2020

ARTIFICIAL INTELLIGENCE & NATIONAL SECURITY

25-T-0299

NATIONAL DEFENSE UNIVERSITY

THE DWIGHT D. EISENHOWER SCHOOL
FOR NATIONAL SECURITY AND RESOURCE STRATEGY

FORT LESLEY J. McNAIR, WASHINGTON, D.C. 20319-5062

INDUSTRY STUDY

EMERGING TECHNOLOGY

Abstract

This paper seeks to examine the implications of artificial intelligence (AI) on U.S. national security organized in concordance with the National Security Commission on Artificial Intelligence Lines of Effort. While countless emerging technologies will be vital to national security in the years to come, AI is the one that has the potential to tie them all together and change how humankind lives. In the era of Great Power Competition, AI also promises to transform how wars are fought. Furthermore, Russia and China are undeterred by privacy concerns or the ethics of how AI should be employed. Thus, gaining a competitive advantage in AI must be a top priority for national strategy. However, while AI promises numerous benefits, it also presents many risks. U.S. policy must account for lost jobs, data security and privacy issues, and misinformation campaigns that will inevitably result as AI becomes more prevalent. The United States is at a critical juncture in the history of AI development and the consequences of failing to adapt are potentially dire. This paper offers analysis and solutions to augment a comprehensive U.S. AI strategy.

Author Team

Mr. Zach Burstein, U.S. Government
LTC Frankie Cochiaosue, U.S. Army
Lt Col Dan Counts, U.S. Air Force
CDR Glenn Goetchius, U.S. Coast Guard
Lt Col Brad Howell, U.S. Air Force
Lt Col Brad Huebinger, U.S. Air Force
GPCAPT D.J. Hunt, New Zealand
Mr. Joseph Jones, U.S. Air Force
LTC Adam Lackey, U.S. Army
Lt Col Michael McCarthy, U.S. Marine Corps
CAPT James Nash, Australia
Ms. Mika Partridge, IBM Industry Fellow
COL Rob Petrosky, U.S. Army
COL Ken Quimby, U.S. Army
Mr. Ken Roy, U.S. Department of State
Mr. Seth Rubin, U.S. Navy
Col Tsegaye Tesfahunegan, Ethiopia
Ms. Patricia Thomas, U.S. Department of State
COL Rob Wolfe, U.S. Army

Professors/Instructors

Dr. Andy Leith, National Defense University
Dr. Jim "Kegs" Keagle, National Defense University
Dr. Steve Brent, National Defense University
Col Bryon McClain, U.S. Air Force
CAPT Renee Squier, U.S. Navy
Librarian Ms. Diana Aram, National Defense University

Field Studies

On-Campus or Digital Guests to Seminar 7, Eisenhower School, and NDU

LTC Matthew A. Bartlett, U.S. Air Force
Alexandra Navarro Nasif, IBM Defense and Intel
Charles H. Rybeck, Senior Technical Advisor & Co-Founder, Digital Mobilizations, Inc.
Jay Heroux, General Manager, Public Sector Programs, Digital Mobilizations, Inc. (DMI)
Scott Lacy, Government and Public Services Specialist Leader, Deloitte
Thomas X. Hammes, INSS
Mark Foulon, Professor of Industry and Business, Dwight D. Eisenhower School for National Security and Resource Strategy.
Colleen Laughlin, Executive Director, Defense Innovation Board
COL (ret.) John 'Wags' Wagner, Vice President, National Security and Space, Sierra Nevada Corporation
Ned Finkle, Vice President of External Affairs, NVIDIA
Kevin Berce, Senior Director of Federal Business, NVIDIA
Sameer Ronnie Dhillon, Technical Marketing Management Team, NVIDIA
Sean Wix, Technical Marketing Management Team, NVIDIA
Mark Fisk, IBM Partner, Digital - Blockchain for Global Business Services
Charles Varvaro, Vice President, Managing Director Intellectual Property & Technology Alliances, IBM
Zach Lemnios, Vice President, Research Strategy and Worldwide Operations, IBM Research Think Lab
Dave McQueeney, Chief Innovation Officer, IBM
Murray Campbell, Distinguished Research Staff Member and Manager - AI, IBM Research Think Lab
Joe Cubba, Vice President and Partner, IBM Defense and Intel, Global Business
Peter Santhanam, Principal Quantum Research Staff Member, IBM Research-AI
Jim Stathis, Principal AI Research Staff Member, IBM Research Think Lab
Dinesh Verma, IBM Fellow, Distributed AI, IBM Research Think Lab
Ian Malloy, Manager - Information Security, IBM Research Think Lab
Fletcher Previn, Chief Information Officer, IBM
Kristie Bradford, Director Intellectual Property, IBM
Mohamed Ahmed, IBM Distinguished Engineer, Master Inventor, Manager AI, Watson and Cognitive Solutions
Marko Erman, Senior Vice President and Chief Scientific Officer, Thales Defence & Security Group
Professor William Overholt, Senior Research Fellow, Harvard Kennedy School of Government
BG Rob Spalding (Ret.), Hudson Institute
Ambassador Craig Allen, United States – China Business Council
Cary Ingram, Senior International Trade Specialist, Department of Commerce
Dr. Justin Sanchez, Life Sciences Research Technical Fellow, Battelle Memorial Institute
Cameron Mayer, Booz Allen Hamilton, Vice President.

Domestic Travels

Washington, D.C., Maryland and Virginia:

National Security Commission on Artificial Intelligence (NCSAI) – Briefing on the Commission's mandate and its chief working groups and five Lines of Efforts (LOE).

NavalX – Site visit and familiarization examining facilities, current projects and organizational overview of the mission and role of NavalX in connecting government to industry while creating greater levels of workforce agility.

DATM War Rooms – Overview and discussion during site visit provided students the opportunity to examine changes in the Navy Material Establishment over the last 240 years in the context of the environment and time.

Council on Competitiveness – Site visit and discussion outlined how a Non-Government Organization such as the Council on Competitiveness shapes policies and runs programs to jump-start productivity and grow America's economy.

Dreamport – Site visit to a cyber innovation, collaboration, and prototyping facility that is a U.S. Cyber Command partnership with the non-profit Maryland Innovation and Security Institute (MISI).

IN-Q-TEL – How IQT works side-by-side with the venture capital community to identify and incubate cutting-edge technology with potential for commercial success.

DCode – Examination of a technology accelerator that helps entrepreneurs of ET break down barriers and rapidly go to market with the federal government. Students received capability briefs and held discussions with startup firms participating in the DCode accelerator program.

Oracle – Briefing and discussion provided insight into how companies like Oracle compete in the ET markets. Analysis of the current relationship the company has built with the Department of Defense, academia, and the private sector.

Pittsburgh:

Carnegie Melon University

Language Technologies Institute – Core research involves the algorithmic aspects of computer voice recognition and AI applied to voice forensics.

CMU's National Robotics Engineering Center – Presentation and tour of the facility.

Dean, School of Computer Science – Introduction to the AI Stack

- Understanding and Leveraging the AI Stack
- A Blueprint for Developing and Deploying AI

Alphalab – Examined cutting-edge startups and products before public release in select fields such as robotics, materials, textiles, consumer electronics, AR/VR, medical devices, energy/cleantech, autonomous vehicles, and more. Students helped evaluate the companies and attendant technologies to assist in determining which companies would be invited to join Alphalab.

University of Pittsburgh's Human Engineering Research Laboratories (HERL) – Briefing and tour of HERL which is part of the U.S. Department of Veterans Affairs that aims to help create a world where all people with disabilities have unencumbered mobility and function so that they can fully participate in and contribute to society.

Executive Summary

When Bernard Baruch called for the establishment of a "little school…to preserve experience and keep touch with industry" after World War I, he could not have imagined the world that faculty and students of the Eisenhower School for National Security and Resource Strategy would study a century later. Advances in technology have changed perceptions of what industries are necessary for the preservation of the common defense and pursuit of the U.S. national security objectives. As part of the current curriculum, today's Eisenhower students are assigned to one of eighteen seminars, each tasked with studying a specific industry relevant to national security. This paper represents the culmination of a semester's work of the Emerging Technology (ET) Industry Study seminar.

ET is not really an industry, per se, rather it is an umbrella under which many new and developing ideas incubate before they ripen into common use. During the spring semester, the 2020 ET Industry Study examined many aspects of an array of technologies. Some of these will be discussed briefly below, but none are more central, or have more potential to change the world, than AI. Recognizing this, the ET Industry Study partnered with the National Security Commission on Artificial Intelligence (NSCAI) to help guide our studies and to produce scholarship that we hope will help to inform national security professionals on the strengths, weaknesses, opportunities, and threats that AI brings.

Summary of Findings

Using the National Security Commission on Artificial Intelligence's (NSCAI) five lines of effort as framework, this report examines various aspects of AI and offers the following findings and proposals:

LOE 1 - Invest in AI Research and Development

Finding: There is a lack of leadership over AI R&D efforts within the federal government, preventing the development of a whole-of-government strategic AI plan. Furthermore, U.S. spending on AI R&D is insufficient, and the federal budgeting and acquisition process is too slow to keep pace with our competitors.
Proposal: The United States should designate the NSCAI as the lead body to coordinate all federal AI R&D and to develop a comprehensive strategic AI R&D plan for the nation, including priorities for investment. The government should also fund an organization that makes non-controlling equity investments in start-up AI companies.

LOE 2 – Apply AI to National Security Missions

Finding: Although AI promises innumerous benefits, its advanced computing capacity can also be used for ill. AI-enabled information attacks and deepfake technology threaten the stability of global systems and undermine the legitimacy of government institutions and public trust in AI systems
Proposal: The United States must establish a national data management system to set data security and access standards. The U.S. must pursue policies to verify and validate publicly available information to ensure data validity and counter misinformation campaigns.

LOE 3 – Train and Recruit AI Talent

Finding: We are at the advent of the "Age of AI," yet AI professionals are scarce worldwide. In the era of Great Power Competition, the United States is in a global race for AI talent to gain the competitive advantage.
Proposal: The United States must grow the tech workforce by identifying and nurturing talent early, melding the education system with national interests, utilizing new education incentives and hiring strategies, and breaking down gender biases that limit its potential.

LOE 4 – Protect and Build Upon U.S. Technology Advantages

Finding: China is poised to overtake the United States as the global leader in AI, in part, because U.S. AI policy and resources have focused on R&D for defense applications to the exclusion of building and supporting the commercial overall AI industry.
Proposal: The United States must leverage existing authorities to invest the in the non-defense AI industry and standardize AI infrastructure and supporting technologies. At the same time, the nation must enact new legislation to build economic resilience and emergency response preparedness.

LOE 5 – Marshal Global AI Cooperation

Finding: The United States lacks a cohesive narrative for international cooperation on AI. China, on the other hand, is growing its data network through its Belt and Road Initiative, putting the United States and its allies at a disadvantage.

Proposal: The United States must work with industry, academia, and local governments to establish a cohesive national narrative that promotes international cooperation. The United States must also take the lead in “data diplomacy” to promote international standards for data sharing to maximize cross-border data flows and a global alliance to this end would facilitate success.

Table of Contents

Introduction

ET and AI: Definition and Report Methodology

Emerging Technologies (ET) create, transform, and destroy comparative advantage. As a result, business and government leaders must understand how to integrate ET into their organization or nation. U.S. economic growth and national security hinge on its understanding of ET impacts and ability to nurture a productive environment for development, adoption, and security of ET, especially during the current age of Great Power Competition.

There is no agreed-upon list of technology that nests under the banner of ET. The type of technologies that fall within the ET remit is as significant and varied as the industries that will be impacted, and ET is a relative term that morphs over time.

For purposes of this report, the characteristics of ET as described by Halaweh[1] have been used to assist in understanding the impact that ET has on the economic growth and national security of the United States. These characteristics are defined in Table 1.

Table 1 – Characteristics of Emerging Technology

Characteristics	Description
ET Uncertainty	The uncertainty associated with ET takes several forms with unknown and unpredictable values and outcomes, such as standards and specifications (maturity), business models, price, and adoption rate uncertainties. As time passes, the ET becomes more matured and diffused and the number of adopters increases while costs drop. In contrast, ethical and social concerns might increase as ET is used in new applications.
ET Network Effect	The value of an ET increases by increasing the number of ET users.
ET Costs	The cost of owning the ET is high, and the cost of substituting traditional technology with the ET is high.
Unobvious ET Impact	The social and ethical impacts associated with the use of ET are unseen, unknown, or unexpected before its adoption/use or at an early stage of the ET life cycle.
ET is limited to Creator or Inventor Country (Availability of ET)	ET is usually available for use in a particular context or in the country that creates or invents it.
ETs are not fully investigated or researched	Most of the materials on ET are white papers and technical reports produced by the manufacturers of the ET with little scientific/academia research.

Given recent advancements in computing power, algorithms, and market conditions, Artificial Intelligence (AI) has become a part of everyday life for most people worldwide. Yet despite a growing understanding and acceptance, it still possesses many of the characteristics of an ET. Most importantly, we have not even come close to tapping AI's potential and its ultimate impact on humankind remains unknown. This report analyses AI specifically because it is perhaps the one ET that will tie all others together and will likely lead to the creation of new ET not yet imagined. However, while the focus is on AI, the general conclusions can be applied to any ET.

This report is guided by the groundwork set forth by the National Security Commission on Artificial Intelligence (NSCAI). The paper is organized by the NSCAI's Lines of Effort (LOE) to develop policy actions to support AI adoption and exploitation. Furthermore, it relies on the NSCAI's definition of AI that is "the ability of a computer system to solve problems and to perform tasks that would otherwise require human intelligence."[2] AI is actually a collection of technologies such as pattern recognition, machine learning, computer vision, natural language understanding, and speech recognition that combine to solve problems that "in some respects, parallel the cognitive process of humans: perceiving, reasoning, learning, communicating, deciding, and acting."[3] This paper is not, however, an examination of the technical aspects of AI. Rather, it seeks to understand how AI should fit within grand strategy and what is the right mix of resources, actors, policies, and efforts so that AI will contribute to U.S. national security.

ET and AI in the Great Power Competition

AI's revolutionary computing power promises to change the world. As a result, the Great Powers (the United States, China, and Russia) have made ET and AI a priority. In 2017, Vladimir Putin stated that whoever becomes the leader in AI will "become ruler of the world."[4] China's 2017 National AI Development Plan announces its goal to become world leader in AI by 2030 through "an all-element, multi-domain, highly efficient new pattern of civil-military integration" and expressly names swarming technology one of its top AI priorities.[5] Thus, the development of AI has clear national security implications. Executive Order 13859 demonstrates the national interest stating, "continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our nation's values, policies, and priorities."[6]

China has become a more visible competitor to the United States for AI global leadership, with the goal of dominating through hybrid warfare. This places at risk the ability for the United States to maintain a strategy of overmatch across the full Competition-Conflict Spectrum of military operations[7].

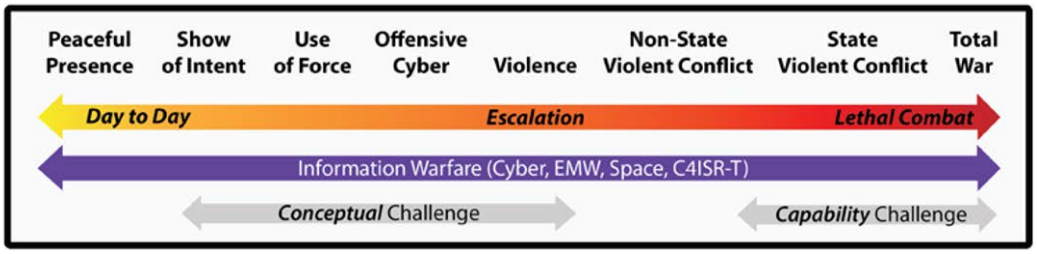

Figure 1 - The Competition Conflict Spectrum for the Military Dimension of Power, Navy concepts and capabilities to improve our ability to respond to an adversary across the spectrum from day to day operations, to escalation, to lethal combat.

Authoritarian governments in Russia and China have structural advantages for AI development. AI depends on massive amounts of meaningful data to recognize patterns and learn. Russian and China can more easily access data from all sectors of the economy for use in government applications. Democratic values and free market capitalism in the United States—while traditionally our source of strength—can actually limit AI applications because data is in the hands of various commercial businesses and the government has only limited ability to capture that data. Additionally, China is poised to accept ET and AI in part because it has little "old tech" standing in the way of progress.

This reality is complicated by the fact that many AI companies within the United States are multinational corporations that desperately want to enter the massive Chinese market. China's widely reported policies of requiring cooperation with state-owned enterprises, predatory conditions for market entry, and outright intellectual property theft, erode the competitive advantage for U.S. innovation and investment. This is not to say the United States should adopt the Russia and China models, but it does present a challenge for which our national AI strategy must account.

Vulnerability of ET and AI

Admittedly then, the widespread adoption of AI will have many positive global effects, but the technological revolution will also carry significant risks. If these are not effectively mitigated, such disruptions could significantly threaten the U.S. economy and national security. Some experts estimate that nearly 50% of jobs in America could be replaced by AI. The U.S. trucking industry alone employs almost a million workers, all of whom could soon be replaced with automation. As such, the severity of these impacts cannot be understated. The U.S. government must work with industry, labor, and academia to ensure that the U.S. workforce is best prepared to integrate human-machine cooperation and thereby, maximize the potential gains from AI and automation while supporting tomorrow's workforce.

The United States is more likely than other nations to experience adverse economic effects because of its high worker wages and standard of living.[8] U.S. employers will have greater incentive to replace high-cost American workers with AI-driven automation than countries with quick access to cheap labor. If implemented too quickly, AI adoption risks mass unemployment and the potential for civil unrest among a disenchanted population. The effects of this trend could exacerbate the already historic unemployment caused by the current COVID-19 pandemic.

This paper does not, however, advocate a Luddite-like revolt against AI. Planning for its implementation must be a national priority, and that planning process must account for both the

costs and the benefits of AI. However, given the speed at which AI and other ET are developing, the role of policymakers is perhaps more important than ever. Rather, this report offers recommendations for U.S. policymakers embrace and enable AI while at the same time anticipate and account for its inevitable risks. The ability for nations to harness AI to create comparative advantage is critical to both economic growth and national security. In the era of Great Power Competition, it is essential that the United States develop a comprehensive national strategy for AI. The findings, analysis, and proposals found infra are offered to inform this strategy.

LOE 1 – Investing in AI R&D

General Overview

AI is a transformative technology that has the potential to revolutionize how we live, work, learn, discover, and communicate.[9] AI research can increase economic prosperity, improve quality of life, and enhance national security.[10] Consequently, AI R&D is a fertile battleground with many nations competing for advantage. The United States, Russia, and China have all prioritized the development and implementation of AI as the key variable in their respective quests for worldwide technological dominance.[11]

In response to President Trump's EO emphasizing the importance of AI, the Committee on Artificial Intelligence updated its National Artificial Intelligence Research and Development Strategic Plan to provide further coordination and guidance for AI R&D.[12] Despite this, the United States is still lacking in intentional guidance and direction for specific national security related AI research investments and development priorities. With the exception of the Defense Advanced Research Project Agency (DARPA), most government agencies are instructed only to make investments with industry and academia in AI R&D related to mission requirements.[13] This section provides several recommendations which build upon the foundation of the Committee's Strategic Plan.

Findings

The United States must **refine its AI strategic plan**. It must provide a unified expectation for where to invest, with established priorities for the development of hardware and software. It should provide a method of standardization and security for research databases while providing protection and incentives for AI R&D investment. The **government should lead in the development and implementation of AI** that supports the national security strategy. In this vein, the United States should **create a federally-funded organization for AI investment** that makes non-controlling equity investments in start-up technical companies that focus on delivering AI technology with national security and dual-use benefits.

LOE 1 - Recommendation 1 -- Refine the AI Strategic Plan

Establish a national agenda and roadmap for the development and advancement of AI based on requirements aligned to the National Security Strategy and the National Defense Strategy pertaining to innovation, inventions, research, and technology. This effort should be led by the NSCAI, who will provide guidance and direction on a whole-of-government approach at least through its current mandate ending in March 2021.

1.1 Rationale:

Although EO 13859 solidifies the United States' emphasis on advancing AI research, the majority of AI R&D is still funded through private sector investments. Current investment plans focus on general, or strong, AI over the next 5 to 10 years, but they should also consider near-term investments in narrow AI. Capitalizing on narrow AI investments in a 1- to 5-year timeframe may reduce the timeline for certain long-term AI developments. For example, using narrow AI in the development of new materials may yield better performing materials with enhanced properties. These enhanced properties could lead to higher transistor density on chips. In parallel, utilizing AI to improve and enhance current technology may allow for better AI

infrastructure and hardware. Prioritizing technology development should be led by experts in the AI field, such as the National Science Foundation (NSF). The NSF could function as the evaluator for research across the whole-of-government and focus on technologies that will contribute to the overall advancement of AI technology. Organizations like the Joint Artificial Intelligence Center (JAIC), the NSCAI, and the Defense Industrial Board (DIB), would all serve as guiding functions to help ensure funding is applied in areas most important to national security.

Critical to AI research is the establishment of standardized databases. Data standardization ensures information fields contain accurate information that is easily validated. These databases must be secured to prevent adversarial intrusion and theft of intellectual property. Protection of intellectual property is key to ensuring the United States maintains its technological lead in the development and advancement of AI. Placing these databases in a collocated location, such as the National Laboratories, will pave the way for establishing AI innovation centers, which can facilitate the integration of security and research. These trusted spaces can be utilized by multinational researchers, partners, and U.S. researchers for developing AI and provide a mechanism for the NSCAI to maintain control.

Finally, the development of dual-use AI technology has the potential to attract venture capital and corporate investment. The United States must create an investment model in which dual-use technology investments are incentivized and attractive for industry. For example, providing tax offsets for those who invest in government research could effectively triple the R&D dollars going to AI programs.

LOE 1 – Recommendation 2 – Coalesce around the NSCAI

Redefine a national AI whole-of-government approach under the guidance and supervision of the NSCAI. By placing control of the AI R&D efforts under the NSCAI, all AI programs can be unified while targeting the objectives outlined in EO 13859. Enforcing that AI R&D efforts fall within these objectives ensures that appropriate priorities are established and identified, security of research is maintained, and the United States maintains control over AI advancements while integrating public and private initiatives to maintain technological superiority over our adversaries.

1.2 Rationale:

The U.S. government should lead in AI R&D. Shortly following the release of EO 13859, the National Artificial Intelligence Research and Development Strategic Plan specifically addressed long-term investments in AI research.[14] Over the past year, development in AI applications has focused on narrow AI, specifically in the areas of weather, healthcare, transportation, and other commercial markets.[15] Per direction of the White House, federal agencies invest in AI initiatives according to their specific agency requirements. However, academia and industry dictate where AI R&D is focused. Thus, these government agencies must make individual efforts to leverage, incorporate, modify, and implement AI advancements to meet their mission requirements.

China's military and commercial AI programs are credible threats to the U.S.'s status as the world's leader.[16] Under its "China Dream" strategy, China invests in AI, autonomous vehicles, and robotics research and development at three times the rate of the United States.[17]

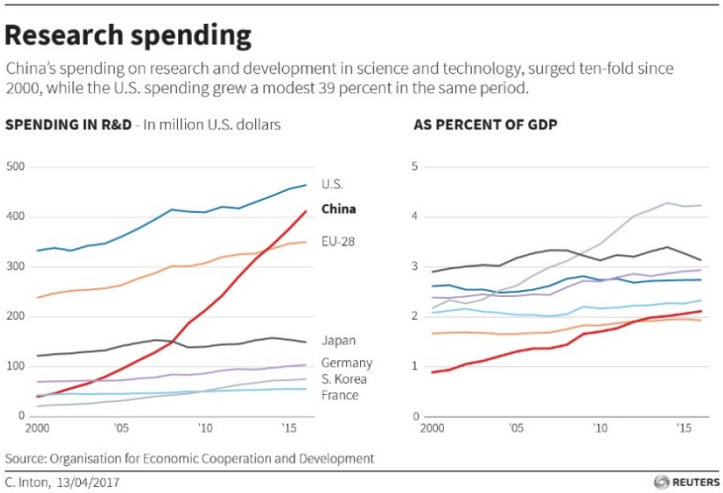

Figure 2 - China's R&D Spending Pattern verses the U.S.[18]

China's unified national strategy for AI aims to make them the world's dominating technological power by 2030.[19] The United States lacks such a unified national plan that clearly defines its national AI R&D priorities. The Department of Defense JAIC attempts to implement the DoD's AI strategy. Currently, the JAIC is focused on the following key mission areas: situational awareness, decision-making tools, developing partners, automating maintenance, and improving supply lines.[20] Similarly, the NSCAI focuses on implementing the U.S.'s national AI strategic plan, but there seems to be limited coordination to ensure industry, academia, and government efforts are synchronized.

LOE 1 – Recommendation 3 – Invest in AI Start-Ups

Create a new federally-funded AI investment organization. The U.S. government will offer an alternative to the venture capital (VC) funding ecosystem that provides lucrative opportunities in government research. Through this approach, the government will harness the power of the private sector while leveraging the vast technical talent that resides within the United States.

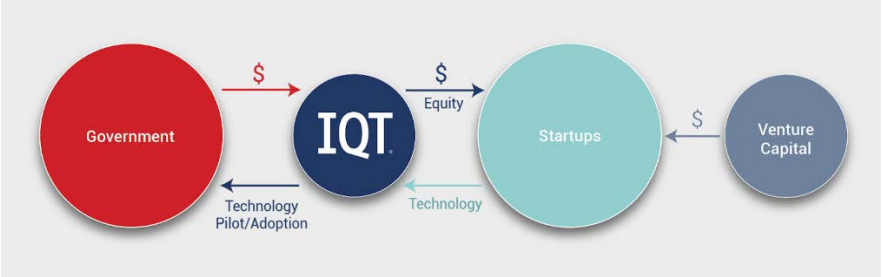

Figure 3 - Typical Government to VC Investment Model

1.3 Rationale:

In this current era of Great Power Competition, the United States must dedicate valuable resources to achieving and maintaining global leadership in research, development, and deployment of AI. The direction and pace of advancement in AI will solely depend on the source and extent of funding. Research organizations such as the Defense Advancement Research

Projects Agency (DARPA) and Federally Funded Research and Development Centers (FFRDC) currently develop technologies that advance U.S. national security and offer dual-use opportunities. Technologies like the Global Positioning System (GPS) and the predecessor to today's internet were born from these organizations.

During the 1990's, venture capitalists stepped into the driver's seat, dominating finances and altering the focus of research and innovation. Over time, their influence on minimizing loss and maximizing revenue caused commercial industry to recruit the best technical talents. As such, investors today favor short-term growth potential before considering any investments. This same mentality applies to the advancement of AI and related technologies. Increased public attention and source of investments continue to command AI's direction and scope. Narrow AI research and applications are beginning to deliver benefits with the promises of continued value in the future. Although various government agencies are investing in AI R&D, the scale and pace of these investments will be inadequate compared to what is required for national security.

LOE 2 –Applying AI to National Security

General Overview

AI is an ET that, when applied correctly, can promote and protect national security. Central to this application is the ability to ensure the validity and security of data that drives the AI system. This approach to data management must also include the ability to identify fake or untrue information.

It is in the national interest of the United States to prevent information attacks from eroding national institutions or harming the public. Information attacks, including such things as deepfake messages, can threaten "the viability and stability of major global systems" and directly threaten the national interest of promoting "democracy, prosperity, and stability."[21] These misinformation campaigns can, in particular, undermine security during a crisis or a major event such as elections. AI can be used to identify and defeat such threats but is reliant on valid data to be effective.

One of the advantages of AI is its ability to process large amounts of data quickly and use this data to better inform decision making. If computers are the engine for AI, then data is the fuel. In the 21st century, data is abundant, and, as the use of technology expands, the volume of data will continue to increase. One of the fundamental requirements for using this data in AI algorithms is the ability to ensure its validity. Therefore, as the value and use of this data increases, it must be effectively managed to allow AI to be utilized in defense of national security. This structured approach will create a standardized environment that allows additional AI capabilities to be developed, utilizing the same data sets.

Findings

To support national security, we must **establish national data standards to enable effective management and validity of data** for AI applications. To protect against AI driven misinformation campaigns we need to **establish a system to verify and validate publicly available information**.

LOE 2 - Recommendation 1 - A Strategy for National Data Management

Establish a national data management system that defines data and architecture standards to feed a nationally managed master data management system. A national data management system will:

- Establish data standards for U.S. data systems as a vision or a model to support the eventual interactions between data systems.
- Create master data management protocols (tool) – to identify key data sources of national security interest and how to access data if needed.
- Create trust with the American people that personal data, while available, is protected and used only in the interest of national security.

2.1 Rationale:

The use of AI for analysis and predictive analytics in support of decision-making is data dependent. Access to trusted data results in increased confidence in analytics, ultimately

increasing speed to informed and insight driven decisions. The U.S. ability to implement such a strategy will enable the use of AI to protect and promote national security and interests. The U.S.'s need for access to timely and reliable data is a constant talking point during the coronavirus disease of 2019 (COVID-19) pandemic. While part of the COVID-19 data issue is the limited volume of data, another issue is the lack of coherent data content standards across multiple data sources. Data content standards are the rules for how data are entered, for example, cataloging rules and syntax conventions.

China has stated they want to be the leader in technology standards by 2035.[22] Assuming this includes a data standard which encompasses methods, protocols, terminologies, and specifications for the collection, exchange, storage, and retrieval of information, this will limit the ability of the United States and its partner nations to access data necessary to inform decision making.

China runs the risk of losing credibility following its lack of transparency and misleading narratives regarding the origin and reporting on the COVID-19 pandemic. Coupled with existing concerns over its expansionist bent (evidenced by China's Belt and Road Initiative and its actions in the South China Sea) and about Huawei's ties to the government, the United States might find opportunities to curry favor in leading the development of international technology and data standards.

Many commercial groups and government agencies have implemented data management systems to manage and ensure the validity and availability of data for analytical purposes. The United States government needs similar data standards to allow analysis in support of national security objectives.

LOE 2 - Recommendation 2 - Verifiable Information Management & Countering Deepfakes

Develop and implement a whole-of-government policy for safeguarding the integrity of information and communications before threat entities use further information attacks to undermine U.S. vital interests.

This policy should:

- Establish an independent, non-partisan Information and Data Security Office (IDSO) under the direction of Congress to implement and oversee information security policy and data security guidelines and standards.
- Increase U.S. government funding for research and development of AI deepfake detection algorithms.
- Require all official government-created media (including video) to be digitally signed.
- Establish of an official IDSO website to act as a repository of verified and trustworthy guidance about national security, as well as personal health, wealth, and security information. This website should also highlight prevalent instances of fake information being disseminated in other channels.

- Assign well-known, well-respected, non-partisan leaders to lead the messaging campaign to the American public. Public support will be paramount to the success of the effort. Partner with a small, diverse group of popular culture icons – not politicians – to reach multiple generations and socioeconomic classes.

Because many will not trust the U.S. government's message in this matter, the government should seek solutions where private industry addresses the problem such as incentivizing private "watchdogs" and fact-checkers to better take on the role of highlighting fakes in the media and publicly hold media outlets accountable for their content.

2.2 Rationale:

As evidenced by recent events, the United States is not impervious to kinetic, cyber, information, and biological threats. While a whole of government approach is required to protect and combat against these threats, a similar effort is required to manage the information available and disseminated to the American public to prepare for, and maintain resiliency during a national security crisis. Simultaneously, the evolution of AI technology enables computers to generate "deepfake" video, audio, text, and imagery in such high fidelity that humans cannot distinguish them from their real counterparts. Deepfakes threaten to wreak havoc with functions of national institutions by distorting or faking communications, especially those from the government.

In this age of infinite information vectors, adversary influence campaigns, and the soon-to-be exponential rise in deepfake audio and video, the noise and misinformation can be overwhelming and has the capacity for large scale harmful effects. The issue becomes how to limit the dissemination of unverified and potentially harmful information and direct the public towards verified, non/bi-partisan, and 'wholesome' information. ET like Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI) will prove integral in assisting to solve this issue, as will the new capabilities and reach of 5G communications and quantum computing in the near future.

The following points must be considered as part of establishing information safeguards:

- The U.S. government is not without a history of 'information management.' On a scale far greater than recommended here, the WWII-era U.S. government employed extensive management in the form of censorship and propaganda disseminated by thousands of public news organizations.[23]

- The rate of technology adoption today far surpasses historical cases. The rate of digital usage has doubled in just the last ten years. "Social media platforms are used by one-in-three people in the world, and more than two-thirds of all internet users."[24]

- Trust in mainstream media is being eroded as "fake news" from the upper levels of government and social media is increasingly used as a news source with a cottage industry of outlets reinforcing users' confirmation biases.[25]

- The rise of AI-enabled Generative Adversarial Network (GAN) technology has enabled deepfake video that humans cannot distinguish from reality. Incentives in the entertainment industry create more investment in the creation of deepfakes than their detection.[26] Deepfake authoring applications are publicly available.

Today, the government is again called upon to mobilize the management of information. Rather than the WWII model of control, times call for one of assisted-focus and verification of truth.

The U.S. government's objectives for information resilience should be:

- Defend the ability to disseminate authentic verifiable government messages.
- Impede the use of deepfake media to undermine domestic and international public confidence in institutions.
- Create a safe environment for internet users, particularly the youth.
- Identify and inform users of false and potentially harmful information.
- Provide a focused, truthful, and resilient source of information in a national security crisis.

Any information resilience policy must consider the following:

- Balancing actions with the First Amendment will prove challenging. Government promoting information to citizens will elicit claims of an authoritarian government. Approaches to this problem must not become government censorship.
- Leadership will prove paramount in communicating the need to the public, the assistance it will provide them and their children, and the preservation of their rights to both read and write freely in all media formats.
- ET will offer increased ability to intelligently manage and customize information by any number of qualifiers, scan social media for "harmful" content, and provide focused messaging to assist those in need in times of need.

LOE 3 – Train and Recruit AI Talent

General Overview

AI professionals are hard to find, which translates to an intensely competitive market to employ and retain such uniquely talented professionals. The supply of top-tier AI talent cannot fulfill the current demand. According to the White House's Council of Advisors on Science and Technology, the U.S. shortfall of technical professionals over the past decade is nearly one million.[27] Amidst the advent of technology and absent coordinated action, this gap will widen.

Since human talent forms the base of the triangle of talent, data, and computing that will enable the use of AI, finding tech talent is vital to ensuring the economic and industrial success of nations as they transition to more networked systems and the Internet of Things (IoT). We do not have the luxury of neglecting any segment of the population that can contribute to the effort. We must address this scarcity immediately to grow the number of qualified professionals to meet future needs. If we do not, we will find ourselves obliged to "steal" talent from Allies and partners who also need it, thereby straining bilateral relationships the world over. Worse, we may be forced to siphon talent from less reliable source nations, creating additional security vulnerabilities in fields of study least able to withstand such turbulence.

Findings

The United States must grow its tech workforce by **identifying and nurturing talent early**, **fostering coherence** between the education system and national interests**,** utilizing **new hiring strategies**, and **breaking down gender biases** to maximize the full use of resources at our disposal.

LOE 3 - Recommendation 1 – Identify and Nurture Talent by Incentivizing K-12 STEM

Develop and roll-out a STEM credit system, like Social Security, whereby students bank "credits" for time spent studying preferred STEM-specific fields they can later "cash in" for student loan forgiveness. The Department of Education should design the program in close collaboration with the Social Security Administration to take advantage of the Administration's lessons learned over 85 years of practice and to minimize duplicative efforts. Such a policy would be easy for the public to understand and is based on a proven model that all of America already knows, trusts, and has (or will) derive benefit. It is worth noting that with the future of Social Security facing financial hardship and in need of reform, there may be a reluctance by some to adopt something akin to it.

3.1 Rationale:

Historically, the U.S. federal government has taken a backseat to the states in K-12 education. Since its foundation, the United States has enjoyed a community-based educational structure. Each state has its department of education and enjoys a high degree of control, setting standards for curricula and administering personnel. Attempts to federalize the system have historically been met with resistance, as we saw roughly twenty years ago. In 2002, Congress passed the controversial No Child Left Behind Act, which brought the federal government closer to the front lines of education, but primarily resulted in a hefty burden for students as standardized testing ran rampant. Some publications estimated that over the 12-year career of students, this legislation could add as many as 112 tests per student to meet the federal burden. [28]

In 2015, Congress replaced this act with Every Student Succeeds Act, which reduced the federal footprint in part by dropping the frequency of federal standardized tests administered in K-12. The federal government still exerts some influence through a set of minimum standards known as the "Common Core," however, nine states have opted out and several others have introduced legislation to withdraw from the Common Core. [29] Any further attempt to foist additional federal education standards on the states may result in an even more pronounced exodus from a perceived "Washington agenda".

The United States is still working to align the educational system with national AI goals and should expedite efforts to enrich the United States K-12 educational system with greater emphasis on skills needed to operationalize AI. Thus far, mandates – the stick – have not worked well. Incentives – the carrot – may work better. The federal government can play an essential role without intervening directly into the minefield that is curriculum management. It should shape the workforce currently inhabiting K-12 to guide top performers toward government-sponsored practicums in academia, at Federally Funded Research Development Centers (FFRDCs), at the NSF, and within industry. Providing a path to student loan forgiveness in certain key identified sectors will foster the growth of trained professionals within those sectors.

Examining the Commission on American National Interests reveals such an incentive program would support many "vital" national interests (the most important category identified by the Commission), as well as several interests from the next-highest category.[30] Developing a technically proficient citizenry is a precursor to developing and implementing AI and a secure IoT, having a safe and prosperous economy and industrial base, and shaping an international order and preserving major global systems.

Even before the U.S.-China "trade war" raged and COVID-19 reared its ugly head, the United States had begun reducing its intake of international students. The numbers were in continual decline from 2016-2019, marking the first three-year slide since statistics have been kept, according to the Association of International Educators (NAFSA). [31] Chiefly, this decline hurts our competitiveness, but it also debilitates the financials of a formidable national network – American universities. Addressing that deficiency then, should find support in all 50 states and among the respective members of Congress, especially those in states with high concentrations of academic institutions and/or with one or more of the 42 FFRDC recognized under Title 48 of the Code of Federal Regulations. Unlike a curriculum change, this would not require teacher support, so finding footholds within the thorny thickets of teacher unions would be unnecessary. This would instead be a direct campaign to the parents and students, who would most benefit from such a plan. Finding allies in academia would be feasible and advisable.

LOE 3 - Recommendation 2 – Meld K-12 with National Interests

Foster coherence between the education system and national interests. Motivate and facilitate domestic students to engage in AI-related educations; create a special financial and moral support system for motivating students from low-income families; launch special ET schools to develop national talents and motivate AI-related entrepreneurs; expand the scope of the Guidance for Regulation of AI Applications to include "general" AI; and establish a council or committee (within the National Science and Technology Council (NSTC) Select Committee on AI) to expand the ethical discussion to "general" AI and the interactions created with the associated technologies.

3.2 Rationale:

Although states and local governments primarily control the U.S. K-12 educational system (as discussed above), the federal government has an opportunity to foster greater coherence nationally in the education system by rallying the development of talents needed for AI technology. Every American child needs to have the opportunity to access STEM skills starting with the K-12 curriculum. To fortify these efforts, the United States should establish inclusive social systems that maximize the opportunity for the lower and middle-income students to participate in the curriculum needed for AI.

LOE 3 - Recommendation 3 – Grow AI from Within via New Hiring Strategies

Reorient from a model of recruiting established talent to a groom-and-develop model. The United States must shift focus to target undervalued skills and develop those individuals to maintain a competitive advantage in AI development. Targeting the top-tier AI personnel provides some immediate benefits, but also investing in the development of the youth can provide a long-term sustainable talent pool. Shifting the focus from top-tier candidates to recruiting high school, vocational school, and non-degreed talent is a way for government agencies in a highly competitive environment to acquire talented individuals before private industry, and other countries have an opportunity. Recruiting non-traditional candidates early and aligning their talents against current demands will exercise the purposeful expansion and development of their capabilities and allow the United States to overcome future challenges in the war for AI talent.

3.3 Rationale:

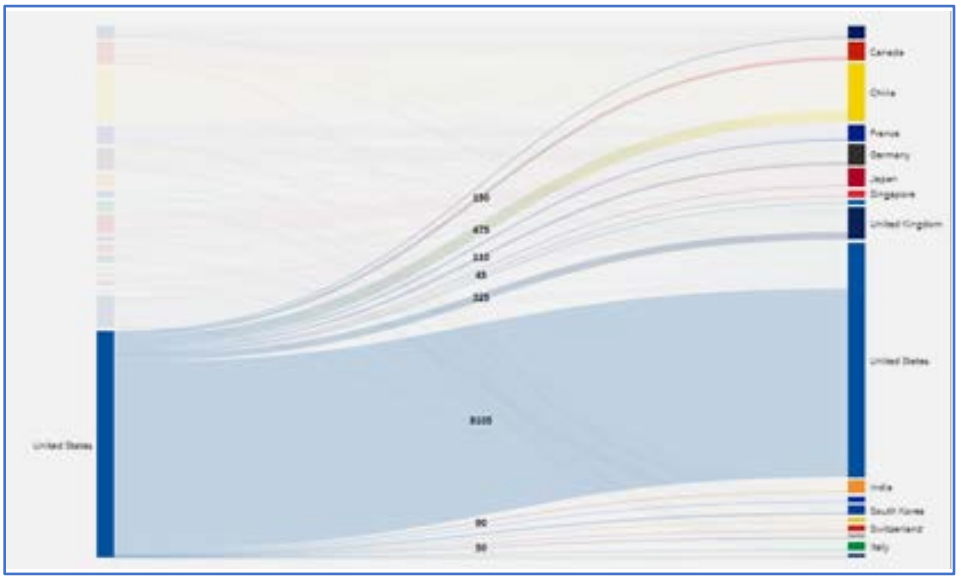

Figure 4 - The United States is currently the front-runner in AI development, and the bulk of global AI talent is trained and resident in the United States.[32]

The federal government needs to expand America's AI workforce to maintain a competitive edge. Countries are searching for ways to increase the size and enhance the skills of their AI workforce. The overall goal in the AI talent war is to widen the talent gap and ensure that competitors do not have the workforce to occupy AI positions to train, innovate, and deploy AI systems and research. Without bringing new AI talent aboard, the U.S. government cannot

move specific AI projects from ideation to implementation, therefore losing the competitive advantage over other adversaries in the Great Power Competition.

The ever-changing strategic environment and technological advancements create a desire and drive in governments to take the lead in research and AI development. The United States is currently the front-runner in AI development, and the bulk of global AI talent is trained and resident in the United States. However, that is not to say that the bulk of global AI talent is native to the United States. A recent Georgetown University study showed half of the AI talent in the United States was born abroad, as are two-thirds of graduate students in AI-related fields,[33] yet American immigration policies do not encourage international students to remain and work in the United States. Moreover, most international students hail from countries that rival the United States for developing AI. Whereas this is a potential benefit for global AI development and building international cooperation, it does not directly support U.S. national interests.

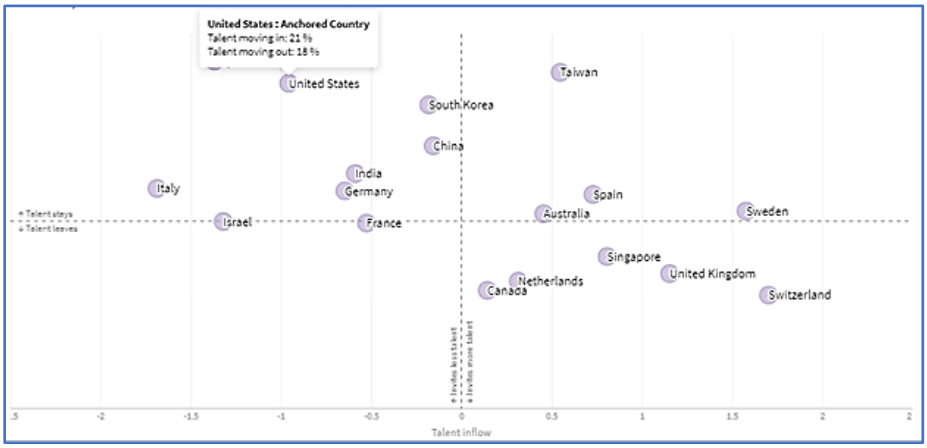

Figure 5 - A 2019 AI global talent report highlighted that 26% of AI talent resides in the United States (China is second at 13%), and 70% of talent is spread between five countries (U.S., China, United Kingdom, Germany, and Canada).[34]

A 2019 AI global talent report highlighted that 26% of AI talent resides in the United States (China is second at 13%), and 70% of talent is spread between five countries (U.S., China, United Kingdom, Germany, and Canada).[35] However, competitors are rapidly narrowing the gap. Countries like China, the United Kingdom, and Germany are continuing to make significant investments in growing their talent, either through training or through attractive visa opportunities and work conditions that lure foreign experts.[36] To maintain a lead, the United States must also recruit AI talent to remain in, or move in. The more talent that works in the United States, the more challenging the obstacles are for other countries to advance in AI.

LOE 3 - Recommendation 4 – Break Down Gender Biases in Hiring

Improve the Female Talent Pipeline. Develop public-private partnerships to create additional 'new collar' education programs and workforce re-entry programs for female talent, like IBM's P-TECH and IBM's Tech Re-Entry Program.[37]

LOE 3 - Recommendation 5 – Break Down Gender Biases in AI Systems

Address Gender Bias and Discriminations in AI Systems. Require the use of tools to identify and mitigate biases in systems, such as AI Fairness 360 by IBM. [38]

3.4 and 3.5 Rationales:

The AI sector suffers from a gender diversity crisis. This crisis impacts the U.S.'s AI talent pipeline, as well as the fairness of our nation's AI systems. The United States must build a diverse and inclusive workforce that closes the AI gender gap while also combating potential gender-related biases in AI. Narrowing the AI gender gap in the workforce will also help close gender parity while improving the economy. Achieving full, or even partial, gender parity results in significant economic gains for the nation. If the United States achieves partial parity, this will translate to an overall gain of $2.7 trillion to its gross domestic product (GDP).[39]

AI tools can be biased technically, but they are shaped by the environments in which they are built and by the people that create them. Addressing the underrepresentation of women in STEM fields is critical for narrowing the gender gap in the talent pipeline for AI. A more diverse AI workforce may contribute to fewer biases in AI systems by nature of increased diversity among system programmers.

A powerful web of systemic biases, discrimination, and power in society not only form gender biases but also profoundly influence women's participation in tech. The gender gap in STEM has widened since the 1980s when 37% of all computer science graduates in the United States were women.[40] Today, that number is a mere 18%. Currently, women make up 24.4% of the computer science workforce.[41] The percentage of computing occupations held by women has been declining since 1991 when it reached a high of 36%.[42] Now, only 26% of computing jobs are held by women.[43] Women represent only 18% of AI talent. Additionally, in the last five years, companies leading the charge in ET have only moved the needle a few percentage points toward increasing the representation of female tech talent in their companies. Technical female talent at Apple, Facebook, Google, and Microsoft ranges from 20 to 23 percent.[44]

LOE 4: Protect and Build Upon U.S. Technology Advantages

General Overview

Experts generally recognize the United States as the global leader in AI, but most also concede that China is quickly gaining ground. China's AI strategy envisions a coordinated effort between government, military, and industry to rapidly develop and implement AI throughout all aspects of society.[45] The United States has recently increased federal spending on AI, but this spending is devoted almost entirely to research and development (R&D) for defense solutions. While these efforts are essential, they are insufficient to keep pace with the coordinated efforts of our adversaries.

The U.S. government must play a vital role in building upon AI industrial and technological advantages beyond R&D spending. U.S. policy and resources must focus on setting favorable conditions for AI commercial innovation and investing in AI infrastructure and supporting technologies. This will, in turn, open the floodgates for innovative AI applications, which has the potential to spur exponential economic growth and improved national security.

Recent standardization developments pursuant to Executive Order 13859 are promising, such as the Office of Management and Budget (OMB) request for comment on AI regulations[46] and the National Institute of Standards and Technology (NIST) strategy for federal engagement in the development of AI technical standards.[47] But these are preliminary efforts with few resources attached. The United States needs immediate action to accelerate AI innovation and AI infrastructure and build a more resilient economy through improved emergency response coordination and supply chain security.

Findings

The United States must **leverage existing authorities**, such as the Defense Production Act (DPA), to seek non-defense AI solutions and make investments directly into domestic AI infrastructure and clusters throughout the country. Furthermore, the DPA allows the government to seek consensus advice from the AI industry to establish national data and security standards. This advice should form the basis for **an integrated national infrastructure (INI)**. The INI will form a standardized and integrated backbone on which AI-enabled applications can flourish. Finally, as the COVID-19 pandemic has demonstrated, the United States desperately needs to **strengthen its national readiness** for emergent crises. As such, we propose a cross-agency, cross-threat National Response Act that relies heavily on strengthened federal, state, and industry partnerships to maintain economic prosperity and resilience no matter the threat.

LOE 4 - Recommendation 1 – Expand DPA Title III Beyond the DOD

Expand Title III DPA offices to agencies outside of the DoD. Doing so will multiply Title III expertise and increase investments into more diverse AI fields, including the AI enabling infrastructure such as advanced semiconductors and 5G equipment. These offices should also give priority for DPA funding to AI projects.

LOE 4 - Recommendation 2 – Reinvigorate DPA Title III Loan Authority

Investigate opportunities for Title III loans with small AI companies and AI enabling technology and infrastructure sectors. Finally, although Title III loan authority has lain dormant, the Department of Treasury, in consultation with the Office of Management and

Budget, should investigate the potential market for such loans, particularly for enabling technologies and infrastructure for which there are no domestic manufacturers.[48] Alternatively, Title III loans could target smaller AI companies that are looking to partner with local governments and academia to create AI clusters.[49]

LOE 4 - Recommendation 3 – Build U.S. Infrastructure via DPA, Title VII

Form a consortium of AI developers, computer manufactures, and federal agencies for data standardization. The United States should also leverage Title VII voluntary agreement authority to form a consortium of AI developers, computer manufacturers, and various federal agencies to seek consensus on standards for AI implementation, data sharing, and data protection, which will inform the INI discussed below.

4.1, 4.2, 4.3 Rationales:

The Defense Production Act of 1950 (DPA) is an authority to "ensure the vitality of the domestic industrial base" and "provide for the national security."[50] Through its history, it has been effective at quickly procuring steel, aluminum, and other material goods. The DPA has yet to meaningfully contribute to the U.S. technological base—particularly AI. Although the FY21 Budget makes AI a priority,[51] the NSCAI's First Quarter Recommendations argue that more non-defense R&D funding is needed to keep pace with the economic and military threat from China.[52] Therefore, additional authorities—such as the DPA—should be leveraged to the maximum extent practicable to support the AI technological base.

The DPA currently consists of three general authorities:

- **Title I:** prioritizes government orders over all others through the Federal Priorities and Allocations System (FPAS) and Defense Priorities and Allocations System (DPAS)
- **Title III:** provides financial incentives and loans for U.S. industry
- **Title VII:** allows government and industry cooperation with antitrust protections.[53]

Title I is the most used authority within the DPA, but Titles III and VII provide the most potential support to the AI industry. DoD's Office of the Deputy Assistant Secretary of Defense for Industrial Policy (Office of Industrial Policy) is the only dedicated DPA Title III office in government, and the only one to recently receive Title III funds.[54] The office has successfully leveraged the DPA for technological solutions (sonobuoys, sUAVs, and rare earth element processing), but has done little with AI.[55] This is a lost opportunity because, in the Office's own words, Title III "has been used to forge new military capabilities and push the boundaries of science and technology" and is "an exceptionally effective tool for transitioning new technologies from research and development to production."[56]

While the COVID-19 pandemic has demonstrated that the DPA's authorities go beyond defense issues, its primary use has remained low-tech material goods. In 2009, Congress amended Title III to allow the President to make increased use of ET in security program applications and the rapid transition of ET from Government-sponsored research and development to commercial applications and from commercial research development to national

defense applications.[57] It is not apparent the government has yet used this authority to support ET. If the United States wants to maintain its global leadership in AI, it should leverage existing authorities like these to invest in the U.S. technological base.

LOE 4 – Recommendation 4 – Protect U.S. National Security Interests in the use of AI

Add AI to the Department of Commerce, Commerce Control List as a separate category. Label AI as a dual-use technology.

4.4 Rationale:

Rapid progress and development in AI create explosive potential for its value as a dual-use technology. From autonomous systems, to facial recognition, to decision-making algorithms, each emerging application of AI brings capability for public and government use.[58] This also brings enormous security risks. Consequently, AI must be considered a national security technology and added to the Commerce Control List (CCL) as a new category. The CCL already has categories including nuclear, chemical, telecommunications, electronic, and computers; however, there is no mention of AI in the latest update (March 2020). The separate category on the CCL will focus the department on the technology separately and create subcategories necessary to delineate the self-driving car AI from the political propaganda deep-fake AI.

LOE 4 - Recommendation 5 – Develop an Integrated National Infrastructure

***Create an Integrated National Infrastructure (INI) for AI and its supporting technologies*.** The federal government must bring together representatives from state and local governments, major industrial sectors, cellular and internet network providers, AI development companies, and academia to develop comprehensive standards for AI applications, data transmission, and data protection across networks and end-use equipment. State and local governments should develop public/private partnerships to incentivize and facilitate the construction and installation of equipment capable of meeting INI standards. Once established, private industry should be permitted to compete for updates into the INI, thereby ensuring the standards reflect the latest technology standards.

4.5 Rationale:

AI depends on infrastructure in the same manner as water, electricity, and cellular service. Cellphones are much less valuable if they cannot function across state lines or could only call other phones on the same service provider. In AI—as with many ET—the challenge is to harmonize infrastructure that is dispersed and stove-piped in order to reap widespread economic benefit. This requires the reexamination of how infrastructure should link together across the nation. A top-down INI would bring together networks to deliver the scale and data required for advancing the U.S. technological advantage.

AI-enabled technology requires network integration both within and across sectors that employ varying types of infrastructure. Disparities between network infrastructures currently limit the scale and the scope of AI applications—thereby limiting their potential. The INI would consist of a series of national standards to mitigate these disparities. Widespread adoption of these standards throughout the economy will create a technological backbone for integrating these systems across sectors. It will also enable large-scale data access, which will make AI applications more affordable. By focusing on infrastructure instead of specific AI technologies,

the government does not pick champions. Instead, it expands the marketplace by linking what were previously stove-piped applications. Companies will be motivated to adopt these standards in order to gain access to the marketplace, including the all-important data that makes AI run.

The INI seeks to mirror China's advantage in infrastructure synchronization. China has demonstrated that it is more effective at converting technological advantages into economic benefit and national security advantage. This is explained, at least in part, by China's governmental dominance over standards and commercial activities. Within the United States, commercial AI technology—much like most computing technology—has developed on its own, free from regulation. As a result, the concept of an INI is somewhat foreign. In China, on the other hand, the government is driving and, to a large extent, controlling AI innovation. Thus, the concept of a government-mandated infrastructure standard is only natural. While some may bristle about following China's lead, some level of government regulation of AI is inevitable. The goal is to craft regulation that enables technology rather than stifles it.

LOE 4 - Recommendation 6 – Strengthen National Readiness with Legislation

Enact National Readiness Legislation. A National Readiness Act would unify (or replace) existing disparate legislation, for example, The Defense Production Act, The Strategic and Critical Materials Stockpiling Act, The Patriot Act, The Stafford Act, and The CARES Act.[59]

LOE 4 - Recommendation 7 – Strengthen National Readiness with Strategy

Establish a National Readiness Strategy. The purpose of an NRS is to forecast requirements for personnel, material, and activities in response to threats enumerated in the NSS and to create plans to maintain economic capacity during times of crisis.[60] AI-enabled machine learning must be the foundation of the NRS, in that it will inform strategic decisions based on robust databases and modeling in order to reduce ambiguity. Inputs to such a system include not only forecasts but also historic expenditure totals from real-world emergency responses. For example: material used, personnel hours expended, and measured outcomes of actions during a hurricane response should feed the National Readiness System and Strategy.

LOE 4 - Recommendation 8 – Strengthen National Readiness through Industry

Standup Readiness Manufacturing Centers of Excellence. COEs will ensure the nation has resilient production capacity and supply chains during times of crisis, while also providing production capacity for economic growth and R&D when not in crisis. COE facilities will produce a wide array of critical and commercial-use products leveraging AI-enabled robotics.

4.6, 4.7, and 4.8 Rationales:

COVID-19 impacts in the United States highlight a lack of preparation to address the threats identified in the National Security Strategy (NSS). Deficiencies include the failure to understand response requirements (material, personnel, fiscal, etc.), failure to synchronize responses across government levels and agencies, and a lack of capacity to produce goods critical to domestic response efforts. Fortunately, this crisis provides opportunity to propel U.S. government adoption of AI-enabled decision-making processes and to advance domestic AI-enabled manufacturing. To rectify these issues, the United States should enact a National

Readiness Act, create a National Readiness Strategy, and create Centers of Excellence to manufacture critical goods.

The purpose of a National Readiness Act (NRA) is to improve upon the National Response Framework and National Incident Management System by establishing a unifying architecture for federal agencies concerning both preparation and response to threats identified in the NSS. The NRA would mandate a National Readiness Strategy (NRS) to annually synchronize federal and state preparation and responses to potential or active threats. It would also clarify department leadership and agency roles concerning national readiness. The Federal Emergency Management Agency's (FEMA) annual National Preparedness Report is a starting point but should expanded to include all agencies. The Department of Homeland Security, with FEMA as the lead, is likely the best agency to coordinate this strategy. Subordinate to the NSS, the NRS would complement the DOD's NDS through the unification of all agencies with equities concerning readiness and response. The NRS should complement and consider the National Defense Strategy (NDS).[61] Ultimately, the purpose of the Act is to ensure the economic prosperity of the nation during times of crisis. The proposed vehicle for this prosperity is critical material production facilities in nationwide Centers of Excellence.

COVID-19 has also highlighted the lack of domestic manufacturing and the fragility of U.S. supply chains. A robust National Security System must ensure a resilient economy during times of crisis. Thus, the NRA should also mandate Centers of Excellence (COEs), which would consist of manufacturing plants for vital materials. These facilities would be funded by federal grants, owned by the states, and operated through local partnerships with businesses and academic institutions. This framework represents a whole-of-nation approach to economic security, as advocated by Gruber and Johnson in their book "Jump-Starting America."[62] The production mandate for COEs would differ, allowing each one to specialize. The production facilities would employ a split-manufacturing approach: first producing annual quotas of critical goods, and then using any additional production capacity for a blend of private commercial production and R&D projects. As a result, COE's offer both creation of tangible security outcomes and economic investment for depressed areas across America.

LOE 5- Marshal Global AI Cooperation

General Overview

AI is one of the premier ET defining the global economy, warfighting, and even the parameters of the Great Power Competition. The first nation to truly harness this technology will position itself for global dominance. The United States needs a clear national narrative to get the entire country behind mobilizing AI and harnessing it as a comparative advantage in the international arena. Perhaps most importantly, the United States and its partners are in a global competition to shape AI norms.[63]

Marshalling a cohesive national narrative on AI is essential to address divided equities within the United States and to foster greater public trust regarding AI technology so that the United States can engage effectively in international cooperative efforts. Whereas the U.S. government and academia fund and develop the bulk of AI research, much of the expertise in implementing AI resides in the private sector. Some large private corporations have divided multinational interests, often favoring China. Therefore, U.S. investments (including STEM training for AI) have not resulted in immediate and direct returns on investment to Americans. As a result, the United States lacks a cohesive national narrative for engaging effectively internationally and needs to partner with industry and academia to increase U.S. competitiveness and exploit a national comparative advantage in AI.

Findings

As a matter of national security and economic prosperity, the United States must take steps to bring order domestically and internationally to AI technology and its infrastructure. These efforts should include an improved national narrative to **foster trust in AI technology**, the formal establishment of **public-private partnerships** to harness industry expertise in alliance building, and designing international agreements that **create global alliances for talent management** and **establish a framework for cross-border data flow**.

LOE 5 - Recommendation 1 – Create a Global Alliance for Talent Exchange

Complete a Five Eyes nation memorandum of agreement (MOU) on AI talent management. Include an annual AI talent symposium and promote collaboration utilizing the current classified intelligence network. In a two-to-five-year timeframe, expand the MOU to include other nations (a potential expansion group would include Germany, Singapore, Japan, and South Korea).

5.1 Rationale:

Building a global pool of talent between Allied nations will retain talent and facilitate AI technology for growth and development while denying it to adversaries. The current advantage the United States has in AI talent, particularly in the training realm, must continue. This talent will be the basis for future AI development. Allowing this talent and knowledge to migrate to adversary nations would be foolhardy. To counter China's strategy that aims to increase its AI capability, global alliances can protect, develop, and retain AI talent for the United States and its allies as well as prevent adversaries from acquiring AI talent and knowledge. [64] An alliance will reduce the likelihood that a nation or rogue actor will be able to access and develop talent and the AI capability to threaten national security.

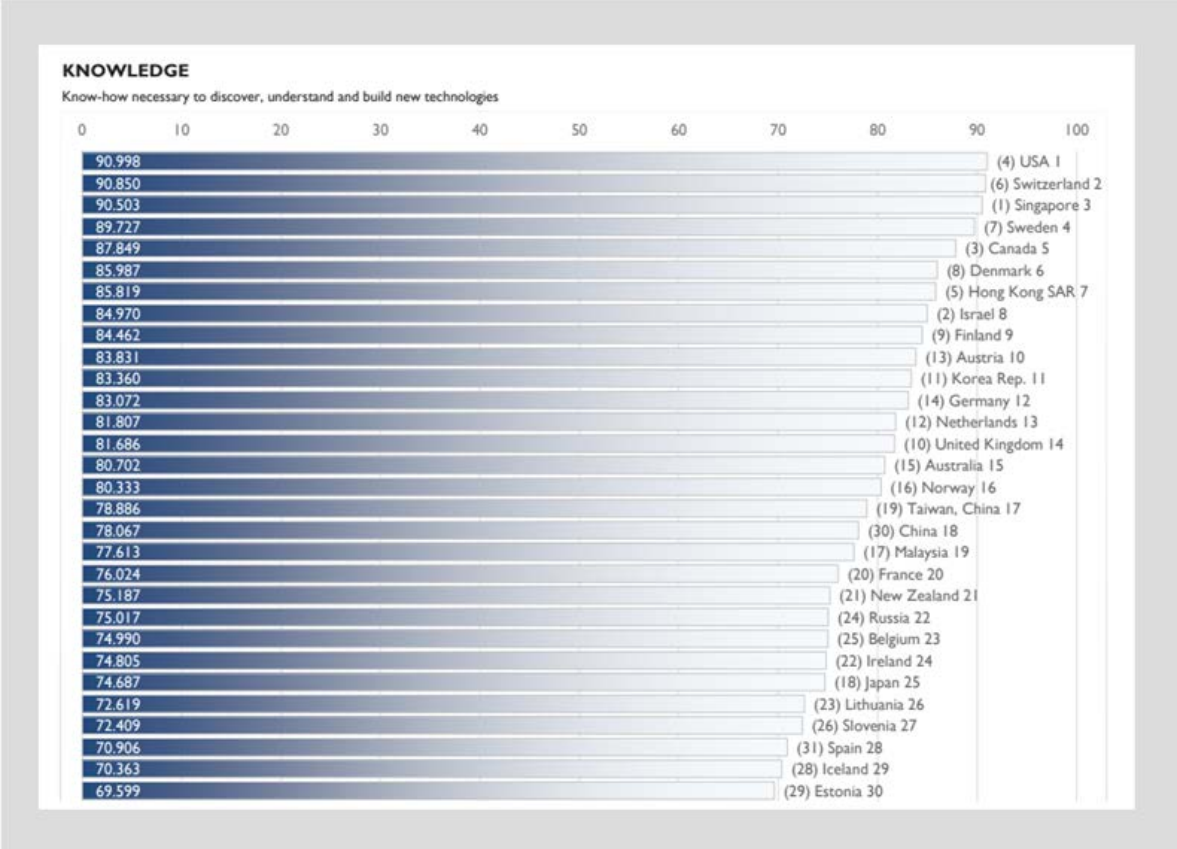

Figure 6 - World digital competitiveness knowledge rankings for 2019.[65]

The basis for partnerships is outlined in the 2018 DoD AI Strategy.[66] One way to enact this is to modify the Technical Cooperation Program (TTCP) to include AI and expand it to include other nations (either as is or in a modified form for non-five eyes nations). Alternatively, this could be completed under the NATO subgroups banner; this may counter the 'protect' aspect of the AI knowledge as it increases the likelihood of compromise and unauthorized release. A preferential system must also be put in place to make it easier for students from allied countries to study in the AI area. This system would be part of the alliance agreement and allow flexibility in how it is applied (e.g., foreign government-funded; or partial/full funding from DoD).

LOE 5 – Recommendation 2 – Foster Public Trust in AI Technology

Enact AI legislation which standardizes data collation. These laws should be founded in the principles of liberalism and focused on protecting human rights, with AI augmenting humans not replacing humans.

5.2 Rationale:

More Americans think AI will have a harmful impact on humanity than think its effects will be positive.[67] In order to fortify public trust, AI must perform in congruence with American values. The U.S. population is somewhat distrustful of AI primarily because so little is understood about the technology and the ethical collection, handling, and analysis of its underlying data. Therefore, the federal government needs to foster a culture of healthy trust through systems that ensure the protection of civil liberties, rights, the rule of law, autonomy, and other ethical American values.

Data collation methods and bias avoidance are critical to ensure AI is human-centered. AI development is a race and the winner will set the parameters for data usage. AI is heavily reliant on data and so data sharing standards are the foundation of AI. By establishing technical leadership with key partners, the United States can set standards and generate global support for what is right and ensure AI reflects American principles.

LOE 5 – Recommendation 3 – U.S. Public-Private Partnerships for AI Technology

Create Public-Private Partnerships (PPP) to advance AI nationally and interface with key partners. The United States should collaborate with partners now to establish AI alliances that leverage U.S. AI industry leaders and government leaders.

5.3 Rationale:

Public-Private Partnerships are critical for AI cooperation among allies and partners. The open design architecture of AI makes it accessible and applicable to an economically diverse set of players. The U.S. government has invested deeply in innovation, but AI is a technology that industry has outpaced government investment. A harmonized U.S. perspective would likely strengthen the U.S.'s bargaining position internationally. Therefore, to build upon the U.S. lead, synchronizing multilateral alliances and Public-Private Partnerships (PPP) is essential to ensuring AI is developed in the interests of the United States and its allies.

These PPP's should consist of companies like NVIDIA, Intel, Microsoft, Alphabet, Facebook, Amazon, and IBM. Certainly, any PPP company should be limited to U.S.-controlled companies with no connections to the Chinese Communist Party (CCP) or other foreign entities. These industry leaders will partner with government leaders from Commerce, Defense, Intelligence, State, and DARPA to form an AI conglomerate specializing in hardware, software, cloud, and communications with the mission to encourage interoperability, unbiased data, and standards for ethical use.

LOE 5 – Recommendation 4 – Establishing a Framework for Cross-border Data Flow

Lead the establishment and use of a Governance, Risk and Compliance (GRC) framework to scale-up and systemize the harmonization of cross-border data flows.

5.4 Rationale:

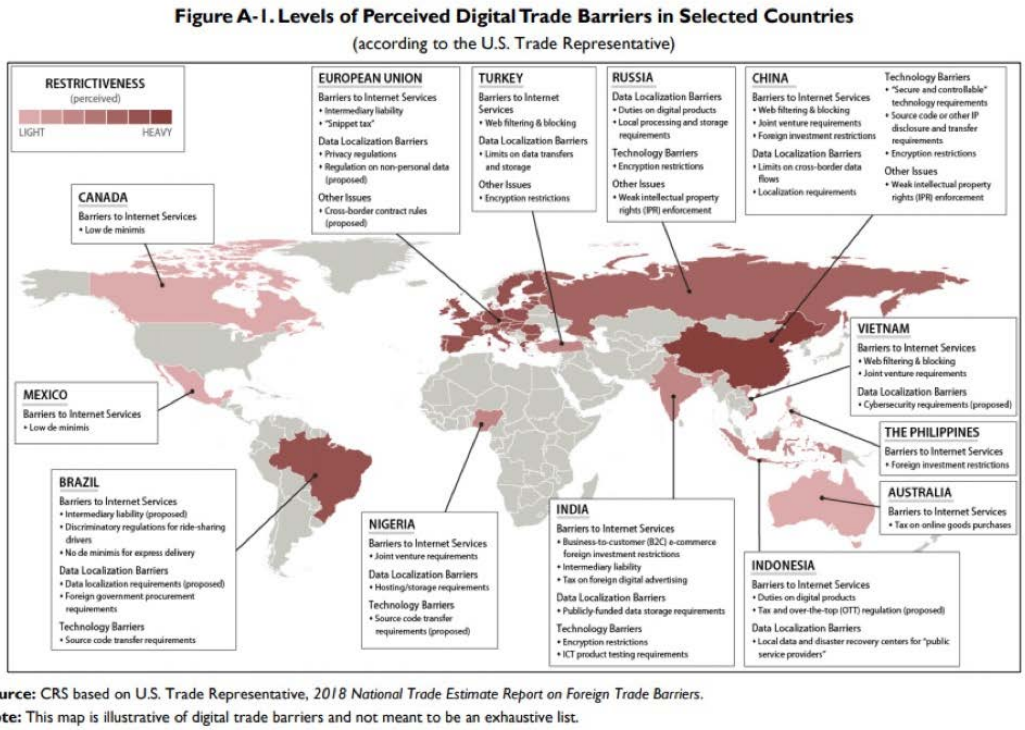

Figure 7 - Levels of perceived digital trade barriers in select countries according to the United States Trade Representative.[68]

AI and machine learning are powered by data – big data.[69] [70] However, the lack of international cooperation in cross-border data flows impedes the U.S. government's ability to fully capitalize on these technologies for addressing threats to national security as well as industry's ability to foster trade and economic expansion. The lack of common ethical standards for sharing data exacerbates the severity of common threats as evidenced by the global outbreak of COVID-19 and the resulting unprecedented disruption.[71] International standards in harmonized data flows and integrated global data will unleash the full potential of AI and ML as well as other data-driven technologies.

As of 2017, the Information Technology & Innovation Foundation (ITIF) determined that 34 countries (and counting) at every stage of development maintain barriers in cross-border data flows, often for sovereign data privacy and security rights but also to game the lack of systemization to their advantage for purely mercantilist reasons. Such a chaotic environment results in inefficiencies that restrict U.S. trade, reduce productivity and investment opportunities, and increase information technology (IT) costs. Therefore, the United States must lead the way for a harmonized international system that will bring order and efficacy to the data flows.

The issue of resolving competing risks, equities, and barriers in cross-border data flows is complicated but not unresolvable. [72] A Governance, Risk and Compliance (GRC) type of framework could systemize the harmonization of cross-border data flows. [73] GRC is recognized by the National Institute of Standards and Technology (NIST) and others for its viability in managing the complexities of big data and is used by many organizations to manage and mitigate competing risks and regulatory compliance (i.e., cybersecurity and audit governance) based on

organizational risk appetite.[74] GRC could serve as a baseline model for scaling up a harmonized international data risk framework that could be governed by an international data risk council comprised of global member states aimed at building consensus. Such an approach could improve the world order of data in contrast to the current chaotic environment as well as how stakeholders respond collaboratively to global cosmology risks and events (i.e., COVID-19).

Annex

The 2020 Global Pandemic and ET

The true impacts and implications of COVID-19 on ET are impossible to theorize, much less understand in May of 2020. The action-reaction cycles of governments around the world are churning with varying types and degrees of ET ranging from smart surveillance to disinfecting robots.[75] Demand signals are abundant, such as calls for AI-supported models and data analytics, but employing ET in this time of crisis presents concerns over privacy, data security, and freedom of movement. Now is the time to identify the hard questions confronting leaders today concerning the adoption and development of crisis-oriented technologies. What follows are five observations which serve to encourage further discussion.

How can ET be systemically adopted into leaders' decision-making processes in the absence of a catalytic crisis?

Decision making. Leaders in crisis need competitive tools to facilitate their decision-making processes, but they need them fully operational before the emergency strikes. At the executive level of large nation-states, decisions are not only life and death today, but may have uncorrectable consequences for generations to come. For example, the choice to risk economic prosperity for the health of the population is not one that can be overthought. Today's ET are accelerating the ability to gather and analyze data for leaders; however, the ability to efficiently process that analysis in time of true crisis is almost universally unpracticed.[76]

How can ET reduce the uncertainty of forecasts in crisis through understanding causalities?

Uncertainty. The uncertainty we see today has not been seen since World War II. That means most of today's leaders are not equipped with the inoculation of personal experience. While 9/11 and the 2008 financial crisis were significant challenges, they did not produce the scale of uncertainty caused by COVID-19. Today, people across the income spectrum do not know when or if their livelihoods will return. The uncertainty of economic prosperity and health safety is destabilizing. Leaders call upon ET to tighten probabilities through better understanding of causal relationships.[77] Leaders need to know what the impacts of their decisions will yield, but information is never perfect.[78] Their immediate needs range from forecasting virus movement and behavior to mitigating fragile, multi-national supply chains. Long term, every dollar spent today is an opportunity cost for tomorrow and every move creates risk balanced by opportunities.

How do leaders responsibly fast-track ET <u>believed</u> to be valuable during an ongoing crisis without creating externalities potentially more damaging than the original problem?

Opportunism. At the core of this discussion are opportunities created by a crisis – the Yin and Yang of opportunity and threat. This crisis is creating unprecedented opportunity for the advancement of ET. Public calls for a new 'Manhattan Project' are indicative of the willingness to pursue bold and risky ventures under the auspices of combatting the virus.[79] The reality is far more complicated, not unlike the drive for atomic weapons. What must be discussed is the space between *opportunity* for ET outcomes to advance health, security, and prosperity and *opportunism* advanced by those who would act to benefit personally from rapid and potentially reckless adoptions. Virus tracking applications may indeed provide a public good, but if they produce externalities which create biased outcomes, then pushing the ET may result in the long-term loss of public support.[80]

How do leaders in government and industry communicate the forecasted costs, benefits, and risks of adopting ET?

Trust. ET have an immense opportunity to gain the long-term trust of their global customers. Companies now have the tools and public attention needed to host honest dialogue about costs and benefits of adoption. However, if new tech is rapidly implemented in the name of pandemic response and long-term costs subsequently prove to outweigh the benefits, then trust is in jeopardy.[81] Measuring trust is not a matter of polling; rather, it is about behaviors.[82] How people spend their time, money, and votes reveal who and what they trust. Anti-movements around the world – 5G, vaccines, tracking – are emblematic of people who lack trust to the extent that they speak-out against adoption. Today, people in aggregate are listening more because of the uncertainty; this is an opportunity to be transparent, inclusive, and build trust in ET.[83]

How do ET potentially impact balances of power, domestically and internationally?

These five questions are designed to stimulate further discussion about the role of ET as an aggregate worthy of its own designation. The 2020 pandemic is destined to become the largest case study since the Cold War. What is done – or not done – will be analyzed by every academic discipline in perpetuity. It is therefore critical that policy recommendations concerning ET employment for the short-term mitigation of the pandemic be weighed in the context of long-term outcomes to the United States, its allies and partners, and the greater global commons.

Policy Recommendation for AI Enabled Pandemic Mitigation Tools.

General Overview

All technology is agnostic and can be used for good or ill. AI-Enabled tools, such as contact tracing or infection detection tools, may have valuable national security applications, but can also be used for racial profiling, violations of privacy, and targeting of vulnerable populations.[84] As the nation struggles with the spread of COVID-19, virtually every public health expert counsels us to undertake widespread monitoring and tracking coupled with effective utilization of the resulting data to curtail disease spread.[85] Technology is currently able to do all of this and more; the issue is how to do it within American principles. The U.S. government must pursue policies that maximize AI's potential but protect its citizen's privacy and civil liberties – the American way of AI must reflect American values.[86]

The U.S. currently lacks any comprehensive national data privacy laws, instead choosing to rely on contractual privacy restrictions generated from industry (through user consent). The only meaningful legal restrictions for AI enabled privacy concerns are Constitutional. The extent to which people are concerned about privacy depends on what the relative benefits are. In a time when people are concerned about life and death, people may be more willing to give up their data for greater health.[87] Even if this data is intended only for noble health or national security purposes, there are legitimate concerns for misuse, abuse, and cybersecurity threats.

Findings

Policy for AI enabled COVID-19 mitigation tools should: define the scope of collection, identify who collects, analyzes, and maintains the data, defines who is permitted to have access to the data, define the bounds for data usage and its timely destruction, and provide for public reporting and independent oversight.

Recommendations

The U.S. government should adopt a federal policy on AI enabled tools in support of pandemic relief. This memo recommends a **decentralized approach** and offers the following recommendations:

- The **scope of collection** must be limited to the data deemed necessary *by public health officials* to limit the spread of the pandemic. In order to limit potential abuse and engender maximum user trust, the data collected must be limited only to that relevant to combating the pandemic, seek patient consent when possible, and maximize de-identification of patient data in order to abide by existing healthcare privacy regulations, e.g. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- **Who collects, analyzes, and maintains the data** should include both industry *and* government entities in partnership. The government should in no way compel or force the adoption or use of any application but should remain involved in the process to counterbalance private industry motivations. Furthermore, AI-enabled pandemic mitigation tools should use a **decentralized approach** and store encrypted data on user's own device(s). A **third-party free approach** is necessary to further reduce potential misuse of data.[88]

- Only agencies and entities affiliated with counter-pandemic operations should be **permitted to have access to the data and only for uses** relevant to healthcare or pandemic related issues and only with explicit user consent. Legislation should require that users must explicitly consent to the use of any application and the data collected before any data is collected or analyzed.

- To avoid storing data beyond its intended useful purpose, and tempting entities to use it for other purposes, it is critical to mandate **timely destruction of collected data**. Legislation should mandate automatic deletion of data after a defined time, for example after 21 days (assuming a 14-day contagious period). Furthermore, policy should define the conditions where collection will cease, and all data deleted. Defined program termination conditions will help prevent collection extending beyond the pandemic threat.

- To provide transparency and engender trust, a combination of **public reporting and independent oversight** is necessary.[89] The government should publish, and continually update, exactly what data is collected and for what purpose. Moreover, the government should establish an independent oversight entity, reporting directly to Congress, to ensure compliance with all relevant policies and guidance.

- Additional **legal restrictions** should be explored. For example, several U.S. states have already adopted legislation limiting the use of facial recognition software due to privacy concerns. The government should explore privacy best practices as it pertains to AI-enabled tools, including those adopted abroad (like those in Europe, Japan, and elsewhere).

EndNotes

[1] Mohanad Halaweh. "Emerging Technology: What Is It?". *Journal of Technology Management & Innovation* Vol 8 No. 3, 108-15, accessed May 14, 2020, https://doi.org/10.4067/S0718-27242013000400010.
[2] National Security Commission on Artificial Intelligence (NSCAI), *Interim Report*, November 2019, 7, https://drive.google.com/a/nscai.org/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view?usp=sharing.
[3] Ibid.
[4] Alina Polyakova, "Weapons of the Weak: Russia and AI-driven asymmetric warfare," *Brookings*, last modified November 15, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.
[5] *Ibid.*, 5.
[6] Exec. Order No. 13859, 84 F.R. 3967 (Feb. 11, 2019).
[7] United States Navy, Chief of Naval Operations, "A Design for Maintaining Maritime Superiority," Version 2.0, December 2018.
[8] James Manyika et al., Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation, McKinsey Global Institute (Dec 2017).
[9] National Science and Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (Washington, DC: GPO, June 2019), 3.
[10] Ibid.
[11] Oliver Mitchell, "Is China An AI Security Concern," *AlleyWatch*, last modified on November 2019, https://www.alleywatch.com/2019/11/is-china-an-ai-security-concern/
[12] National Science and Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (Washington, DC: GPO, June 2019), iii.
[13] Loren Blinde, "DARPA Launches AI Exploration Funding Opp," *Intelligence Community News*, last modified on August 2, 2019, https://intelligencecommunitynews.com/darpa-launches-ai-exploration-funding-opp/.
[14] Ibid.
[15] Office of Science and Technology Policy, *American Artificial Intelligence Initiative Year One Annual Report* (Washington, DC: GPO, February 2020), 5.
[16] Gregory C. Allen, "China's Artificial Intelligence Strategy Poses a Credible Threat to U.S. Tech Leadership," *Council on Foreign Relations*, last modified on December 4, 2017, https://www.cfr.org/blog/chinas-artificial-intelligence-strategy-poses-credible-threat-us-tech-leadership
[17] Oliver Mitchell, "Is China An AI Security Concern," *AlleyWatch*, last modified on November 2019, https://www.alleywatch.com/2019/11/is-china-an-ai-security-concern/.
[18] Marius Zaharia, "Global R&D Spending is Now Dominated by Two Countries," *World Economic Forum*, last modified April 24, 2018, https://www.weforum.org/agenda/2018/04/trade-war-or-not-china-is-closing-the-gap-on-u-s-in-technology-ip-race.
[19] Oliver Mitchell, "Is China An AI Security Concern," *AlleyWatch*, last modified on November 2019, https://www.alleywatch.com/2019/11/is-china-an-ai-security-concern/.
[20] Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy* (GPO: Washington, DC, 2018), 11-12.
[21] Graham T. Allison, et al. "America's National Interests: A Report from the Commission on America's National Interests." Commission on America's National Interests, July 2000, 6.
[22] Emily de La Bruyère and Nathan Picarsic, "China Standards 2035 Bejing's Platform Geopolitics and 'Standardization Work in 2020'," *Horizon Advisory*, April 2020, accessed May 11, 2020, https://www.horizonadvisory.org/china-standards-2035-first-report.
[23] "The War, At Home, Communication," *Public Broadcast Station*, last modified September 2007, https://www.pbs.org/thewar/at_home_communication_news_censorship.htm.
[24] Esteban Ortiz-Ospina, "The Rise of Social Media," *Our World in Data*, las modified September 18, 2019, https://ourworldindata.org/rise-of-social-media.
[25] Rachel Dicker, "Avoid These Fake News Sites at All Costs," *U.S. News and World Report*, last modified November 14, 2016, https://www.usnews.com/news/national-news/articles/2016-11-14/avoid-these-fake-news-sites-at-all-costs.

[26] J.M. Porup, "How and Why Deepfake Videos Work –And What is At Risk," *Cyber Security Online*, last modified April 10, 2019, https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html
[27] President's Council of Advisors on Science and Technology, *Engage to excel: Producing one million additional college graduates with degrees in science, technology, engineering, and mathematics* (Washington, DC: GPO, February 2012), i.
[28] "K-12 Curriculum and pupil assessment," *Relocate Magazine*, last modified June 1, 2017, www.relocatemagazine.com/articles/education-k-12-curriculum-the-us-education-system.
[29] Kate Barrington, "An In-Depth Look at Common Core – What's Working and What Isn't?" *Public School Review*, last modified February 21, 2019, www.publicschoolreview.com/blog/an-in-depth-look-at-common-core-whats-working-and-what-isnt.
[30] Graham T. Allison, et al. "America's National Interests: A Report from the Commission on America's National Interests." Commission on America's National Interests, July 2000, 5.
[31] Evelina Nedlund, "The US economy is losing billions of dollars because foreign students aren't enrolling," *CNN Business*, last modified November 19, 2019, https://amp.cnn.com/cnn/2019/11/19/business/international-students-decline/index.html.
[32] "Some Observations on the Worldwide AI Talent Pool in 2019," *Jfgagne*, accessed May 9, 2020, https://jfgagne.ai/blog/ai-talent-2019/.
[33] Remco Zwetsloot et al., "Findings And Policy Options For International Graduate Student Retention," n.d., 27.
[34] "Some Observations on the Worldwide AI Talent Pool in 2019," *Jfgagne*, accessed May 9, 2020, https://jfgagne.ai/blog/ai-talent-2019/.
[35] Global AI Talent Report 2019 - *Jfgagne*," accessed May 9, 2020, https://jfgagne.ai/talent-2019/.
[36] "Some Observations on the Worldwide AI Talent Pool in 2019 - *Jfgagne*," accessed May 9, 2020, https://jfgagne.ai/blog/ai-talent-2019/.
[37] "IBM Tech Re-Entry Program," *IBM*, accessed on May 14, 2020, https://www.ibm.com/employment/inclusion/techreentry.html.
[38] "AI Fairness 360 Open Source Kit," *IBM Research Trusted AI*, accessed on May 14, 2020, http://aif360.mybluemix.net/.
[39] "Growing Economies Through Gender Parity," *Council on Foreign Relations*, Accessed April 28, 2020, https://www.cfr.org/interactive/womens-participation-in-global-economy/.
[40] Darina Lynkova, "Women In Technology Statistics: What's New?" *Techjury*, last modified May 7, 2019, https://techjury.net/stats-about/women-in-technology/#gref.
[41] Sarah Myers West, Meredith Whittaker and Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI", *AI Now Institute*, April 2019, accessed May 14 2020, https://ainowinstitute.org/discriminatingsystems.pdf.
[42] Catherine Ashcraft, Brad McLain and Elizabeth Eger, "Women in Tech: The Facts," *National Center for Women and Information Technology*, 2016, accessed May 14, 2020, https://www.ncwit.org/sites/default/files/resources/womenintech_facts_fullreport_05132016.pdf.
[43] Ibid.
[44] Sara Harrison, "Five Years of Tech Diversity Reports—and Little Progress." *Wired*, last modified October 1, 2019, https://www.wired.com/story/five-years-tech-diversity-reports-little-progress/.
[45] Government of China, *State Council Notice on the Issuance of the Next Generation Artificial Intelligence Development Plan, July 20, 2017*, posted at *NewAmerica.org*, translated by Roger Creemers, Graham Webster, Paul Triolo, and Elsa Kania, last accessed February 19, 2020, https://www.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf.
[46] Office of Management and Budget, *Draft Guidance for Regulation of Artificial Intelligence Applications*, https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.
[47] National Institute of Standards and Technology (NIST), *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, August 9, 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.
[48] Ellen Nakashima and Jeanne Whalen, "Barr suggests U.S. consider investing in Nokia, Ericsson to counter Huawei," *The Washington Post*, last modified February 6, 2020, https://www.washingtonpost.com/national-security/barr-warns-against-chinese-dominance-of-5g-super-fast-networks/2020/02/06/1da26794-48ec-11ea-9164-d3154ad8a5cd_story.html.
[49] Robert D. Atkinson and Stephen J. Ezell, *Innovation Economics* (New Haven: Yale University Press, 2012), 155.
[50] 50 U.S.C. § 4502.

[51] Office of Management and Budget, *A Budget for America's Future Budget of the U.S. Government* (Washington, DC: GPO, Fiscal Year 2021), 14, 21, 27, 29, 33-36, 44, https://www.whitehouse.gov/wpcontent/uploads/2020/02/budget_fy21.pdf.
[52] National Security Commission on Artificial Intelligence (NSCAI), *First Quarter Recommendations*, March 2020, 22, https://drive.google.com/file/d/1wkPh8Gb5drBrKBg6OhGu5oNaTEERbKss/view.
[53] "Defense Production Act Program," Federal Emergency Management Agency (FEMA), last accessed May 8, 2020, https://www.fema.gov/defense-production-act-program.
[54] Congressional Research Service (CRS), *The Defense Production Act of 1950*: *History, Authorities, and Considerations for Congress*, CRS Report R43767, Updated March 2, 2020, 12-13, https://crsreports.congress.gov/product/pdf/R/R43767.
[55] "Defense Production Act Title III," *DoD Office of Industrial Policy*, accessed May 10, 2020, https://www.businessdefense.gov/Programs/DPA-Title-III/.
[56] Department of Defense, *Fiscal Year 2017 Annual Industrial Capabilities Report to Congress*, March 2018, 31, https://www.businessdefense.gov/Portals/51/Documents/Resources/2017%20AIC%20RTC%2005-17-2018%20-%20Public%20Release.pdf?ver=2018-05-17-224631-340.
[57] "The Defense Production Reauthorization Act of 2009," P.L. 111-67 (September 30, 2009), § 303.
[58] Jayshree Pandya, "The Dual-Use Dilemma of Artificial Intelligence," *Forbes*, last modified January 7, 2019, https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/#6c775e616cf0
[59] "The Robert T. Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities as of June 2019," *FEMA*, last modified February 19, 2020, https://www.fema.gov/media-library/assets/documents/15271.
[60] National Security Council on Artificial Intelligence, *First Quarter Recommendations* (Washington, DC: GPO, March 2020).
[61] Homeland Security, *2019 National Preparedness Report* (Washington DC: GPO, 2019), https://www.fema.gov/media-library/assets/documents/184950.
[62] Jonathan Gruber and Simon Johnson, *Jump-Starting America* (New York: Public Affairs, 2019).
[63] National Security Commission on Artificial Intelligence (NSCAI), *Interim Report for Congress*, November 2020, 44.
[64] James Manyika and William H McRaven, "Innovation and National Security Keeping our Edge," *Council on Foreign Relations*, September 2019, accessed May 14, 2020, https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf.
[65] "IMD World Digital Competitiveness Ranking 2019," *IDM World Competitiveness Center* (2019), 12, access on May 19, 2020, https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/.
[66] Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: GPO, 2018), 13, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.
[67]Allan Dafoe and Baobao Zhang, *Artificial Intelligence: American Attitudes and Trends* (Center of Governance of AI, Future of Humanity Institute: University of Oxford: 2019), accessed on May 14, 2020, https://governanceai.github.io/US-Public-Opinion-Report-Jan-2019/high-level-machine-intelligence.html#subsecharmgood.
[68] CRS Report R44565, Digital Trade and U.S. Trade Policy, May 21, 2019, 40.
[69] Willem Sundblad, "Data Is The Foundation For Artificial Intelligence And Machine Learning," *Forbes*, last modified October 18, 2018, https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#1d70d17651b4.
[70] "Are data more like oil or sunlight?," *The Economist*, last modified February 20, 2020, https://www-economist-com.nduezproxy.idm.oclc.org/special-report/2020/02/20/are-data-more-like-oil-or-sunlight.
[71] National Security Council for Artificial Intelligence, *Privacy and Ethics Recommendations for Computing Applications Developed to Mitigate COVID-19: White Paper Series on Pandemic Response and Preparedness, No. 1*, accessed May 7, 2020, https://drive.google.com/file/d/1m0AT21dS2XJ6JIGMgo7SuLSLveWIO8WK/view.
[72] Henry H. Willis, Genevieve Lester and Gregory F. Treverton, "Information Sharing for Infrastructure Risk Management: Barriers and Solutions." Intelligence and National Security Vol. 24, No. 3, 339–365, June 2009, Accessed May 6, 2020,

http://eds.b.ebscohost.com.nduezproxy.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=1&sid=834e79b8-4f48-4088-b84d-e44bf58581a4%40pdc-v-sessmgr04.

[73] "NIST Special Publication 1500-4r2, *NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Version 3*, United States Department of Commerce, National Institute of Standards and Technology (NIST), October 2019,: 40-48, accessed May 7, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-4r2.pdf.

[74] Ty Greenhaigh, "Aligning Governance, Risk, and Compliance." *Journal of the American Health Information Management Association*, last modified February 1, 2020, https://journal.ahima.org/aligning-governance-risk-and-compliance/.

[75] "8 Ways Emerging Technologies Tackle the Coronavirus Pandemic," *StartUs Insights*, accessed May 14, 2020, https://www.startus-insights.com/innovators-guide/6-ways-technologies-tackle-the-global-coronavirus-pandemic/

[76] Brandi Vincent, "Pentagon Task Force Turns to Data to Shape COVID-19 Response," *Nextgov*, last modified May 12, 2020, https://www.nextgov.com/analytics-data/2020/05/pentagon-task-force-turns-data-shape-covid-19-response/165345/

[77] Dana Mackenzie, and Judea Pearl, *The Book of Why: The New Science of Cause and Effect*. New York: Basic Books, 2018.

[78] "Donald Rumsfeld Quotes," *BrainQuote*, accessed May 14, 2020, https://www.brainyquote.com/quotes/donald_rumsfeld_148142

[79] "A Manhattan Project for COVID-19," *The Wall Street Journal*, accessing on May 14, 2020, https://www.wsj.com/podcasts/the-journal/a-manhattan-project-for-covid-19/0e00ca30-b67f-404d-9b65-f9e6d1f5bf92

[80] "White Paper Series on Pandemic Response and Preparedness," *NSCAI*, accessed May 14, 2020, https://www.nscai.gov/

[81] Consider dissent over the Patriot Act years after 9/11. Also consider Amara's Law.

[82]Aaron Bycoffe, Christopher Groskopf and Dhrumil Mehta, "How American's view the Coronavirus Crisis And Trump's Response," *FiveThirtyEight*, last modified May 14, 2020, https://projects.fivethirtyeight.com/coronavirus-polls/

[83]"Discover What Americans are Watching, Playing, Listening To, and More," *Nielsen*, accessed May 14, 2020, https://www.nielsen.com/us/en/top-ten/

[84] NSCAI, *Interim Report for Congress*. 2019. National Security Commission on Artificial Intelligence, 49.

[85] Glenn S. Gerstell "Public Surveillance to Keep us Healthy and Protect our Privacy," *Center for Strategic & International Studies*, last modified April 16, 2020, https://www.csis.org/analysis/public-surveillance-keep-us-healthy-and-protect-our-privacy?utm_source=CSIS+All&utm_campaign=ce024e0e04-EMAIL_CAMPAIGN_2018_11_19_06_21_COPY_01&utm_medium=email&utm_term=0_f326fc46b6-ce024e0e04-150501265

[86] NSCAI, *Interim Report for Congress November 2019* (Washington, DC: GPO, 2019): 6.

[87] Patrick McGee, Hannah Murphy and Tim Bradshaw. "Coronavirus apps: the Risk of Slipping into a Surveillance State," *The Financial Times*, April 28, 2020, https://www.ft.com/content/d2609e26-8875-11ea-a01c-a28a3e3fbd33

[88] NSCAI, *Privacy and Ethics Recommendations for Computing Applications Developed to Mitigate COVID-19.* National Security Commission on Artificial Intelligence, 11.

[89] Glenn S. Gerstell "Public Surveillance to Keep us Healthy and Protect our Privacy," *Center for Strategic & International Studies*, last modified April 16, 2020, https://www.csis.org/analysis/public-surveillance-keep-us-healthy-and-protect-our-privacy?utm_source=CSIS+All&utm_campaign=ce024e0e04-EMAIL_CAMPAIGN_2018_11_19_06_21_COPY_01&utm_medium=email&utm_term=0_f326fc46b6-ce024e0e04-150501265