U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND ARMAMENTS CENTER

Armaments Center Analysis of Artificial Intelligence and Machine Learning Impacts to Army Safety and System Assurance

Benjamin Schumeg

Combat Capabilities Development Command Armaments Center

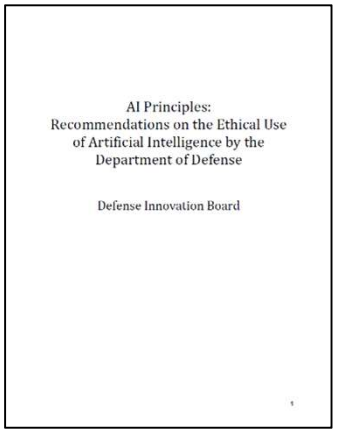
Army Futures Command

UNCLASSIFIED // APPROVED FOR PUBLIC RELEASE // DISTRIBUTION IS UNLIMITED

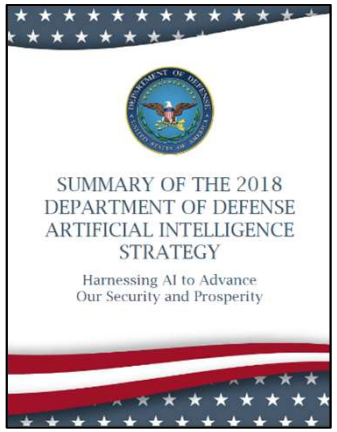
AI EXTERNAL RECOMMENDATIONS

Reports, policies and strategies all point to increased need for assurance, integration, and trust of AI enabled systems fielded by DoD

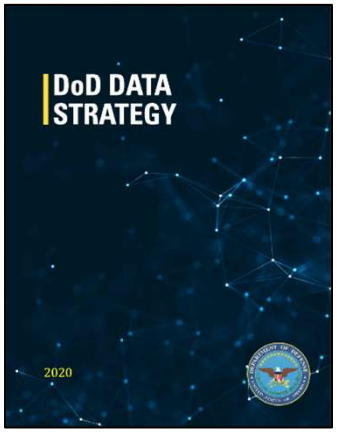
NSCAI Final Report (2021)



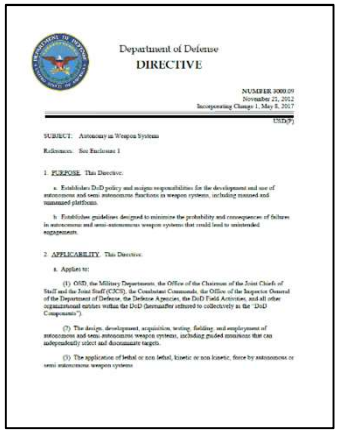
DIB Report (2019)



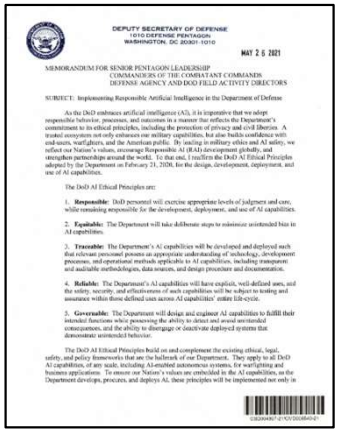
DoD AI Strategy (2018)



DoD Data Strategy (2020)



DoDD 3000.09 (2017)



RAI Memorandum (2021)

- Data Science
- Verification and Validation
- Reliability
- Safety
- Human System Integration

INTRODUCTION

DEVCOM Armaments Center

Lead in the research, development, acquisition and lifecycle management of ***advanced conventional weapon systems and ammunition***.

Artificial Intelligence and Machine Learning (AI/ML) can revolutionize existing and future technologies developed by DEVCOM Armaments Center

Presents Unique Challenges and Disruptions to Deployment

- Uncertainty in continuous learning, complex logic, and configuration management
- Novel methods needed for analysis and certification of AI training data sets
  - Training data determines how the system operates under expected conditions
- Critical assessments required of essential enabling sensors/systems
- Unknown user buy-in, trust, and confidence of full system capabilities
- New methods for T&E/V&V to ensure AI is reliable, ethical, safe, and robust
- Possible impacts to existing development methodologies

Army Materiel Release Process is Critical Path for Deployment

MATERIEL RELEASE QUESTIONS & ARTIFACTS

PROCESS THAT CERTIFIES THAT ARMY MATERIEL
IS **SAFE, SUITABLE AND SUPPORTABLE** BEFORE ISSUED TO THE FIELD

AR 770-3

SAFETY

Questions:

- Is the system safe?
- Have hazards to Soldiers, civilians, and equipment been identified and mitigated or accepted?
- Has AEC confirmed the system is safe?
- Have hazards related to health, EOD, energetics, or environment been identified and mitigated or accepted?

Artifacts:

- Safety Certification & Safety Data Package or Safety & Health Data Sheet
- AEC Safety Confirmation
- Mishap Risk Acceptance or System Safety Risk Assessment (SSRA)
- Health Hazard Assessment
- Surface Danger Zone
- ATEC Assessment or Evaluation
- Final Hazard Classification
- Army Fuze Safety Review Board Certification
- Energetic Materials Qualification Board Statement
- EOD Support Statement
- Environmental Support Statement
- Nuclear Regulatory Commission Licensing
- Air Worthiness Release
- Ignition System Safety Review Board Certification
- Hazards of Electromagnetic Radiation to Ordnance (HERO) Certification

SUITABILITY

Questions:

- Is the system suitable?
- Does the system meet requirements?
- Has the system been evaluated by ATEC? Do they concur?
- How will it function in operational setting?
- Does the system have sufficient reliability for intended missions?
- Have cyber security vulnerabilities been identified and mitigated?
- Has the software been assessed?
- Can the system be used on the network and interface?
- Are TIR/PCRs documented and resolutions effective?
- Have physical and functional configuration audits been conducted?

Artifacts:

- ATEC Assessment or Evaluation
- Quality and Reliability Statement
- Army Interoperability Certification
- Risk Management Framework
- Software Quality Statement
- Human Systems Integration (HSI) Assessment

SUPPORTABILITY

Questions:

- Is the system supportable?
- Has the sustaining command approved of the plan?
- How will software be supported?
- Has test and diagnostic equipment been identified?
- Has training been developed and approved?
- What is the fielding plan?
- Have the Gaining Commands been notified of the system that will be fielded?

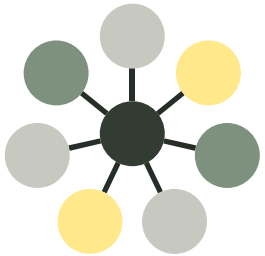
Artifacts:

- Proof of TC-STD
- Logistics Certification from Sustainment Organization
- Software Supportability Statement
- Test, Measurement and Diagnostic Equipment (TMDE) Support Statement
- Signed Materiel Fielding Agreement (MFA)/Materiel Fielding Plan (MFP)/ Memorandum of Notification (MON)
- Training Assessment from Capability Developer

SAFETY ENGINEERING AND AI

Safety challenges are significant

- Complexity of the design and architecture
- Changing operational environments
- Interactions with human in/on the loop
- Perceived changing and adapting behavior
- Level of Rigor requires adaptation for AI development pipeline



Collaborating across Army and Services to shape guidance and policy

Document System Safety and Software System Safety Plan with AI Safety Approach

- Apply/Adapt current Safety methodologies/precepts
- Identify Hazard analyses, artifacts, safety requirements, AI Safety Critical Functions and data
- Understand AI System functions, CONOPs, environments and enabling technology to include Level of Autonomy
- Develop/Modify Level of Rigor (LOR) tasks and metrics
- Develop hazard mitigation guidance for AI technologies
- Establish Risk Assessment Approach for AI: Define Level of Autonomy, Criticality Index, LORs

MIL-STD-882E

PATH TO ASSURED AI

Policy
- Review of existing policy
- Identify gaps to better form requirements

Data Science
- Acknowledge criticality of data to AI
- Identify way and means to evaluate data sets for risk and readiness for AI application

Verification and Validation
- Develop framework for V&V of AI
- Establish procedures and measures for AI performance and reliability

Safety
- Identify unique hazards presented by AI
- Define appropriate design criteria and mitigations to ensure safety

Materiel Release
- Review current requirements
- Adapt and develop necessary deliverables to ensure safe/suitable/supportable

Trust
- Deliver product that the warfighter has trust in to deliver desired capability
- Deliver product that the evaluation community trusts to deliver desired capability

Assured AI: Product can be released and fielded with confidence that is it robust and resilient after rigorous application of best practices and risk mitigation