An Overview of Administration Activities in Artificial Intelligence

and the importance of R&D in AI+Cybersecurity

Lynne Parker, Ph.D.
Assistant Director for Artificial Intelligence
Office of Science and Technology Policy

Computational Cybersecurity in Compromised Environments (C3E)
Organized by SCORE (Special Cyber Operations Research and Engineering)

September 18, 2018

Artificial Intelligence: an Administration Perspective

"We're on the verge of new technological revolutions that could improve virtually every aspect of our lives, create vast new wealth for American workers and families, and open up bold, new frontiers in science, medicine, and communication."

- President Donald J. Trump

"Artificial intelligence holds tremendous potential as a tool to empower the American worker, drive growth in American industry, and improve the lives of the American people. Our free market approach to scientific discovery harnesses the combined strengths of government, industry, and academia, and uniquely positions us to leverage this technology for the betterment of our great nation."

- Michael Kratsios, Deputy Assistant to the President for Technology Policy

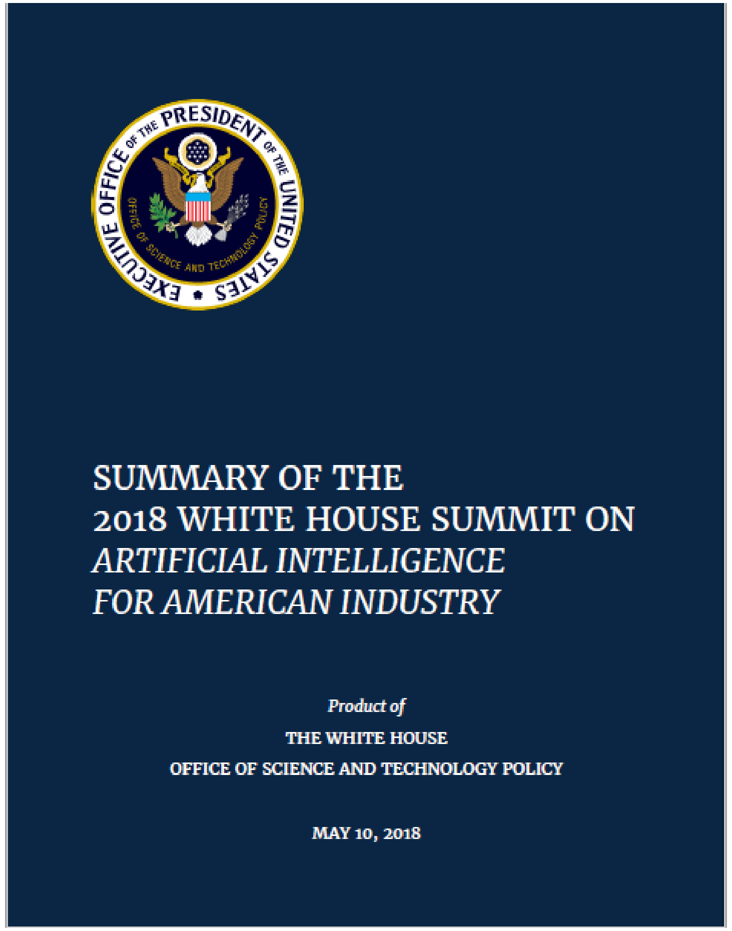
2018 White House Summit on AI for American Industry

- May 10, 2018
- 100+ participants: senior government officials, top AI academics, heads of industrial research labs, American business leaders
- two sets of breakout sessions:
  - *cross-cutting issues:* AI R&D, workforce development, regulatory barriers to AI innovation
  - sector-specific applications: food and agriculture, energy and manufacturing, financial services, healthcare, and transportation and logistics

2018 White House Summit on AI for American Industry

Key takeaways:

- Support the national AI R&D ecosystem, including stronger public-private partnerships to accelerate AI R&D
- Remove barriers to AI innovation in the United States.
- Develop the American workforce to take full advantage of the benefits of AI.
- Enable high-impact, sector-specific applications of AI



SUMMARY OF THE
2018 WHITE HOUSE SUMMIT ON
ARTIFICIAL INTELLIGENCE
FOR AMERICAN INDUSTRY

Product of
THE WHITE HOUSE
OFFICE OF SCIENCE AND TECHNOLOGY POLICY

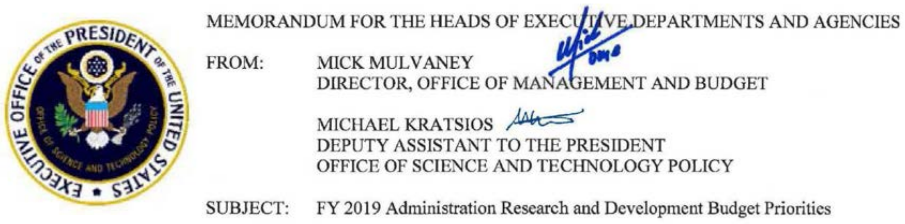
MAY 10, 2018

Summary report available:
https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf

Artificial Intelligence for the American People: *Key Priorities*

- Prioritizing funding for AI R&D including machine learning, autonomous systems, research cyberinfrastructure
- Removing Barriers to AI Innovation: removing regulatory barriers to deployment of AI-powered technologies
- Ensuring an AI-ready future American workforce: K-12, re-training/Re-skilling, undergraduate, R&D workforce
- Achieving strategic military advantage: recognizing need to lead in AI, with DoD investing accordingly.
- Leveraging AI for government services: applying AI to improve the provision of government services
- Leading international AI negotiations: OSTP led U.S. delegations to 2017 & 2018 G7 Innovation and Technology Ministerials, working with our allies to recognize potential benefits of AI, promote AI R&D.

Prioritizing Funding for AI R&D



MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

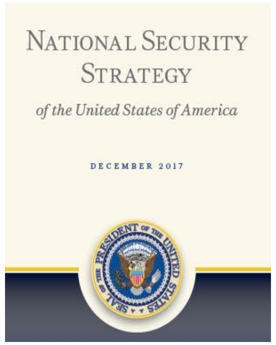
FROM: MICK MULVANEY
DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET

MICHAEL KRATSIOS
DEPUTY ASSISTANT TO THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY

SUBJECT: FY 2019 Administration Research and Development Budget Priorities

FY 2019 R&D Budget Priorities memo

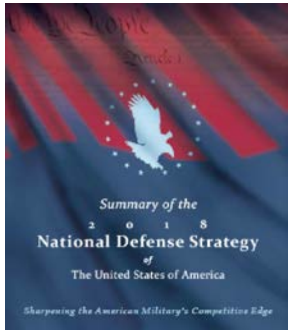
“autonomous systems, … machine learning, and quantum computing ….. coordinated interagency initiatives, … STEM education, including computer science education "



NATIONAL SECURITY STRATEGY
of the United States of America
DECEMBER 2017

National Security Strategy

“prioritize emerging technologies critical to economic growth and security, such as data science, encryption, autonomous technologies,… advanced computing technologies, and artificial intelligence. “



Summary of the
2018
National Defense Strategy
of
The United States of America
Sharpening the American Military's Competitive Edge

National Defense Strategy

“.. invest broadly in military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs.”

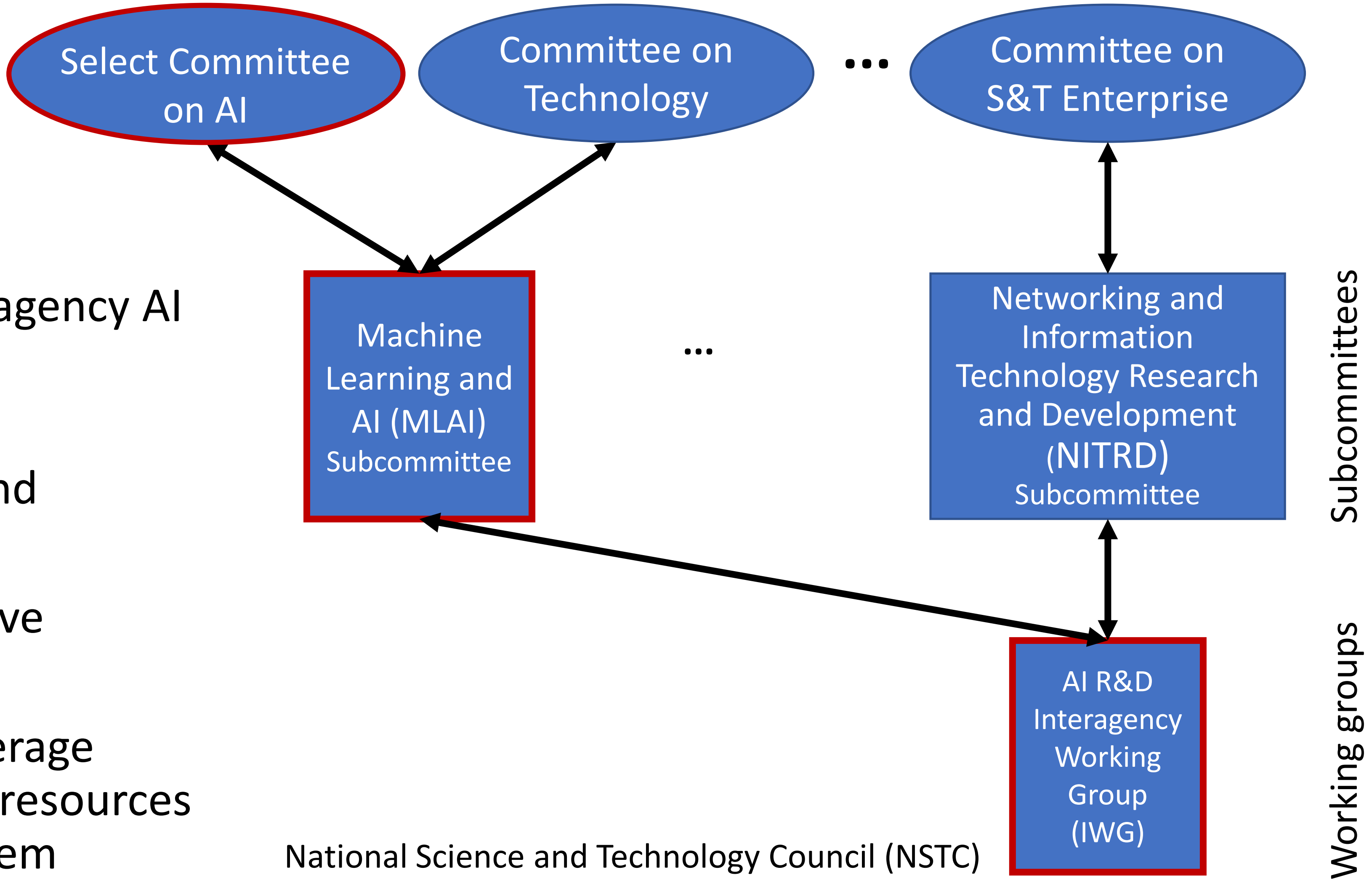
“AI holds the potential to transform the lives of Americans.”

FY19 President’s Budget, Analytical Perspectives

Coordinating Federal AI R&D: Select Committee on AI

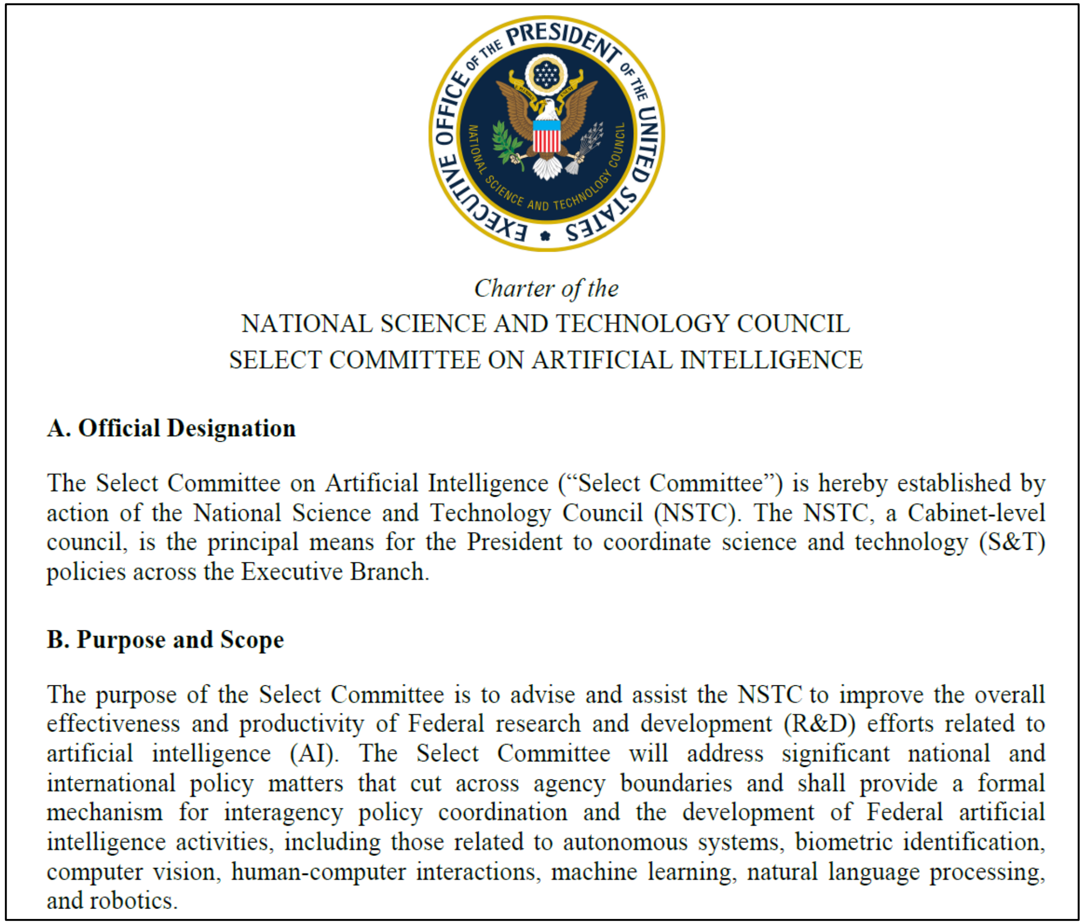
Membership: most senior Federal R&D officials:

- advise White House on interagency AI R&D priorities;
- consider creation of Federal partnerships with industry and academia;
- establish structures to improve coordination of AI R&D; and
- identify opportunities to leverage Federal data, computational resources in support of AI R&D ecosystem


Select Committee on AI
Committee on Technology
…
Committee on S&T Enterprise
Machine Learning and AI (MLAI) Subcommittee
…
Networking and Information Technology Research and Development (NITRD) Subcommittee
Subcommittees
AI R&D Interagency Working Group (IWG)
Working groups
National Science and Technology Council (NSTC)

Membership of Select Committee on AI

- Undersecretary of Commerce for Standards and Technology
- Undersecretary of Defense for Research and Engineering
- Undersecretary of Energy for Science
- Director, NSF (co-chair – F. Córdova)
- Director, DARPA (co-chair – S. Walker)
- Director, IARPA
- Representatives from:
  - National Security Council
  - Office of the Federal CIO
  - Office of Management and Budget
  - Office of Science and Technology Policy (co-chair – M. Kratsios)



Charter of the
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE

A. Official Designation

The Select Committee on Artificial Intelligence ("Select Committee") is hereby established by action of the National Science and Technology Council (NSTC). The NSTC, a Cabinet-level council, is the principal means for the President to coordinate science and technology (S&T) policies across the Executive Branch.

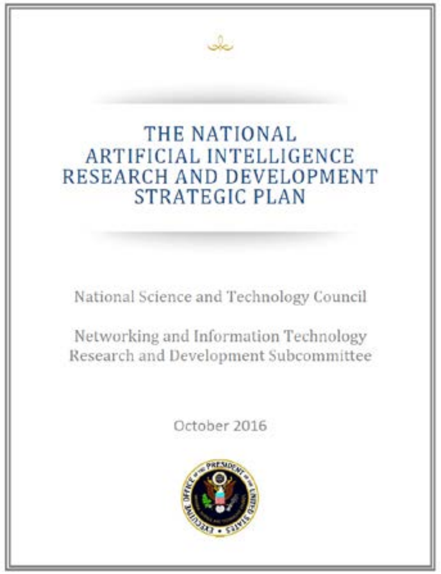
B. Purpose and Scope

The purpose of the Select Committee is to advise and assist the NSTC to improve the overall effectiveness and productivity of Federal research and development (R&D) efforts related to artificial intelligence (AI). The Select Committee will address significant national and international policy matters that cut across agency boundaries and shall provide a formal mechanism for interagency policy coordination and the development of Federal artificial intelligence activities, including those related to autonomous systems, biometric identification, computer vision, human-computer interactions, machine learning, natural language processing, and robotics.

May 2018

Guiding Federal AI R&D Investments: *National AI R&D Strategic Plan* (2016) (1/2)

- ***Strategy 1: Make long-term investments in AI research.*** Prioritize investments in the next generation of AI that will drive discovery and insight and enable the United States to remain a world leader in AI.
- ***Strategy 2: Develop effective methods for human-AI collaboration.*** Rather than replace humans, most AI systems will collaborate with humans to achieve optimal performance. Research is needed to create effective interactions between humans and AI systems.
- ***Strategy 3: Understand and address the ethical, legal, and societal implications of AI***. We expect AI technologies to behave according to the formal and informal norms to which we hold our fellow humans. Research is needed to understand the ethical, legal, and social implications of AI, and to develop methods for designing AI systems that align with ethical, legal, and societal goals.
- ***Strategy 4: Ensure the safety and security of AI systems.*** Before AI systems are in widespread use, assurance is needed that the systems will operate safely and securely, in a controlled, well-defined, and well-understood manner. Further progress in research is needed to address this challenge of creating AI systems that are reliable, dependable, and trustworthy.



THE NATIONAL
ARTIFICIAL INTELLIGENCE
RESEARCH AND DEVELOPMENT
STRATEGIC PLAN

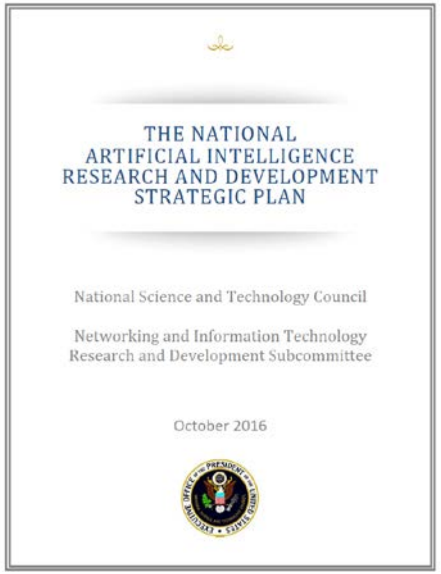
National Science and Technology Council

Networking and Information Technology
Research and Development Subcommittee

October 2016

Guiding Federal AI R&D Investments: *National AI R&D Strategic Plan* (2016) (2/2)

- ***Strategy 5: Develop shared public datasets and environments for AI training and testing.*** The depth, quality, and accuracy of training datasets and resources significantly affect AI performance. Researchers need to develop high quality datasets and environments and enable responsible access to high-quality datasets as well as to testing and training resources.
- ***Strategy 6: Measure and evaluate AI technologies through standards and benchmarks.*** Essential to advancements in AI are standards, benchmarks, testbeds, and community engagement that guide and evaluate progress in AI. Additional research is needed to develop a broad spectrum of evaluative techniques.
- ***Strategy 7: Better understand the national AI R&D workforce needs.*** Advances in AI will require a strong community of AI researchers. An improved understanding of current and future R&D workforce demands in AI is needed to help ensure that sufficient AI experts are available to address the strategic R&D areas outlined in this plan.



THE NATIONAL
ARTIFICIAL INTELLIGENCE
RESEARCH AND DEVELOPMENT
STRATEGIC PLAN

National Science and Technology Council

Networking and Information Technology
Research and Development Subcommittee

October 2016

What does the *Plan* say about AI+cybersecurity?

Securing against attacks:

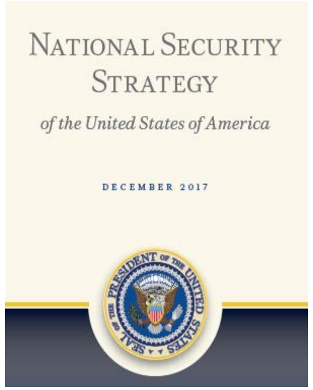
- "AI embedded in critical systems must be robust … to accidents and ... secure to a wide range of intentional cyber attacks."
- AI-specific cybersecurity risks include *Adversarial machine learning* – compromising AI by:
  - Contaminating training data
  - Modifying algorithms
  - Making subtle changes to an object to prevent it from being correctly identified
- Increase understanding of how to use AI to autonomously analyze and counter cyber attacks (e.g., *DARPA's Cyber Grand Challenge)*

(from the *National AI R&D Strategic Plan,* pg. 29-30)

Broad R&D Challenges in AI+Cybersecurity

- Data poisoning attacks (data that causes learning system to make mistakes)
- Adversarial examples (inputs designed to be misclassified by AI systems)
- Exploitation of flaws in design of AI system’s goals
- Etc.

Cybersecurity is Fundamental to National Prosperity and Security



NATIONAL SECURITY STRATEGY

of the United States of America

DECEMBER 2017

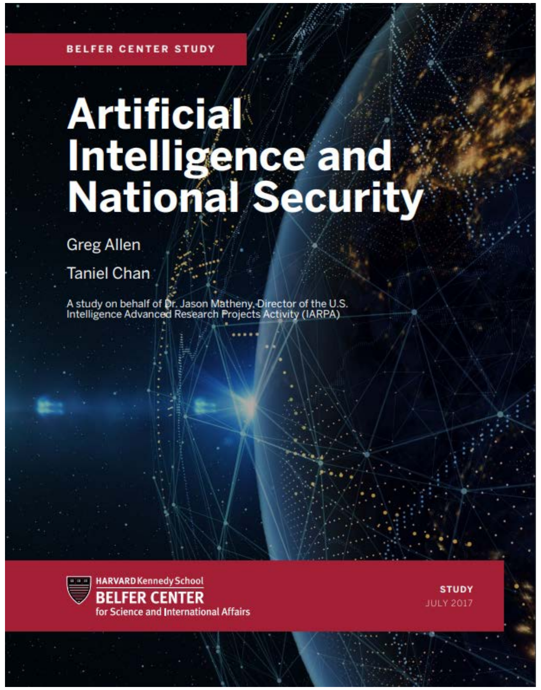
From National Security Strategy, 2017:

- *America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security.*
- *Cyberattacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.*
- *The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication. Adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.*

AI’s role in cybersecurity

From *Artificial Intelligence and National* Security, the Harvard Kennedy School study by Greg Allen and Taniel Chan for IARPA, July 2017 (pg. 18):

- *In response to a question from the authors of this report, Admiral Mike Rogers, the Director of the National Security Agency and Commander of U.S. Cyber command, said “****Artificial Intelligence and machine learning—I would argue—is foundational to the future of cybersecurity*** *[…] We have got to work our way through how we’re going to deal with this. It is not the* if, *it’s only the* when *to me.”*



BELFER CENTER STUDY

Artificial Intelligence and National Security

Greg Allen

Taniel Chan

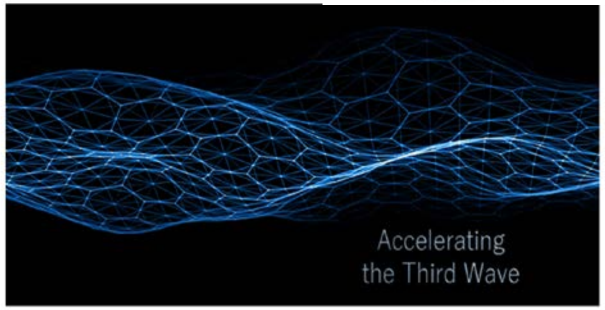
A study on behalf of Dr. Jason Matheny, Director of the U.S. Intelligence Advanced Research Projects Activity (IARPA)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

STUDY
JULY 2017

Prioritizing AI: DARPA’s “AI Next” Investments

AI Next Campaign

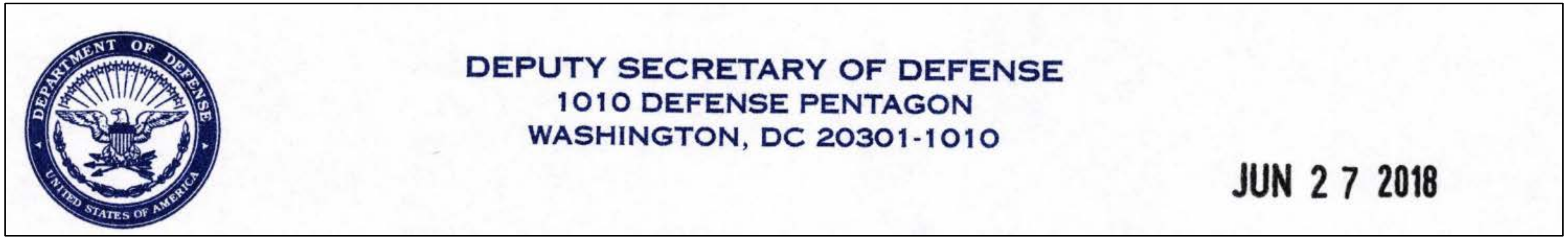


Accelerating the Third Wave

- In Sept. 2018, announced “AI Next”:

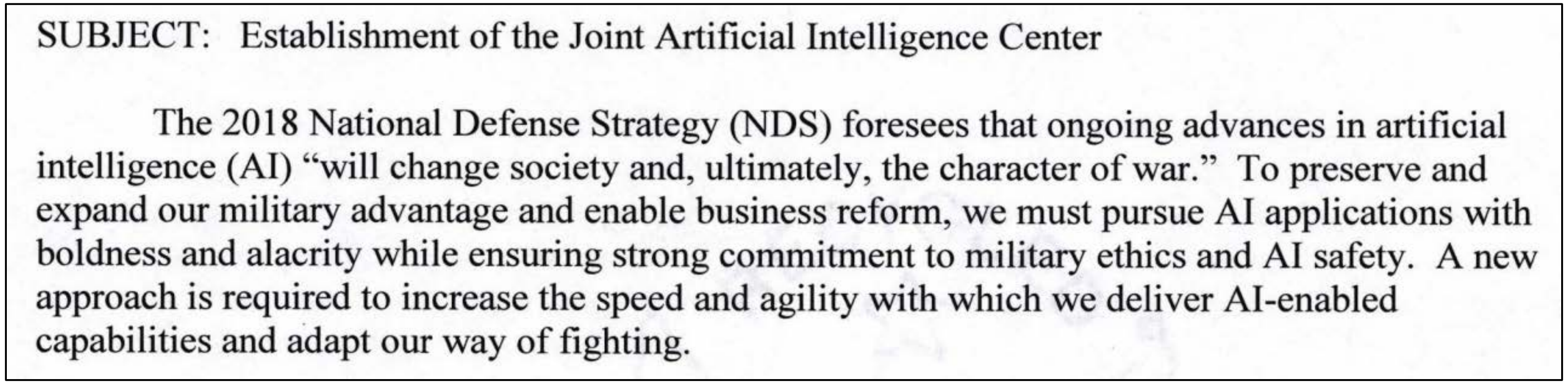
  $2B investments (over several years) in “Third Wave” AI
- Key investments:
  - Automating critical DoD business processes (e.g., security clearance vetting or accrediting software systems for operational deployment)
  - Improving the robustness and reliability of AI systems
    - Better understand failure modes of AI technologies – using both analytic and empirical R&D
  - Enhancing the security and resiliency of machine learning and AI technologies
    - Focus on adversarial AI
  - Reducing power, data, and performance inefficiencies
    - AI-specific hardware
    - Drastically reduce need for large amounts of labeled data
  - Pioneering the next generation of AI algorithms and applications, such as “explainability” and common sense reasoning

Prioritizing AI:
Establishment of New DoD Joint AI Center



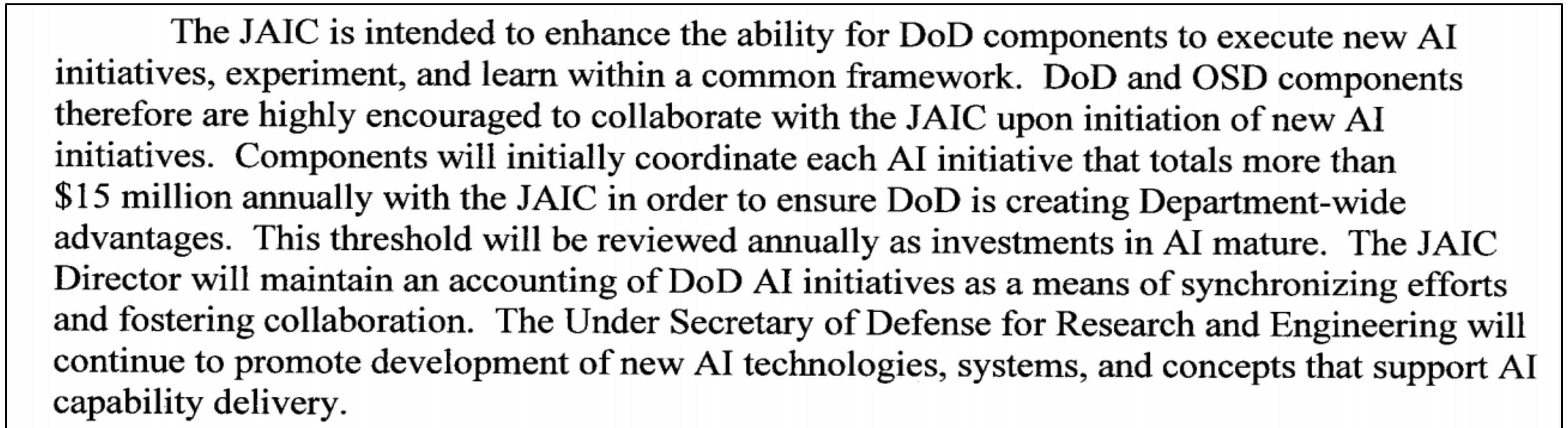
DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JUN 27 2018



SUBJECT: Establishment of the Joint Artificial Intelligence Center

The 2018 National Defense Strategy (NDS) foresees that ongoing advances in artificial intelligence (AI) "will change society and, ultimately, the character of war." To preserve and expand our military advantage and enable business reform, we must pursue AI applications with boldness and alacrity while ensuring strong commitment to military ethics and AI safety. A new approach is required to increase the speed and agility with which we deliver AI-enabled capabilities and adapt our way of fighting.



The JAIC is intended to enhance the ability for DoD components to execute new AI initiatives, experiment, and learn within a common framework. DoD and OSD components therefore are highly encouraged to collaborate with the JAIC upon initiation of new AI initiatives. Components will initially coordinate each AI initiative that totals more than $15 million annually with the JAIC in order to ensure DoD is creating Department-wide advantages. This threshold will be reviewed annually as investments in AI mature. The JAIC Director will maintain an accounting of DoD AI initiatives as a means of synchronizing efforts and fostering collaboration. The Under Secretary of Defense for Research and Engineering will continue to promote development of new AI technologies, systems, and concepts that support AI capability delivery.

Cyberinfrastructure for AI

- ORNL's Summit supercomputer – unveiled by DOE in June 2018
- Designed to advance science and research in AI
- Over 27,000 NVIDIA GPUs
- Includes IBM's Power9 chips designed for AI

- Other AI Hardware of interest:
  - Novel designs for neuromorphic computing
  - Hardware accelerators for machine learning
  - Embedded systems
  - Parallel architecture research motivated by AI processing requirements

Data Resources for AI R&D

- NSF is pursuing “Big Idea”: *Harnessing the Data Revolution*
- Purpose is to engage research community in:
    - Advancing fundamental data-centric research and data-driven domain discoveries
    - Building data infrastructure for research
    - Developing a 21st-century data-capable workforce

Educating and Training Workforce for Emerging Industries

Workforce challenges (from National Security Strategy):

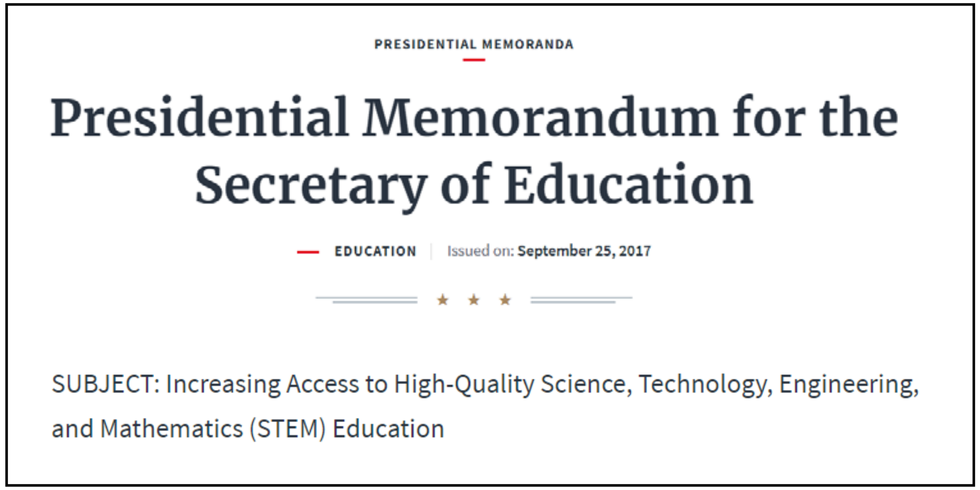
- *"As America's manufacturing base has weakened, so too have critical workforce skills ranging from industrial welding, to high-technology skills for* ***cybersecurity*** *and aerospace."*

- *"Protect and Grow Skills: The United States must maintain and develop skilled trades and high-technology skills through increased support for technical college and apprenticeship programs. We will support STEM efforts, at the Federal and state levels, and target* ***national security technology areas****."*

Increasing Access to STEM+C

September 2017 Presidential Memorandum for the Secretary of Education:

- Emphasizes STEM education as a key Administration priority
- Establishes goal of devoting at least $200 million in grant funds per year to the promotion of high-quality Computer Science and STEM education.
- Addresses both shortages in STEM teachers at all levels and expanding access to Computer Science and STEM education
- NSTC Committee on STEM Education (CoSTEM) is the Administration’s vehicle to execute policy on this central element of American leadership in AI



PRESIDENTIAL MEMORANDA

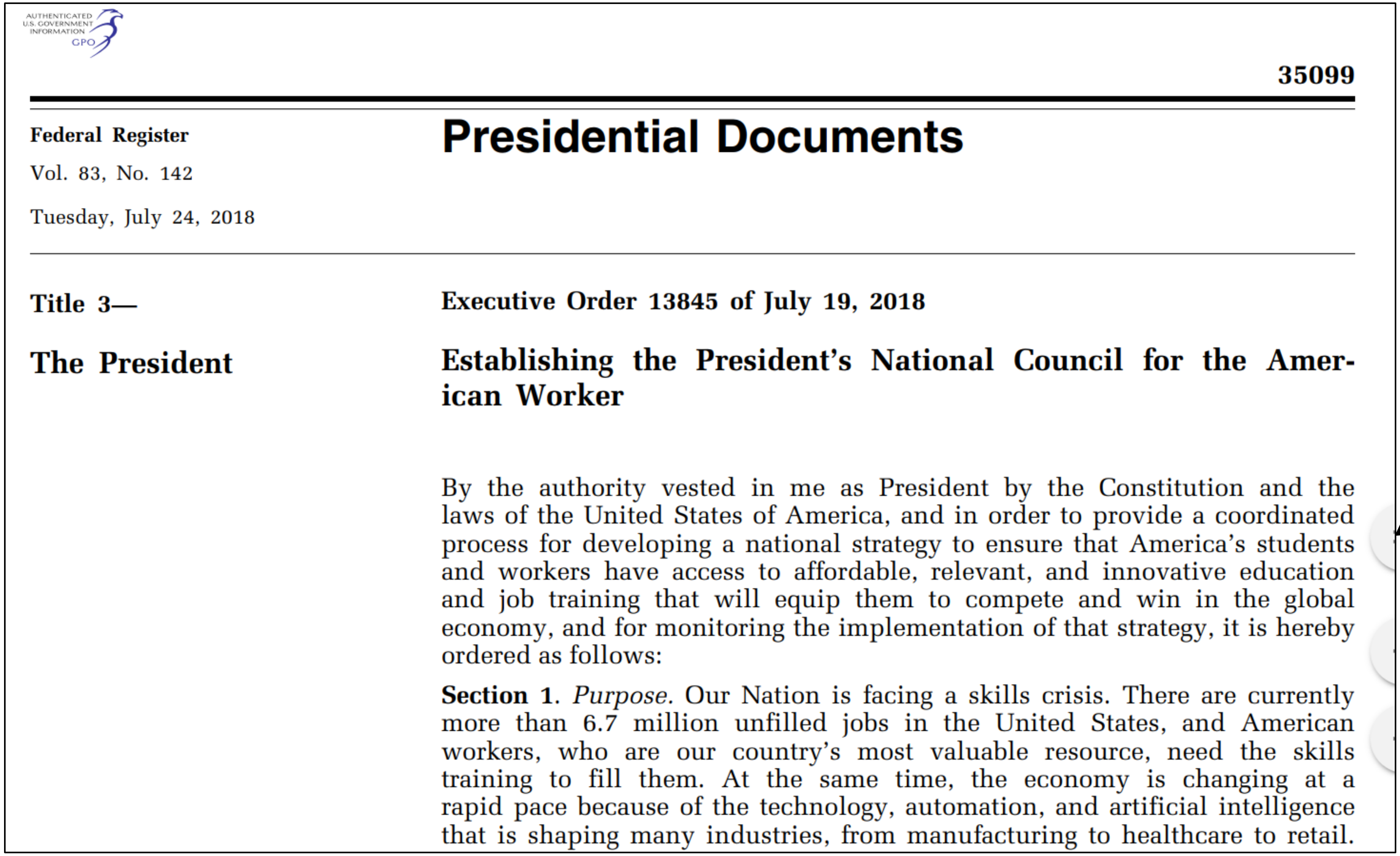
Presidential Memorandum for the Secretary of Education

EDUCATION | Issued on: September 25, 2017

★ ★ ★

SUBJECT: Increasing Access to High-Quality Science, Technology, Engineering, and Mathematics (STEM) Education

Creation of National Council for American Worker (July 2018)



AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

35099

Federal Register

Vol. 83, No. 142

Tuesday, July 24, 2018

Presidential Documents

Title 3—

The President

Executive Order 13845 of July 19, 2018

Establishing the President's National Council for the American Worker

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to provide a coordinated process for developing a national strategy to ensure that America's students and workers have access to affordable, relevant, and innovative education and job training that will equip them to compete and win in the global economy, and for monitoring the implementation of that strategy, it is hereby ordered as follows:

Section 1. *Purpose.* Our Nation is facing a skills crisis. There are currently more than 6.7 million unfilled jobs in the United States, and American workers, who are our country's most valuable resource, need the skills training to fill them. At the same time, the economy is changing at a rapid pace because of the technology, automation, and artificial intelligence that is shaping many industries, from manufacturing to healthcare to retail.

Ensuring students and workers have access to … innovative education and job training

Recognizes economy's rapid pace of change due to technology, automation, AI

International Engagement:

G7 Innovation Ministers’ Statement on Artificial Intelligence

“Artificial intelligence (“AI”) represents a set of complex and powerful technologies that will touch or transform every sector and every industry and will help society address some of our most challenging problems.

…Innovations in AI technologies have the potential to introduce new sources of economic growth especially in countries struggling with an aging population or economies highly dependent on traditional levers of production, including by helping overcome hurdles to full participation in the workforce and in our societies.”

G7 2018

CHARLEVOIX

International Engagement:

G7 Innovation Ministers' Statement on Artificial Intelligence

- **Supporting economic growth from AI innovation** is about using AI applications to help improve economic performance.
- **Increasing trust in and adoption of AI** are necessary ingredients for economic growth and the fuel for future innovations
- **Promoting inclusivity in AI development and deployment** is critical to ensuring broad public support for AI adoption and ensuring all members of society can benefit from this technology.

G7 2018
CHARLEVOIX

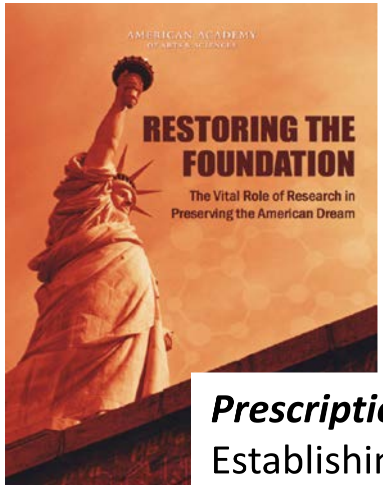
- G7 members will endeavor to:
  - invest in basic and early-stage applied R&D to produce AI innovations, and support entrepreneurship in AI and labour force readiness
  - continue to encourage research, including solving societal challenges, advancing economic growth, and examining ethical considerations of AI
  - support public awareness efforts to communicate actual and potential benefits, and broader implications, of AI
  - …

Review of Key Administration Priorities for AI

- Prioritizing funding for AI R&D including machine learning, autonomous systems, research cyberinfrastructure
- Removing Barriers to AI Innovation: removing regulatory barriers to deployment of AI-powered technologies
- Ensuring an AI-ready future American workforce: K-12, re-training/re-skilling, undergraduate, R&D workforce
- Achieving strategic military advantage: recognizing need to lead in AI, with DoD investing accordingly.
- Leveraging AI for government services: applying AI to improve the provision of government services
- Leading international AI negotiations: OSTP led U.S. delegations to 2017 & 2018 G7 Innovation and Technology Ministerials, working with our allies to recognize potential benefits of AI, promote AI R&D.

Looking forward: what’s needed

- *Robust AI research ecosystem:*
  - foundational research, AI in application domains, systems architecture, research cyberinfrastructure
- *Workforce:*
  - K-12 STEM workforce, computational thinking
  - lifelong learning, retraining, reskilling
  - R&D workforce
- *Partnerships:* leverage unique US research ecosystem of academia (driven by federal R&D investment), industry, federal government


AMERICAN ACADEMY OF ARTS & SCIENCES
RESTORING THE FOUNDATION
The Vital Role of Research in Preserving the American Dream

Prescription 3: Establishing a More Robust National Government-University-Industry Research Partnership

Thanks for your work in this important area

We’re always open to good ideas – engage with us!

Email: Lynne.E.Parker@ostp.eop.gov