fund its military and economic modernization.

Russia also poses a significant illicit technology transfer threat, particularly as it relates to technologies with defense applications. Although the Russian government's efforts to steal U.S. technology and intellectual property do not operate at the same scale of comparable CCP efforts, Russia nonetheless is an aggressive and capable collector of technologies. It is likely to pose continued technology transfer threats over the coming decade, utilizing existing commercial and academic entities, as well as traditional and cyber espionage.[367]

Modernizing Export Controls and Investment Screening. How the United States designs policies to limit the movement of commercial goods or capital in the interests of national security will be one of the defining challenges of the next decade, as dual-use commercial technologies become

[363] CSET Translation of *Outline of the National Innovation-Driven Development Strategy,* Central Committee of the Communist Party of China and the PRC State Council (May 19, 2016) (translation by CSET on Dec. 11, 2019), https://cset.georgetown.edu/research/outline-of-the-national-innovation-driven-development-strategy/.

[364] *Deputy Assistant Attorney General Adam S. Hickey of the National Security Division Delivers Remarks at the Fifth National Conference on CFIUS and Team Telecom*, U.S. Department of Justice (Apr. 24, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-adam-s-hickey-national-security-division-delivers-0.

[365] *China Theft of Technology is Biggest Law Enforcement Threat to U.S., FBI Says*, The Guardian (Feb. 6, 2020), https://www.theguardian.com/world/2020/feb/06/china-technology-theft-fbi-biggest-threat (quoting William Evanina, director of the National Counterintelligence and Security Center).

[366] A recent JASON study on the issue found that "[a]ctions of the Chinese government and its institutions that are not in accord with U.S. values of science ethics have raised concerns about foreign influence in the U.S. academic sector . . . there are problems with respect to research transparency, lack of reciprocity in collaborations and consortia, and reporting of commitments and potential conflicts of interest, related to these actions." JASON, *Fundamental Research Security,* MITRE Corporation at 39 (Dec. 2019), https://www.nsf.gov/news/special_reports/jasonse13curity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[367] In 2018 the U.S. National Counterintelligence and Surveillance Center stated: "The threat to U.S. technology from Russia will continue over the coming years as Moscow attempts to bolster an economy struggling with endemic corruption, state control, and a loss of talent departing for jobs abroad." *Foreign Economic Espionage in Cyberspace*, National Counterintelligence & Security Center at 8 (2018), https://s3-us-west-2.amazonaws.com/cyberscoop-media/wp-content/uploads/2018/07/26114025/2018ForeignEconomic-Espionage-Pub_FINAL.pdf.

increasingly important to national security. Export controls can and should be utilized not only to prevent the transfer of particularly sensitive equipment to strategic competitors, but also to slow competitors' efforts to develop indigenous industries in sensitive technologies with defense applications. If executed properly, export controls which slow competitors can sustain existing U.S. defense advantages over long periods of time. For instance, U.S. export controls on jet engine technology have stymied Chinese government-led efforts to produce a modern jet engine domestically for use in military aircraft for nearly 30 years.[368]

However, as currently designed and utilized, U.S. export controls and investment screening procedures are imperfect instruments for the AI competition. As a policy matter, investment screening and export controls were designed for a different era, when the distinction between civil and military technologies was clearer and there was little overlap between the economies of the United States and its competitors. Both conditions have changed. AI is dual-use and the emerging technology economies of the United States and China are deeply interconnected, which makes it extremely difficult to design controls which are feasible, maximize strategic impact, and minimize economic costs. While these tradeoffs are not new, they are becoming more extreme, as the dual-use nature of AI means many of its individual components most critical to national security are also commonplace in the commercial sector.

Meanwhile, U.S. regulatory capacity has not kept pace with technical developments, as the Departments of Commerce, Treasury, and State all lack sufficient technical and analytical capacity to effectively design and efficiently enforce technology protection policies on dual-use emerging technologies. Congress has taken some important steps in recent years to adapt technology protection regimes to challenges posed by emerging technologies, most notably the Export Control Reform Act of 2018 (ECRA), and the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[369] However, more than two years after their passage, implementation of key aspects of both laws remains unfinished, hindering enforcement and confounding the affected industries.[370]

These conditions present policy makers with a difficult choice between under-protection, which will give competitors unacceptable levels of access to sensitive technologies, and over-protection, which has the potential to stifle innovation and harm overall U.S. competitiveness. Effective controls must target choke points which impose significant trickle-down strategic costs on competitors, but minimal economic costs on U.S. industry. But such choke points are increasingly elusive.

✦ **Clarify U.S. technology protection principles and build regulatory capacity to implement ECRA and FIRRMA.** The United States must take a smarter and more predictable approach to applying export controls to AI. The government should state that future technology protection policies will be guided by four basic principles:

[368] Robert Farley & J. Tyler Lovell, *China's Air Force is Being Held Back by Its Terrible Jet Engines,* The National Interest (Apr. 3, 2020) https://nationalinterest.org/blog/buzz/chinas-air-force-being-held-back-its-terrible-jet-engines-140252.

[369] Pub. L. 115-232, Title XVII, Subtitle B, 132 Stat. 1636, 2208, as amended by Pub. L. 116-6, Division H, Title II, Section 205 Consolidated Appropriations Act, 2019, 133 Stat. 13, 476; Pub. L. 115-232, Title XVII, Subtitle A, 132 Stat. 1636, 2174.

[370] Of particular note, ECRA requires the Department of Commerce to identify "emerging and foundational technologies that are essential to the national security of the United States" that are not otherwise controlled, but to date Commerce has not identified a single technology under this provision. This has left gaps in the U.S. approach to protecting its advantages in high-tech sectors, including AI, and created uncertainty for industry. See Pub. L. 115-232, Title XVII, Subtitle B, 132 Stat. 1636, 2208, as amended by Pub. L. 116-6, Division H, Title II, Section 205 Consolidated Appropriations Act, 2019, 133 Stat. 13, 476.

- U.S. technology controls will not supplant investment and innovation.

- U.S. strategies to promote and protect U.S. technology leadership will be integrated.

- The United States will be judicious in applying export controls to AI-related technologies, targeting discrete chokepoints and coordinating policies with allies.

- The United States will broaden investment screening on AI-related technologies.

On a technical level, AI poses particular challenges to control regimes given it is dual-use, widespread, and largely open-source. Moreover, it builds on a host of other technologies. Given the ubiquitous nature of AI, export controls on AI algorithms carry substantial risk—as improperly defined controls could inadvertently restrict the export of significant numbers of commercial products and cause substantial harm to the U.S. technology industry. While some AI algorithms are clearly candidates for export controls, such as those meant for use in battlefield applications, such software is largely already controlled under the Commerce Control List.[371] Data is also a potential target for controls—especially sensitive bulk data—but effective data controls face similar challenges to AI algorithms.[372] Looking across the AI stack, the hardware component of the AI stack contains the most viable targets for traditional export controls.

The United States must also take steps to improve its capacity to implement effective technology protection policies. In the near-term, the Departments of Commerce, Treasury, and State must increase their internal technical capacity to facilitate more rapid design of effective policies. The Department of Commerce must also finalize its initial list of "emerging" and "foundational" technologies which must be controlled, as mandated by ECRA over two years ago, and work to comprehensively adapt U.S. export control lists to address modern technology-focused security challenges.[373] Doing so is a critical step to implementing both ECRA and FIRRMA. Finally, departments and agencies should consider efforts to expedite and automate export licensing and Committee on Foreign Investment in the United States (CFIUS) filing proceedings, which could improve the effectiveness and reduce the economic costs of these regimes.

✦ Require companies to disclose investments in AI and other sensitive technologies to CFIUS. The United States must amend CFIUS' authorities and procedures to enable it to better address modern challenges associated with sensitive, dual-use technologies. Specifically, it must enhance its ability to monitor investments from competitors in critical U.S. technology industries to prevent theft of intellectual property and ensure the United States retains control of sensitive technologies. U.S. competitors are investing heavily in U.S. AI firms. From 2010 to 2017, China-based investors poured over $1.3 billion into U.S. AI startups and AI remains among the top technology areas for VC investment in the United States by China-based firms.[374] However, the U.S. government has limited

[371] Carrick Flynn, *Recommendations on Export Controls for Artificial Intelligence*, Center for Security and Emerging Technology (Feb. 6 2020), https://cset.georgetown.edu/research/recommendations-on-export-controls-for-artificial-intelligence/.

[372] There is also room to work with allies and partners to create standards for securely transferring key datasets and limiting their distribution to certain trusted nations; see Chapter 15 for additional details on this topic.

[373] See Chris Darby, Gilman Louie, & Jason Matheny, *Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence*, NSCAI at 16 (May 19. 2020), https://www.nscai.gov/reports.

[374] Chinese venture capital investment in the U.S. increased substantially after 2014 but has stalled since 2018. Nevertheless, AI remains one of the top sectors for Chinese VC investment in the U.S. Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy*, Defense Innovation Unit Experimental (Jan. 2018),

insight into these transactions. CFIUS is responsible for screening foreign investments for national security risks, but only requires firms to disclose investments when the U.S. firm produces an export controlled good—which very few AI firms do.[375] Therefore, many firms based in U.S. competitors that invest in U.S. AI companies have no obligation to report their investment to CFIUS. While CFIUS has broad authority to unwind such transactions, it currently has no visibility before they are consummated—creating a significant technology transfer risk.

CFIUS should increase disclosure requirements for investments in sensitive technologies for firms from China and Russia. Congress should mandate that all investments originating from "countries of special concern," to include China and Russia, in national security-relevant applications of AI and other "sensitive technologies" as defined by CFIUS, must be disclosed to allow CFIUS the opportunity to review prior to the completion of the transaction. This list of sensitive technologies should be distinct and broader than the list of "emerging" and "foundational" technologies required under ECRA, and include industries key to U.S. national security that face persistent threats from adversarial capital, specifically national-security relevant applications of AI, semiconductors, telecommunications equipment, quantum computing, and biotechnology, as well as other sectors identified in Made in China 2025. De-linking investment screening from export controls acknowledges that these two tools can and should be applied in different ways, permitting more expansive investment screening while maintaining targeted export controls focused on choke points. Limiting the scope of the mandatory filing requirements for this broader set of technologies to only firms from select U.S. competitors would prevent over-regulation and preserve the free flow of capital, increase insight into China's and Russia's investments in critical technologies, deter state-sponsored intellectual property (IP) theft, and preserve U.S. leadership in AI for national security purposes.[376]

✦ **Utilize targeted export controls on key semiconductor manufacturing equipment.** Where possible, the United States should use export controls to prevent competitors from obtaining AI capabilities that would grant them strategic or military advantages. The primary U.S. export control target to constrain competitors' AI capabilities should be sophisticated semiconductor manufacturing equipment (SME) necessary to manufacture high-end chips. SME is a critical choke point and an attractive target for export controls for the following reasons:

- Advanced AI is increasingly dependent on high-end computing capabilities;[377]
- China relies on international firms for its supply of high-end semiconductors; and
- SME manufacturing is specialized and dominated by the United States and its allies.

https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf; Adam Lysenko, et al., *Disruption: US-China Venture Capital in a New Era of Strategic Competition*, (Jan. 2020), https://publications-research.s3-us-west-2.amazonaws.com/RHG_Disruption_US+China+VC_January2020.pdf; Mercedes Ruehl, et al., *Chinese State-Backed Funds Invest in U.S. Tech Despite Washington Curbs*, Financial Times (Dec. 2, 2020), https://www.ft.com/content/745abeca-561d-484d-acd9-ad1caedf9e9e.

[375] As a result, CFIUS disclosure requirements disproportionately impact investments from U.S. allies; of the 94 mandatory CFIUS filings in 2019, 14 were from Japan, 12 from Canada, 11 from the UK, and only 3 were from China. *Annual Report to Congress*, CFIUS at 33-36 (2019), https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf.

[376] This would require an amendment to CFIUS' authorizing legislation.

[377] OpenAI estimates that since 2012, the amount of compute used in the largest AI training runs is doubling every 3.4 months. See Dario Amodei & Danny Hernandez, *AI and Compute*, OpenAI (May 16, 2018), https://openai.com/blog/ai-and-compute/.

China is the only U.S. competitor attempting to cultivate a domestic, cutting-edge microelectronics fabrication industry capable of producing advanced chips at scale. Slowing the growth of China's high-end semiconductor manufacturing ability would set back China's attempts to build a cutting-edge microelectronics industry capable of fabricating chips most useful for advanced applications of AI for defense. Coupled with the efforts to promote U.S. semiconductor leadership in Chapter 13, this will further the Commission's proposed U.S. policy goal of remaining two generations ahead of China in cutting-edge microelectronics design and fabrication. However, controls on general-purpose semiconductors are unlikely to be effective given the larger number of countries capable of producing such chips. If implemented unilaterally, such controls could harm the U.S. semiconductor industry.

✦ **Align the export control policies of the United States, the Netherlands, and Japan regarding SME.** The sophisticated photolithography tools needed to produce chips at the 16nm node and below, particularly extreme ultraviolet (EUV) and argon fluoride (ArF) immersion lithography tools, are the most complex and expensive type of SME. These tools are even more specialized than SME writ large, and the United States, the Netherlands, and Japan control the entire market.[378] The Departments of State and Commerce should work with the governments of the Netherlands and Japan to align the export licensing processes of all three countries regarding high-end semiconductor manufacturing equipment, particularly EUV and ArF immersion lithography equipment, toward a policy of presumptive denial of licenses for exports of such equipment to China. This would slow China's efforts to domestically produce 7nm or 5nm chips at scale, and constrain China's semiconductor production capability of chips at any node at or below 16nm—which the Commission assesses to be most useful for advanced AI applications—by limiting the capability of Chinese firms to repair or replace existing equipment.[379]

✦ **Utilize targeted end-use export controls and reporting requirements to prevent use of high-end U.S. AI chips in human rights violations.** The United States must take steps to prevent and deter U.S. firms from wittingly or unwittingly enabling uses of AI which violate human rights. List-based controls are ill suited for this task given the commercial nature of most AI equipment, as the vast majority of its uses are legitimate. However, end-use and end-user export controls could be more effective. Although end-use controls are unlikely to prevent the transfer of strategic technologies to U.S. competitors determined to obtain them, they could prevent or deter U.S. firms from allowing certain key pieces of equipment, particularly high-end chips, to be utilized in malicious AI applications. Reporting revealing that U.S.-made chips are powering a supercomputer in Xinjiang used for mass surveillance of Uyghur populations and that firms in China have filed patents for facial recognition specifically targeting Uyghurs illustrates the need to more closely monitor how high-end U.S. enabling hardware is utilized.[380]

[378] The Dutch firm ASML has a monopoly on EUV lithography tools, which are the most advanced type, and ArF immersion lithography tools are only produced by ASML and the Japanese firm Nikon.
[379] The Wassenaar Arrangement lists lithography equipment capable of making chips with features of 45nm or below as a controlled item. However, because the Wassenaar Arrangement is not binding, states parties are not obligated to comply with this as a legal restriction. See *List of Dual-Use Goods and Technologies and Munitions List,* Wassenaar Arrangement Secretariat at 72 (Dec. 2018), https://www.wassenaar.org/app/uploads/2019/consolidated/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18-1.pdf.
[380] Paul Mozur & Don Clark, *China's Surveillance State Sucks Up Data. U.S. Tech is Key to Sorting It.*, New York Times (Nov. 24, 2020), https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html. Leo Kelion, *Huawei Patent Mentions Use of*

The Department of Commerce should prohibit the export of specific, high-performing AI chips for use in mass surveillance applications, compel U.S. firms which export such chips to certify that the buyer will not utilize them to facilitate human rights abuses, and require that firms submit quarterly reports to Commerce listing all such chip sales to China. This would not constitute a licensing requirement that would introduce uncertainty and cause delays, but rather a self-certification and semi-regular report from industry. Such an action would demonstrate the U.S. commitment to ethical and responsible uses of AI, promote ethical behavior among U.S. firms, and make it harder for bad actors to utilize advanced U.S. chips for nefarious purposes.[381]

Strengthening Research Protection. The U.S. research enterprise should be protected as a national asset. China's campaign to exploit U.S.-based research violates the research community's core principles of integrity, openness, accountability, and fairness.[382] U.S. response measures to counter the actions of China's government are nascent.[383] There is a need for more technically-versed intelligence collection and analysis on threats to the science and technology sector, and a need to disseminate that information more broadly. Government agencies, law enforcement, and research institutions need ready access to tools and resources to conduct nuanced risk assessment and build transparency around specific threats and tactics. The government and research institutions share responsibility for protecting core values and countering malicious activities. Responses should be coordinated with like-minded allies and partners to reinforce norms around openness of fundamental research, research integrity, and protection of intellectual property.

Strengthening the integrity of the research process will support the foundations of open research. However, if not approached thoughtfully, U.S. policy actions to counter technology transfer could harm U.S. competitiveness and global scientific progress. Countering the CCP's actions does not require severing most ties between research communities in China and the United States. The United States benefits from collaboration by staying connected with cutting edge work in China and welcoming their PhD-level top talent[384] that comes to study at U.S. universities and remains in the United States at rates of 85 to 90 percent after graduating.[385]

Uighur-spotting Tech, BBC (Jan. 13, 2021), https://www.bbc.com/news/technology-55634388. Reporting indicates firms in China may be in the process of altering these patents to remove references to specific ethnic groups.

[381] This action would build on recent State Department guidance regarding best practices for transactions linked to foreign government end-users for products or services with surveillance capabilities. See *U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, U.S. Department of State (Sept. 30, 2020), https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/.

[382] JASON, *Fundamental Research Security,* MITRE Corporation (Dec. 2019), https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[383] Promising efforts have been initiated through the National Counterintelligence Task Force and the Office of Science and Technology Policy's Joint Committee on Research Environments. See *NSTC*, The White House (last accessed Jan. 1, 2021), https://www.whitehouse.gov/ostp/nstc/. As well as among universities to build communities of interest to share best practices and conduct internal audits around disclosure policies and cybersecurity. For example, the Academic Security and Counter Exploitation Program launched by the Texas A&M University System, See *Academic Security and Counter Exploitation Program*, Texas A&M University (last accessed Jan. 11, 2021), https://asce.tamus.edu/.

[384] The Commission supports measures to strengthen the ability of the United States to attract and retain top AI talent coming from China and elsewhere. See Chapter 10 of this report.

[385] Remco Zwetsloot, *U.S.-China STEM Talent "Decoupling,"* Johns Hopkins Applied Physics Laboratory at 13 (2020), https://www.jhuapl.edu/assessing-us-china-technology-connections/dist/407b0211ec49299608551326041488d4.pdf.

✦ **Build capacity to protect the integrity of the U.S. research environment.** Congress should start by passing the Academic Research Protection Act (ARPA) and establishing a government-sponsored center of excellence on research security.[386] The ARPA legislation would create a dedicated National Commission on Research Protection, improve dissemination of open source intelligence relating to foreign threats, and facilitate the sharing of studies and practices between government and research organizations.

✦ **Coordinate research protection efforts internationally with allies and partners.** China's efforts to acquire foreign technology extend far beyond the United States.[387] The Office of Science and Technology Policy, the Department of State, and the Department of Justice should coordinate with allies and partners to further information sharing on detrimental academic collaboration with PLA-affiliated entities and to develop multilateral responses to mitigate the harm from these actions. Such diplomacy should seek to reinforce global norms around commitment to open fundamental research, as formalized in the United States in National Security Decision Directive 189.[388] The United States should strive to build a coalition committed to this principle and to research integrity, sidelining those who do not abide by the values that underpin innovation and global science cooperation.

✦ **Bolster cybersecurity support for research institutions.** Protection of research data and IP from cyber-enabled theft is perhaps the most important measure and most easily achieved layer of security. This is particularly salient for AI, when theft of training data or trained models essentially provides access to a final product. Federal grant-making agencies should ease the ability of research institutions to maintain a baseline level of cybersecurity by issuing clear guidance, establishing incentives, and sharing state of the art best practices and resources.

Agencies such as DHS and FBI should increase support to information sharing constructs and provide timely and actionable alerts on cyber threats and intrusions.[389] In addition, the government should broker commercial cloud credits for universities to support secure data storage for research groups and laboratories conducting research known to be of high interest to foreign adversaries.

✦ **Counter foreign talent recruitment programs.** China's national plan for AI development directs use of foreign talent recruitment programs as a means to create a "high ground" for China's AI experts.[390] These problematic programs have received increasing attention in recent years. Rather

[386] H.R. 8346, Academic Research Protection Act, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/8346. The legislation, if passed, would establish a National Commission on Research Protection; establish an open source intelligence clearinghouse relating to foreign threats to academic research overseen by the Director of National Intelligence; improve guidance from the Departments of State and Commerce to ensure academic institutions are meeting export control responsibilities; and develop a Federal Bureau of Investigation (FBI) outreach strategy on threats to the academic community.

[387] Notably, two thirds of overseas professional associations that transfer technology to China are located outside the United States, mainly distributed among U.S. allies and partners. Ryan Fedasiuk & Emily Weinstein, *Overseas Professionals and Technology Transfer to China*, Center for Security and Emerging Technology at 11 (July 2020), https://cset.georgetown.edu/research/overseas-professionals-and-technology-transfer-to-china/.

[388] The directive defines fundamental research as: "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." *National Policy on the Transfer of Scientific, Technical, and Engineering Information*, Executive Office of the President (Sept. 21, 1985), https://fas.org/irp/offdocs/nsdd/nsdd-189.htm.

[389] Such as the Research and Education Networks Information and Sharing Analysis Center (REN-ISAC). REN-ISAC (last accessed Jan. 2, 2021), https://www.ren-isac.net/.

[390] William C. Hannas & Huey-meei Chang, *China's Access to Foreign AI Technology*, Center for Security and Emerging Technology at 9-10 (Sept. 2019), https://cset.georgetown.edu/wp-content/uploads/CSET_China_Access_To_Foreign_AI_Technology.pdf.

than legitimate competition for scientific talent through attractive job offers, many are constructed in a manner that contradicts U.S. norms of research integrity, violates rules around disclosure, and creates vectors for technology transfer.[391]

The programs often employ a model of "part-time" recruitment, in which participants retain positions in the United States, while accepting an affiliation with an institution in China.[392] This often involves signing contracts that create conflicts through requirements to attribute patents to an institution in China, even if the research was conducted with U.S. funding. Participants often train other talent recruitment program members, and replicate U.S.-funded work at an institution in China.

We commend recent action by Congress to limit the detrimental impact of these programs by mandating standardized disclosure requirements for federally-funded research that will require comprehensive disclosure of conflicts of interest, conflicts of commitment, and all outside and foreign support.[393] This should be strengthened by a standardization and unification of grant application and documentation processes in machine readable formats. Together, these measures would enable effective oversight, automated fraud detection, and data sharing across the federal research funding agencies. Standardization should be complemented with mandated and resourced compliance operations at each research funding agency—creating a layer of accountability to enforce disclosure policies and deter bad actors.

✦ **Strengthen visa vetting to limit problematic research collaborations.** Some U.S. universities and researchers are unknowingly entering into collaborative research arrangements with researchers from universities in China with close ties to the PLA and conducting research that directly contributes to China's military and security capabilities.[394] China's military-civilian fusion strategy and pursuit of technological leadership has been supported by a push from PLA-affiliated research institutions to send personnel abroad. Visiting scholars or students have been found to downplay ties to the military or deliberately obscure affiliation by using alternate names for their home institutions.[395]

The United States should guard against the entrance of researchers with problematic affiliations through implementation of a special review process for visa applications from advanced degree

[391] The Office of Science and Technology Policy defines foreign government talent recruitment programs as "an effort directly or indirectly organized, managed, or funded by a foreign government to recruit science and technology professionals or students (regardless of citizenship or national origin)." *Enhancing the Security and Integrity of America's Research Enterprise*, White House Office of Science and Technology Policy at 18 (July 2020), https://www.whitehouse.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf.

[392] David Zweig & Siqin Kang, *America Challenges China's National Talent Programs,* Center for Strategic and International Studies at 5 (May 2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20505_zweig_AmericaChallenges_v6_FINAL.pdf?bTLm4WdtG93lAVmxLdlWsgkgeNQDQUAv.

[393] Pub. L. 116-283, sec. 223, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

[394] Glen Tiffert, *Global Engagement: Rethinking Risk in the Research Enterprise*, The Hoover Institution (July 2020), https://www.hoover.org/sites/default/files/research/docs/tiffert_globalengagement_full_0818.pdf. A subsequent study of a larger database of research papers conducted by *Nature* identified more than 12,000 papers from the years 2015-2019 that were co-authored by researchers in the U.S. with those at the Seven Sons Universities. Furthermore, *Nature* found that "among those, 499 authors had a dual affiliation with a U.S. institution and a Seven Sons university and were listed on papers declaring grant funding from the NIH or the U.S. National Science Foundation." Nidhi Subbaraman, *US Investigations of Chinese Scientists Expand Focus to Military Ties*, Nature (Sept. 9, 2020), https://www.nature.com/articles/d41586-020-02515-x.

[395] Alex Joske, *Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities*, Australian Strategic Policy Institute (Oct. 2018), https://www.aspi.org.au/report/picking-flowers-making-honey.

students and researchers with ties to research institutions affiliated with foreign military and intelligence organizations of designated countries of concern.[396] This should be accompanied with adequate resources to enable heightened review and paired with penalties that ban entry to visa applicants found to have intentionally not disclosed or improperly disclosed their military and intelligence affiliations.

[396] The Commission recommends this as an update to Presidential Proclamation 10043 that suspends F or J visas to study or conduct research for Chinese nationals affiliated with the Chinese government military-civil fusion strategy. Donald J. Trump, *Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China*, The White House (May 29, 2020), https://www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/.

Chapter 15: A Favorable International Technology Order

The United States cannot compete with and counter the global technology ambitions of authoritarian rivals if it acts alone. Like-minded countries must work together to advance an international rules-based order, protect free and open societies, and unleash economic innovation. The authoritarian challenge to the global technology order encompasses five distinct but related elements:

- A rising challenge to U.S. and Western technology firms for global market share, impacting the prosperity and global economic position of the United States and its allies and partners;

- China's increasing influence and strategic leverage over countries that utilize technologies and infrastructure built and developed in China;

- The prospect of authoritarian consolidation in states that gain easy access to digital tools that can strengthen repressive rule;

- The prospect of democratic backsliding in states with governments that may be tempted to utilize digital tools in ways that undermine liberal values; and

- A threat to the cohesion of democratic allies as an influential bloc of states with the capacity to shape global technology norms and standards.[397]

The United States must pursue a comprehensive strategy in close coordination with our allies and partners for artificial intelligence (AI) innovation and adoption that promotes values critical to free and open societies. Furthermore, the United States must collaborate with its closest allies and partners to develop principles for employing AI tools ethically and responsibly, defend the integrity of international technical standards, promote digital markets, leverage comparative expertise to develop privacy-preserving technologies, and share practices and resources to defend against authoritarian attacks on digital infrastructure and democratic values.

To achieve these goals, the Commission proposes that the White House request, the Department of State to lead an effort with and other key agencies to:

✦ **Develop and implement an International Science and Technology Strategy (ISTS)** to help coordinate AI and emerging technology policies government-wide and with our closest allies and partners, apply the tools of foreign assistance, technical expertise and guidance, and development finance, and foster collaborative research and development (R&D). The ISTS should serve as the international component of the National Technology Strategy (see Chapter 9). The ISTS should be centered around four big initiatives:

- *Build an Emerging Technology Coalition* of allies and partners that use emerging

[397] The threat to allied cohesion also extends to the military realm, insofar as building divergent or incompatible digital systems poses challenges for interoperability or creates risks for U.S. forces operating in allied countries. See Daniel Kliman, *Why the United States Needs a Digital Development Fund*, Center for a New American Security at 2 (Oct. 10, 2019), https://www.cnas.org/publications/commentary/why-the-united-states-needs-a-digital-development-fund ("Over the long term, China's digital investments could render some developing countries off-limits to U.S. forces, constricting the geography of American military access.").

technologies according to democratic norms and values; coordinate policies to counter the malign use of these technologies by authoritarian regimes; and provide concrete, competitive alternatives to counter the adoption of digital infrastructure made in China.

- As part of the Emerging Technology Coalition, *launch an International Digital Democracy Initiative* with allies and partners to align international assistance efforts to develop, promote, and fund the adoption of AI and associated technologies that comports with democratic values and ethical norms around openness, privacy, security, and reliability.

- *Implement a comprehensive U.S. national plan to support international technology efforts* around technical standards, foreign assistance, development finance, and export controls.

- *Enhance the United States' position as an international emerging technology research hub* for collaborative R&D efforts by formalizing a partnership between the U.S. National AI Research Institutes and multilateral initiatives like the Global Partnership on AI (GPAI), creating a Multilateral AI Research Institute (MAIRI) in the United States with key allies and partners, and catalyzing international collaboration and talent exchanges.

✦ **Build an Emerging Technology Coalition.** The United States should lead an Emerging Technology Coalition (ETC) of like-minded nations either as part of a larger democracy summit or as a stand alone endeavor. The immediate step for the ETC should be to organize its efforts to synchronize policies around the following seven critical areas:

- *Developing and operationalizing standards and norms,* in order to uphold democratic values and support secure, reliable, and trusted technologies;

- *Promoting and facilitating coordinated and joint R&D on AI and digital infrastructure* that advances shared interests and benefits humanity;

- *Exploring ways to facilitate data-sharing* among allies and partners, by exploring enabling agreements and addressing legal and regulatory barriers;

- *Promoting and protecting innovation,* particularly through export controls, investment screening, supply chain assurance, emerging technology investment, trade policy, and intellectual property alignment;

- *Developing AI-related talent,* by addressing challenges and increasing talent exchanges, joint training, and workforce development initiatives;

- *Promoting human rights and democracy* through joint efforts to counter censorship, malign information operations, human trafficking, and illiberal uses of surveillance technologies; and

- *Launching the International Digital Democracy Initiative* (see below).

✦ **Launch an International Digital Democracy Initiative (IDDI).** As part of the ETC, the United States, with its allies and partners, should launch an IDDI to align international assistance efforts to develop, promote, and fund the adoption of AI and associated technologies that comport with democratic values and ethical norms around openness, privacy, security, and reliability.

IDDI will be critical for enabling nations around the world to adopt secure, trusted, and open digital ecosystems,[398] empowering communities to use AI and digital technologies in ways that strengthen democracies, promote sustainable development, and advance shared values like privacy, human rights, and the rule of law. IDDI further provides an opportunity for the United States and like-minded allies and partners to counter authoritarian uses of AI, particularly by providing alternatives to digital infrastructure projects that are used for illiberal ends, endanger the social cohesion among and between democracies, and threaten collective security.[399] As international digital and telecommunications infrastructure investment needs continue to grow[400] and China continues to use digital development to export authoritarianism and expand influence, the United States and its allies and partners must join forces to coordinate a strategy that maximizes the impact of government assistance efforts and also catalyzes private sector investment to address shared challenges.

✦ **Implement a comprehensive U.S. national plan to support international technology efforts.** The ISTS should include an integrated government-wide plan for using and bolstering the tools of U.S. foreign policy -- including technical and foreign assistance, development financing, and export controls -- to advance the ETC, the IDDI, and standalone projects. As demonstrated below, the plan should include methods to shape international technical standards; coordinate and expand programs of the Department of State, the United States Agency for International Development, the U.S. Development Finance Corporation, and other federal agencies; and use targeted export controls to preserve key U.S. and allied technical advantages and also further transparency and accountability. It will require significant, dedicated appropriations to achieve meaningful results.

✦ **Enhance the United States' position as an international emerging technology research hub.** The United States must maintain its leadership in international R&D by further establishing itself as a hub of international research into and involving emerging technologies to foster AI collaboration and coordination with key allies and partners. These efforts will facilitate critical support to the ETC and IDDI by developing digital technologies and best practices that comport with democratic values; enhance U.S. contributions to existing and future international efforts like GPAI; and provide avenues for the United States and allies—particularly European allies—to pool resources to address commercial gaps in R&D and overcome challenges to collaboration around cross-border data sharing. Making the United States an international digital research hub has three components:

[398] USAID's Digital Strategy defines the "digital ecosystem" as the "stakeholders, systems, and enabling environments that together empower people and communities to use digital technology to gain access to services, engage with each other, or pursue economic opportunities." This includes "a sound enabling environment and policy commitment; robust and resilient digital infrastructure; capable digital service providers and workforce; and, ultimately, empowered end-users of digitally enabled services." *Digital Strategy 2020-2024,* USAID at 4 (June 2020), https://www.usaid.gov/usaid-digital-strategy.

[399] The Chinese government's global infrastructure projects and its widespread state influence within its private sector has enabled Chinese firms to provide surveillance and smart city technologies to hundreds of cities globally, particularly in developing countries, bolstering autocratic regimes and enabling Chinese geopolitical coercion and government data collection. See, e.g., Hugh Harsono, *China's Surveillance Technology is Keeping Tabs on Populations Around the World*, The Diplomat (June 18, 2020), https://thediplomat.com/2020/06/chinas-surveillance-technology-is-keeping-tabs-on-populations-around-the-world/; Testimony of Steven Feldstein before the U.S.-China Economic and Security Review Commission, *Hearing on China's Strategic Aims in Africa* (May 8, 2020), https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.

[400] To support the G20, the Global Infrastructure Hub has forecasted global telecommunications infrastructure investment needs at $8.9 trillion over the next approximately 20 years, with current trends falling short of these needs by $1 trillion. *Forecasting Infrastructure Investment Needs and Gaps*, Global Infrastructure Hub (last accessed Jan. 13, 2021), https://outlook.gihub.org/.

- *First, the United States should provide formal research support to key international efforts such as GPAI and the Organisation for Economic Cooperation and Development (OECD),*[401] particularly through the National Science Foundation (NSF)'s National AI Research Institutes.[402] The important research undertaken by the National AI Research Institutes—run by the NSF and other U.S. agencies—and by other United States departments and agencies is an incredible resource that should support these international efforts and advance AI and digital goals of the U.S. and like-minded partners.

- *Second, the United States should work with key allies and partners to establish the MAIRI.* MAIRI will facilitate joint efforts to develop technologies that advance responsible, human-centric, and privacy-preserving AI/ML that better societies, and allow allies to pool their talents and resources. It will provide a model for equitable, multilateral research, facilitate AI R&D that builds on like-minded countries' strengths, and foster a global AI workforce for the next generation. MAIRI will be key to a U.S.-led effort to promote values of free and open societies, win the global technology competition, unleash AI innovation and economic prosperity, and develop AI applications that benefit humanity. MAIRI members will champion agreed upon research integrity principles, leverage trusted infrastructure and research resources, and seek to be a part of a federated network of global research institutes. NSF should be the anchor partner, but MAIRI should be structured to enable participation of other federal agencies, like the Departments of State and Energy.[403] The United States should fund the initial startup costs, including acquisition of MAIRI's physical center located in the United States.

- *Third, the United States should leverage existing O and J visa programs to facilitate foreign researchers' involvement in joint projects.* Sustained, strong collaboration between the United States and allies and partners is critical to winning this techno-competition and unleashing innovation and entrepreneurship across like-minded countries. There is no substitute for shoulder-to-shoulder research for building relationships, exchanging ideas and expertise, and sparking future collaboration.

✦ **Reorient U.S. foreign policy and the Department of State for great power competition in the Digital Age.** New outward-facing digital foreign policy initiatives are only part of the equation for ensuring the long-term success of global technology policy. The United States must make inward-focused reforms to the Department of State as well. There is currently no clear lead for emerging technology policy or diplomacy within the State Department, which hinders the Department's ability to make strategic technology policy decisions. It also creates confusion for allies and partners, who

[401] GPAI was launched in 2020 to "foster responsible development of AI grounded in these principles of human rights, inclusion, diversity, innovation and economic growth." Current members include Australia, Brazil, Canada, the European Union, France, Germany, India, Italy, Japan, Mexico, the Netherlands, New Zealand, Poland, Singapore, Slovenia, South Korea, Spain, the United Kingdom, and the United States, with the OECD and UNESCO as Permanent Observers. GPAI bridges "the gap between theory and practice," particularly through research and technical expertise shared via multi-stakeholder working groups. *About GPAI*, GPAI (last accessed Jan. 6, 2020), https://www.gpai.ai/about/; *UNESCO Joins Global Partnership on Artificial Intelligence as Observer*, UNESCO (Dec. 10, 2020), https://en.unesco.org/news/unesco-joins-global-partnership-artificial-intelligence-observer.

[402] *Artificial Intelligence at NSF*, NSF (Aug. 26, 2020), https://www.nsf.gov/cise/ai.jsp.

[403] For example, the Department of Energy may provide critical expertise on undertaking applied research with industry or through its national laboratories, particularly on high performance and quantum computing, while the Department of State can provide foreign policy expertise and support initiatives on data-sharing and AI research clouds with allies and partners.

regularly express uncertainty regarding which senior official should be their primary point of contact for issues related to key topics such as AI, 5G, quantum computing, biotechnology, or new emerging technologies.

Competitive diplomacy in AI and emerging technology arenas is a strategic imperative in an era of great power competition and necessitates an intensified reorientation of the Department of State.[404] The United States must redesign the internal structure, focus, and culture of the State Department to adapt U.S. diplomacy for the digital age, and empower diplomats to advance American interests at the intersection of technology, security, commerce, and human rights. Supporting these efforts and succeeding in U.S. diplomacy will require targeted appropriations from Congress.

The Commission recommends the following immediate actions to reorient U.S. diplomacy:

- *First, the Deputy Secretary of State for Management and Resources's (D/MR)* portfolio should prioritize reorienting and reorganizing the Department for technology diplomacy. Past administrations have used the D/MR position to lead on strategic priorities and ensure execution. The D/MR should provide direction for immediate and long-term planning around technology diplomacy, including policy development, coordination, and resourcing . The D/MR should also have a lead role in oversight and implementation of the ISTS.

- *Second, the State Department should expedite and prioritize efforts to staff, resource, and build out the newly created Bureau of Cyberspace Security and Emerging Technologies (CSET Bureau).* The CSET Bureau, launched in January 2021, led by an official with the title Ambassador-at-Large and Coordinator, will have a critical role as the focal point for U.S. diplomatic efforts around security challenges associated with emerging technologies and will provide an accountable home for AI advocacy within the Department.[405] The Department, with congressional support, must ensure the CSET Bureau is adequately staffed and resourced. To ensure coordination across the Department, the Commission recommends that the CSET Bureau have a direct reporting line to the Deputy Secretary of State or to the D/MR.

- *Third, the State Department should enhance its presence in foreign and U.S. technology hubs* with a cadre of dedicated technology officers at U.S. missions to strengthen diplomatic advocacy, improve technology scouting, and inform policy and foreign assistance.

- *Fourth, AI-related technology modules should be incorporated into Foreign Service Institute training courses* at multiple levels to ensure U.S. diplomats are equipped to lead in an environment being transformed by emerging technology.

[404] China surpassed the United States in the total number of diplomatic missions, with 276, staffed by a diplomatic corps that has become more vociferous in recent years. The United States has 273. See *Global Diplomacy Index*, Lowy Institute (2019), https://globaldiplomacyindex.lowyinstitute.org/; Chun Han Wong & Chao Deng, *China's 'Wolf Warrior' Diplomats are Ready to Fight*, Wall Street Journal (May 19, 2020), https://www.wsj.com/articles/chinas-wolf-warrior-diplomats-are-ready-to-fight-11589896722; see also Martijn Rasser, *Countering China's Technonationalism: A New Approach is Needed if Today's Leaders are to Maintain Their Primacy in Cutting-edge Technology*, The Diplomat (Apr. 24, 2020), https://thediplomat.com/2020/04/countering-chinas-technonationalism/.

[405] *Secretary Pompeo Approves New Cyberspace Security and Emerging Technologies Bureau*, U.S. Department of State (Jan. 7, 2021), https://www.state.gov/secretary-pompeo-approves-new-cyberspace-security-and-emerging-technologies-bureau/.

- *Fifth, Congress must appropriate funds necessary for urgent State Department needs* both to augment the U.S. diplomatic corps and to support critical State Department programs focused on AI and emerging technologies to advance U.S. interests.

These steps are essential but not sufficient to further U.S. interests in tech diplomacy. Eventually, the D/MR role should transition into a permanent Under Secretary for Science, Research and Technology (State/Q). State/Q would lead a reorganization of the Department, combining offices and bureaus to further robust, coordinated approach to science and technology diplomacy and foreign assistance in the context of great power competition.[406]

[406] These components of the State Department should include key functions of the CSET Bureau; the Bureau of Oceans, Environment and Science; the Office of the Science Advisor to the Secretary; the Coordinator for Cyber Issues; and the Center for Analytics.

Chapter 16: Associated Technologies

The Commission's work ends where it began, with the conclusion that artificial intelligence (AI) will transform virtually every aspect of our existence. However, leadership in AI is not an end unto itself; it is a necessary, but not sufficient, condition for the overarching goal of preserving U.S. leadership in technology. That reality presents a challenge for U.S. strategy: how to prioritize investments in AI and other key emerging technologies, and support specific projects which will build on and amplify cross-technology strengths. The United States must view its efforts to lead in AI through the broader lens of competition across a range of emerging technologies, and, therefore, also support a comprehensive strategy to sustain U.S. leadership in key associated technologies.

Leadership in AI relies on and drives leadership across a suite of emerging technologies. AI sits at the center of the constellation of emerging technologies, enabling some and being enabled by others.[407] For instance, 5G and quantum computing are poised to enable new growth in AI capabilities, while AI stands to transform the biological sciences, producing significant technological breakthroughs and turning the biotechnology sector into one of the primary drivers of overall economic competitiveness.[408]

China is pursuing a comprehensive technology leadership strategy. China's strategic investments in key sectors through its Made in China 2025 initiative threaten U.S. technological prowess, economic prosperity, and national security.[409] In addition to investments in AI, China is seeking to become a world leader in quantum, 5G and biotech, among other areas, and sees its strategies to lead in AI and each of these other technologies as mutually reinforcing. It has made clear which technologies it views as key national priorities, and is investing heavily in a wide-range of sectors it assesses are essential to overall technical leadership.

The United States has neither identified, nor prioritized leadership in, the technologies which are central to national competitiveness. The first-mover advantage for technologies like microelectronics, biotechnology, and quantum computing means that the United States risks being unable to catch up to China in the research, application, manufacturing, and deployment of the technologies which will underpin national power in the twenty-first century. In sectors with strong network effects like 5G, the U.S. also faces a winner-take-all dynamic that raises the stakes for rapidly developing a successful technology platform.[410] The lack of a clear, unified list of technologies that are key to U.S. competitiveness results in disparate funding and policy approaches across departments and agencies and makes it difficult for legislators to identify funding priorities.

[407] Recognizing this connection, Congress included AI and "associated technologies" as they relate to national security within the scope of the Commission's mandate.

[408] The Commission's first Interim Report identified biotechnology, quantum computing, and 5G as key emerging technologies associated with AI. See *Interim Report*, NSCAI at 50 (Nov. 2019), https://www.nscai.gov/reports.

[409] Made in China 2025 includes the following sectors: New generation information technology, high-grade machine tooling and robotics, aviation and aerospace equipment, marine engineering equipment and high-tech ships, advanced rail transportation equipment, new energy automobiles, electric power equipment, agriculture equipment, new materials, and biomedicine and high-tech medical devices. See Alice Tse & Julianna Wu, *Why 'Made in China 2025' Triggered the Wrath of President Trump*, South China Morning Post (Sept. 11, 2018), https://multimedia.scmp.com/news/china/article/made-in-China-2025/index.html.

[410] According to McKinsey, "Platforms are the back-end technology capabilities, whether provided by individual systems or by assemblies of multiple systems, that power products." Ross Frazier, et al, *Products and Platforms: Is Your Technology Operating Model Ready?*, McKinsey Digital (Feb. 28, 2020), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/products-and-platforms-is-your-technology-operating-model-ready.

The result is muddled priorities and disparate approaches to technology promotion and protection. The absence of clear priorities also makes it more difficult to effectively marshal private sector investment in key technologies.

Ensuring U.S. leadership in the manufacturing of key emerging technology platforms will be an essential component of national competitiveness. Identifying and supporting research in priority technologies is a necessary but insufficient step to maintain national competitiveness in emerging technologies. The United States will also have to invest in the production of strategic physical elements of these technologies to create game-changing platforms, maximize U.S. competitiveness, and reduce dependencies which create national security vulnerabilities. Such investments are often expensive, but a strategic approach does not require manufacturing every advanced component domestically and will pay tremendous long-term dividends. The need to support advanced manufacturing applies to nearly every key emerging technology sector, including semiconductors, quantum computing, biotechnology, telecommunications equipment, and others, is reflected in the recommendations below.

The United States must identify the broader list of emerging technologies that underpin U.S. national competitiveness and solidify U.S. leadership in these critical areas to national security. AI is only one element of the long-term technology competition ahead.

Identifying and Prioritizing Technologies Central to National Competitiveness. While the United States should by no means adopt China's centrally-planned and state-directed economic model, it must start by developing better strategic planning, forecasting, and prioritization of emerging technologies to ensure long-term competitiveness. The government should:

✦ **Define and prioritize the key emerging technologies that are needed to ensure U.S. national competitiveness.** As part of its national technology competitiveness strategy (see Chapter 9), the White House should publish a list of critical and emerging technologies in which U.S. leadership is essential. It should develop detailed implementation plans for each sector to determine how the government should best work with industry to promote U.S. leadership, assess which specific sub-sectors are crucial to national security, and determine what regulatory steps or incentives are necessary to create the required investment environment. These plans should promote investment in specific platforms which will have a force multiplier effect on U.S. technology leadership, identify key choke points where competitors could potentially be blocked with minimal impact on U.S. industry, and promote supply chain resiliency. The creation and maintenance of such a list and the associated implementation plans will help produce a national consensus across government, industry, and academia about which sectors are most important in the emerging techno-economic competition. The result will be an important message to Congress regarding where the country must prioritize and expend resources, as well as a powerful demand signal to industry.

Many similar lists exist throughout the government, but there has been no effort to unify them into a single, authoritative document accompanied by a strategic vision and detailed follow-through actions designed to ensure long-term U.S. leadership.[411] However, the significant overlap between these lists

[411] In their 2018 report, Michael Brown and Pavneet Singh argue that the lack of a unified list of critical technologies harms the ability of the United States to protect against technology transfer. See Michael Brown & Pavneet Singh, *China's Technology Transfer*

demonstrates an emerging national consensus on which technologies are most critical to U.S. national competitiveness. Table 5 illustrates the initial slate of technologies which the Commission recommends including as part of a broader technology leadership strategy, as well as whether or not those technologies have been included on select, existing U.S. government lists of critical technologies. As an initial step, the Commission recommends that the White House designate these technologies as critical through an Executive Order and direct Departments and Agencies to prioritize and coordinate them accordingly.

Table 5. NSCAI-proposed Initial List of Emerging Technologies Key to U.S. National Competitiveness, Noting Whether they are Included on Existing U.S. Government Lists.

NSCAI-Proposed List of Critical Technologies vs Existing U.S. Government Lists						
NSCAI-Proposed Critical Technology List	2018 National Defense Strategy	DoD List of Critical Emerging Technologies	Commerce ANPRM on Emerging Technologies	PCAST List of Industries of the Future	S.3832 - Endless Frontier Act	WH Nat Strategy for C&ET
Artificial Intelligence	✓	✓	✓	✓	✓	✓
Biotechnology	✓	✓	✓	✓	✓	✓
Quantum Computing		✓	✓	✓	✓	✓
Semiconductors and Advanced Hardware	✓	✓	✓		✓	✓
Robotics and Autonomy	✓	✓	✓		✓	✓
5G and Advanced Networking		✓		✓	✓	✓
Advanced Manufacturing			✓	✓	✓	✓
Energy Technology	✓	✓			✓	✓

Actions to Promote Technologies and Platforms Essential to U.S. Leadership and National Security. After reaching consensus on the set of emerging technologies essential to overall U.S. technology leadership, the Executive Branch should assess each sector and identify specific platforms which meet the following criteria:

- Have potential applications of strategic and national security importance;
- could have a significant impact on overall U.S. technical leadership and competitiveness, either alone or when combined with existing U.S. technical strengths; and

Strategy, Defense Innovation Unit Experimental at 37 (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

- require government action to spur or protect its development.

Such platforms could necessitate government support for several reasons. In some instances, a market failure may lead to underinvestment by the private sector in an area of strategic importance to national security. In other instances, seizing a market opportunity may only be possible if the federal government focuses the private sector, academia, and research organizations toward a specific goal. The government must tailor its approach to the context by increasing funding, implementing regulatory changes, or taking other steps aimed at promoting innovation and protecting advantages that fit the circumstances.

The Commission has already presented recommendations to support U.S. leadership in key technology platforms within several of the aforementioned strategic technologies. For example, Chapter 11 recommends establishing a National AI Research Resource, which would create an essential platform to sustain and extend U.S. leadership in AI. Additionally, in Chapter 13, the Commission provided a series of recommendations for promoting U.S. leadership in microelectronics, including specific actions to incentivize the construction of a leading-edge merchant fabrication facility domestically.

The recommendations below build on the Commission's previous work to provide further actions the U.S. government could take to promote U.S. leadership in the key associated technologies and platforms that the Commission assesses to be of greatest strategic importance—specifically, biotechnology, quantum computing, 5G and advanced networking, autonomy and robotics, advanced and additive manufacturing, and energy systems.[412]

Biotechnology. Biology is now programmable, and AI's ability to identify ways to optimize this programming will enable transformational biotechnology breakthroughs. AI was crucial in the rapid development of COVID-19 vaccines, allowing researchers to finalize the genetic sequence of a vaccine candidate only two days after the virus' full genetic sequence was first posted online.[413] Computer vision techniques applied to medical imagery have also enabled more accurate and efficient diagnoses.[414] And recently, an AI network made substantial progress over the last year toward solving one of biology's most daunting challenges: determining a protein's 3D shape from its amino-acid sequence.[415] Tools such as these will become even more powerful in combination with synthetic biology and gene editing. Together they will enhance human health by allowing deeper studies of the building blocks of life and enabling the quicker discovery and fabrication of more advanced drugs and materials. As AI fuels rapid new developments in the biological sciences and biotechnology becomes a greater driver of the overall world economy, the strategic consequences of

[412] This includes all technologies other than AI on NSCAI's proposed critical technologies list with the exception of semiconductors, which are addressed separately in Chapter 13. Elements of AI-enabled biotechnology are also separately addressed in Chapter 1 of this report.

[413] Hannah Mayer, et al., *AI Puts Moderna within Striking Distance of Beating COVID-19*, Harvard Business School (Nov. 24, 2020), https://digital.hbs.edu/artificial-intelligence-machine-learning/ai-puts-moderna-within-striking-distance-of-beating-covid-19/; Noah Weiland, et al., *Modern Vaccine is Highly Protective Against Covid-19, the F.D.A. Finds*, New York Times (Dec. 18, 2020) https://www.nytimes.com/2020/12/15/health/covid-moderna-vaccine.html.

[414] Junfeng Gao, et al., *Computer Vision in Healthcare Applications*, Journal of Healthcare Engineering (Mar. 4, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5857319/.

[415] Ewen Callaway, '*It will Change Everything': DeepMind's AI Makes Gigantic Leap in Solving Protein Structures*, Nature (Nov. 30, 2020), https://www.nature.com/articles/d41586-020-03348-4.

ceding leadership in biotechnology will increase significantly—a fact which the COVID-19 pandemic illustrates in clear and stark terms. The government should:

✦ **Prioritize the development of an advanced biotechnology manufacturing ecosystem.** The United States must take steps to better position itself to benefit from the ongoing and rapid AI-enabled advancements in biology. It should start by prioritizing the development of an advanced biotechnology manufacturing ecosystem and developing a national biomanufacturing strategy. While AI has already begun to rapidly accelerate and enhance drug discovery, U.S. pharmaceutical and biotech manufacturing capabilities must expand in their scope and sophistication to keep pace with AI's transformative impact on the bioeconomy. Given that up to 60 percent of the physical inputs to the global economy could be produced via synthetic biology, there is a clear and pressing need for the United States to retain leadership in biotech manufacturing moving forward.[416] The United States should specifically support efforts to transform the biotechnology industry away from its current, vertically-integrated models and encourage the development of multiple standardized, merchant biofabrication facilities. This can include research and development (R&D) funding and incentives, and expansion of existing relevant programs such as BioMADE.[417] The Department of Health and Human Services should direct funds to support advanced biotech manufacturing initiatives, including through entities such as the Biomedical Advanced Research and Development Authority (BARDA),[418] and Congress should prioritize such initiatives in future health-related spending bills. Doing so would expand access to advanced biofabrication tools among startups and laboratories by allowing firms to rapidly design new molecules and materials via the cloud and place immediate orders for fabrication. This would help ensure the United States remains a hub for biotech manufacturing, and allow biofabrication to keep pace with the rapid analytical improvements AI is facilitating across the biological sciences.

Quantum Computing. Because the pace of innovation predicted by Moore's Law is increasingly difficult for semiconductor manufacturers to maintain due to the physical limits of microchip design, leadership in next-generation computer hardware will be essential to preserving long-term U.S. advantages in strategic technologies like AI.[419] Although classical computers will likely remain the most economical way of performing day-to-day computational tasks in the near future, quantum computers have the potential to outperform their classical counterparts on certain classes of problems related to machine learning and optimization, the simulation of physical systems, and the collection and transfer of sensitive information. For example, quantum computers may be able to efficiently optimize military logistics or discover new materials for weapons systems.[420] Each of these

[416] Michael Chui, et al., *The Bio Revolution*, McKinsey Global Institute at 43 (May 13, 2020), https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/the-bio-revolution-innovations-transforming-economies-societies-and-our-lives.

[417] BioMADE is a public-private partnership with DoD operated under ManufacturingUSA, focused on building a sustainable bioindustrial manufacturing ecosystem and enhancing U.S. bioindustrial competitiveness. See *BioMADE (Bioindustrial Manufacturing and Design Ecosystem)*, Manufacturing USA (last accessed Jan. 9, 2021), https://www.manufacturingusa.com/institutes/biomade.

[418] *Biomedical Advanced Research and Development Authority (BARDA)*, U.S. Department of Health and Human Services (Dec. 4, 2019), https://www.hhs.gov/about/agencies/orgchart/aspr/barda/index.html.

[419] Steve Blank, *What the GlobalFoundries' Retreat Really Means*, IEEE Spectrum (Sept. 10, 2018), https://spectrum.ieee.org/nanoclast/semiconductors/devices/what-globalfoundries-retreat-really-means.

[420] Pontus Vikstål, et al., *Applying the Quantum Approximate Optimization Algorithm to the Tail-Assignment Problem*, Physical Review Applied Vol 14, Iss. 3 (Sept. 3, 2020), https://doi.org/10.1103/PhysRevApplied.14.034009; He Ma, et al., *Quantum Simulations of Materials on Near-term Quantum Computers*, npj Computational Materials (July 2, 2020), https://doi.org/10.1038/s41524-020-00353-z.

applications create novel national security threats and opportunities at the intersection of AI and quantum computing. The government should:

✦ **Transition quantum computing basic research to national security applications and incentivize domestic quantum fabrication.** The United States is a global leader in research of quantum computers, but it risks losing its edge in real-world applications of quantum computers. It must continue investing in development of national security use cases, recognizing that advances in quantum may drive future advances in AI. The U.S. government should announce its priority use cases of quantum technologies, offer access to quantum computers through the National AI Research Resource, and create the conditions for domestic fabrication of quantum computers. Publicly announcing specific government use cases of quantum computers will signal that a market exists for national security applications and encourage further investment by the private sector. And incentivizing the domestic design and manufacturing of quantum computers via tax credits for relevant expenditures, loan guarantees, and equity financing would help to avoid the situation in which the U.S. government currently finds itself regarding access to trusted and assured microelectronics.

5G and Advanced Networking. 5G networks will form the connective tissue between AI platforms, which means maintaining access to trusted and robust 5G networks is a critical component of overall leadership in AI. Huawei is pursuing global dominance in 5G and there is no single supplier that can compete with it in both price and quality. Due to the urgency of the issue, the United States should pursue several complementary approaches concurrently to ramp up deployment of 5G domestically and provide a credible alternative to Huawei. As a starting point, any comprehensive effort should include support for dynamic spectrum sharing.[421] The government should:

✦ **Bolster and accelerate U.S. 5G network deployment through mid-band spectrum sharing.** Expanding spectrum sharing efforts is critical to ensuring that the Department of Defense (DoD) maintains access to spectrum essential for operational effectiveness while broadening commercial access to spectrum for 5G networks. A multi-agency effort is needed to expand sharing arrangements and licenses and permit additional portions of the mid-band to be simultaneously utilized by DoD and commercial carriers. Through this portfolio approach, the United States stands the best chance of accelerating its 5G deployment at a pace that can support the widespread adoption of AI.

Autonomy and Robotics. Autonomous systems are already unlocking value across global markets. In the private sector, they enable products ranging from expert advisory systems and self-driving vehicles to manufacturing. In the realm of national security, autonomous systems generate opportunities to reduce the number of warfighters in harm's way, increase the pace and quality of decisions, and create entirely new military capabilities.[422] The ability to design and produce the hardware and software for advanced robotics is an essential part of autonomous systems. The government should:

[421] *The 5G Ecosystem: Risks & Opportunities for DoD*, DoD Defense Innovation Board (Apr. 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[422] *Summer Study on Autonomy*, DoD Defense Science Board (June 2016), https://dsb.cto.mil/reports/2010s/DSBSS15.pdf.

✦ **Incentivize the development of world-class software platforms for robotic and autonomous systems.** The future of autonomy and robotics will manifest in almost unlimited shapes and sizes as firms develop and tailor robots for different use cases and environments. The U.S. trails nations such as China, Japan, and South Korea in the deployment of robots and robotic hardware and must work to improve its capabilities in such areas as materials design and energy storage for robots.[423] However, U.S. expertise in software development lends itself to creating a world-class digital platform for many classes of robotic hardware. The software powering robotic systems will be built upon several core capabilities rooted in AI: it will need to be able to see its environment, reason, and operate in the world around it.[424] In creating cutting-edge software for these types of capabilities, there is an opportunity for U.S. firms to win the market for the software platforms that power the next wave of industrialization.[425] To promote U.S. leadership in the development of software for autonomous systems, the U.S. government should fuel industry's ongoing efforts by supplementing the basic R&D, standard-setting, and data sharing programs led by National Institute of Standards and Technology (NIST)'s Intelligent Systems Division.[426] It should also incentivize early adoption of automation and create markets for autonomous systems in areas already ripe for them, such as mail sorting, that will yield data and experience relevant for achieving scale and addressing adjacent markets.[427] Combined, a multipronged approach along these lines would position industry to compete more effectively in the market for autonomous system software, a strategically important area aligned with existing U.S. technical strengths.

Advanced & Additive Manufacturing. The capacity to produce high-tech goods domestically is critical to national security, both to maintain access to finished goods and as a driver of innovation. In terms of access, the United States must strive for self-reliance in industries that are critical to national security or that would take too long to regenerate in the event of protracted conflict.[428] Innovation also benefits from a tight feedback loop between technological design and production, which allows for more rapid iteration.[429] This link is particularly important in the defense sector, where feedback from the manufacturing process back into the research and development cycle helps bring technology from lab to military operations. Longer-term disruptions to the manufacturing industry through new techniques such as additive manufacturing also pose threats and opportunities

[423] Maximiliano Dvorkin & Asha Bharadwaj, *Which Countries and Industries Use the Most Robots*, Federal Reserve Bank of St. Louis (Nov. 7, 2019), https://www.stlouisfed.org/on-the-economy/2019/november/robots-affecting-local-labor-markets.

[424] Advanced materials (such as biological components), brain-computer interfaces, and small and efficient power supplies are additional areas of potential innovation that connect robotics to AI and other associated technologies described in this chapter.

[425] For example, core capabilities might include gripping physical objects, which robotics maker ABB and several firms in the U.S. and Europe are currently pursuing. See Jonathan Vanian, *Industrial Robotics Giant Teams Up with a Rising A.I. Startup*, Fortune (Feb. 25, 2020), https://fortune.com/2020/02/25/industrial-robotics-ai-covariant/.

[426] *Intelligent Systems Division*, NIST (last accessed Jan. 6, 2021), https://www.nist.gov/el/intelligent-systems-division-73500.

[427] One specific area to expand demand for autonomous systems could be drastically scaling the U.S. Postal Service's Autonomous Mobile Robot pilot program from 25 sorting facilities to all sorting facilities by 2025. *Autonomous Mobile Robots and the Postal Service*, USPS Office of Inspector General (Apr. 9, 2018), https://www.uspsoig.gov/sites/default/files/document-library-files/2019/RARC-WP-18-006.pdf.

[428] *Critical Technology Accessibility*, National Academies Press (2006), https://www.nap.edu/read/11658/chapter/1; see also *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, Interagency Taskforce in Fulfillment of Executive Order 13806 at 46 (Sept. 2018), https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF (identifying ten risk archetypes threatening America's manufacturing and defense industrial base).

[429] *Strategy for American Leadership in Advanced Manufacturing*, National Science & Technology Council (Oct. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/10/Advanced-Manufacturing-Strategic-Plan-2018.pdf; Gregory Tassey, *Rationales and Mechanisms for Revitalizing US Manufacturing R&D Strategies*, NIST (Jan. 29, 2010), https://www.nist.gov/system/files/documents/2017/05/09/manufacturing_strategy_paper_0.pdf.

for national security. For example, additive manufacturing may enable a step-change in domestic manufacturing capabilities, but also creates new threats by potentially democratizing the production of firearms and other goods with military applications.[430] The government should:

✦ **Accelerate additive manufacturing production of legacy parts across the Department of Defense.** Additive manufacturing and 3D printing have the potential to transform manufacturing. They are capable of rapid, high-quality, and complex production, and flexible enough that 3D printers may be able to be located near the point of need for just-in-time production.[431] Although current additive manufacturing techniques struggle to replicate the quality of advanced traditional manufacturing techniques, AI has already shown the ability to enable significant improvements in their accuracy.[432] The Federal Government should proactively support initiatives which advance the development of additive manufacturing techniques and also provide practical benefits by easing the production of legacy items.[433] The Department of Defense should announce a goal of identifying all legacy parts in active weapon systems which are capable of being produced via additive manufacturing and 3D printing and doing so by 2025.

Energy Systems. Cheap and reliable access to energy is critical to U.S. national security, whether it be to ensure military readiness, facilitate the response to a domestic crisis, or keep the economy functioning smoothly. As an input to nearly every sector, the price of energy directly impacts economic output and is a key determinant of U.S. national competitiveness. Furthermore, dependence on foreign countries for energy resources and technologies would put the United States in a position of vulnerability, especially if those resources or technologies are controlled by strategic competitors. Although the United States is at the forefront of the exploration, extraction, and processing of oil and gas and possesses significant domestic reserves, China is far and away the leading producer of renewable energy and is investing heavily in advanced energy storage technologies, such as batteries and their constituent materials.[434] To remain competitive, U.S. industry will need to achieve aggressive cost targets in terms of kilowatts per hour and energy density. This is especially true in markets with the most substantial growth potential, such as long-duration stationary storage devices and battery packs for electric vehicles.[435] The government should:

✦ **Develop and domestically manufacture energy storage technologies to meet U.S. market demand by 2030.** Developing new technologies to more effectively store electrical energy so it is readily available whenever and wherever needed would drive advances in electricity distribution. It would also offer advantages to the United States both economically and strategically. To accelerate

[430] *3D Opportunity for Adversaries*, Deloitte (Aug. 22, 2017), https://www2.deloitte.com/us/en/insights/focus/3d-opportunity/national-security-implications-of-additive-manufacturing.html.

[431] *Audit of DoD's Use of Additive Manufacturing for Sustainment Parts*, DoD Inspector General (Oct. 17, 2019), https://media.defense.gov/2019/Oct/21/2002197659/-1/-1/1/DODIG-2020-003.PDF.

[432] Mark Anderson, *3D Print Jobs are More Accurate with Machine Learning*, IEEE Spectrum (Feb. 19, 2020), https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/3d-print-jobs-news-accurate-machine-learning.

[433] For instance, in August 2020, the Department of Defense printed the first metal part for a B-52 jet engine. Kyle Mizokami, *The Old School Engine that Powers the B-52 Gets a 3D-Printed Upgrade*, Popular Mechanics (Aug. 10, 2020), https://www.popularmechanics.com/military/aviation/a33535790/air-force-3d-print-metal-part-turbofan-engine/.

[434] Robert Rapier, *Ten Countries That Dominate World Fossil Fuel Production*, Forbes (July 14, 2019), https://www.forbes.com/sites/rrapier/2019/07/14/ten-countries-that-dominate-fossil-fuel-production; *Country Rankings*, International Renewable Energy Agency (last accessed Jan. 6, 2021), https://www.irena.org/Statistics/View-Data-by-Topic/Capacity-and-Generation/Country-Rankings.

[435] *Energy Storage*, U.S. Department of Energy (last accessed Jan. 6, 2021), https://www.energy.gov/oe/energy-storage.

breakthroughs in energy storage,[436] the Department of Energy has set the ambitious goal of developing and domestically manufacturing storage technologies capable of meeting the entirety of U.S. market demand by 2030.[437] Congress should fully fund the federal R&D and establish incentives for commercialization needed to achieve the Department of Energy's Energy Storage Grand Challenge roadmap by 2030.[438]

[436] The field of energy storage includes a broad technology base such as batteries (both conventional and advanced), electrochemical capacitors, flywheels, power electronics, control systems, and software tools for storage optimization and sizing.
[437] *Energy Storage*, U.S. Department of Energy (last accessed Jan. 6, 2021), https://www.energy.gov/oe/energy-storage.
[438] *Energy Storage Grand Challenge: Roadmap*, U.S. Department of Energy (Dec. 2020), https://www.energy.gov/sites/prod/files/2020/12/f81/Energy%20Storage%20Grand%20Challenge%20Roadmap.pdf.

NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE