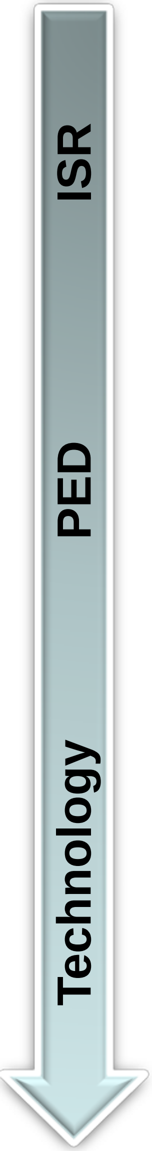
NDIA

Lieutenant General Jack Shanahan
OUSDI Director for Defense Intelligence (Warfighter Support)
26 October 2017

Algorithmic Warfare Cross-Functional Team (AWCFT)

aka Project Maven

Project Maven – Framing the Problem



ISR

Service and partner platforms & sensors are collecting an unprecedented amount of data and information, overwhelming us in terms of volume, variety, and velocity. **Our Processing, Exploitation, and Dissemination (PED) capacity and capabilities are not keeping pace**, largely because our PED processes are suboptimal. More sensors are being fielded to meet growing ISR demand and the current PED enterprise cannot keep pace without technological breakthroughs.

PED

PED has been an afterthought in military planning and acquisition. PED processes are time-consuming and manually intensive, producing largely static, incompletely-fused outputs that leave far too much useful data unexploited or undiscovered. Most of DoD automation applications in PED use traditional, kinetic algorithms for object tracking and change detection. The department is years behind industry in these areas.

Technology

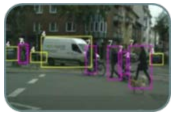
There is no coordinated effort to bring AI/ML/DL/CV technology into DoD. Industry is in the midst of a revolution in artificial intelligence, and computer vision is at the forefront, to include object detection, identification, and tracking. Automation is currently pursued across many agencies (low $$) with no strategy or central direction. Development and integration is slow and tedious. Existing PED weapons systems have closed/block architectures, cannot easily incorporate new capabilities, and require months/years to update. Multiple strategy and policy documents recommend that the department incorporate automation technologies faster and bring unity and central direction to automation efforts.

AWCFT/Maven Goals & Metrics

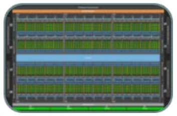
VISION

Project Maven will deliver AI-based algorithms to tactical UAS, MQ-1/9, and MQ-9 WAMI processing & exploitation systems on NIPR/SIPR/JWICS by the end of 2018. Our initial focus is on deploying proven capabilities to the field for warfighters. Serves as proof of concept to bring AI and machine learning to the DoD enterprise at speed and scale.

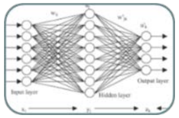
GOALS



DATA LABELING
Teach the computer to recognize objects



AI COMPUTE
Processing power for training models and inferences (GPU)



NEURAL NETS
The AI frameworks, models, and algorithms behind deep learning

ALGORITHM INTEGRATION
Incorporating into programs of record (starting with Full Motion Video)

USER ENGAGEMENT
The interface to display and manipulate data

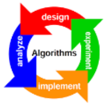
OBJECTIVES

1 million images labeled by January 2018,
build & sustain DoD data labeling enterprise
(including FVEY partners)

GPU purchase in August 2017
Google Cloud accreditation by November 2017

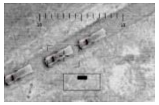
Google

6 vendors currently on contract
Broad Agency Announcement in October 2017
Industry Day on 24 October



1st TUAV Algorithm fielded in December 2017
Algorithm fielded at 10 sites in January 2018

Use Case Analysis ongoing
User algorithm test by November 2017



AWCFT/Maven Acquisition & Contracting Approach

Contracting and buying AI/ML is not like buying a tank, fighter jet, or ammunition. We are using a process that allows speed, agility, and effectiveness while still adhering to the Federal Acquisition Regulation. We adopted a multi-path approach to contracting/acquisition that gives opportunities to the smallest technology start-up, the world's largest companies, universities, open source, etc. who can deliver capabilities to warfighters

OBJECTIVES

AWCFT bring mature AI technology to (1) automate tasks better performed by a machine and (2) augment human performers where machines are incapable of automating a full task

PRINCIPLES

- **Speed + Agility + Effectiveness**
- **Do not develop something that exists commercially and already meets our requirements (prohibited by FAR)**
- **Take advantage of industry expertise and a flood of private sector investment for commercial applications to innovate for DoD**
- **Data integrity + Security + Quality**

PARTNERS

Industry (big, small) + Academia + National/DoD Labs + Open Source

ACQUISITION & CONTRACTING

OTAs, Firm Fixed Price, Cost Plus Fixed Fee, Prime w/ Subs, IDIQ

Big 5 Hurdles

- **Data**
- **Cloud implementation (policy and regulation)**
- **Resourcing**
- **Weapon system block architectures**
- **AI-ready culture and seeing beyond current workflows**

Long-Term Vision for DoD AI/ML

CENTRALIZED DIRECTION

Focus

- Establish DoD Strategy
- Accelerate Investment
- Remove obstacles
- Set research agenda

Improve

- Policy and regulation (FAR, DFAR)
- DODD on use of AI and Warfighting
- Market direction (guide/shape)
- Enhanced AI program protection

National Capabilities

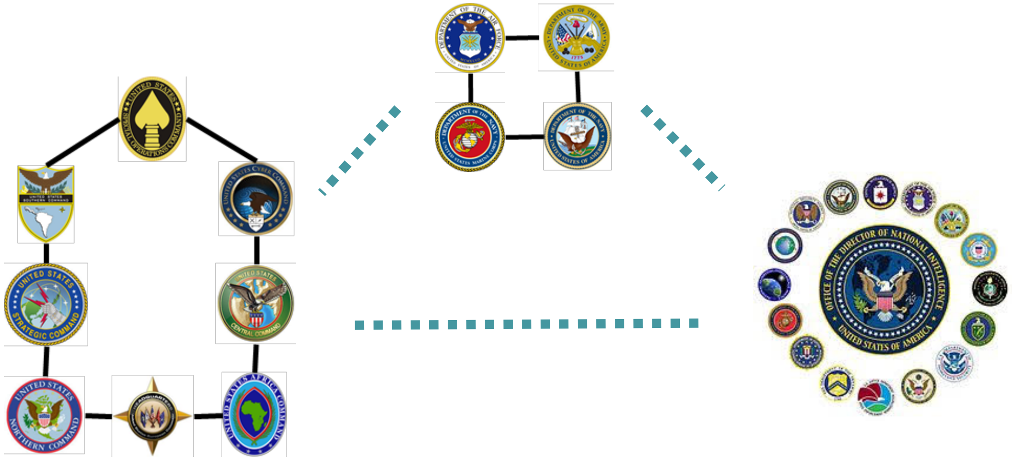
Cloud

AI Simulator

Quantum

Chip Sets
(GPU, FPGA, ASIC)

DECENTRALIZED EXECUTION



AI/ML in the Cyber Domain

Project Maven's underlying pipeline – gather data, label data, engage with partners, develop algorithms, field prototypes, optimize algorithms – applies as much to cyber (or EW) as it does to FMV

- **In future fights, best we can achieve likely to be decision cycle advantage, not information dominance or even information superiority**
- **Cyber historically focused on a "Castle Model" – build a fortress, harden the system, patch software. This kind of *Maginot Line* thinking doesn't work in the digital age.**
- **AI/ML offers sophisticated defense-in-depth – running in the background to provide secure user authentication; identify vulnerabilities, DDOS/botnet detection, zero-day detects, etc. Immediate response rather than slower, set-piece cyber defense**
- **Biggest potential for insider threat identification and mitigation – establishing 'normal', detecting anomalies, data exfiltration recognition, etc.**
- **Quantum computing**

“The Coming Software Apocalypse”

“It’s been said that software is ‘eating the world’. More and more, critical systems that were once controlled mechanically, or by people, are coming to depend on code. This was perhaps never clearer than in the summer of 2015, when on a single day, United Airlines grounded its fleet because of a problem with its departure-management system; trading was suspended on the New York Stock Exchange after an upgrade; the front page of The Wall Street Journal’s website crashed; and Seattle’s 911 system went down again, this time because a different router failed. The simultaneous failure of so many software systems smelled at first of a coordinated cyberattack. Almost more frightening was the realization, late in the day, that it was just a coincidence.”

-- James Somers, Atlantic, 26 Sep 2017

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA