Blueprints for Action

The Final Report presents the NSCAI's recommendations as a strategy for winning the AI era. The 16 chapters in the Main Report provide topline recommendations. The accompanying Blueprints for Action outline concrete steps that departments and agencies can take to implement NSCAI recommendations. The Commission has provided as much specificity as possible—including by providing draft legislative text and executive orders—to help the President and Congress move rapidly from understanding AI to acting for the benefit of the American people.

The Final Report represents an important step, but it is not the NSCAI's final act. For the remaining life of the Commission, our work will focus on implementation to help the President and Congress make the investments and take the actions recommended to win the AI era. [Submitter's Note: This StratML rendition includes the broader recommendations. The proposed actions should be published as performance plans/reports for each agency and group.]

Contents

Vision....6
Mission....6
Values....6
1. DEFENSE....7
1.1. THREATS....7
1.1.1. Strategy....7
1.1.1.1. Societies....7
1.1.1.2. Competition....7
1.1.1.3. Opinion & Advantage....7
1.1.1.3.1. Malign Information....7
1.1.1.3.2. Actions....7
1.1.1.4. Critical Infrastructure....8
1.1.1.5. Organizational Structures....8
1.1.1.6. Complementary Technologies....8
1.1.1.7. Capital....8
1.1.2. Cyber Conflict....8
1.1.2.1. Threats....8
1.1.2.2. Testing....8
1.1.2.3. AI-Cyber Defenses....8
1.1.2.4. Incentives....8
1.1.2.5. Options....9
1.1.2.6. Strategy, Structure, Organization & Authorities....9
1.1.2.7. Security Centers....9
1.2. FOUNDATIONS....9
1.2.1. Leadership....9
1.2.2. Technical Backbone....9
1.2.3. Education & Training....10
1.2.4. Technology Adoption....10
1.2.5. AI Development....10
1.2.6. Capabilities....10
1.3. WARFARE....11
1.3.1. Organizational Reforms....11
1.3.2. Warfighting Concepts....11
1.3.3. Performance Goals....11
1.3.4. Technologies & R&D....11
1.3.5. Interoperability & Adoption....12
1.4. WEAPONS....12
1.5. NATIONAL INTELLIGENCE....12
1.5.1. Science & Technology....12

1.5.2. Risk Management....12
1.5.3. Coordination....13
1.5.4. Open Information....13
1.5.5. Security Clearance....13
1.6. TALENT....13
1.6.1. Digital Corps....13
1.6.2. National Reserve....14
1.6.3. Recruiting Offices....14
1.6.4. Qualification Policies....14
1.6.5. CyberCorps....14
1.6.6. STEM Corps....15
1.6.7. Digital Service Academy....15
1.6.8. Civilian Careers....15
1.6.9. Military Careers....16
1.6.10. Tools, Data & Infrastructure....16
1.7. CONFIDENCE....16
1.7.1. Robustness & Reliability....17
1.7.1.1. R&D....17
1.7.1.2. Risk, Documentation & Architecture....17
1.7.2. Interaction & Teaming....17
1.7.2.1. Research Labs....18
1.7.2.2. Policies, Designs & Training....18
1.7.3. TEVV....18
1.7.3.1. Policies & Capabilities....18
1.7.3.2. Standards, Metrics & Tools....18
1.7.4. Leadership....19
1.7.4.1. Leader....19
1.7.4.2. Expert Body....19
1.7.5. Accountability & Governance....19
1.7.5.1. Policies....19
1.7.5.2. Oversight & Enforcement....20
1.8. VALUES....20
1.8.1. Reporting....20
1.8.2. Privacy & Fairness....20
1.8.3. Due Process & Redress....20
1.8.4. Oversight & Governance....20
2. TECHNOLOGY....21
2.1. STRATEGY....21
2.1.1. Dialogue....21
2.1.1.1. Targeted Areas....21
2.1.1.2. Relationships & Frictions....21
2.2. TALENT....22
2.2.1. Defense Education Act....22
2.2.2. Statistics & Computer Science....22
2.2.3. O-1 Visas....22
2.2.4. International Entrepreneur Rule....23
2.2.5. Job Portability....23
2.2.6. Green Cards....23
2.3. INNOVATION....24
2.3.1. R&D Funding....24
2.3.1.1. Technology Foundation....24
2.3.1.2. Prioritization & Funding....24
2.3.1.3. AI Research Institutes....25

2.3.1.4. Talent & Transformation 25
2.3.2. Research Infrastructure 25
2.3.2.1. AI Research Resource 25
2.3.2.2. AI Testbeds 26
2.3.2.3. Training Data 26
2.3.2.4. Knowledge Network 26
2.3.3. Public-Private Partnership 27
2.3.3.1. Markets 27
2.3.3.2. Clusters 27
2.3.3.3. Competitiveness Consortium 28
2.3.4. Challenges 28
2.3.4.1. QOL 28
2.3.4.2. Education & Learning 28
2.3.4.3. Energy 28
2.3.4.4. Disasters 29
2.4. INTELLECTUAL PROPERTY 29
2.4.1. Policies & Regimes 29
2.4.2. Considerations 29
2.4.2.1. Innovation 29
2.4.2.2. Narrative 30
2.4.2.3. Patent Examination 30
2.4.2.4. Partnerships 31
2.4.2.5. Data 32
2.4.2.6. Theft 32
2.4.2.7. Inventorship 32
2.4.2.8. Global Alignment 33
2.4.2.9. Innovation & IP Ecosystems 33
2.4.2.10. "Standard Essential" Patents 34
2.5. MICROELECTRONICS 34
2.5.1. Executive Order 35
2.5.2. Fabrication 35
2.5.3. Research & Infrastructure 35
2.5.4. Trust & Agility 36
2.6. TECHNOLOGY PROTECTION 36
2.6.1. Dual-Use Technology 36
2.6.2. Capacity 37
2.6.3. Controlled Technologies 37
2.6.4. CFIUS 38
2.6.5. Manufacturing Equipment 38
2.6.6. Export Controls 38
2.6.7. Research Environment 38
2.6.8. Coordination 39
2.6.9. Cybersecurity 39
2.6.10. Foreign Talent-Recruitment 39
2.6.11. PLA Affiliates 39
2.7. ORDER, OPENNESS & PROSPERITY 40
2.7.1. Strategy 40
2.7.2. Coalition 40
2.7.2.1. Norms & Values 40
2.7.2.2. Policies & Investments 40
2.7.2.3. Infrastructure 41
2.7.3. Digital Democracy 41
2.7.3.1. Coordination 41

2.7.3.2. Mobilization 41
2.7.3.3. Adoption 41
2.7.4. Plan 41
2.7.4.1. Technical Standards 41
2.7.4.2. Policy 42
2.7.4.2.1. Interests 42
2.7.4.2.2. Prioritization 42
2.7.4.2.3. Foreign Policy 42
2.7.4.3. Export Controls 42
2.7.5. Research Hub 42
2.7.5.1. Initiatives & Standards 43
2.7.5.2. Talent 43
2.7.5.3. Research 43
2.7.5.4. Regulation 43
2.7.6. Great Power Competition 44
2.8. ASSOCIATED TECHNOLOGIES 44
2.8.1. National Competitiveness 44
2.8.2. Biotechnology R&D 45
2.8.3. Biotechnology Capabilities 45
2.8.4. BGI 45
2.8.5. Disease Monitoring 46
2.8.6. Quantum Computing 46
2.8.7. Quantum Fabrication 46
2.8.8. Quantum Computing Research 47
2.8.9. 5G Deployment 47
2.8.10. Robotic & Autonomous Systems 48
2.8.11. Legacy Parts 48
2.8.12. Energy Storage 48
Administrative Information 49

National Security Commission on Artificial Intelligence (NSCAI)

Description:

The National Security Commission on Artificial Intelligence's (NSCAI) task is to make recommendations to the President and Congress to "advance the development of artificial intelligence [AI], machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States." In establishing the Commission, Section 1051 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 instructs NSCAI to examine AI through the lenses of national competitiveness, the means to sustain technological advantage, trends in international cooperation and competitiveness, ways to foster investment in basic and advanced research, workforce and training, potential risks of military use, ethical concerns, establishment of data standards and incentivization of data sharing, and the future evolution of AI.

Stakeholder(s):

NSCAI Commissioners :
The 15 commissioners were nominated by Congress and the Executive Branch. They represent a diverse group of technologists, business executives, academic leaders, and national security professionals. They have approached all inquiries in bipartisan fashion and reached consensus on the Final Report. The Commission's operations have been guided by two principles: the need for action and the importance of transparency.

Dr. Eric Schmidt :
Chair | Schmidt Futures ~ Nominated by former Chairman Mac Thornberry (R-TX), House Armed Services Committee

The Honorable Robert O. Work :
Vice Chair | TeamWork ~ Nominated by Current Chairman and then-Ranking Member Jack Reed (D-RI), Senate Armed Services Committee

Safra Catz :
Oracle ~ Nominated by then-Chairman and Current Ranking Member Devin Nunes (R-CA), House Permanent Select Committee on Intelligence

Dr. Steve Chien :
Jet Propulsion Lab ~ Nominated by then-Ranking Member and Current Chairman Adam Schiff (D-CA), House Permanent Select Committee on Intelligence

The Honorable Mignon Clyburn :
MLC Strategies ~ Nominated by then-Ranking Member and Current Chairman Frank Pallone, Jr. (D-NJ), House Energy and Commerce Committee

Chris Darby :
In-Q-Tel ~ Nominated by Current Chairman and then-Vice Chairman Mark Warner (D-VA), Senate Select Committee on Intelligence

Dr. Ken Ford :
Florida Institute for Human & Machine Cognition ~ Senate Commerce, Science, and Transportation Committee

Dr. José-Marie Griffiths :
Dakota State University ~ Nominated by then-Chairman John Thune (R-SD), Senate Commerce, Science, and Transportation Committee

Dr. Eric Horvitz :
Microsoft ~ Nominated by Current Chairman and then-Ranking Member Adam Smith (D-WA), House Armed Services Committee

Andy Jassy :
Amazon Web Services ~ Nominated by former Chairman Greg Walden (R-OR), House Energy and Commerce Committee

Gilman Louie :
Alsop Louie Partners ~ Nominated by former Secretary Wilbur Ross, United States Department of Commerce

Dr. William Mark :
SRI ~ Nominated by former Secretary James Mattis, United States Department of Defense

Dr. Jason Matheny :
Georgetown University ~ Nominated by then-Chairman Richard Burr (R-NC), Senate Select Committee on Intelligence

The Honorable Katharina McFarland :
Chair, National Academies of Science Board of Army Research and Development ~ Nominated by then-Chairman and Current-Ranking Member Jim Inhofe (R-OK), Senate Armed Services Committee

Dr. Andrew Moore :
Google ~ Nominated by former Secretary James Mattis, United States Department of Defense

Vision

The national security and defense needs of the United States are comprehensively addressed

Mission

To make recommendations to the President and Congress to advance the development of artificial intelligence, machine learning, and associated technologies

Values

Action: The Commission's work includes an initial report in July 2019, interim reports in November 2019 and October 2020, two additional quarterly memorandums, a series of special papers in response to the COVID-19 pandemic, and now a final report. Waiting to deliver recommendations in a final report was not an option when we began our work in the spring of 2019. Assessing the broad national security implications of a dynamic technology like AI at a single point in time is like trying to catch lightning in a bottle. Scientists continue to deliver AI breakthroughs and the commercial sector is finding new ways to apply AI at an accelerating pace. Competitors around the world are developing AI strategies and investing resources. The Commission delivered recommendations on a continuous basis, aiming to match the speed of AI developments and the desires from the Executive Branch and Congress for help in deciding what to do. Congress has already adopted a number of our recommendations in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and the Executive Branch has incorporated recommendations as well. And we have continuously sought to learn from and educate a wide range of stakeholders to build a shared understanding about how AI will impact national security.

Transparency: The NSCAI has been committed to transparency. As a Federal Advisory Committee, it has held five public plenary sessions totaling approximately 15 hours of deliberations, streamed live online, and archived meeting recordings on the NSCAI website. It has responded to more than two dozen Freedom of Information Act requests and released more than 2,500 pages of material. NSCAI has posted more than 700 pages of draft materials for public review and comment. With the exception of materials and issues classified for national security reasons, the Commission has endeavored to offer full transparency. We have proactively engaged with the media after every plenary session, quarterly report, and submission to Congress. In dozens of separate engagements, we have partnered with non-governmental organizations, federal government organizations, and international organizations to communicate our recommendations to the media and the public. Most important, we have taken on the hardest issues with AI in public settings and made recommendations only after consulting with a wide range of civil society, private sector, and government groups. We have tried to listen and understand views across the spectrum on deeply complicated aspects of AI. We have engaged ethicists, technologists, and national security strategists. We have spoken with warriors and diplomats. We have talked to academics and entrepreneurs. All told, commissioners and staff have participated in hundreds of discussions. As the commissioners built consensus on recommendations, we approached issues with care and humility.

Privacy

Civil Liberties

Civil Rights

1. DEFENSE

Defend America in the AI Era

1.1. THREATS

Combat Malign Information Operations Enabled by AI.

Emerging Threats in the AI 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.

1.1.1. Strategy

Develop a national strategy for the global information domain

A National Strategy for the Global Information Domain ~ Expanding upon the principles of information statecraft outlined in the 2017 National Security Strategy, the President should issue a new national strategy for the global information domain that more fulsomely addresses how AI and associated technologies are defining new fronts in this area. The strategy should:

1.1.1.1. Societies

Acknowledge that the network-connected world is dissolving barriers between societies.

1.1.1.2. Competition

Prioritize the global information domain as an arena for competition.

1.1.1.3. Opinion & Advantage

Detail how adversarial state and non-state actors are attempting to define and control the global information domain in order to shape global opinion and achieve strategic advantage.

1.1.1.3.1. Malign Information

Account for the critical role of AI-enabled malign information in achieving these goals.

1.1.1.3.2. Actions

Designate malign information operations as a national security threat with its own set of priority actions to defend, counter, and compete against them.

1.1.1.4. Critical Infrastructure

As necessary, update critical infrastructure designations and require relevant departments and agencies to update sector-specific plans to reflect emerging technologies.

1.1.1.5. Organizational Structures

Establish organizational structures for U.S. national security agencies to defend, counter, and compete against the threat.

Stakeholder(s):

U.S. National Security Agencies

1.1.1.6. Complementary Technologies

Create a task force to study the use of AI and complementary technologies, including the development and deployment of standards and technologies, for certifying content authenticity and provenance.

1.1.1.7. Capital

Executive Branch departments and agencies should utilize Other Transaction Authorities (OTAs), creative investing, and the Small Business Innovation Research (SBIR) program to deploy capital to companies that offer technical solutions that will assist the United States Government in identifying, countering, and defending against malign information operations.

1.1.2. Cyber Conflict

Prepare for AI-Enabled Cyber Conflict.

1.1.2.1. Threats

Develop and deploy machine-speed threat detection and mitigation

1.1.2.2. Testing

Execute large, instrumented, and realistic tests to gather data and train AI-enabled cyber defenses.

1.1.2.3. AI-Cyber Defenses

Ensure the robustness of AI-cyber defenses

1.1.2.4. Incentives

Improve incentives for information and cyber security

1.1.2.5. Options

Develop additional, impactful non-kinetic options to respond to adversarial cyber and information operations.

1.1.2.6. Strategy, Structure, Organization & Authorities

Reform the U.S. Government's strategy, structure, organization, and authorities for handling AI-enabled cyber threats

1.1.2.7. Security Centers

Create or Designate Critical Technology Security Centers.

1.2. FOUNDATIONS

Foundations of Future Defense ~ 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.

Stakeholder(s):

Department of Defense :

The Department of Defense (DoD) lags far behind the commercial sector in integrating new and disruptive technologies such as Artificial Intelligence (AI) into its operations. Technical, bureaucratic, and cultural challenges must be overcome to adopt AI to maintain the U.S. military advantage. By 2025, the DoD must put in place the foundations for widespread AI adoption, by: 1) Building the technical backbone; 2) Training and educating warfighters; 3) Accelerating adoption of existing digital technologies; 4) Democratizing development of AI; and 4) Investing in next-generation capabilities. To the maximum extent possible, these efforts should be coordinated with the Intelligence Community (IC) and other partners across the national security community.

1.2.1. Leadership

Drive Change through Top-Down Leadership.

Maintaining the defense advantage in an AI-enabled future will require top-down leadership to overcome organizational barriers and create strategic change. Critically, civilian and military leaders across the DoD and the IC must coordinate more closely, aligning priorities, resources, and policies to speed technology adoption and research breakthroughs.

1.2.2. Technical Backbone

Build the Technical Backbone

Integration of AI into DoD operations requires urgent investment in a modern digital ecosystem that will enable ubiquitous development and fielding at all levels—from the headquarters to the tactical edge. It is essential to establish a technical foundation that: 1) Provides access to leading cloud technologies and services for scalable computing; 2) Enables the sharing of data, software, and capabilities through well-documented and hardened application programming interfaces (API) with proper access controls; and 3) Gives all DoD developers and scientists access to the tools and resources they need to drive new AI capabilities. To this end, the figure below depicts the ecosystem managed as a multilayer stack of services, accessed through common interfaces and providing shared access to essential AI building blocks of data, algorithms, tools, trained AI models, and

compute. This should be realized through a federated approach, building on existing resources and pathfinder efforts.

1.2.3. Education & Training

Train and Educate Warfighters

Stakeholder(s):
Warfighters

1.2.4. Technology Adoption

Accelerate Adoption of Existing Digital Technologies

The Department must have an integrated approach to AI and other emerging technologies that ensures the U.S. military can continuously identify, source, field, and update capabilities faster than our competitors. This requires more targeted investment in dualuse technologies, ensuring system adaptability through a more agile budget and oversight process, and streamlining the acquisition process to shed those rules and regulations whose benefits are outweighed by the burdens imposed on the system. Critically, the Defense Acquisition System must shift away from a one-size-fits-all approach to measuring value from the acquisition process. Adherence to cost, schedule, and performance baselines is rarely a proxy for value delivered, but is particularly unsuited for measuring and incentivizing the iterative approaches inherent in AI and other software-based digital technologies. Unless the requirements, budgeting, and acquisition processes are aligned to permit faster and more targeted execution, the U.S. will fail to stay ahead of potential adversaries.

1.2.5. AI Development

Democratize AI Development

An AI-enabled threat environment requires our forces to be able to develop and deploy solutions nearly as quickly as threats arise. However, our forces frequently lack the infrastructure, tools, talent, and support to solve their challenges locally and with modern technology.106 The JAIC cannot develop and proliferate AI applications for every user group or mission area within the DoD. To accelerate adoption of AI, the Department must create the technical infrastructure and organizational structures that pair top-down strategy with bottom-up development.

1.2.6. Capabilities

Invest in Next Generation Capabilities

The DoD must have an enduring process that clearly identifies, prioritizes, resources, and tracks126 critical technologies over multiple time horizons. This will drive an investment strategy that pursues technology applications that close key capability gaps and optimize current operational concepts, and simultaneously makes bets on disruptive technologies to enable transformative capabilities and operational concepts over the long term.

1.3. WARFARE

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 employ AI. | If U.S. forces are not organized, trained, and equipped for a new warfighting paradigm that is emerging because of artificial intelligence (AI) and other emerging technologies, they will be outmatched and paralyzed by the complexity of the future battlefield. This Blueprint for Action includes five top-line recommendations to achieve military AI readiness and prepare our forces for the future: 1) Drive organizational reforms through top-down leadership; 2) Develop innovative warfighting concepts; 3) Establish AIreadiness performance goals; 4) Develop and fund advanced technologies and R&D; and 5) Promote AI interoperability and the adoption of critical emerging technologies among U.S. allies and partners.

1.3.1. Organizational Reforms

Drive organizational reforms through top-down leadership.

Continuously out-innovating the competition requires strong commitment from the top civilian and military leaders directing the rapid development and adoption of innovative and disruptive approaches to warfare through top-down governance and oversight processes.

1.3.2. Warfighting Concepts

Develop Innovative AI-enabled Warfighting Concepts, Informed by Experimentation, Wargames and Real-world Exercises.

Battlefield advantage will shift to those who harness superior data, connectivity, compute power, algorithms, and overall system security to new warfighting concepts. Developing new operational concepts requires Services to incentivize experimentation, and foster a culture of "thinking Red"—in other words, considering the strategies of potential adversaries when developing operational concepts.

1.3.3. Performance Goals

Establish AI and digital readiness performance goals.

To drive outcomes and accountability and provide a means for oversight of Department efforts regulated to AI, DoD should establish key performance objectives and accompanying metrics for AI and digital readiness.

1.3.4. Technologies & R&D

Develop and Fund Advanced Technologies and R&D.

Development and fielding of advanced AI-enabled technologies will remain a critical component of DoD's ability to achieve decision advantage on the battlefield.

1.3.5. Interoperability & Adoption

Promote AI interoperability and the adoption of critical emerging technologies among allies and partners.

America's enduring relationships with allies and partners represent asymmetric advantages over competitors and adversaries. Differential adoption of AI across military alliances and intelligence partnerships creates interoperability risk that threatens allies' political and military cohesion, the resiliency of alliance structures, and the efficacy of coalition operations. The recommendations that follow reflect a holistic approach to furthering cooperation around AI and emerging technologies in the context of defense, intelligence, and security arrangements. They focus on interoperability and improving capacity and capability development to foster competitive military and intelligence advantages.

Stakeholder(s):

Allies **Partners**

1.4. WEAPONS

Autonomous Weapon Systems and Risks Associated with AI-Enabled Warfare ~ While AI-enabled and autonomous weapon systems have the potential to provide substantial military and even humanitarian benefit, the United States must take steps, including with allies and competitors, to mitigate strategic risks posed by AI-enabled and autonomous weapon systems.

1.5. NATIONAL INTELLIGENCE

AI and the Future of National Intelligence ~ Intelligence will benefit from rapid adoption of AI-enabled technologies more than any other national security mission. | Intelligence will benefit from rapid adoption of artificial intelligence (AI)-enabled technologies more than any other national security mission. However, critical barriers keep the Intelligence Community (IC) from turning this potential into real capabilities that are scaled across agencies. 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.

1.5.1. Science & Technology

Empower the IC's science and technology leadership.

1.5.2. Risk Management

Change risk management practices to accelerate new technology adoption.

1.5.3. Coordination

Improve coordination between the IC and DoD

Stakeholder(s):

IC **DoD**

1.5.4. Open Information

Capitalize on AI-enabled analysis of open source and publicly available information.

1.5.5. Security Clearance

Aggressively pursue security clearance reform for clearances at the Top Secret level and above, and enforce security clearance reciprocity among members of the IC.

Stakeholder(s):

Members of the IC

1.6. TALENT

Technical Talent in Government ~ The United States government needs digital experts now or it will remain unprepared to buy, build, and use AI and its associated technologies. | The United States Government needs digital experts now or it will remain unprepared to buy, build, and use AI and its associated technologies. Expanding digital expertise is the most important step the government can take to modernize. While this challenge is recognized, few parts of government have adequately invested in building their digital workforce. To expand its digital and AI digital 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 and future government employees.
- Employ its digital workforce more effectively to ensure digital talent can perform meaningful work once they are in government.

1.6.1. Digital Corps

Create Digital Corps for Cabinet-Level Departments and Select Agencies to Organize the Government's Technical Workforce

Stakeholder(s):

Digital Corps

1.6.2. National Reserve

Create a National Reserve Digital Corps

Stakeholder(s):
National Reserve Digital Corps

1.6.3. Recruiting Offices

Create Digital Talent Recruiting Offices Aligned with Digital Corps

Executive branch agencies should create agency-level digital talent offices of up to 20 personnel responsible for recruiting both early career and experienced professionals. Recruiting offices would monitor their agencies' need for specific types of digital talent. The offices would be empowered to recruit technologists virtually, by attending conferences, career fairs, recruiting on college campuses, and offering scholarships, recruiting bonuses, referral bonuses, non-traditional recruiting techniques such as prize competitions, and other recruiting mechanisms. A recruiting office would assume responsibility for their agency's digital talent recruitment efforts, e.g., Science, Mathematics and Research for Transformation (SMART) Scholarship-for-Service, and partner with agency human resources offices to use direct-hire authorities and the Intergovernmental Personnel Act (IPA) to accelerate hiring. This would help scale digital talent recruitment by creating a central, empowered organization that focuses on a specific mission; concentrates expertise and funds; would help experts move in and out of government positions throughout their career; and can develop relationships with universities and private-sector companies.

1.6.4. Qualification Policies

Grant exemption from OPM General Schedule Qualification Policies for Specific Billets and Position Descriptions

AI practitioners applying for positions within the federal government and their hiring agencies are constrained by OPM minimum qualification standards. While these standards are important, and have increased fairness in hiring, they also prevent expert technologists that do not have master's degrees—and in some cases, bachelor's degrees or comparable work experience—from joining the government at a reasonable level of compensation. For example, a 19-year-old software developer or AI practitioner might have a proven track record on cybersecurity or in AI competitions, but can only enter the government as a GS-7. To reduce this hiring challenge, the government should allow agencies to exempt certain billets from OPM general schedule qualification policies, and instead allow local hiring managers to make an independent decision about both hiring and pay grade based on evaluations, prior work, alternative certification programs, or practical experience.

Stakeholder(s):
OPM

1.6.5. CyberCorps

Expand the CyberCorps: Scholarship for Service

The CyberCorps: Scholarship for Service (SFS) is a recruiting program designed to attract students studying IT, cybersecurity, and related fields into the USG. Expanding it could bring in more people with AI-related skills. It is managed by the National Science Foundation in partnership with the Office of Personnel Management and the Department of Homeland Security. Students enrolled in the program receive a scholarship in exchange for an obligation to work in an approved government agency for a period of time equal to the time covered by the scholarship. Seventy undergraduate and graduate institutions participate in SFS by selecting students for the

program, and since 2001, 3,600 students have received scholarships, 94% of whom went on to serve in government. Hiring typically takes place during annual online and in-person career fairs.

Stakeholder(s):
CyberCorps

1.6.6. STEM Corps

Establish a STEM Corps

A bipartisan group of members of the House Armed Services Committee have proposed H.R. 6526, STEM Corps Act of 2020. The proposal would authorize the appropriation of $5 million per fiscal year, with $500,000 for administrative costs and an advisory board. The program provides a maximum scholarship of $40,000 per student per year. Scholarship recipients would serve in different capacities within the DoD for a minimum of three years, with an option to either remain in the DoD or transfer to a private-sector company that has contributed to STEM Corps funding. The proposal requires participants to be paid at a rate not less than GS-6 for the first three years of their obligation and at not less than as a GS-10 during their fourth year. This proposal has the potential to significantly increase the number of personnel with STEM backgrounds in the DoD civilian workforce for a relatively low cost if a sufficient number of private-sector companies contribute. The potential for recipients to transfer to the private sector after three years of government service may create retention issues, but it may also serve as a mechanism to create bridges between the DoD and private sector companies.

Stakeholder(s):
STEM Corps

1.6.7. Digital Service Academy

Create a United States Digital Service Academy

The United States needs a new academy to train future public servants in digital skills. Civil servants play a critical and often underappreciated role in government. They hold much of the government's niche, long-term expertise. This is especially true for the digital expertise that is badly needed for the government to modernize. Methods like the competitive service and scholarship for service programs have helped recruit talent, but as the government's needs changed, those approaches will no longer address the full scope of the government's needs. Bolder measures are necessary to produce the broad, diverse, and technically educated workforce the government needs. Our proposed United States Digital Service Academy (USDSA) would be an accredited, degree-granting university that receives government funding,14 be an independent entity within the federal government, and have the mission to help meet the government's needs for digital expertise. It would be advised by an interagency board that would be assisted by a federal advisory committee composed of commercial and academic leaders in emerging technology.

Stakeholder(s):
United States Digital Service Academy

1.6.8. Civilian Careers

Establish Career Fields for Government Civilians in Software Development, Software Engineering, Data Science, Knowledge Management, and Artificial Intelligence

Government civilians play a critical role in the national security enterprise. A significant portion of the government's AI talent is likely to exist in the civilian workforce. Government civilians currently do not have career paths outside of research and development that allow them to focus on software development, data science, or AI for the majority of their career. This results in a highly limited ability to recruit talent from outside of government, an inability for an individual to focus on a skill set for an extended time, a lack of continuing education opportunities for these government civilians, and retention issues. It also causes the government to

struggle to identify and manage the software development, data science, and AI talent within its workforce. Digitally focused occupational series will better allow the government to track and manage its digital workforce, to attract new talent that wants to focus on a technical skill set, and to create new positions. The government should create software development, software engineering, data science, knowledge management, and AI occupational series. This combination of occupational series would significantly improve the government's ability to recruit and manage experts that will supervise the collection and curation of data, build human-machine interfaces, and help end users generate and act on data-informed insights. Many successful private-sector organizations use a version of this combination of skills. The government should follow their example.

Stakeholder(s):

Government Civilians

1.6.9. Military Careers

Establish Digital Career Fields for Military Personnel

Digital subject matter experts' inability to spend a career working on digital topics while serving in the military is arguably the single most important issue impeding military modernization.26 Much like their civilian counterparts, U.S. military personnel do not have career paths that allow them to focus on software development, data science, or AI for the majority of their career.27 The military has established career fields for doctors and lawyers that allow them to focus on a technical field, develop their skill over time, and advance within their service. The military is choosing not to do the same for many types of digital talent. While some of the services train some operational research and systems analysis (ORSA) personnel to perform machine learning and AI tasks, these personnel may be shifted to work on other ORSA tasks rather than AI. Phrased differently, AI practitioners have some background in ORSA, but not all ORSA personnel are trained to work in machine learning or AI.

Stakeholder(s):

Military Personnel

1.6.10. Tools, Data & Infrastructure

Provide Government Technologists with World-Class Tools, Data Sets, and Infrastructure.

Highly skilled technologists working in government are regularly denied access to software engineering tools. They have to jump bureaucratic hurdles to accomplish basic job functions such as sharing source code or downloading data sets, leading to frustration and periods of idling. To perform meaningful work in government, employees within the digital workforce need access to enterprise-level software capabilities at par with those found in the private sector. Capabilities include software engineering tools, access to software libraries, open-source support, and infrastructure for large-scale collaboration. Employees within the AI career field in particular will need access to further specialized resources such as curated data sets and compute power.

Stakeholder(s):

Government Technologists

1.7. CONFIDENCE

Establishing Justified Confidence in AI Systems ~ AI systems must be developed and fielded with justified confidence. The recommendations cover five issue areas: robust and reliable AI; human-AI interaction and teaming; testing and evaluation; leadership; accountability and governance. | Artificial intelligence (AI) systems must be developed and fielded with justified confidence. | If AI systems routinely do not work as designed, or are unpredictable in ways that can have significant negative consequences, then leaders will not adopt them, operators will not use them, Congress will not fund them, and the American people will not support them.

Achieving acceptable AI performance often is linked to the decision to accept some level of 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. Ultimately, they need to formulate an educated answer to this question: In the given circumstance, how much confidence in the machine is enough confidence? Five Key Challenges and Recommendations: The Commission has produced a detailed framework to guide the responsible development and fielding of AI across the national security community. 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.

1.7.1. Robustness & Reliability

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.

1.7.1.1. R&D

Focus more federal 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.

1.7.1.2. Risk, Documentation & Architecture

Consult interdisciplinary groups of experts to conduct risk assessments, improve documentation practices, and build overall system architectures to limit the consequences of system failure.

Such architectures should securely monitor component performance and handle errors when anomalies are detected4; 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.

1.7.2. Interaction & Teaming

Augment and complement human understanding and decision-making

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.

1.7.2.1. Research Labs

Pursue a sustained, multidisciplinary 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.

Stakeholder(s):

National Security Research Labs

1.7.2.2. Policies, Designs & Training

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

1.7.3. TEVV

Assurance that AI systems will perform as intended

Testing and Evaluation, Verification and Validation (TEVV) ~ 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.

1.7.3.1. Policies & Capabilities

Develop TEVV policies and capabilities to meet the changes needed for AI as AI-enabled systems grow in number, scope, and complexity

DoD should tailor and develop TEVV policies and capabilities to meet the changes needed for AI as AI-enabled systems grow in number, scope, and complexity in the Department. 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); updating or creating live, virtual, and constructive test ranges for AI-enabled systems; and restructuring the processes that underlie requirements for system design, development, and testing.

Stakeholder(s):

Department of Defense

1.7.3.2. Standards, Metrics & Tools

Provide standards, performance metrics, and tools for qualified confidence in AI models, data, and training environments, and predicted outcomes.

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.

Stakeholder(s):

National Institute of Standards and Technology

1.7.4. Leadership

Provide full-time staff dedicated to responsible AI

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.

Stakeholder(s):

DoD **National Security Agencies**

1.7.4.1. Leader

Appoint a full-time, senior-level Responsible AI lead in each department or agency critical to national security 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.

1.7.4.2. Expert Body

Create a standing body of multidisciplinary experts in the National AI Initiative Office.

Stakeholder(s):

Multidisciplinary AI Experts :
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.

National AI Initiative Office

1.7.5. Accountability & Governance

Monitor AI performance

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 instrumentation to do so. 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.

1.7.5.1. Policies

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

1.7.5.2. Oversight & Enforcement

Empower individuals to raise concerns about irresponsible AI development and institute comprehensive oversight and enforcement practices

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.

1.8. VALUES

Uphold Democratic Values

Upholding Democratic Values: Privacy, Civil Liberties, and Civil Rights in Uses of AI for National Security ~ With new models of techno-authoritarian governance gaining traction abroad, the United States must continue to serve as a beacon of democratic values. | The U.S. needs an approach for adopting AI domestically for national security that upholds and bolsters respect for democratic values, including privacy, civil liberties, and civil rights. Such an approach must strengthen, provide, and show leadership with regard to: 1) transparency; 2) approaches for AI system development and testing; 3) the ability to contest AI decisions; 4) oversight over AI development and use; and 5) legislative and regulatory controls on how AI is used. Our recommendations include immediate actions that the President, the Congress, and agencies should take; a comprehensive assessment by a Task Force that leads to reforms for AI governance and oversight; and areas for continued work. The recommendations are aimed at assuring that AI systems used by national security agencies uphold democratic values. Secondarily, the adoption of these recommendations can earn and inspire public confidence, both domestically and abroad, in uses of AI by national security agencies.

1.8.1. Reporting

Increase Public Transparency about AI Use through Improved Reporting

1.8.2. Privacy & Fairness

Develop & Test Systems per Goals of Privacy Preservation and Fairness

1.8.3. Due Process & Redress

Strengthen the ability of those aggrieved by AI to seek redress and have due process.

1.8.4. Oversight & Governance

Strengthen Oversight and Governance Mechanisms to Address Current and Evolving Concerns

2. TECHNOLOGY

Win the Technology Competition

2.1. STRATEGY

Develop a strategy for U.S. technological competitiveness and international cooperation

A Strategy for Competition and Cooperation ~ AI and other emerging technologies are driving the broader U.S. -China competition. The Commission urges the creation of a new White House body to develop a strategy for U. S. technological competitiveness and to identify areas for international cooperation. | The United States should advance a comprehensive policy on China that promotes and protects a rules-based international order. By investing in U.S. competitiveness and resilience at home, safeguarding critical technologies, and deepening coordination with allies and partners, the United States can pursue cooperation with China—where it is in the national interest and from a position of strength. Properly sequenced and resourced, such a strategy would generate solutions to global challenges and leverage formal diplomatic dialogue to address critical issues around emerging technology.

2.1.1. Dialogue

Establish a High-Level U.S.-China Comprehensive Science and Technology Dialogue (CSTD)

The United States should establish a regular, high-level technology dialogue with China that benefits the American people, remains faithful to our allies, and presses China to abide by international rules and 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, public health, and natural disasters; and
- Provide a forum to air a discrete set of concerns or friction points around specific uses of emerging technologies while building relationships and establishing process between the two nations. The United States should be clear-eyed that the dialogue will not solve all our differences with China. The CSTD should be results-oriented, and it should achieve concrete outcomes for the American people.

2.1.1.1. Targeted Areas

Identify targeted areas of cooperation on emerging technologies to solve global challenges such as climate change, public health, and natural disasters

2.1.1.2. Relationships & Frictions

Provide a forum to air a discrete set of concerns or friction points around specific uses of emerging technologies while building relationships and establishing process between the two nations.

2.2. TALENT

Invest in AI talent pipelines

The Talent Competition ~ The United States is in a global competition for scarce AI and science, technology, engineering, and mathematics (STEM) talent. 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. | The United States must dramatically invest in its artificial intelligence (AI) talent pipelines in order to remain at the forefront of AI now and into the future. It is imperative that the United States strategically invest in science, technology, engineering, and mathematics (STEM) education at all levels and improve the immigration system to allow for more AI talent to enter and remain in the United States. Therefore, this Blueprint for Action is organized into two broad categories of recommendations for strengthening the U.S. talent pipeline: the U.S. education system and immigration. Talent Pipeline: U.S. Education System ~ Investments in STEM education are a necessary part of increasing American national power and improving national security. This requires the United States to reform its education system to produce both a higher quality and quantity of graduates.

2.2.1. Defense Education Act

Pass a New National Defense Education Act

In response to the Soviet launch of Sputnik in 1957, the United States passed the National Defense Education Act (NDEA) in 1958 to extend U.S. leadership in education and innovation. The NDEA promoted the importance of science, mathematics, and foreign languages for students, authorizing more than $1 billion 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 bill; 3.6 million students attended college in 1960, and by 1970, it was 7.5 million. This act helped America win the Space Race and accelerated our ability to innovate, and it is widely regarded as one of the most successful pieces of education legislation in U.S. history. Now is the time for a new NDEA. The NDEA greatly increased the number of Americans with a college degree, expanded the number of math and science teachers to meet the demand of the K-12 system after the postwar baby boom, and was focused on defensecentric fields, particularly a deficiency in mathematicians. The impacts of federal spending on higher education today are echoes of the investments made in the late 1950s by the Eisenhower administration. The United States needs a second NDEA (NDEA II) in order to address the current digital talent gap and prevent the United States from falling behind in the race for AI and STEM talent.

2.2.2. Statistics & Computer Science

Require Statistics in Middle School and Computer Science Principles in High School

Stakeholder(s):

Middle Schools **High Schools**

2.2.3. O-1 Visas

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. O-1 visas are valid for three years and can be renewed annually an unlimited number of times. There is also no limit on the number of visas issued per year. Currently, about 15,000 to 18,000 new O-1 visas are issued annually. For these reasons, the O-1 visa is generally a more flexible visa category than the H-1B visa, which is, with some exceptions, capped in duration and number. While O-1 visas provide many advantages, they are a poor fit for many highly skilled workers due to the uncertainty of their criteria and the administrative burden of the application and adjudication process. Adjudicators determine an applicant's eligibility through subjective assessments of

whether applicants received nationally recognized prizes, have been published in major outlets, have done original work of major significance, and meet other similar criteria. 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.

2.2.4. International Entrepreneur Rule

Implement and Advertise the International Entrepreneur Rule

The International Entrepreneur Rule (IER) allows 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." The IER would be relatively easy for the Executive Branch to implement and is more directly tied to job creation than most other immigration proposals, making it more helpful to most Americans.

Stakeholder(s):
International Entrepreneurs

2.2.5. Job Portability

Expand and Clarify Job Portability for Highly Skilled Workers

The Department of Homeland Security (DHS) published a final rule in November 2016 that made a number of reforms to improve temporary work visa programs, including some measure of relief for workers tethered to the employer sponsoring their green card petition during a potentially decades-long waiting period. The rule allows workers on H-1B, O-1, and other temporary work visas to obtain open-market work permits for a one-year renewable period under compelling circumstances. Compelling circumstances include:

- Serious illness or disability faced by the worker or his/her dependents,
- Employer retaliation against the worker,
- Other substantial harm to the worker, and
- Significant disruption to the employer. The criteria for compelling circumstances are too limited and ambiguous. Expanding visa holders' ability to obtain a work permit would allow for greater rates of entrepreneurship, tighter skill-matching with new employers, and for visa holders to negotiate compensation on a level playing field with domestic workers.

Stakeholder(s):
Highly Skilled Workers

2.2.6. Green Cards

Recapture Green Cards Lost to Bureaucratic Error

Congress mandates annual caps on the number of green cards that may be issued to certain family-based immigrants (226,000) and employment-based immigrants (140,000). Because federal agencies do not want to exceed the annual green card caps, they generally issue fewer green cards than they are allowed to. Due to this trend, as of 2009, the Federal Government had not issued more than 326,000 green cards. The number today is likely higher, but DHS has not published updated statistics

2.3. INNOVATION

Accelerate AI Innovation

Accelerating AI Innovation ~ To remain the world's leader in AI, the U.S. government must renew its commitment to investing in America's national strength—innovation. This will require making substantial new investments in AI R&D and establishing a national AI research infrastructure that democratizes access to the resources that fuel AI. | The United States remains the world's artificial intelligence (AI) leader. However, trends within the United States indicate underlying weaknesses. The Federal Government holds the responsibility to provide strategic direction and long-term resources to strengthen the nation's foundation for AI innovation. The United States—through government leadership, and in partnership with industry and academia—must increase the diversity, competitiveness, and accessibility of its AI innovation environment to ensure continued leadership.

2.3.1. R&D Funding

Scale and Coordinate Federal AI R&D Funding

The United States must reinforce the foundation of technical leadership in AI by enacting a bold, sustained federal push to invest in AI R&D to foster a nationwide landscape of AI innovation and drive breakthroughs in the next generation of AI technologies by establishing a National Technology Foundation, funding AI R&D at compounding levels, establishing additional National AI Research Institutes, and making big bets on talent and innovative ideas.

2.3.1.1. Technology Foundation

Establish a National Technology Foundation

In the wake of Russia's successful launch of the Sputnik satellite in 1957, Congress made significant investments in the National Science Foundation (NSF) to shore up U.S. leadership in science and technology. Since then, the NSF has supported research across the frontiers of science and engineering, funding efforts that contributed to the development of the Internet, smartphones, and additive manufacturing.2 However, in today's heightened geopolitical technology competition, even bolder action is needed to meet the promise of emerging and disruptive technologies like AI, drive U.S. innovation toward the national interest, and secure our economic future. The Commission recommends the creation of a National Technology Foundation (NTF) as an independent federal agency and sister organization to the NSF to provide the means to move science more aggressively into engineering and scale innovative ideas into reality. This will require an organization that is structured to accept higher levels of risk and empowered to make big bets on innovative ideas and people. It also demands an emphasis on the transition of technology from the lab to the market.

2.3.1.2. Prioritization & Funding

Increase Federal Funding for Non-Defense AI R&D at Compounding Levels and Prioritize Key Areas of AI R&D

Research is the linchpin of America's global leadership in AI. However, current federal funding is not adequate to meet the growth of the field, let alone support its continued expansion. The Trump Administration's proposed budget for non-defense AI R&D in Fiscal Year 2021 was $1.5 billion, a growth from around $1 billion spent in Fiscal Year 2020. Further building on this investment, Congress included the National AI Initiative Act of 2020 in the National Defense Authorization Act for Fiscal Year 2021, which creates a structure for a more strategic approach to harnessing AI and includes authorization for additional investments in AI at the NSF, Department of

Energy (DoE), National Institute of Standards and Technology (NIST), and the National Oceanic and Atmospheric Administration (NOAA).

2.3.1.3. AI Research Institutes

Triple the Number of National AI Research Institutes

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—topics for which were determined through coordination with interagency and community stakeholders. NSF 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.18 Congress took steps to support the initiative through the National AI Initiative Act of 2020, which formalizes the effort, provides all agencies the authority to financially support formation of a National AI Research Institute, and directs NSF to bring together the institutes as an "Artificial Intelligence Leadership Network."

Stakeholder(s):

National AI Research Institutes

2.3.1.4. Talent & Transformation

Invest in Talent that Will Transform the Field

Top talent in AI is a scarce commodity, and investing in talent holds the potential to not only unlock breakthroughs in the science and application of AI but also to attract and retain top talent in the United States. Similarly, investing in research initiatives conducted by integrated, multidisciplinary teams is a proven mechanism to prompt breakthroughs, address complex problems, and challenge the status quo. The launch of an AI Innovator Award and complementary team-based AI award would strengthen the ability of federal AI research funding to push the boundaries of the field, providing a mechanism to complement ongoing investments in incremental progress with bets on revolutionary breakthroughs.

2.3.2. Research Infrastructure

Expand Access to AI Resources through a National AI Research Infrastructure

If not addressed, the growing divide between "haves" and "have nots" in AI R&D will degrade the long-term research and training functions performed by U.S. universities, limit the ability of small businesses to innovate, and exacerbate the lack of diversity in the field. While developments in the past five years have dramatically increased access to baseline ML tools and cloud-based computation, progress on the cutting edge of many important AI approaches requires significant amounts of data and computing power, expensive infrastructure, and substantial hardware and software engineering. The United States should foster the world's leading environment for AI innovation through democratized access to AI R&D that supports more equitable growth of the field and expansion of AI expertise across the country; enables application of AI to a broad range of fields of science and engineering, commercial sectors, and public services; and fuels the next waves of innovation.

2.3.2.1. AI Research Resource

Launch the National AI Research Resource

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. Availability and type of compute resources have been found to levy "outsized" influence in the direction of research pursued by researchers, as has the ascendency of the well-equipped firms in shifting the overall direction of AI research toward applied, "narrow AI" efforts. To bridge the compute divide, the Federal Government should establish a National AI Research Resource (NAIRR) to provide verified researchers and students with access to compute resources, co-located with AI-ready government and non-government data sets, educational tools, and user support. This infrastructure should leverage public-private partnerships and cutting-edge private-sector technology and build on existing government efforts—avoiding high startup costs of a government-run data center. Congress has taken the first step in the Fiscal Year 2021 National Defense Authorization Act, implementing a component of the Commission's prior recommendation to create a task force to develop a roadmap for a NAIRR. The result of this effort will be due to Congress 18 months after appointment of task force members.

2.3.2.2. AI Testbeds

Create a Network of National AI Testbeds to Serve the Academic and Industry Research Communities

Sponsored through various federal agencies, this network of national AI testbeds would provide real-world, domain-specific resources open to the academic, business, and government research communities to drive basic and applied research to address complex problems and develop robust, usable AI systems ripe for commercialization (for example, a self-driving vehicle test range, an instrumented humanitarian aid and disaster relief test site, or an instrumented home environment). Such resources would help establish and maintain benchmarking standards that enable measurable research progress through comparable approaches and reproducibility testing. Testbeds should support experimentation with both novel software and hardware, equipped with rich simulation capabilities to model the physical world. Supported by simulated, live, and blended environments, these platforms would support research and experimentation that tackles open-ended, real-world problems. Furthermore, they should be architected to collect valuable data that could be made accessible to the community for training and evaluation, providing additional fuel for progress.

Stakeholder(s):

Academic Research Community **Industry Research Community**

2.3.2.3. Training Data

Invest in Large-Scale, Open Training Data

Data is critical currency for today's popular AI approaches. Promising work in the realm of low-shot learning, semi-supervised learning, and learning from synthetic data provides glimpses of a future in which performance of an AI system is not directly tied to big data, and the Federal Government should continue to prioritize funding for research in these areas. However, balancing these bets on the future with investments in resources to further U.S. leadership in the current leading AI approaches would strengthen the foundation of both current and future AI-based technology and applications.

2.3.2.4. Knowledge Network

Sponsor an Open Knowledge Network

Open knowledge networks (or repositories) with massive amounts of world knowledge could fuel the next wave of AI exploration, driving innovations from scientific research to the commercial sector. Today, only the biggest tech companies have the resources to develop significant knowledge graphs and networks. Various federal agencies have invested in specialized, domain-specific knowledge networks that could provide a starting point for an open knowledge network. Beginning with a push to federate and map together existing specialized

knowledge networks and government data platforms, and then building in real-world knowledge and context, the government could sponsor an Open Knowledge Network that would serve verified U.S.-based companies and researchers of all backgrounds to use world knowledge to develop AI systems that operate effectively and efficiently. This type of resource, particularly if paired with the complementary research infrastructure above, could unlock frontiers of technology yet unexplored.

2.3.3. Public-Private Partnership

Leverage Both Sides of the Public-Private Partnership

U.S. companies are at the forefront of AI R&D, and their investments benefit consumers globally through the rapid development and adoption of AI-enabled products. But the impact of AI-enabled products on U.S. society and national security has largely come as an afterthought. The speed of technology development by the private sector has vastly outpaced federal policies and regulations. To address these challenges, the public and private sector must share responsibility for the safety, security, and well-being of Americans. The following recommendations would make the government a better partner for industry, broaden the benefits of strategic emerging technologies like AI through regional innovation clusters, and expand opportunities to access AI research and education through private-sector philanthropy.

2.3.3.1. Markets

Create Markets for AI and Other Strategic Technologies

The government's buying power cannot compete with a global consumer market, but it can influence investment decisions in technologies essential to overall U.S. technical leadership. Many potential public-sector applications of AI, such as education and labor, fall under agencies with limited R&D budgets. As the government increases investment in basic research, it must also fully leverage its purchasing power to support AI and other strategic technologies. The scale of government funding can influence the research priorities and viability of early-stage startups, which often succeed or fail in the first year; and, if leveraged collectively, it can draw private-sector resources toward areas of strategic priority. This makes investors and technology companies important partners for AI R&D that can build future defense and national security capabilities. Yet the government remains a difficult customer—especially for small and medium-sized businesses—because of its complex contracting process and unique requirement. Making the U.S. government a more compelling customer and effective buyer of commercial technology will help drive technology development in the commercial sector that is in the national interest. It will also assist the government in almost every aspect of its mission, from providing basic public services to driving economic policy and protecting national security.

2.3.3.2. Clusters

Form a Network of Regional Innovation Clusters Focused on Strategic Emerging Technologies

Competition is critical to a vibrant national security innovation base. If a strategic industry lacks competition, one wrong bet by an incumbent can place the nation's technological leadership in jeopardy. The U.S. government should create an environment in which innovative startups are able to disrupt inefficient or outdated ways of doing business and grow into industry leaders themselves. The right mix of policies and incentives can help firms overcome mounting barriers to entry at the cutting edge of emerging technologies like AI. This approach will promote innovation in industries that are essential to U.S. leadership in AI and the nation's economic and technological competitiveness more broadly.

2.3.3.3. Competitiveness Consortium

Establish a Private Sector–Led Competitiveness Consortium

The private sector shares responsibility with the government to strengthen the foundations of the R&D ecosystem that underpins breakthroughs they will commercialize and the training pipeline needed to meet their increasing demand for technical talent. Companies are already struggling to find these qualified applicants for technical roles, with one estimate showing more than 400,000 open computing jobs nationwide. Furthermore, as described above, researchers in academia who will undertake the high-risk, high-gain research that will push the frontiers of the field are finding themselves locked out from the computing and data resources needed to fuel this work. How well the nation addresses this looming challenge has widespread implications for the economy, society, and U.S. global competitiveness.

Stakeholder(s):
Competitiveness Consortium

2.3.4. Challenges

Tackle Some of Humanity's Biggest Challenges

If the investments detailed above are implemented, they will set the conditions to harness AI to tackle some of the biggest challenges in science, society, and national security. Examples of promising initiatives that could improve societal well-being and advance scientific frontiers include, but are not limited to:

2.3.4.1. QOL

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.

2.3.4.2. Education & Learning

Revolutionize education and lifelong 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.

2.3.4.3. Energy

Transform energy management.

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

2.3.4.4. 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 cleanup in the wake of natural or man-made disaster, providing force-multiplying support to first responders and hazardous materials professionals.

2.4. INTELLECTUAL PROPERTY

Safeguard U.S. national security interests

Intellectual Property ~ China is both leveraging and exploiting intellectual property (IP) policies as a critical tool within its national strategies for emerging technologies. 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. | America's intellectual property (IP) laws and institutions must be considered as critical components for safeguarding U.S. national security interests, including advancing economic prosperity and technology competitiveness. Prioritization of IP policy is especially important given China is both leveraging and exploiting IP policies as a tool within its national strategies for emerging technologies. The United States must, at a minimum, articulate and develop national IP reforms and policies with the goal of incentivizing, expanding, and protecting artificial intelligence (AI) and emerging technologies,1 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.

2.4.1. Policies & Regimes

Develop and implement national IP policies and regimes to incentivize, expand, and protect AI and emerging technologies as part of national security strategies.

2.4.2. Considerations

Assess and examine IP considerations

The Secretary of Commerce should assess and examine the following non-exhaustive list of "IP considerations," in coordination with the Under Secretary of Commerce for IP and the Director of the USPTO, as part of developing and proposing reforms and new IP policies and regimes to the Vice President.

Stakeholder(s):

Secretary of Commerce

Director, USPTO

Under Secretary of Commerce for IP

Vice President

2.4.2.1. Innovation

Assess and articulate the impact of current patent eligibility laws on innovation in AI and emerging technologies

Patent Eligibility: The Secretary of Commerce should assess and articulate the impact of current patent eligibility laws on innovation in AI and emerging technologies from an economic, trade, and national security policy perspective to better inform the legislative and agency efforts on patent eligibility reform. America's IP regime has spurred American ingenuity since the late 18th century. By protecting "any new and useful process, machine, manufacture, or composition of matter" through stable legal institutions governed by the rule of law,

inventors and investors have relied on America's IP system to provide the certainty necessary to justify large and risky R&D investments, which are critical for technologies. A strong and robust patent system is equally critical to incentivizing American innovation in AI and emerging technologies that affect national security.9 Unfortunately, recent patent eligibility court rulings have narrowed the scope of inventions that are eligible for patent protection. This has resulted in a broad swath of innovation that is now ineligible for patent protection in both digital technologies and biopharma, among others. The legal uncertainty for U.S. innovators and companies as to whether their inventions will be eligible for patent protection or susceptible to invalidation once granted is pervasive. This uncertainty in turn has impacted investments in AI and technologies critical to national security. Empirical studies have proven that patents are causally linked to venture capital investments in startups, and, as a result, are causally linked to the success of startups. Recent reports, however, reveal that investments in patent-intensive U.S. startups that develop critical technologies (e.g., computer hardware, semiconductors, medical devices and supplies, and pharmaceuticals and biotechnology) have declined relative to non– patent-intensive companies. This is consistent with investors consistently reporting that patent eligibility is a key factor in their decisions whether to invest in a particular company's technologies or bring a new product to market.

Stakeholder(s):

Secretary of Commerce

2.4.2.2. Narrative

Address how the United States might best counter China's efforts to shape the narrative that it is winning the innovation competition

Counter China's narrative on winning the innovation competition: The Secretary of Commerce, in coordination with relevant departments and agencies (e.g., Department of State, USTR), should address how the United States might best counter China's efforts to shape the narrative that it is winning the innovation competition based in part on its patent application filings and other interventions in its technology markets. China has become the domestic forum with the highest number of patent application filings, and China's companies and inventors are the most prolific AI patent application filers globally. This benchmark helps to shape the narrative that China has become the leader in innovation because intensive patenting has been shown to generally correlate to economic growth. China also is garnering this reputation when it comes to emerging technologies such as AI. Sources claim that China is outpacing the United States in filing worldwide AI-related patent applications. However, high levels of patenting output is not necessarily indicative of high levels of inventive output. Specifically, non-market factors driven by state-sponsored interferences can distort filings. Moreover, China often files patents as a "numbers game," which can lead to mischaracterizing its technological prowess. Similarly, China's 5G companies declare the most patents as "standard essential," appearing to marry China's concerted, top-down strategy to advance its AI and emerging technology agenda by influencing international standards setting with its goals to dominate numeric benchmarks. The Secretary of Commerce should examine what measures need to be undertaken to counterbalance the narrative of China's technological dominance based on selective patenting data.

Stakeholder(s):

Secretary of Commerce **Department of State**

USTR

2.4.2.3. Patent Examination

Assess whether the USPTO requires additional resources to ensure high-quality patent examination and recommend policies to address any concerns

Impact of China's patent application filings on USPTO and U.S. inventors: The Secretary of Commerce, in coordination with the USPTO Director, should assess whether the USPTO requires additional resources, both human and technical, to ensure high-quality patent examination and recommend policies to address any

concerns. In doing so, the Secretary of Commerce should assess the impacts of increased filings from China and AI-generated 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). The large body of often low-quality prior art created by China's high-volume patenting has the potential to adversely impact global patent examination systems, including those of the USPTO. At the same time, U.S. inventors may face hurdles in patenting around massive amounts of low-quality Chinese prior art. The USPTO has also noted that stakeholders have raised the issues of whether AI may generate a proliferation of prior art, making it difficult to find relevant prior art for examination.

Stakeholder(s):

Secretary of Commerce **U.S. Inventors**

USPTO

2.4.2.4. Partnerships

Assess any impediments to the IP contractual ecosystem to strengthen AI partnerships

Impediments to AI public-private partnerships and international collaboration: The Secretary of Commerce should assess any impediments to the IP contractual ecosystem to strengthen AI partnerships among national security departments and agencies, industry, and international collaboration. This should include assessing and addressing ambiguities in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement relevant to AI and data. AI development presents unique IP contractual issues. For example, industry AI developers will likely need access to relevant U.S. Government training data to develop AI-enabled government solutions or applications. If the solution or application is dual-use, the private entity may want to provide a license for the U.S. Government agency to access the AI application, but retain the IP in the AI model to license to others. But there are unanswered questions as to whether the U.S. Government agency has any IP rights or ownership in the model that was trained on its data. The U.S. Government agency may also want to retain IP rights in order to avoid "vendor lock." These outstanding questions about IP rights and ownership issues could also arise in international AI system R&D collaboration, where impediments can be amplified by conflicting national laws on IP and/or data protections.

Stakeholder(s):

Secretary of Commerce

2.4.2.5. Data

Assess whether there is a need for additional IP-type of protections for data and propose policies and/or legislation if protection is deemed necessary

IP protection for data: The Secretary of Commerce should assess whether there is a need for sui generis protection or additional IP-type of protections for data and propose policies and/or legislation if protection is deemed necessary. Data is critical to AI and machine learning (ML), but gaps may exist in current protection regimes afforded by patent or copyright. Inadequate protections for data may disincentivize the necessary investments in developing these critical data sets as well as public disclosure and sharing agreements. While protections for data might be a future need, the U.S. should be proactive in assessing and addressing the necessity of such protections. The Secretary of Commerce also should explore ways to protect and incentivize creation of data sets while allowing the data to be shared at some point, particularly with smaller entities that might not otherwise be able to enter the market. An analysis of the strengths and weaknesses of the European sui generis database protections should inform this assessment.

Stakeholder(s):

Secretary of Commerce

2.4.2.6. Theft

Assess and identify additional efforts that the Executive Branch should undertake to counter IP theft threats

Combat IP theft: The Secretary of Commerce, in coordination with relevant departments and agencies (e.g., USTR, Intellectual Property Enforcement Coordinator, the National Science Foundation, the Office of Science and Technology Policy, as well as the Departments of Homeland Security, Justice, and State) should assess and identify additional efforts that the Executive Branch should undertake to counter IP theft threats, including actions in collaboration with allies and partners.38 In particular, the Secretary of Commerce should clearly articulate that the U.S. counter–IP theft strategy will contain both criminal and civil economic dimensions. The Department of Commerce should utilize all available tools for establishing a deterrence regime to punish firms guilty of stealing U.S. IP and deter future IP theft to level the playing field for U.S. and allied firms. These tools should include placing offending companies on the Bureau of Industry & Security entity list, blocking visas of key employees, or levying tariffs against products derived from stolen IP. Solutions that should be explored include training for allies and partners to stop counterfeits at borders and efforts to increase individuals' respect for IP and recognition of and ways to avoid counterfeits. In addition, the Secretary should assess methods and means for strengthening and updating existing mechanisms available to American victims of trade-secret theft, including reintroducing legislation to strengthen the Economic Espionage Act by, for example, increasing damages available to trade-theft victims and extending the statute of limitations.

Stakeholder(s):

Secretary of Commerce

USTR

Intellectual Property Enforcement Coordinator

National Science Foundation

Office of Science and Technology Policy

Department of Homeland Security

Department of Justice

Department of State

2.4.2.7. Inventorship

Assess the need for policy changes for issues raised by AI-generated inventions and creations

Inventorship by AI: The Secretary of Commerce should assess the need for policy changes for issues raised by AI-generated inventions and creations, particularly as technologies evolve. The USPTO has determined that under current legal doctrine, an inventor must be a natural person and denied a patent application naming a machine as the inventor. The U.S. is not alone in this position. The USPTO also issued extensive requests for

public comments on a variety of AI IP policy issues, including AI's impact on inventorship and ownership, as well as impacts on non-patent IP protections, such as copyright. As a result, the USPTO issued a comprehensive report of public views on AI and IP policy. The majority of commenters agreed that, given that current AI capabilities are limited to "narrow AI" (AI systems that are trained and perform individual tasks in well-defined domains) and artificial general intelligence is not yet a reality, current AI could neither invent nor author without human intervention. The Secretary of Commerce should consult with allies and partners to ensure continued harmonization around the various IP issues raised by AI-generated inventions and creations and gain an understanding of China's strategies for addressing these issues, particularly as AI technologies move past narrow AI.

Stakeholder(s):

Secretary of Commerce **USPTO**

2.4.2.8. Global Alignment

Develop global disincentives for IP theft and alleviate any inconsistencies in patent regimes

Global IP alignment: The Secretary of Commerce, in coordination with relevant departments and agencies (e.g., USPTO, IPEC, USTR, Department of Defense, Department of State), should work with partners and allies to develop global disincentives for IP theft and alleviate any inconsistencies in patent regimes that make it overly difficult for companies to protect their patents in multinational markets. In doing so, the Secretaries should leverage the Commission's recommendation that the United States and allies—through the Emerging Technology Coalition—explore coordinated approaches to IP (as part of the NSCAI-proposed critical area No. 4: Promoting and Protecting Innovation), including a mutual agenda within the WIPO's Conversation on AI and IP and forums with broader mandates. The Secretaries also should assess whether current forums for dialogues on global IP alignment are sufficient or whether new forums or venues are necessitated, particularly given any changes to domestic IP policies or regimes identified during the review of the other IP considerations. For example, if the U.S. determines new protections or policies are needed for data, it may need to work with key allies and partners—bilaterally and multilaterally—to ensure global harmonization.

Stakeholder(s):

Secretary of Commerce **USTR**

USPTO **Department of Defense**

IPEC **Department of State**

2.4.2.9. Innovation & IP Ecosystems

Assess whether additional Executive Branch efforts are necessary to expand the innovation base and democratize access to and create more jobs in the innovation and IP ecosystem

Democratize innovation and IP ecosystems: The Secretary of Commerce should assess whether additional Executive Branch efforts are necessary to expand the innovation base and democratize access to and create more jobs in the innovation and IP ecosystem.

Stakeholder(s):

USPTO :
The USPTO, in collaboration with the Secretary of Commerce, has undertaken initiatives to expand the U.S. innovation base by creating the National Council for Expanding American Innovation (NCEAI) to develop a comprehensive national strategy to increase equity and fuel the U.S. innovation ecosystem by encouraging, empowering, and supporting all future innovators.

Secretary of Commerce :
The Secretary of Commerce should ensure that the USPTO has the full support of the Executive Branch in these initiatives. As part of the NCEAI initiative, the Secretary of Commerce also should focus on assessing and identifying potential actions and tools that can fast-track processes and streamline guidance for startups seeking IP protections and ensuring resources for assisting small and medium-sized enti-

— continued next page

Stakeholders (continued)

ties. Such a focus is particularly important when comparing the impact of litigation costs and potentially overly burdensome processes in the U.S., relative to other countries, on U.S. inventors' decisions to pursue IP protections in the United States

2.4.2.10. "Standard Essential" Patents

Assess policies by which the U.S. can serve a leadership role in and ensure U.S. firms are able to fully participate in the processes by which "standard essential" patents are claimed and asserted

"Standard essential" patents process: The Secretary of Commerce, in coordination with relevant departments and agencies (e.g., USPTO, NIST, and the Department of State), should assess policies by which the U.S. can serve a leadership role in and ensure U.S. firms are able to fully participate in the processes by which "standard essential" patents are claimed and asserted. This would help ensure the continuing legitimacy of the standard-setting process, a privately developed method for efficiently coordinating development and deployment of new technologies in the marketplace, and deflect Beijing's attempt to dominate or manipulate these processes through its own coordination of firms from China. Chinese Communist Party leadership has articulated a linkage between patent leadership in emerging technologies like AI and the standards-setting processes for these same technologies. Current trends confirm China's intention to use both patents and standards to lead in technological innovation. Additional mechanisms may be necessary to protect the integrity of international standards-setting as well as to protect and promote U.S. innovation, such as identifying efforts by foreign governments to influence, directly or indirectly, standard-setting organizations. This would also include identifying foreign governments subsidizing or otherwise incentivizing the over-declaration of patents as "standard essential" or creating barriers to U.S. participation in foreign standard-setting bodies. The Secretary of Commerce also should explore how the U.S. government might support smaller U.S. companies and inventors fully participating in the standard-setting process and encourage the observation of licensing or legal disputes in foreign jurisdictions by U.S. government officials from U.S. Embassies and Missions. Relatedly, the Secretary of Commerce, in coordination with the Director of the USPTO, should assess foreign court rulings on licensing that may impact U.S. national sovereignty to determine a coherent U.S. position or response.

Stakeholder(s):

Secretary of Commerce | **NIST**

USPTO | **Department of State**

2.5. MICROELECTRONICS

Revitalize domestic semiconductor fabrication

Microelectronics ~ U.S. leadership in microelectronics is critical to overall U.S. leadership in AI. But the United States is losing its edge and must take bold action to stay at least two generations ahead of potential adversaries and revitalize domestic semiconductor fabrication. | Regaining microelectronics leadership requires meeting an explicit objective: Stay at least two generations ahead of China in state-of-the-art microelectronics and maintain multiple sources of cutting-edge microelectronics fabrication in the United States. To do this, the Executive Branch must prepare and implement a National Microelectronics Strategy while Congress simultaneously institutes new tax credits, subsidizes the construction of semiconductor manufacturing facilities, and grows federal microelectronics R&D and infrastructure funding. Achieving this goal will require roughly $30 billion in additional federal funding, but these funds should attract more than five times as much privatesector investment. Additional federal funding on this scale will likely boost economic activity domestically and could add more than $100 billion to U.S. gross domestic product (GDP).1 Inside the U.S. government, agencies must also expand access to trustworthy, high-performance microelectronic components by shifting from serial to concurrent development of hardware and software to catch up to the commercial sector and make use of new microelectronics produced in the United States.

2.5.1. Executive Order

Issue an Executive Order on Microelectronics Strategy and Leadership

The United States needs a National Microelectronics Strategy to coordinate semiconductor policy, funding, and incentives within the Executive Branch and externally with industry and academia.

Stakeholder(s):
President of the United States

2.5.2. Fabrication

Revitalize Domestic Microelectronics Fabrication

Existing U.S. incentives offset the cost of semiconductor foundry construction attributable to capital expenses, operating expenses, and taxes by 10% to 15%. Yet additional tax credits and subsidies are needed to make the United States a globally competitive market for semiconductor manufacturing, especially leading-edge logic facilities. Other leading semiconductor manufacturing nations such as South Korea, Taiwan, and Singapore offer 25% to 30% cost reduction, roughly double what the United States currently offers. This gap in incentives is one driving factor behind the lack of an advanced logic merchant foundry in the United States. Closing the gap will encourage U.S. firms to construct facilities domestically while also attracting foreign firms. In fact, a program of the size described here is projected to attract roughly 14 new fabs in the United States over 10 years. 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 U.S. policies prohibiting the export of such equipment to China. A refundable investment tax credit should be instituted in combination with funding for federal grants for the expansion, construction, and modernization of SME authorized in the NDAA.

2.5.3. Research & Infrastructure

Double Down on Funding for Research and Infrastructure to Lead the Next Generation of Microelectronics

Four research arms of the U.S. government focused on medium- and long-term microelectronics breakthroughs through engagement with academia and industry are the Department of Energy (DOE), the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (NSF), and the Department of Commerce. Their suite of existing programs, such as DARPA's Electronics Resurgence Initiative (ERI), are targeting the right research areas but must be expanded by an order of magnitude to achieve the necessary breakthroughs to maintain U.S. competitiveness. Additional funding should support not only research projects, but also the capital-intensive infrastructure for microelectronics development, including the National Semiconductor Technology Center and advanced packaging prototyping programs authorized in the FY 2021 NDAA. In line with the existing focus areas of these programs and the Commission's prior recommendations, funding should pursue breakthroughs in promising technologies such as 3D chip stacking, photonics, carbon nanotubes, gallium nitride transistors, domain-specific hardware architectures, electronic design automation, and cryogenic computing. In particular, funding should prioritize the development of manufacturing equipment and tools to reach 3nm and beyond at production scale. However, this funding should not solely be directed to classical computing technologies. The U.S. government should also support efforts to research and develop hybrid quantum-classical techniques that leverage noisy intermediate-scale quantum computers. The Commission offers detailed recommendations on this subject in Chapter 16 of this report.

2.5.4. Trust & Agility

Continue DoD's Trusted Microelectronics Program and Adopt Agile Hardware Development

Semiconductor manufacturing has moved offshore, expanding threat vectors to hardware security and leaving the U.S. government unable to trust sensitive electronic components it needs for defense systems. And while the U.S. government is now recognizing that it must take steps to adopt modern software practices, there has been less attention on incorporating hardware into the agile development process. Both issues require attention from the Department of Defense (DoD) and other government agencies. The U.S. government needs to inject security and agility into its microelectronics acquisition and development process to leverage the best technology possible for defense systems.

Stakeholder(s):

Department of Defense

2.6. TECHNOLOGY PROTECTION

Protect ideas, hardware, and companies

Technology Protection ~ As the margin of U.S. technological advantage narrows and foreign efforts to acquire American know-how and technology increase, the United States must reexamine how it can protect ideas, hardware, and companies, without unduly hindering innovation and research. | This Blueprint for Action provides detail for how the United States must craft technology protection policies to ensure it retains existing advantages in technology areas with national security applicability but avoids stifling innovation. U.S. research, entrepreneurship, and talent development remain the key ingredients of success. However, as dualuse technologies become more important to U.S. national security, 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 its commercial and academic ecosystem from foreign exploitation. The United States faces substantial challenges in adapting its technology protection regime to address threats related to emerging, dual-use technologies such as artificial intelligence (AI) without hindering the free flow of commerce or its open research environment, both of which are systemic U.S. strengths. This Blueprint for Action proposes reforms for (1) modernizing export controls and investment screening and (2) protecting the U. S. research environment in ways which are consistent with U.S. national security, commercial interests, and values. Modernizing Export Controls and Investment Screening ~ How the U.S. Government regulates competitors' access to sophisticated U.S. technologies with national security applications will be one of the principal challenges of current and future geoeconomic competition. The United States must modernize its export control and investment screening regimes to better address the challenges posed by dual-use emerging technologies, to include AI. These reforms are necessary to allow the government to implement technology protection policies in ways which maximize their impact on the military capabilities of U.S. strategic competitors and minimize any resulting harms to U.S. industry.

2.6.1. Dual-Use Technology

Clearly State the Overarching Principles to Guide Future U.S. Dual-Use Technology Protection Policies

The U.S. Government must clearly state the principles that will guide future U.S. decisions regarding policies to protect critical technologies. This will enable more consistent and cohesive technology protection policies and provide clarity to industry regarding how the government intends to utilize these regulatory tools in the current competitive environment, thereby reducing uncertainty for U.S. businesses. No such framework currently exists.

2.6.2. Capacity

Enhance U.S. Capacity to Carry Out Effective Technology Protection Policies

Departments and agencies responsible for protecting U.S. technologies lack the organizational and technical capacity to design and implement effective policies to prevent the transfer of the national security–sensitive components of emerging technologies such as AI. They suffer from a dearth of technical talent needed to identify effective new policies and lack the analytical capacity to enforce their policies efficiently, especially on dual-use goods. Filling these gaps in key elements of the Executive Branch—particularly in the Departments of Commerce, the Treasury, and State—will enhance the government's ability to craft targeted export controls that have the greatest strategic impact and pose the least harm to U.S. competitiveness.

Stakeholder(s):

Department of Commerce **Department of State**

Department of the Treasury

2.6.3. Controlled Technologies

Identify "Emerging" and "Foundational" Technologies Which Must Be Controlled, as Required by the Export Control Reform Act of 2018

The Export Control Reform Act of 2018 (ECRA) and the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) are intended to overhaul the U.S. export control and investment screening regimes to better accommodate emerging technologies. ECRA requires the Department of Commerce to develop a regular, formal interagency process to identify "emerging and foundational technologies that … are essential to the national security of the United States," and are not otherwise controlled.9 Any such technologies identified by Commerce become subject to U.S. export controls, and any foreign investment in a U.S. company which "produces, designs, tests, manufactures, fabricates, or develops" one or more such technologies must be reviewed by CFIUS.10 This list must be distinct from efforts within the Commission-proposed National Technology Strategy (NTS) to define emerging technologies key to U.S. national competitiveness and national security. The ECRA list must be more narrowly defined and focused only on specific technologies for which export controls are necessary, whereas the TCC and NTS' focus should be on identifying broader technologies and particular platforms in which continued U.S. leadership is essential... Identifying this list of technologies is critical to enabling the United States to fully implement both ECRA and FIRRMA. As ECRA and FIRRMA are structured, until the Department of Commerce defines a technology which is not otherwise controlled as "emerging and foundational" as part of this review process, with rare exceptions CFIUS cannot require foreign companies to disclose non-controlling investments in U.S. technology firms. Although the Commission also recommends breaking CFIUS' reliance on this ECRA list for mandatory disclosures (see recommendations on reforming CFIUS for emerging technology competition, below), currently Commerce's delay in identifying such technologies is hindering the full implementation of both ECRA and FIRRMA.

Stakeholder(s):

Department of Commerce :

... as of March 2021, the Department of Commerce has yet to identify a single emerging or foundational technology as mandated by ECRA. While there is reason to be judicious in developing this list, given its implications on U.S. industry, and Commerce faces legitimate capacity and resourcing limitations, the magnitude of the delay is unacceptable. The delay has garnered bipartisan criticism, created uncertainty for firms working in fields that could be labeled as emerging or foundational technologies, and delayed the government's ability to either control the export of, or more importantly gain insight into transactions involving, critical technologies that are not otherwise controlled.

2.6.4. CFIUS

Reform CFIUS for Emerging Technology Competition

CFIUS is not currently postured to address the range of threats that the United States faces from adversarial capital from strategic competitors such as China and Russia. The Department of the Treasury has little insight into Russian and Chinese investments in U.S. emerging technology firms, as CFIUS filings are still largely voluntary for noncontrolling investments in industries such as AI, semiconductors, quantum computing, and telecommunications equipment. While FIRRMA took positive steps in broadening CFIUS' authorities, it also left critical gaps in the investment screening regime. Additional steps are necessary to enable CFIUS to protect sensitive U.S. industries from adversarial capital, while ensuring the continued free flow of capital from trusted investors from allied nations.

2.6.5. Manufacturing Equipment

Utilize Targeted Export Controls on Key Semiconductor Manufacturing Equipment

Although the Commission believes that export controls on AI algorithms would likely be ineffective given their widespread availability and commercial use, export controls on specific hardware components are capable of constraining competitors' AI capabilities with national security applications and slowing their advancement. Policymakers must be judicious in their application of such controls, as sweeping controls on general-use semiconductors are likely to cause substantial damage to the U.S. semiconductor industry and could have a net negative effect on overall U.S. competitiveness in microelectronics. However, targeted controls on key components that only the United States—or the United States and a small group of close allies—produce which are essential for cutting-edge defense applications could have a significant strategic impact at a relatively minimal cost. The primary target for such controls should be select, high-end semiconductor manufacturing equipment (SME) needed to produce high-end chipsets, particularly photolithography equipment. China is the world's largest importer of SME, accounting for 29% of global imports from 2014 to 2018, and none of the largest or most sophisticated SME manufacturing firms are located in China. Simultaneous to implementing such controls, as discussed in Chapter 13 of this report, the United States should also fund efforts to prioritize the domestic development and manufacturing of SME tools and components needed to produce chips at scale at the 3nm node and beyond.

2.6.6. Export Controls

Utilize End-Use Export Controls to Prevent Malicious Use of AI

Export controls that restrict transfer of dual-use items for specific end uses will not be effective at preventing technology transfer to determined adversaries, but they can still play a role in preventing the involvement of U. S. firms and technology in human rights abuses. For specific, high-end, dual-use equipment prone to facilitating uses of AI which enable human rights abuses, such as mass surveillance, U.S. firms should be required to certify that the equipment will not be used for specific nefarious ends and keep logs of their transactions. End-use controls and reporting requirements would not substantially delay sales and present a lower barrier to commerce compared to list-based controls. Requiring companies to self-certify and self-report could deter U.S. firms from knowingly enabling bad behavior abroad.

2.6.7. Research Environment

Build Capacity to Protect the Integrity of the U.S. Research Environment

2.6.8. Coordination

Coordinate Research Protection Efforts Internationally with Allies and Partners

The United States should build a coalition of like-minded nations committed to the principle of open fundamental research and the associated values of research integrity—sidelining nations and organizations that do not abide by the values that provide the foundation for international innovation and science cooperation.

Stakeholder(s):

Allies **Partners**

2.6.9. Cybersecurity

Bolster Cybersecurity Support to Research Institutions

Protection of research data and intellectual property from cyber-enabled theft is perhaps the most important and actionable layer of security for the U.S. R&D environment. This is particularly true for AI, when theft of training data or trained models essentially provides malicious actors access to a final product. Federal investments in priority emerging technology research areas such as AI should be accompanied by a requirement and support for institutions—whether academic or private sector—to implement cybersecurity measures that adequately guard research data from cyber-enabled theft.

Stakeholder(s):

Research Institutions

2.6.10. Foreign Talent-Recruitment

Counter Foreign Talent-Recruitment Programs

China uses foreign talent-recruitment programs to achieve a "high ground" of AI experts. Rather than pursue legitimate competition for scientific talent through attractive job offers, China's talent-recruitment plans are designed in a manner that contradicts U.S. norms of research integrity, violates rules around disclosure, and creates vectors for technology transfer. The FBI and Intelligence Community assess that "participants are often incentivized to transfer to China the research they conduct in the United States, as well as other proprietary information to which they can gain access." There is an urgent need to reinforce standards around disclosure of conflicts of interest and commitment and to create mechanisms that enable a heightened level of transparency and accountability. This applies to researchers' individual transparency and institutional accountability, as well as to the government in identifying problematic affiliations and enforcing standards. Currently, U.S. grant-making agencies lack common processes, coordination, and compliance mechanisms to enable this level of transparency and effective oversight.

2.6.11. PLA Affiliates

Limit Collaboration with PLA-Affiliated Persons and Entities

PLA-affiliated universities and research labs send personnel abroad, with the overarching aim to obtain knowledge that can directly feed defense research and development priorities. Visiting scholars or students from PLA institutions often downplay their ties to the military or deliberately obscure affiliation by using alternate, external names for their home institutions that do not mention military or defense mandates. The government should take actions through designation of institutions of concern and heightened visa vetting to assist universities in making risk assessments around research collaborations—becoming an effective partner in protecting research integrity.

2.7. ORDER, OPENNESS & PROSPERITY

Advance international rules-based order, protect free and open societies, and unleash economic prosperity

A Favorable International Technology Order ~ The U.S. must work with allies and partners for AI innovation and adoption that advances the international rules-based order, protects free and open societies, and unleashes economic prosperity. | This Blueprint for Action provides detail for a comprehensive strategy to further U.S. interests with allies and partners to shape a favorable international technology order, win the technology competition against authoritarian states, and advance artificial intelligence (AI) innovation and adoption across the world to promote the values of free and open societies. This Blueprint for Action also proposes reforms to reorient U.S. foreign policy and the Department of State for great power competition in the digital age.

2.7.1. Strategy

Develop an International Science & Technology Strategy

The International Science & Technology Strategy (ISTS) will help coordinate emerging technology policies across the government and with our closest allies and partners; apply the tools of foreign assistance, technical expertise and guidance, and development finance and investment; and foster collaborative R&D. The ISTS should serve as the international component of the National Technology Strategy (NTS) and provide an organizing framework to drive U.S. foreign policy with regard to emerging technologies.1 The ISTS should center on four big initiatives:

- Building an Emerging Technology Coalition (ETC);
- Launching an International Digital Democracy Initiative (IDDI);
- Implementing a coordinated U.S. national plan to support international efforts; and
- Enhancing the United States' position as an international digital research hub.

2.7.2. Coalition

Build an Emerging Technology Coalition

As part of the ISTS, the United States, led by the White House and the Department of State, should lead in forming an Emerging Technology Coalition (ETC) of countries respectful of democratic values. The ETC would be a body of likeminded allies and partners to work with each other and with help from international and non-governmental organizations, civil society actors, and the private sector to develop and implement a coordinated strategy and associated policies to:

Stakeholder(s):
White House **Emerging Technology Coalition**

Department of State

2.7.2.1. Norms & Values

promote the design, development, and use of emerging technologies according to democratic norms and values

2.7.2.2. Policies & Investments

coordinate policies and investments to counter the malign use of these technologies by authoritarian regimes

2.7.2.3. Infrastructure

provide concrete, competitive alternatives to counter the adoption of digital infrastructure made in China.

2.7.3. Digital Democracy

Launch an International Digital Democracy Initiative

The Commission recommends that the United States and ETC partner states launch an International Digital Democracy Initiative (IDDI), a coordinated effort to align partner states' foreign assistance policies and programs 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. The IDDI will:

2.7.3.1. Coordination

Coordinate partner-state approaches to adopting and governing digital technologies

2.7.3.2. Mobilization

Mobilize coalition efforts to provide alternatives (through funding assistance, technology development, and private-sector investment) to digital infrastructure and AI/machine language (ML)-enabled technologies that are used for illiberal ends and to promote technologies that enhance democratic participation, human rights, and the rule of law

2.7.3.3. Adoption

Facilitate adoption of secure, reliable, and trusted digital infrastructure, AI/ML-enabled technologies, and information and communications technology (ICT)

2.7.4. Plan

Develop and Implement a Comprehensive U.S. National Plan to Support International Technology Efforts

The ISTS should include an integrated government-wide plan for coordinating the tools of U.S. foreign policy to advance the ETC, the IDDI, and stand-alone projects. This plan should leverage technical expertise, foreign assistance, development financing and investment, policy guidance, and export controls in support of three core goals:

2.7.4.1. Technical Standards

Shape International Technical Standards

The United States and its allies should lead the way on international technical standardization for AI. U.S. government-led dialogue with U.S. industry, as well as democratic allies, can help overcome information asymmetries and clarify objectives for technical standards on AI that foster economic growth, protect consumers, and safeguard democratic values. Partnership and information-sharing between the U.S. govern-

ment, industry, and academia is critical to ensure protection of national security concerns involving standards and the neutrality of international standards-setting bodies.

2.7.4.2. Policy

Implement a Coordinated U.S. National Policy for the IDDI

A national policy for U.S. digital development efforts and involvement in IDDI will provide high-level strategic vision and coordination necessary to:

2.7.4.2.1. Interests

Advance the interests of the United States and its allies and partners in the development and global adoption of AI/ML-enabled technologies and secure, trusted, and open digital ecosystems that promote values critical to free and open societies

2.7.4.2.2. Prioritization

Elevate—across U.S. departments and agencies—the prioritization of digital development necessary to advance U.S. interests and IDDI goals and reorient U.S. development efforts for a digital age

2.7.4.2.3. Foreign Policy

Strengthen U.S. foreign policy through significant appropriations for digital development, increased resourcing and staffing, and expanded authorities for federal departments and agencies, particularly the Department of State, USAID, and DFC.

Stakeholder(s):

Department of State **DFC**

USAID

2.7.4.3. Export Controls

Promote Transparency and Accountability Through Export Controls

ISTS objectives will be furthered by the U.S. government's ability to harness the power of the U.S. private sector. A critical tool for achieving this involves incentivizing the export of technologies that align with democratic values.

Stakeholder(s):

U.S. Private Sector

2.7.5. Research Hub

Enhance the United States' Position as an International Emerging Technology Research Hub

The third component of the ISTS is to enhance the role of the United States as an international emerging technology research hub. The goals are to:

2.7.5.1. Initiatives & Standards

Facilitate U.S. government contributions to collaborative initiatives and technical standards, such as Global Partnership on AI (GPAI) and digital projects of the OECD

Support International Digital and AI R&D ~ International efforts, like the GPAI and the OECD's AI and digital initiatives, are critical forums for facilitating alignment among like-minded countries on advancing the responsible and human-centric development and use of AI. Research undertaken by the National AI Research Institutes—run by the NSF and other U.S. agencies—and by other programs across Federal departments and agencies, is an incredible resource that should support these key international efforts and advance AI and digital goals of the U.S. and like-minded partners.

Stakeholder(s):

Global Partnership on AI **OECD**

2.7.5.2. Talent

Strengthen the talent of the United States, allies, and partners by investing in people through workforce development, mentorship, and exchange programs facilitated through the recommended Multilateral AI Research Institute (MAIRI)

Establish the Multilateral AI Research Institute (MAIRI) ~ The Multilateral AI Research Institute (MAIRI) will provide a model for equitable, multilateral research, facilitate AI R&D that builds on like-minded countries' strengths, and develop the next-generation global AI workforce. With a physical center located in the United States with a virtual presence, MAIRI will enable collaborative research among key allies and partners and contribute to a broader effort—reflected in the Emerging Technology Coalition and IDDI—to preserve free and open societies, win the global technology competition, and foster AI innovation in a manner that comports with democratic values. Ultimately, to further these objectives, MAIRI should seek to facilitate a federated network of research institutes across the globe and with national labs and university hubs.

Stakeholder(s):

Multilateral AI Research Institute

2.7.5.3. Research

Foster collaborative research relationships and pool research resources for the development of technologies (particularly in civilian applications) that comport with democratic values and address gaps in commercial R& D, including joint research in privacy-enhancing technologies

Expand Talent Exchanges ~ The United States must attract talent to collaborative research endeavors at both the National AI Research Institutes and MAIRI. Sustained, strong collaboration between MAIRI partners is critical to ensure that responsible, secure, human-centric AI prevails over authoritarian AI. Shoulder-to-shoulder research and talent exchanges are invaluable, enabling researchers to build relationships, learn from each other, exchange ideas, and spark future collaborations.

2.7.5.4. Regulation

Enable the U.S. and allies to overcome current regulatory challenges currently inhibiting collaboration, particularly in Europe, such as data-sharing restrictions and liability agreements.

2.7.6. Great Power Competition

Reorient U.S. Foreign Policy and the Department of State for Great Power Competition in the Digital Age

In the near term, it is imperative to establish a Department of State focal point for emerging technology policy and expertise and resourcing through steps the Commission proposes below. In the longer term, the United States must fundamentally reorganize the structure, focus, and culture of the Department of State to advance American interests at the intersection of democracy, technology, security, commerce, and human rights.68 Without high-level support in the Department, technology competition is unlikely to become a core aspect of U. S. foreign policy.

Stakeholder(s):
Department of State

2.8. ASSOCIATED TECHNOLOGIES

Lead in AI through the broader lens of competition across a range of emerging technologies

Associated Technologies ~ 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. | Recognizing that leadership in artificial intelligence (AI) relies on leadership across a suite of emerging technologies, the United States must prioritize the research and development (R&D), application, and adoption of not just AI, but the technologies that enable it and are enabled by it. This process should be based on a careful analysis of the national security threats and opportunities at the intersection of AI and its associated technologies. If the U.S. government fails to adopt a more strategic approach to protecting and promoting U.S. advantages in these areas, it risks jeopardizing the country's technological leadership, economic prosperity, and national security. In accordance with its mandate to consider both AI and "associated technologies," the Commission identifies and proposes steps to maintain U. S. leadership across the spectrum of technologies it believes are most critical to U.S. national competitiveness. The Commission then offers specific recommendations on how the United States can proactively address the novel national security threats and opportunities posed by three technologies in particular: biotechnology, quantum computing, and 5G telecommunications.1 Finally, the Commission expands its analysis to include recommendations on a broader set of emerging technologies critical to U.S. national competitiveness. Technologies Critical to U.S. National Competitiveness The Commission has identified eight technologies and related platforms that are key to U.S. leadership. Two of these technologies—AI and microelectronics—are addressed elsewhere in this report. The remaining six—biotechnology, quantum computing, 5G and advanced networking, autonomy and robotics, advanced and additive manufacturing, and energy systems—are covered below. These recommendations build on the Commission's previous work by providing actions the U.S. government could take to promote overall U.S. leadership and long-term competitiveness across the constellation of emerging technologies.

2.8.1. National Competitiveness

Identify and Prioritize Technologies Central to National Competitiveness

The Commission has identified eight technologies and related platforms that are key to U.S. leadership. Two of these technologies—AI and microelectronics—are addressed elsewhere in this report. The remaining six—biotechnology, quantum computing, 5G and advanced networking, autonomy and robotics, advanced and additive manufacturing, and energy systems—are covered below. These recommendations build on the Commission's previous work by providing actions the U.S. government could take to promote overall U.S. leadership and long-term competitiveness across the constellation of emerging technologies.

2.8.2. Biotechnology R&D

Prioritize the Development of an Advanced Biotechnology R&D Ecosystem

The United States must invest in key platforms that better position the U.S. academic and commercial biotech industry to benefit from AI-enabled advancements in biology. It should specifically look to support platforms that aggregate biodata, and specifically genetic data, in a secure manner in order to enhance the ability of U.S. researchers to utilize AI to facilitate breakthrough biotechnology research and innovation. Additionally, the United States should support efforts to expand the scope and sophistication of U.S. biofabrication capabilities to ensure it can keep pace with forthcoming research advancements. It 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. 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.

2.8.3. Biotechnology Capabilities

Prioritize Advanced Biotechnology Capabilities as Imperative for National Security and Economic Competitiveness

The growing importance of biotechnology leadership to health, food, production, and science also makes it a national security imperative that the United States take proactive steps to facilitate long-term U.S. leadership in the field. Advancements in biotechnology will also create novel national security challenges, ranging from engineered pathogens to augmented competitor human physiological or mental capabilities. The United States currently is not postured to address such challenges, and biological threats have rarely been a priority issue for the U.S. national security community. The COVID-19 pandemic clearly illustrates that the United States must think more broadly about national security threats than it has in the past, and that biological threats in particular have the potential to impose significant costs on U.S. society and security. U.S. competitors see the potential for AI to spur new, transformational advances in biotechnology. China in particular is actively seeking global leadership in both fields, sees its AI and biotechnology strategies as mutually reinforcing, and believes the synergies between the two will translate into military advantage.10 China also faces fewer barriers to collecting, using, and combining human biological data given its disregard for individual privacy and bioethical principles. The global reach of China's genomics giant, BGI, poses similar threats in the biotechnology sector as Huawei does in the communications sector.

2.8.4. BGI

Publicly Highlight BGI's Links to the Chinese Government

BGI is China's de facto national champion in genetic sequencing and research and is among the world leaders in DNA sequencing. It has research affiliations with multiple U.S. universities, including the University of Washington and Washington State University. BGI has also benefited from substantial support from the Chinese government, as well as its 2013 acquisition of a competing U.S. firm, Complete Genomics. There are indications that BGI's links with the Chinese government may run deeper than it publicly claims, as it built and operates China National Gene Bank, the Chinese government's national genetic database, and has used PLA-owned supercomputers to process genetic information. Chinese diplomats have pushed BGI-built COVID-19 testing kits, including in the United States, and by August 2020 BGI had "sold 35 million rapid COVID-19 testing kits to 180 countries, and built 58 labs in 18 countries." BGI may be serving, wittingly or unwittingly, as a global collection mechanism for Chinese government genetic databases, providing China with greater raw numbers and diversity of human genome samples as well as access to sensitive personal information about key individuals around the world. The highest levels of the United States government should publicly state these

concerns so as to raise awareness among the U.S. commercial and academic biotechnology communities, as well as U.S. allies, many of which currently have partnerships or business dealings with BGI.

2.8.5. Disease Monitoring

Pursue Global Cooperation on Smart Disease Monitoring

While pivoting to a more competitive national approach toward biotechnology policy, the United States should also pursue efforts to enhance global cooperation on disease monitoring. By pooling existing open-source health-related data with improved early warning signals and data on zoonotic spillovers and transmission of novel viruses, governments will be better postured to use AI to predict and contain future pandemics. Combining increased transparency and data sharing on disease outbreaks with AI tools—which can enhance early outbreak detection and contribute to real-time disease monitoring—could provide substantial benefit for global public health if all countries, including China, participated in good faith.

2.8.6. Quantum Computing

Transition from Basic Research to National Security Applications of Quantum Computing

Although the United States is well-positioned to take advantage of its early success in the basic science of quantum computing, the U.S. Government must increase its focus on fielding national security applications or risk falling behind strategic competitors. Most notably, China has made significant investments in military applications of quantum computing in an attempt to offset U.S. strengths.22 The Department of Defense (DoD) is still refining its approach to rapidly transition commercial technologies from research to fielding in high-cost, hardware-intensive sectors such as quantum computing. In the long term, DoD should prioritize efforts to rapidly procure technology across its innovation offices, but this process could take several years of dedicated effort. In the interim, announcements of priority applications will help spur private-sector investment and innovation in quantum computing despite the absence of an integrated technology-procurement apparatus.

2.8.7. Quantum Fabrication

Foster a Vibrant Domestic Quantum Fabrication Ecosystem

Due to the strategic implications of quantum computing and its application to AI, the United States must take steps now to cement its long-term status as the global leader in the design and manufacturing of quantum processing units (QPUs). To avoid the situation in which the U.S. semiconductor industry currently finds itself, the United States must establish trusted and assured sources for critical materials and components of QPUs, ranging from manufacturing equipment to superconductors and dilution refrigerators. Although these materials and components may not yet represent choke points, they will inevitably become more specialized as the manufacturing processes required to design and produce QPUs continue to advance. Rather than reshoring the entire supply chain for QPUs, the United States should work with its allies to develop a resilient network of suppliers for critical components that directly impact U.S. national security. However, a secure supply chain is not sufficient to ensure U.S. leadership in quantum computing. To benefit from future breakthroughs in the field, the United States must create a robust domestic ecosystem for the research, development, and application of quantum computers that attracts top-tier talent from around the world. The U.S. Government should offer incentives for the R&D of quantum computers and their components while simultaneously creating demand for national security applications of quantum technologies. The Quantum Economic Development Consortium (QED-C), proposed in the National Quantum Initiative (NQI) Act of 2018, is an important step toward extending U.S. leadership in next-generation computer hardware for years to come.

2.8.8. Quantum Computing Research

Make Quantum Computing Accessible to Researchers via the National AI Research Resource (NAIRR)

Despite recent advances in the fields of quantum hardware and software, fault-tolerant quantum computers (FTQCs) capable of performing general-purpose tasks are unlikely to replace classical computers anytime soon. In the near term, the United States should invest in noisy intermediate-scale quantum (NISQ) computers that are capable of deriving probabilistic solutions from imperfect qubits. Hybrid quantum-classical techniques have also shown promise, whereby classical computers delegate certain tasks to purpose-built quantum devices within the same workflow. However, resources suitable for developing this type of software are not readily accessible. By making classical and quantum computers available in the same workflow, the U.S. Government would lower barriers to innovation for startups in the quantum computing space and attract top-tier talent from around the world. The resulting public-private partnerships would also encourage the commercialization of quantum computers and help the U.S. Government adopt those products for national security use cases.

Stakeholder(s):

Researchers

2.8.9. 5G Deployment

Accelerate U.S. 5G Deployment Through Spectrum Sharing

The slow rollout of 5G networks in the United States compared to China risks undermining U.S. advances in AI, both in the government and the private sector. The sub-6 GHz spectrum, sometimes referred to as the mid-band or the "goldilocks" band of spectrum, is the critical portion of the spectrum for both DoD and commercial 5G operations. Sub6 GHz spectrum is critical for 5G civilian communications since it combines high data rates with good range and penetration. Within DoD, it is also already used by many radar and communication systems because it also combines high discrimination capability with long-range operations. In part due to its importance to military operations, DoD has retained exclusive access to significant portions of the mid-band spectrum, which limits commercial uses. Unfortunately, the lack of U.S. mid-band spectrum commercial availability is substantially slowing the deployment of 5G networks domestically. Given that sub-6 GHz is important for sensing using radar and civilian communications, spectrum sharing between DoD and the private sector is the ideal approach to enabling access for both purposes in a manner that balances national security and economic interests. Several U.S. Government agencies are working to address this problem by developing spectrum-sharing capabilities within the 3- to 6-GHz range. In 2015, the Federal Communications Commission (FCC) established the Citizens Broadband Radio Service (CBRS), the first U.S. spectrum sharing model. Since that time, the National Telecommunications and Information Administration (NTIA) has studied, and has collaborated with the DoD and FCC on, maximizing spectrum-sharing capabilities. The CBRS enables shared federal and non-federal use of the band. This work allows the U.S. Navy and non-government providers to share the 3550-3700 MHz band across three dynamically managed tiers: the Navy will maintain first priority access, followed by companies and organizations that purchase priority-access licenses, and finally companies and organizations that register at no cost. The FCC held its first auction for priority-access licenses for this band in July 2020, which raised more than $4.5 billion through the sale of 20,625 licenses. This is a promising but modest start and these efforts must expand to a larger portion of the mid-band spectrum to be competitive with China. To achieve spectrum sharing at a competitive level will require technical analysis and engagement with industry. A comprehensive process will be critical to ensuring that DoD maintains access to spectrum essential for operational effectiveness while also broadening commercial access to spectrum for civilian 5G networks.

Stakeholder(s):

DoD

Private Sector

National Telecommunications and Information Administration

FCC

U.S. Navy

2.8.10. Robotic & Autonomous Systems

Incentivize the Development of World-Class Software Platforms for Robotic and Autonomous Systems

Autonomous systems that rely on robotics to execute tasks in the real world are being applied to everything from advanced manufacturing to warfighting. As AI continues to improve the ability of these systems to match or exceed human capabilities, the United States must position itself as a leading producer and adopter of robotic hardware and software for civilian and military use cases. The United States currently lags behind countries such as Japan and Korea on the manufacturing and installation of industrial robots, and China has declared robotics as a core industry. As the United States reshores certain strategic supply chains and increases its reliance on autonomous systems, continued access to cutting-edge robotics will be a national security imperative

2.8.11. Legacy Parts

Accelerate Additive Manufacturing Production of Legacy Parts Across the Department of Defense

The ability to manufacture high-tech products domestically is critical to a nation's security and its economic productivity. The United States must strive to develop manufacturing capabilities in industries that are essential to crisis response or that would take too long to bring online in the event of a protracted conflict. Innovation also benefits from the co-location of firms engaged in technological design and those that produce finished products, which enables rapid feedback and continuous iteration on product design. This link is particularly important in the defense sector, where communication between researchers, designers, and manufacturers can help quickly transition a technology from the lab to the field. However, the United States has relinquished manufacturing leadership in high-tech industries that employ highly skilled workers to high-wage nations like Germany and Japan. Meanwhile, China and other lower-wage nations are moving up the value chain from low-value manufacturing processes, such as assembly, to more sophisticated techniques. Although the supply chain disruptions resulting from the COVID-19 pandemic may prompt the return of some manufacturing to the United States, the broader trend of offshoring the manufacturing of next-generation technologies appears likely to continue unless the U.S. government takes appropriate action.

2.8.12. Energy Storage

Develop and Domestically Manufacture Energy Storage Technologies to Meet U.S. Market Demand by 2030

Cheap and reliable access to energy is critical to U.S. national security. 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 by 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. As the cost of intermittent renewable sources continues to fall, the United States must commit to developing and deploying the next generation of energy storage devices, from long-duration stationary applications to battery packs for electric vehicles.

Administrative Information

Start Date:
End Date:

Publication Date: 2021-04-24
Source: https://reports.nscai.gov/final-report/table-of-contents/

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: