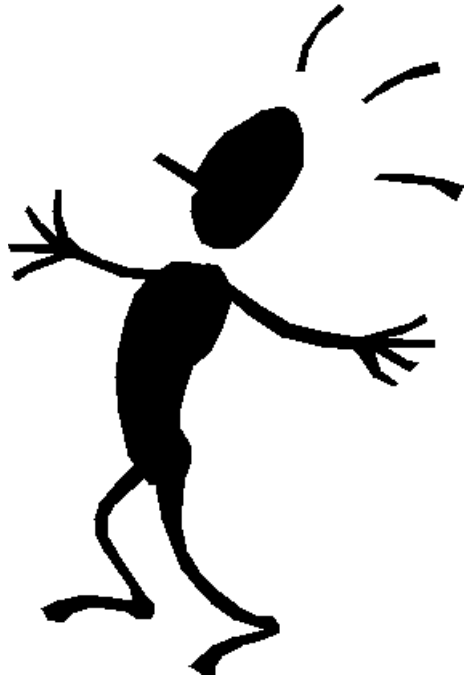
Today's AI and Spectrum – Realizing the Potential

Michael Garris

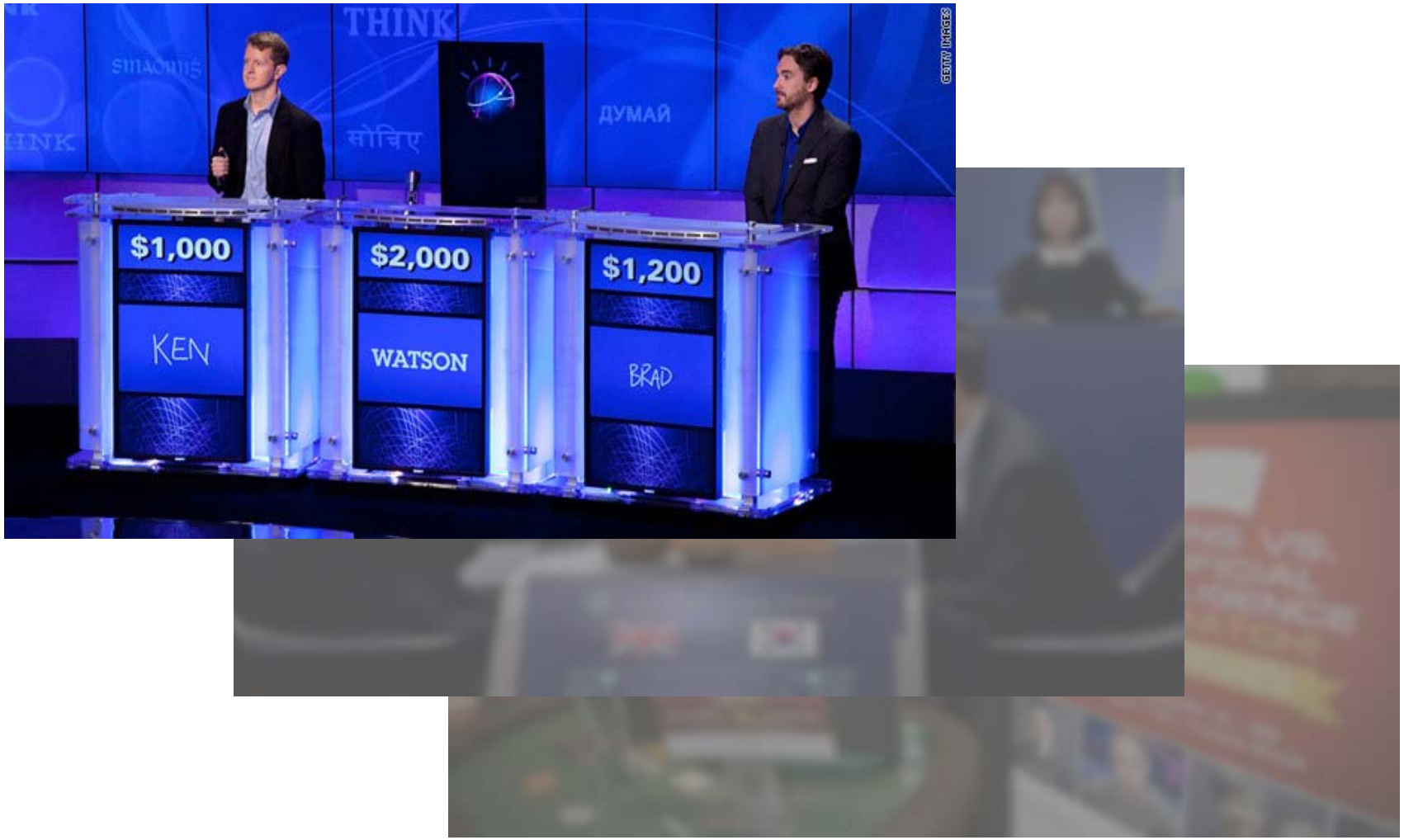
Senior Scientist / National Institute of Standards and Technology

Chief Technology Advisor / National Security Commission on Artificial Intelligence

What’s all the fuss?

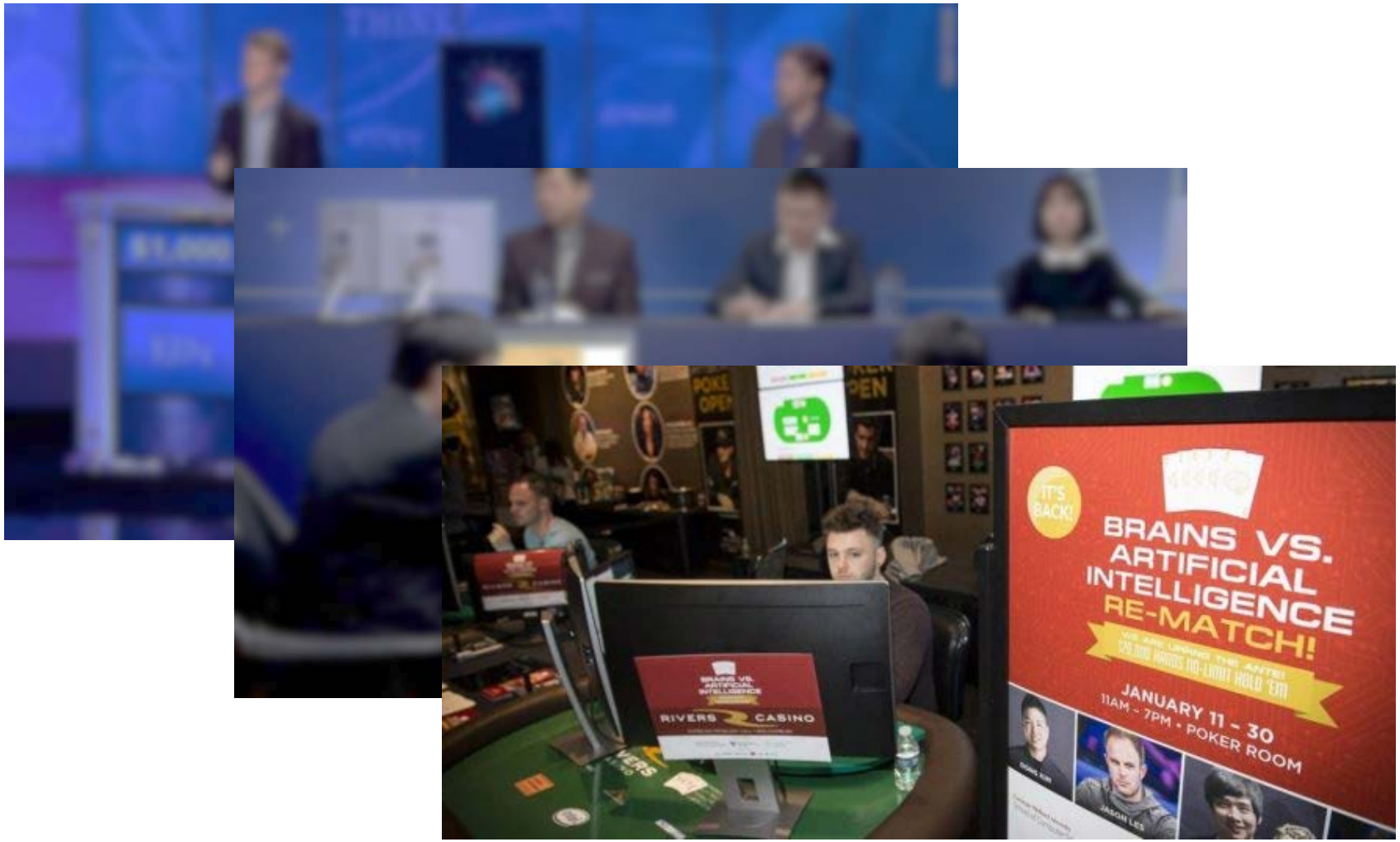


Emerging Technology



Emerging Technology

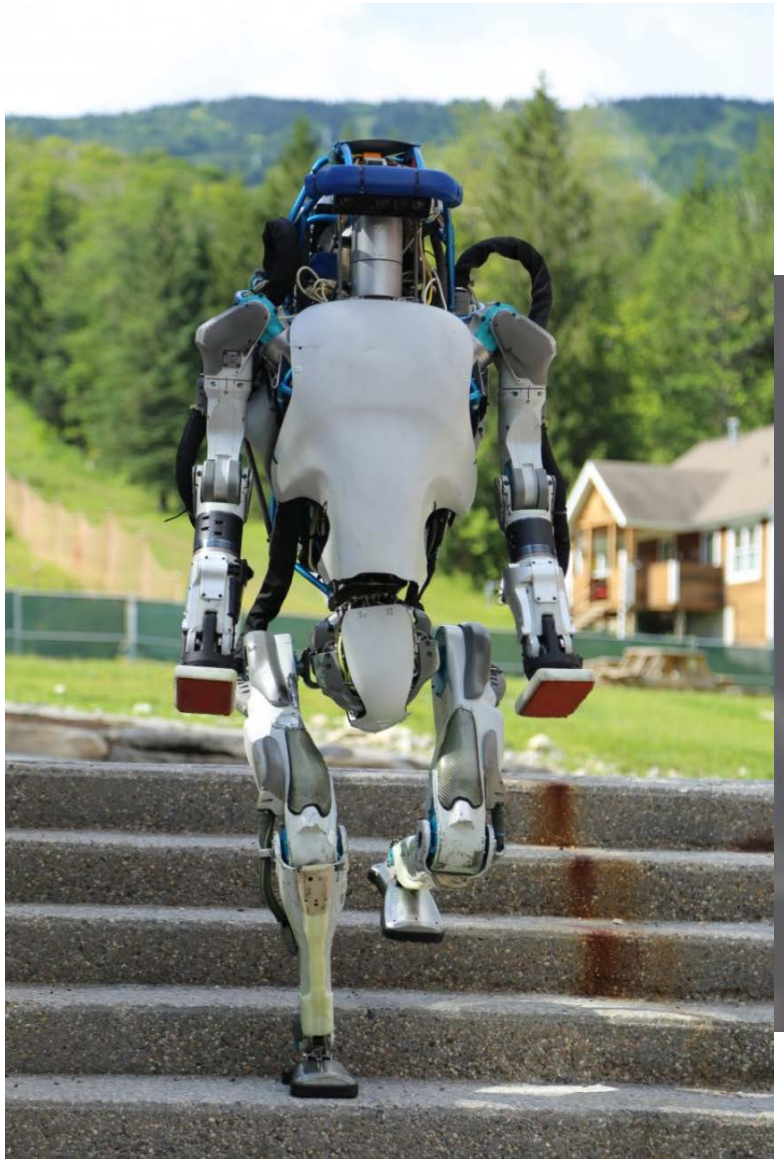
Emerging Technology

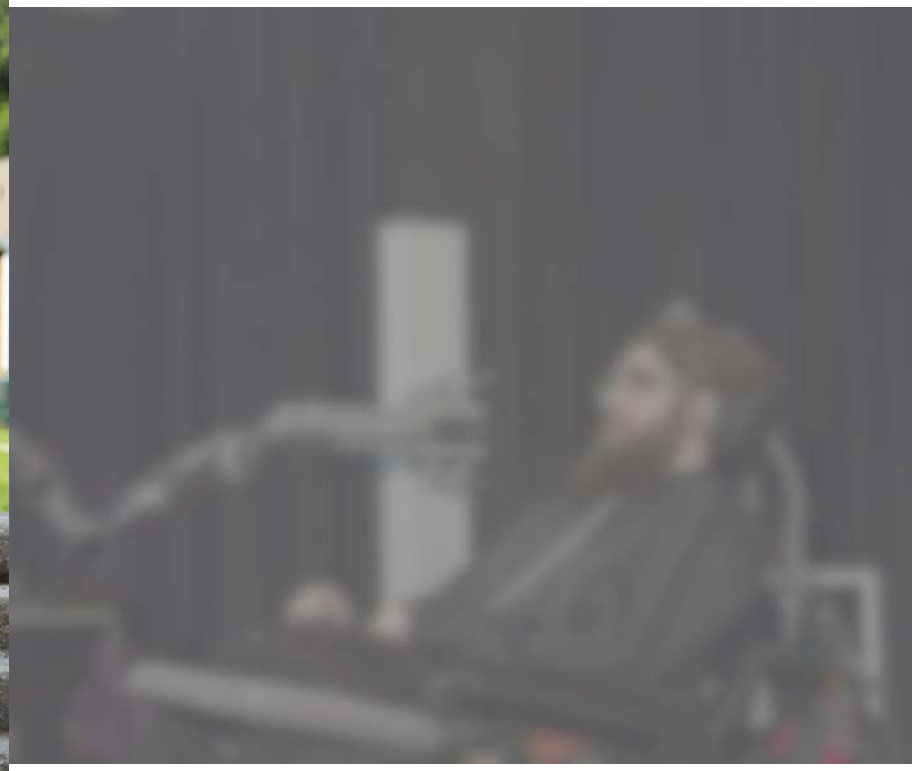


Emerging Technology

Emerging Technology

Emerging Technology





Emerging Technology

What is AI?

What is AI?

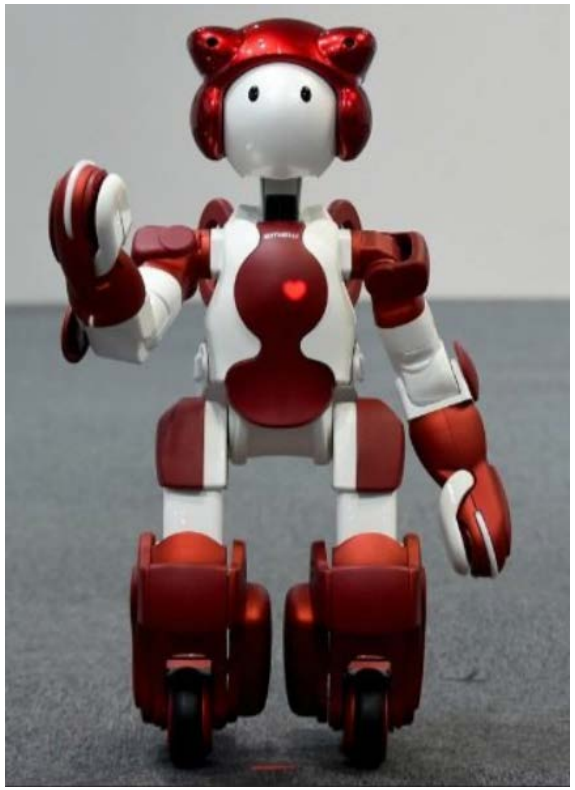
- **ANSI INCITS 172-2002 (R2007) - Artificial Intelligence:**
  - (1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.
  - (2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.

- **ISO/IEC JTC 1/SC 42 Working *Draft* 22989 - Artificial Intelligence:**
  - Capability of a system to acquire, process, and apply knowledge.
  - Note: knowledge are facts, information, and skills acquired through experience or education.

- **AI Problem Space Categories**
  - Knowledge Representation
  - Perception
  - Logical Reasoning
  - Planning and Navigation
  - Prediction

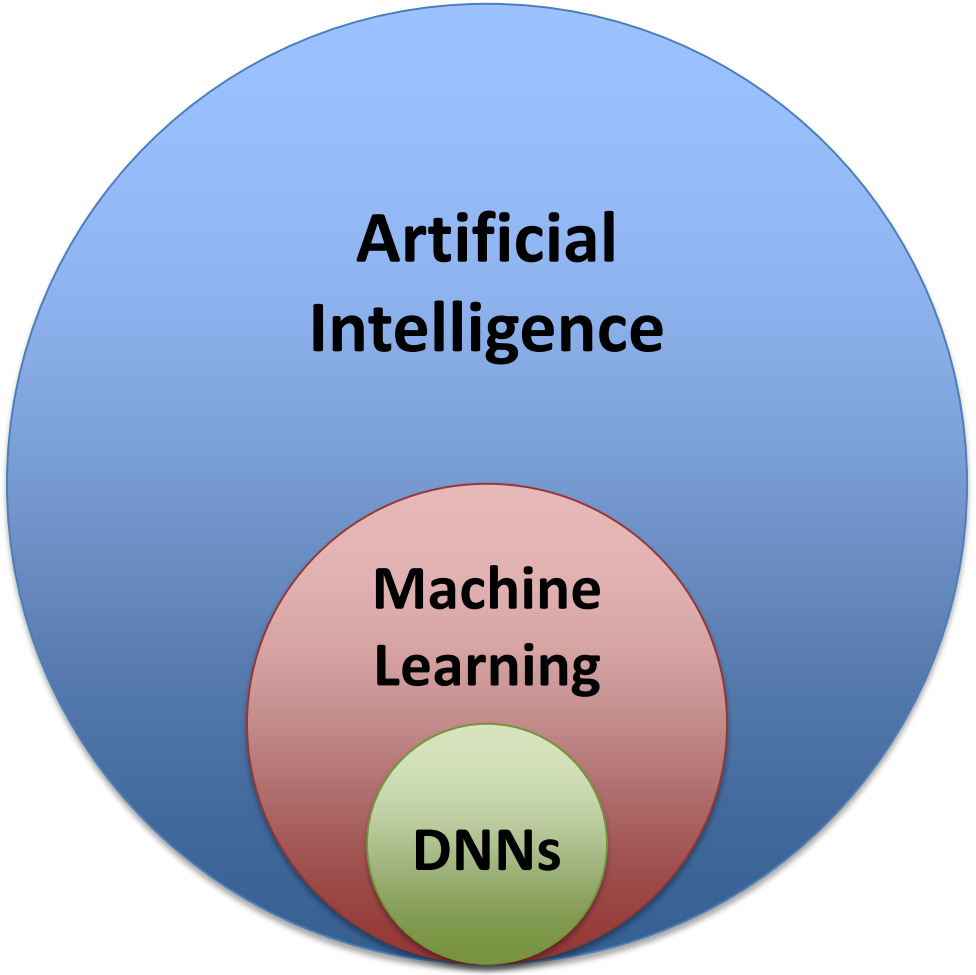
AI Conceptualization (1 of 3)

Embodied



Embedded

AI Conceptualization (2 of 3)



* DNN = Deep Neural Network

AI Conceptualization (3 of 3)

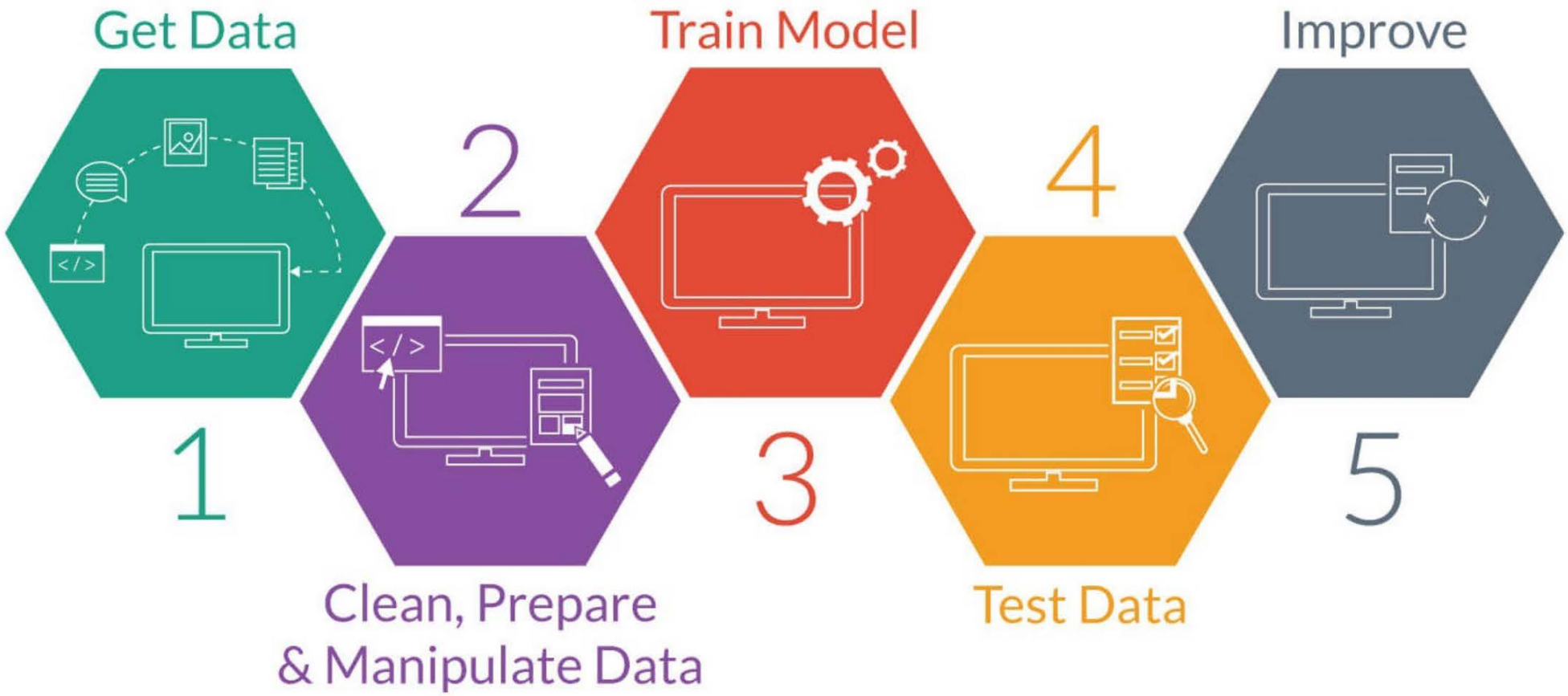
Narrow AI	General AI
o Application specific/ task limited	o Perform general (human) intelligent action
o Fixed domain models provided by programmers	o Self-learns and reasons with its operating environment
o Learns from thousands of labeled examples	o Learns from few examples and/or from unstructured data
o Reflexive tasks with no understanding	o Full range of human cognitive abilities
o Knowledge does not transfer to other domains or tasks	o Leverages knowledge transfer to new domains and tasks
o Today's AI	o Future AI?

New Wave of AI

- Availability of Big Data
- Improved Machine Learning (ML) Algorithms
- More Powerful Computing
- Mobile Connectivity

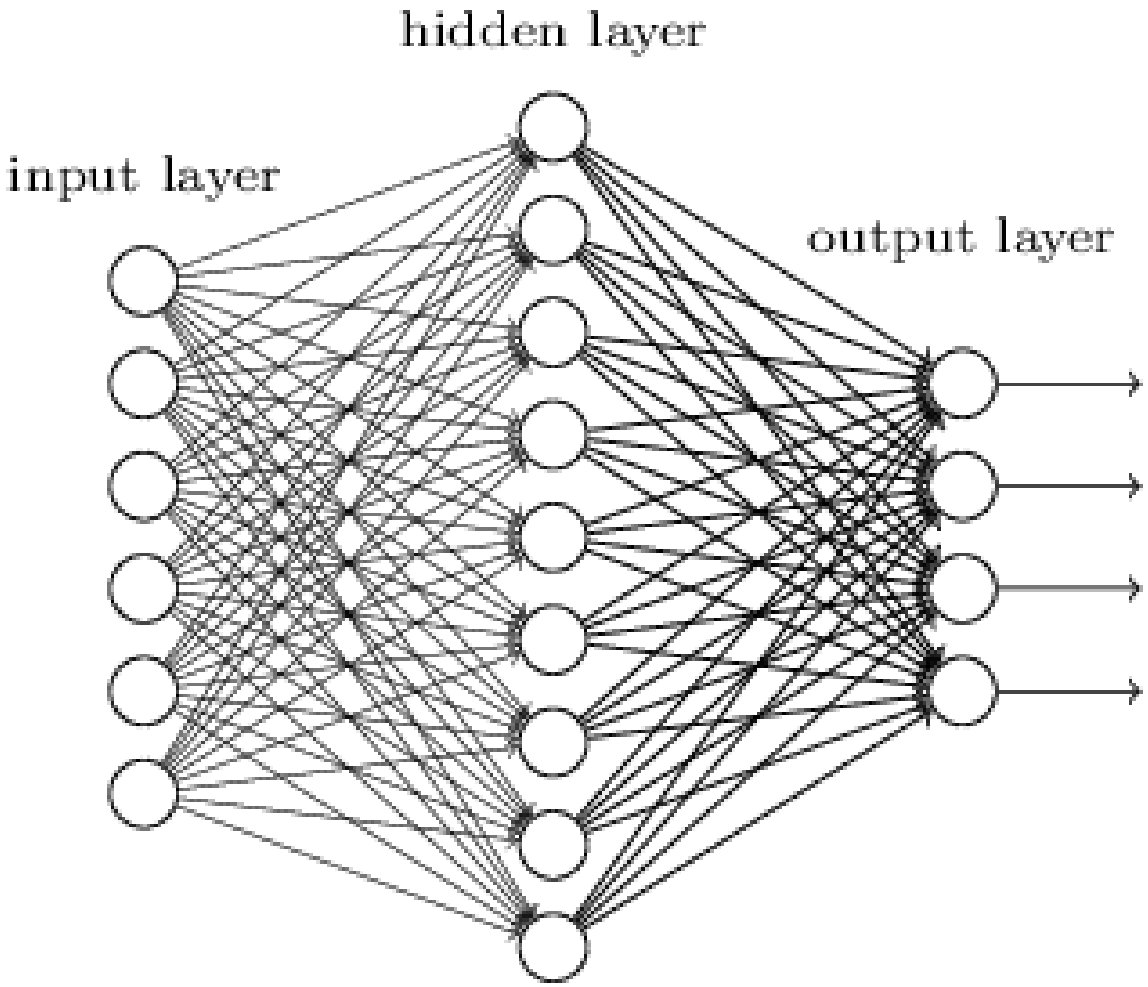
How is AI/ML Different?

Machine Learning Workflow



https://machinelearning-blog.com/2017/11/19/fsgdhfju/

1980's Neural Network



https://stats.stackexchange.com/questions/182734/what-is-the-difference-between-a-neural-network-and-a-deep-neural-network-and-w

Today's (Deep) Neural Networks

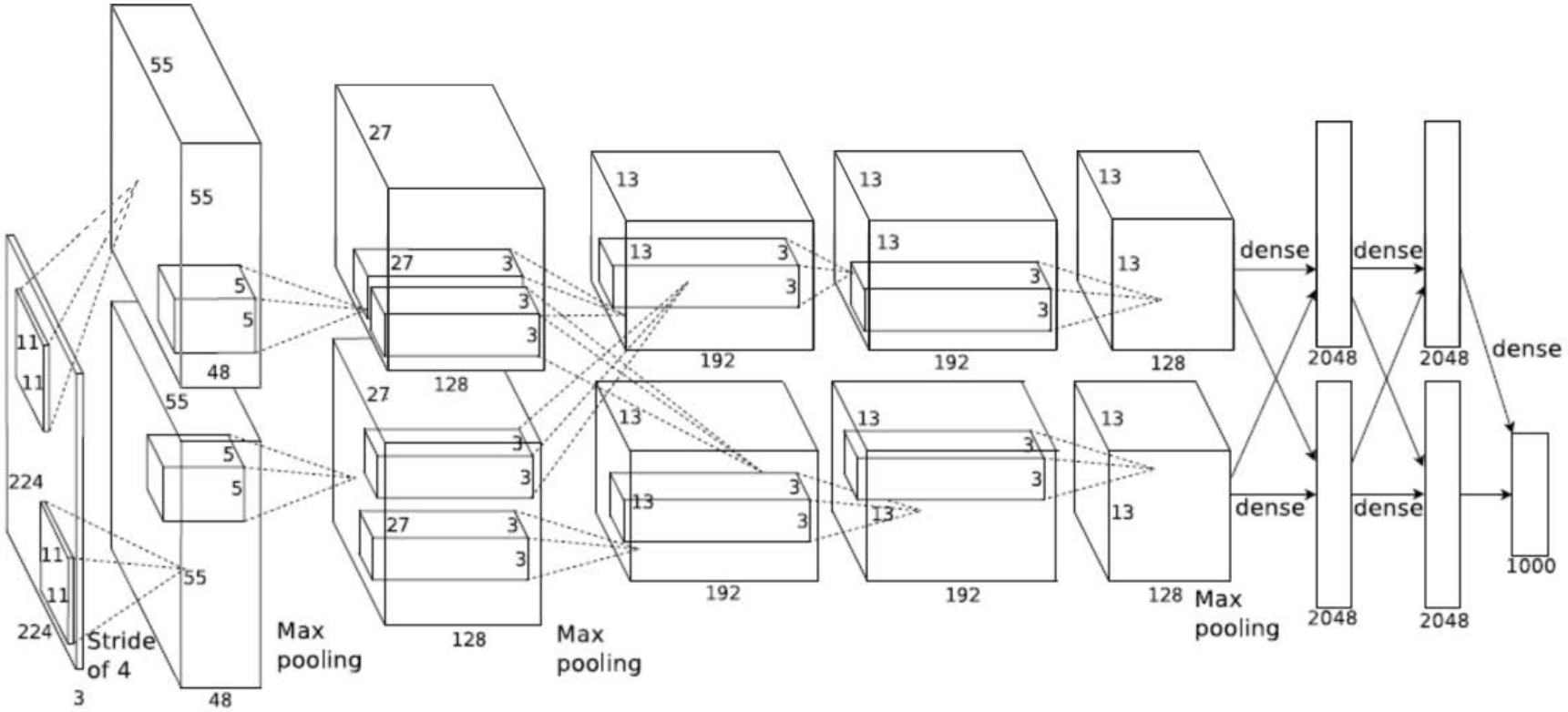


Figure 2: An illustration of the architecture of our CNN, explicitly showing the delineation of responsibilities between the two GPUs. One GPU runs the layer-parts at the top of the figure while the other runs the layer-parts at the bottom. The GPUs communicate only at certain layers. The network's input is 150,528-dimensional, and the number of neurons in the network's remaining layers is given by 253,440–186,624–64,896–64,896–43,264–4096–4096–1000.

https://papers.nips.cc/paper/4824-imagenet-classification-with-deep-convolutional-neural-networks.pdf

ML/AI Challenges

- Probabilistic
  - With inherent error rates and uncertainty
- Data Driven
  - With vulnerability to learning unwanted patterns of bias
- Extreme Dimensionality
  - Making decisions opaque (little explainability)
- Model Validation
  - Bound performance
  - Account for unforeseen outliers
  - How good is good enough?
  - Now introduce dynamic / continuous learning!?*

What can AI do?

AI for …

- Anomaly Detection
- Prediction
- Recommendation
- Translation
- Classification
- …

AI for Wireless Spectrum

- Monitoring
- Diagnose
- Mitigation / Actions
- Network Integration
- Spectrum Sensing

AI for Wireless Spectrum

- Monitoring -> Anomaly Detection
- Diagnose -> Prediction
- Mitigate / Actions -> Recommendation
- Network Integration -> Translation
- Spectrum Sensing -> Detection & Classification

Data Considerations for ML/AI

- Types
- Documenting, Preprocessing, Labeling
- Formats & Compression
- Sampling (Representative vs. Outlier)
- Data Sharing

AMERICAN ARTIFICIAL INTELLIGENCE INITIATIVE

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

President's Executive Order: Maintaining American Leadership in Artificial Intelligence

- Establishes the *American AI Initiative* to promote and protect national AI technology and innovation
- Multipronged approach:
  - Prioritizing sustained AI R&D
  - Enhancing access to high-quality data and cyberinfrastructure
  - Removing regulatory barriers
  - Ensuring leadership in technical standards
  - Providing education &training
  - Developing action plan to protect technological advantage in AI

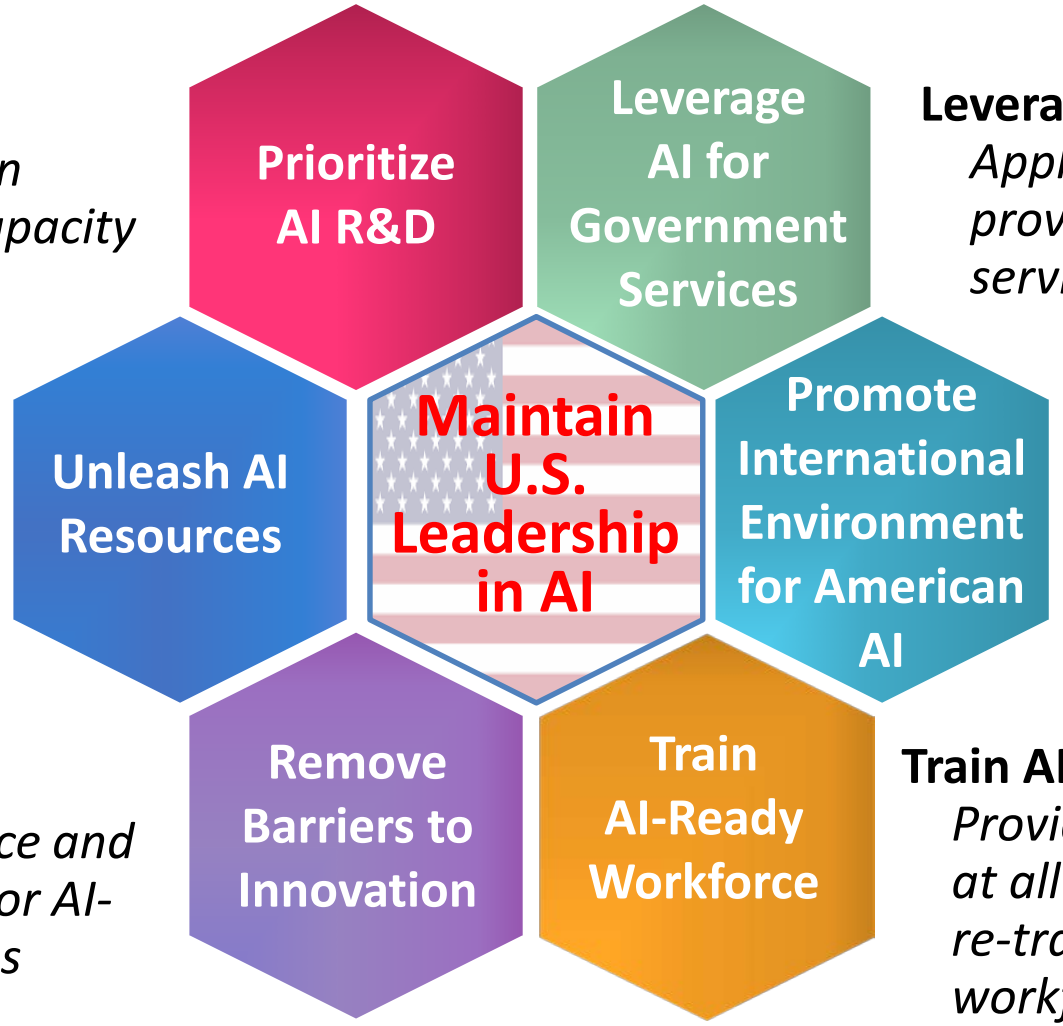
Feb. 11, 2019

AI for the American People

Prioritize AI R&D
Grow and sustain American research leadership and capacity

Unleash AI resources
Enhance access to high quality data, models, and computing resources

Remove barriers to AI innovation
Modernize governance and technical standards for AI-powered technologies



Leverage AI for government
Apply AI to improve provision of government services

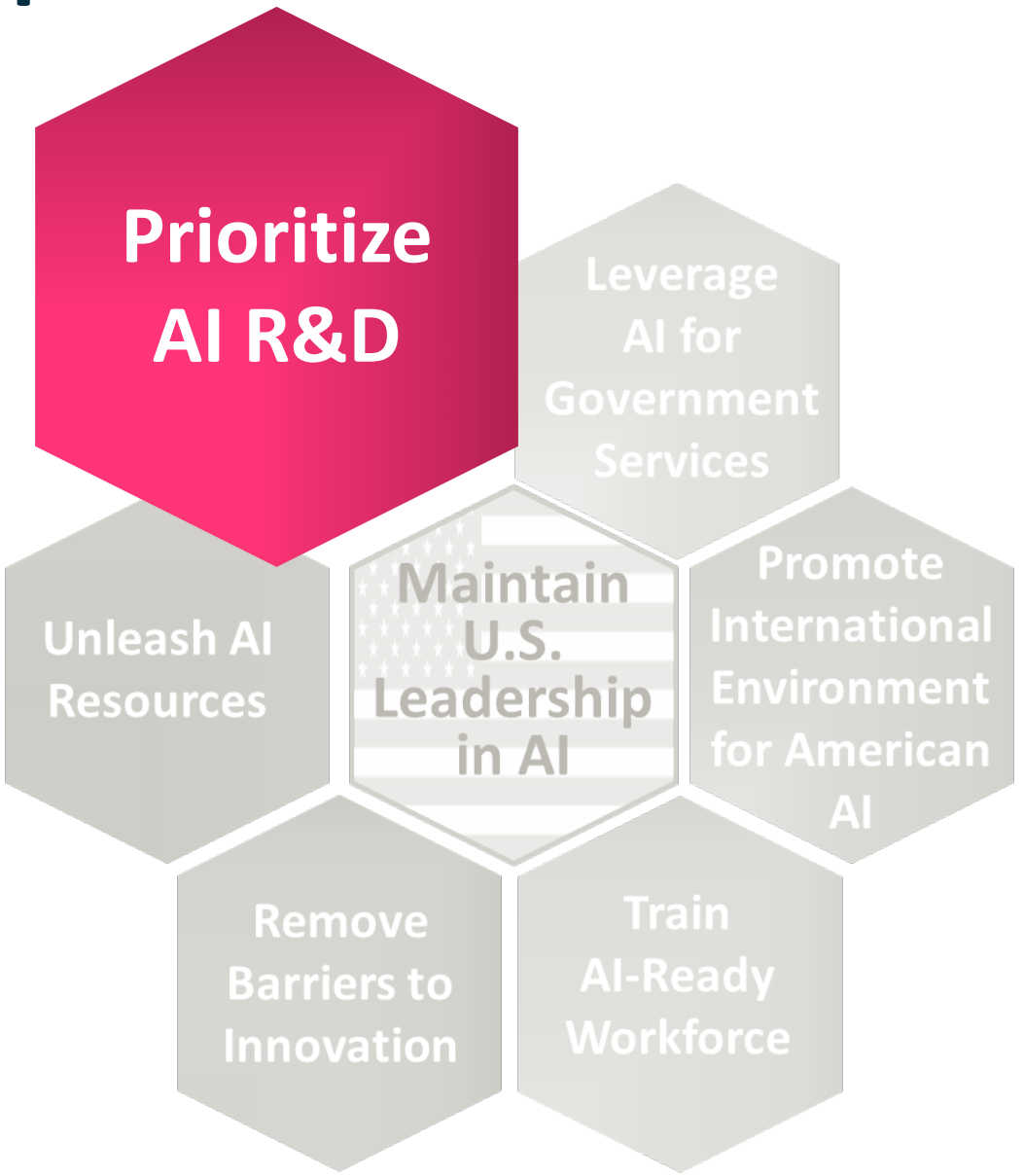
Promote international environment for American AI
Promote global environment supportive of American AI innovation, while protecting strategic advantage

Train AI-Ready Workforce
Provide AI-ready education at all levels: K-12, college, re-training, re-skilling, R&D workforce

AI for the American People

Prioritize AI R&D

Grow and sustain American research leadership and capacity



Coordinating Federal AI R&D

Select Committee on AI:

- Most senior Federal R&D leadership
- Advises White House on interagency AI R&D priorities
- Identifies opportunities to improve coordination of AI R&D, including ways to leverage Federal resources

Machine Learning and AI Subcommittee:

- Senior Federal leaders with AI R&D budget authority
- Operational and implementation arm of Select Committee

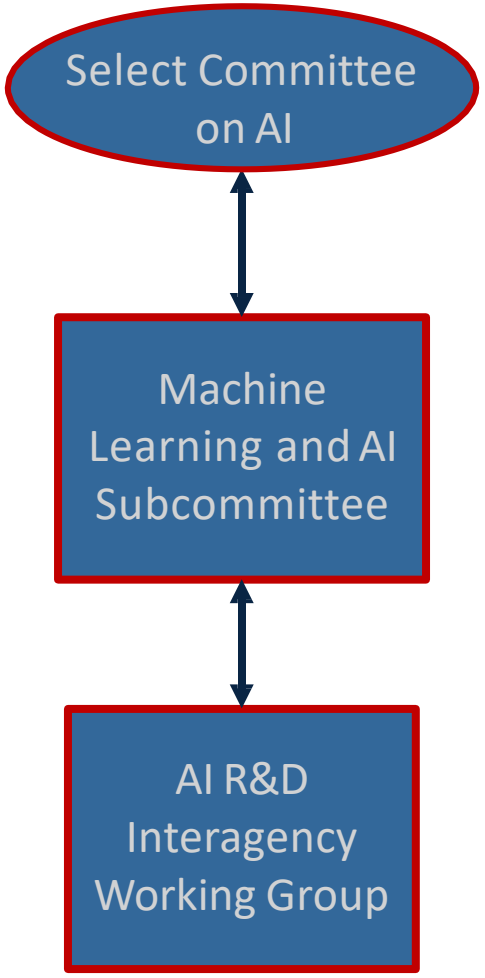
AI Interagency Working Group:

- AI experts across Federal agencies
- Community of practice

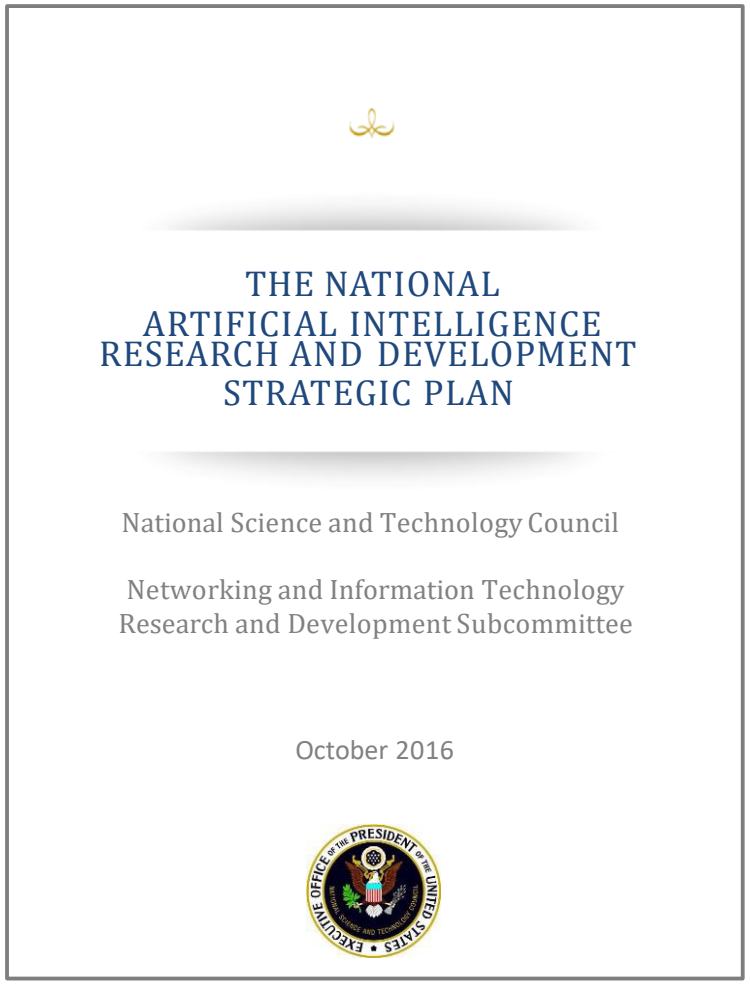
White House Office of Science and Technology Policy

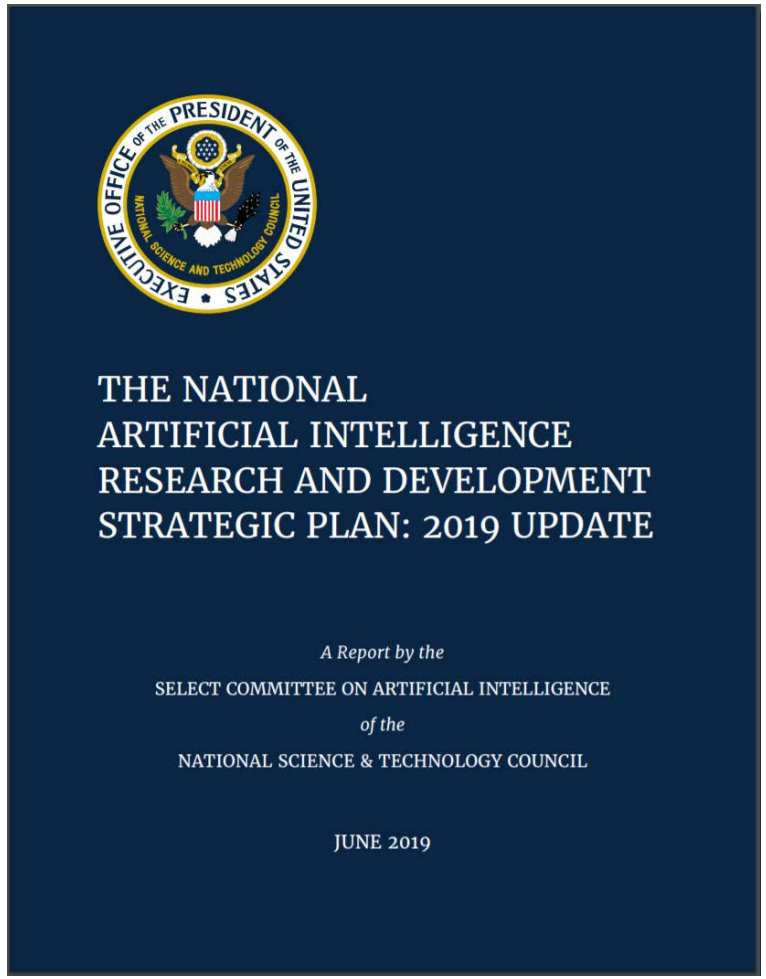
National Science and Technology Council

Select Committee on AI
November, 2018



Guiding R&D Investments:
National AI R&D Strategic Plan





National AI R&D Strategic Priorities

Strategy 1: Make long-term investments in AI research

Strategy 2: Develop effective methods for human-AI collaboration

Strategy 3: Understand and address the ethical, legal, and societal implications of AI

Strategy 4: Ensure the safety and security of AI systems

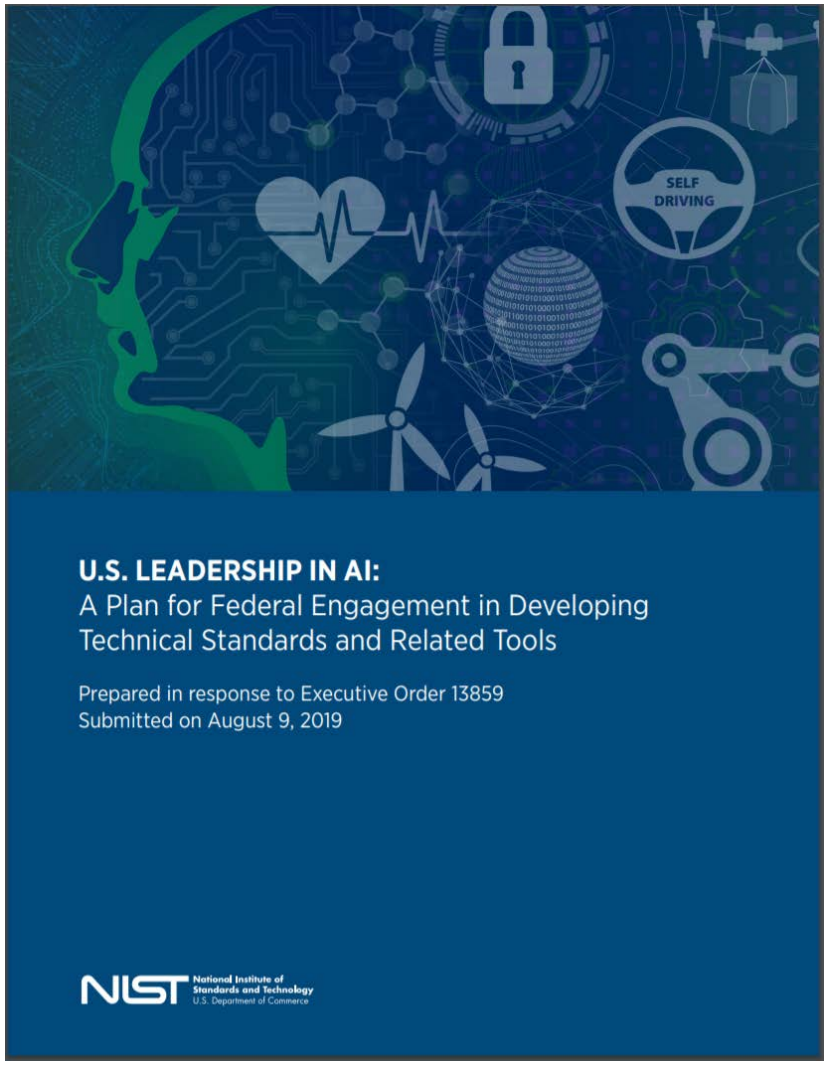
Strategy 5: Develop shared public datasets and environments for AI training and testing

Strategy 6: Measure and evaluate AI technologies through standards and benchmarks

Strategy 7: Better understand the national AI R&D workforce needs

Strategy 8: Expand Public–Private Partnerships to Accelerate Advances in AI

AI EO – Ensuring Leadership in Technical Standards



AI EO Tasking & Process

The EO directed the Secretary of Commerce, through the National Institute of Standards and Technology (NIST), to issue *"a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies."*

Broad public and private sector input in 180 days

- RFI (May 1, 2019) - NIST Requests Information on Artificial Intelligence Technical Standards and Tools
- Workshop (May 30, 2019) - Federal Engagement in Artificial Intelligence Standards Workshop
- Public Comment (July 2, 2019) - NIST Releases Draft Plan for Federal Engagement in AI Standards Development
- Final Report (August 9, 2019) - Plan Outlines Priorities for Federal Agency Engagement in AI Standards Development

AI Standards - Government's Role

United States global leadership in AI depends upon the Federal government playing an active and purpose-driven role in AI standards development. That includes AI standards-related efforts needed by agencies to fulfill their missions by:

- Supporting and conducting AI research and development
- Actively engaging in AI standards development
- Procuring and deploying standards-based products and services
- Developing and implementing supportive policies, including regulatory policies where needed

AI Standards – Focus Areas

- Concepts and terminology
- Data and knowledge
- Human interactions
- Metrics
- Networking
- Performance testing and reporting methodology
- Safety
- Risk management
- Trustworthiness

Trustworthy AI

- Accuracy
- Explainability
- Resiliency
- Safety
- Reliability
- Objectivity
- Security

AI Standards Tools

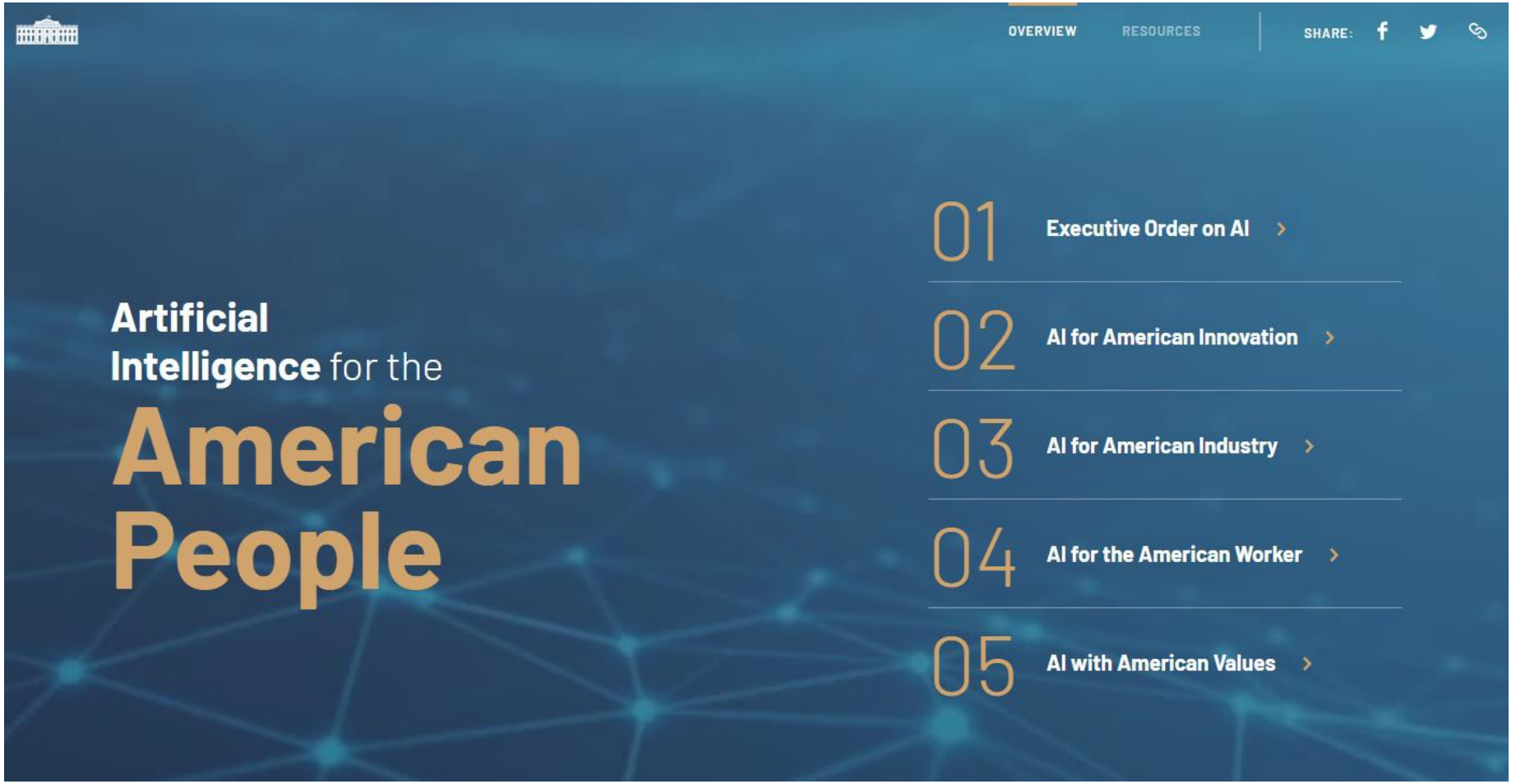
- Data sets - standardized formats plus metadata
- Tools for knowledge representation & reasoning
- Tools for accountability & auditing
- Use cases - fully documented applications
- Testing methodologies & metrics
- Benchmarks, evaluations, and challenge problems
- AI testbeds

AI Standards – Federal Recommendations

Federal government commit to deeper, consistent, long-term engagement in AI standards development activities to help the U.S. to speed the pace of reliable, robust, and trustworthy AI technology development. Specifically, the Federal government should:

- Bolster AI standards-related knowledge, leadership, and coordination among Federal agencies to maximize effectiveness and efficiency.
- Promote focused research to advance and accelerate broader exploration and understanding of how aspects of trustworthiness can be practically incorporated within standards and standards-related tools.
- Support and expand public-private partnerships to develop and use AI standards and related tools to advance reliable, robust, and trustworthy AI.
- Strategically engage with international parties to advance AI standards for U.S. economic and national security needs.

AI.gov –"All of Government" Portal for Federal AI Activities



NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE

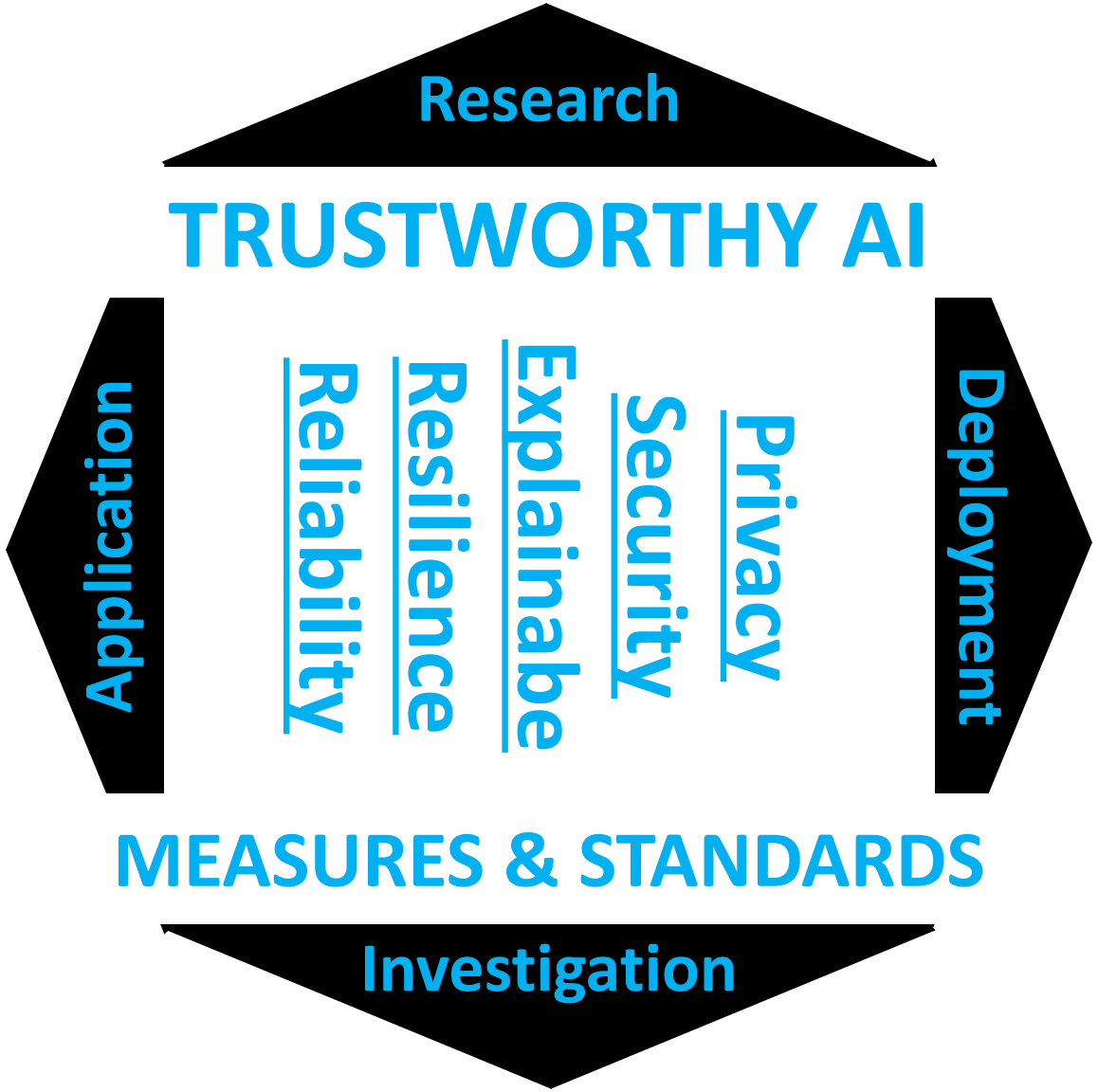
Questions?

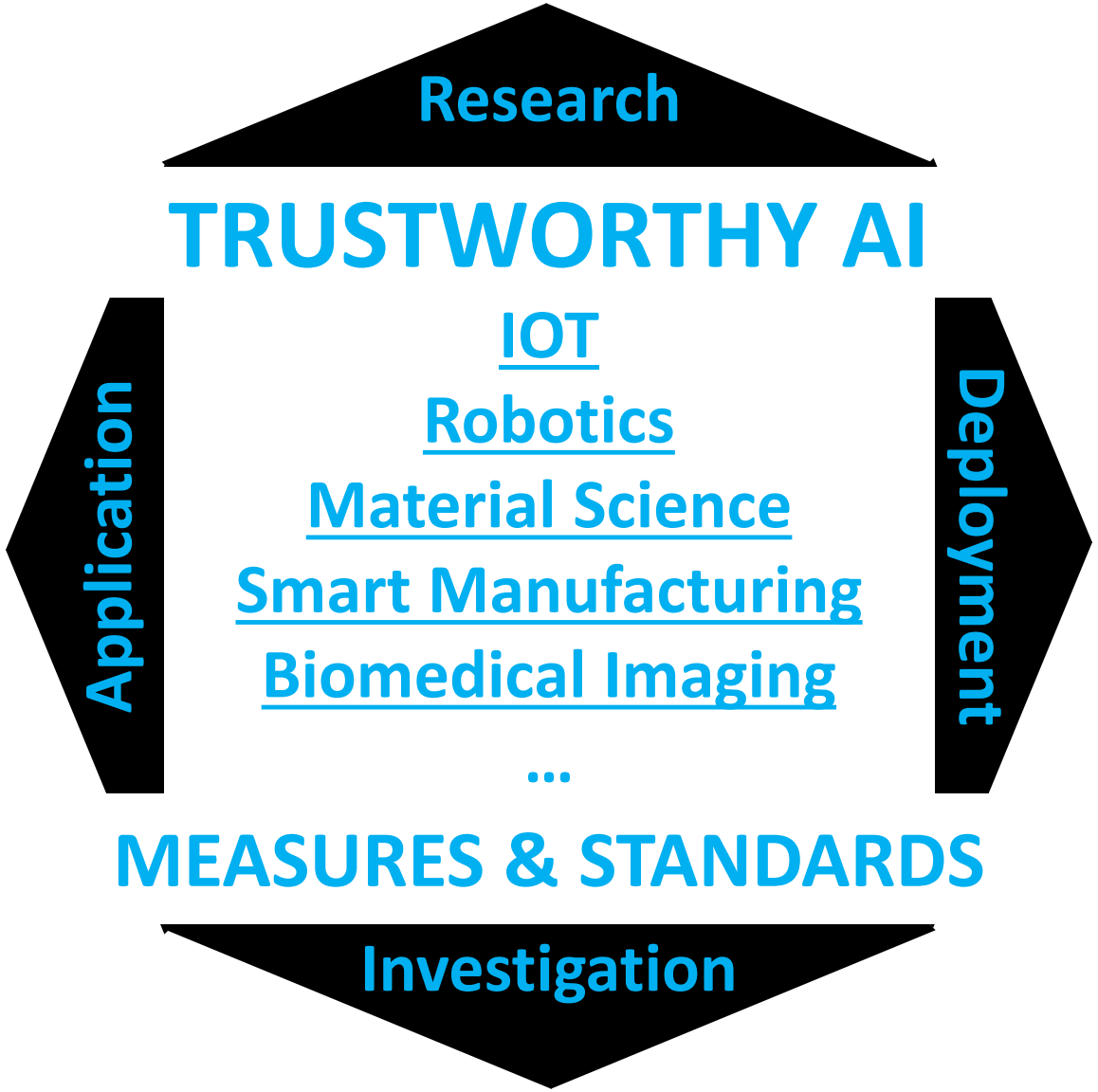
Michael Garris

(mgarris@nist.gov)

Back Up Slides


Research
TRUSTWORTHY AI
Application
NIST
Deployment
MEASURES & STANDARDS
Investigation


Research
TRUSTWORTHY AI
Application
Deployment
Reliability
Resilience
Explainabe
Security
Privacy
MEASURES & STANDARDS
Investigation


Research
TRUSTWORTHY AI
IOT
Robotics
Material Science
Smart Manufacturing
Biomedical Imaging
...
Application
Deployment
MEASURES & STANDARDS
Investigation

Topics @ NIST
(relating to AI/ML)

- AI/ML Foundations
  - Improving ML
  - Knowledge Management
  - Ontologies
  - Visualization
- Datasets & Data Management
- Image Understanding
  - Biomedical
  - Biometrics
  - Neutron Radiation
- Information Search & Summarization
- Internet of Things & Cyber Physical Systems
- Materials Science & Discovery
- Natural Language Processing
- Neuromorphic Design
- Quantum AI/ML
- Robotics
  - Agility
  - Collaboration
- Security and Privacy
- Smart Manufacturing
- Spectrum
- Standardization
- Training (staff)
- Trustworthiness
  - Bias
  - Methods & Metrics
  - Validation

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov