

# Cybersecurity Test and Evaluation: The Army Perspective

**Mr. Joshua Miller**

**Senior Evaluator, Survivability Evaluation Directorate  
Army Test and Evaluation Command/Army Evaluation Center**

**Prepared for TSIS**

**18 June 2015**

U.S. Army Test and Evaluation Command





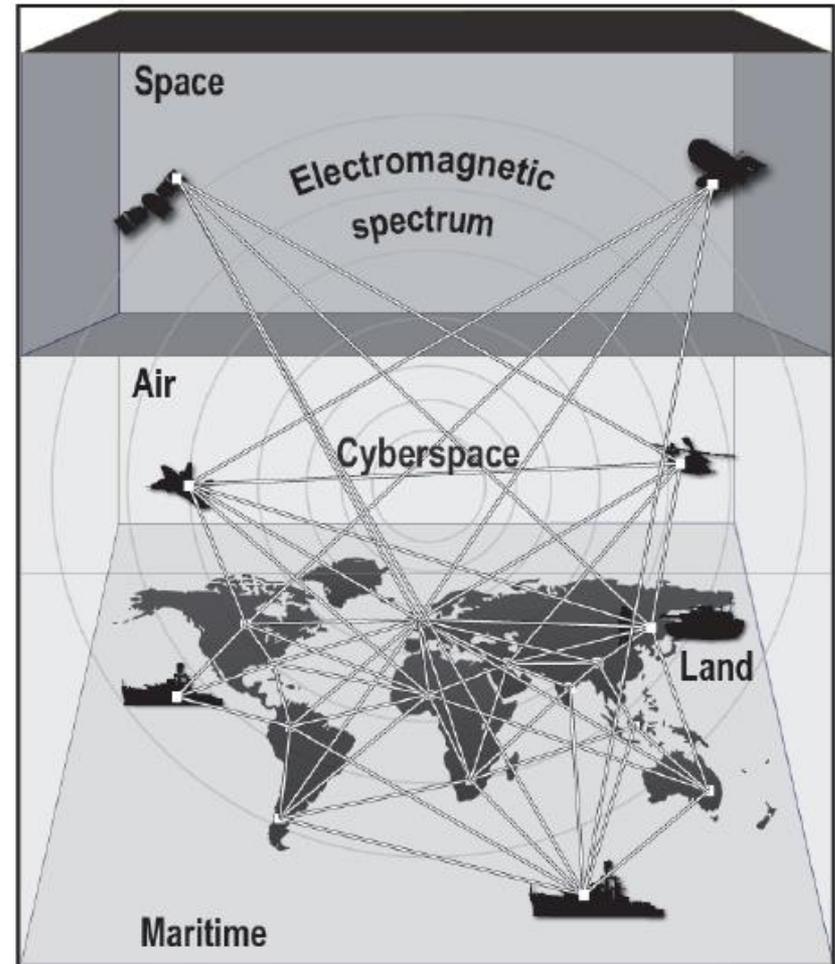
# Operational Environments

## Operational Environment domains:

- Air (naturally occurring)
- Land (naturally occurring)
- Maritime (naturally occurring)
- Space (naturally occurring)
- Cyberspace (manmade)

## DoD Reliance on Cyberspace for:

- Military Command and Control
- Intelligence
- Business Operations



Reference: FM 3-38: Cyber Electromagnetic Activities





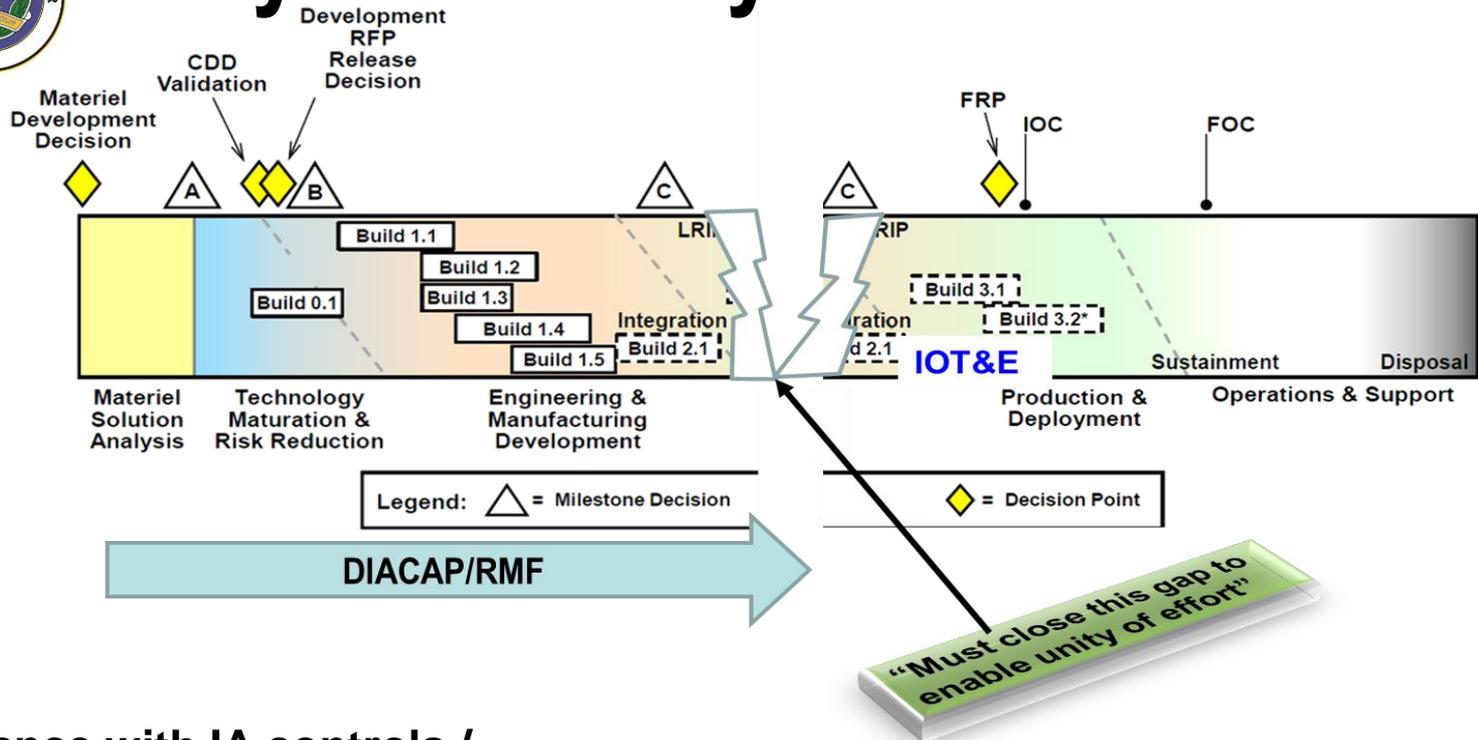
# ATEC Initiatives

- **Shift Left**
- **Earlier Developmental T&E for Cyber Security – Cooperative Vulnerability and Penetration Assessments (CVPA) to Prepare Systems for Record Test**
- **Test & Evaluation Program Synchronization (TEPS)**
  - **Early communication on Test and Evaluation metrics**
  - **The Cybersecurity Scorecard**
- **EW - investments in signals collection and automation**
- **Realistic Threat Portrayals**
- **Metrics Study**
  - **Effort in partnership with MIT – Lincoln Labs**
  - **Examine the application of continuous monitoring**





# Cybersecurity "Shift Left"



Compliance with IA controls / standards and profiles are necessary but not sufficient

Fielded systems found to have novice IA vulnerabilities during OT, which is problematic and costly.

## Shift Left

to discover cybersecurity issues earlier in the acquisition lifecycle.





# Effect on Cybersecurity Testing

- Shift Left
  - Formally add cybersecurity DT to the TEMP
- ATEC: Leverage existing test capabilities rather than build new
- 
- Build T&E plans starting with Risk Management Framework (RMF) products
  - RMF replaces DIACAP with intent to manage risk over the system's lifecycle





# Effect on Cybersecurity Evaluation

- Assess program readiness for major events such as MS C or Initial Operational Test (IOT)
  - AEC cybersecurity scorecard to continually assess
- Incorporate DOT&E 1 August 2014 policy memorandum
  - Protect, Detect, React, Restore

Planning for (event/milestone)

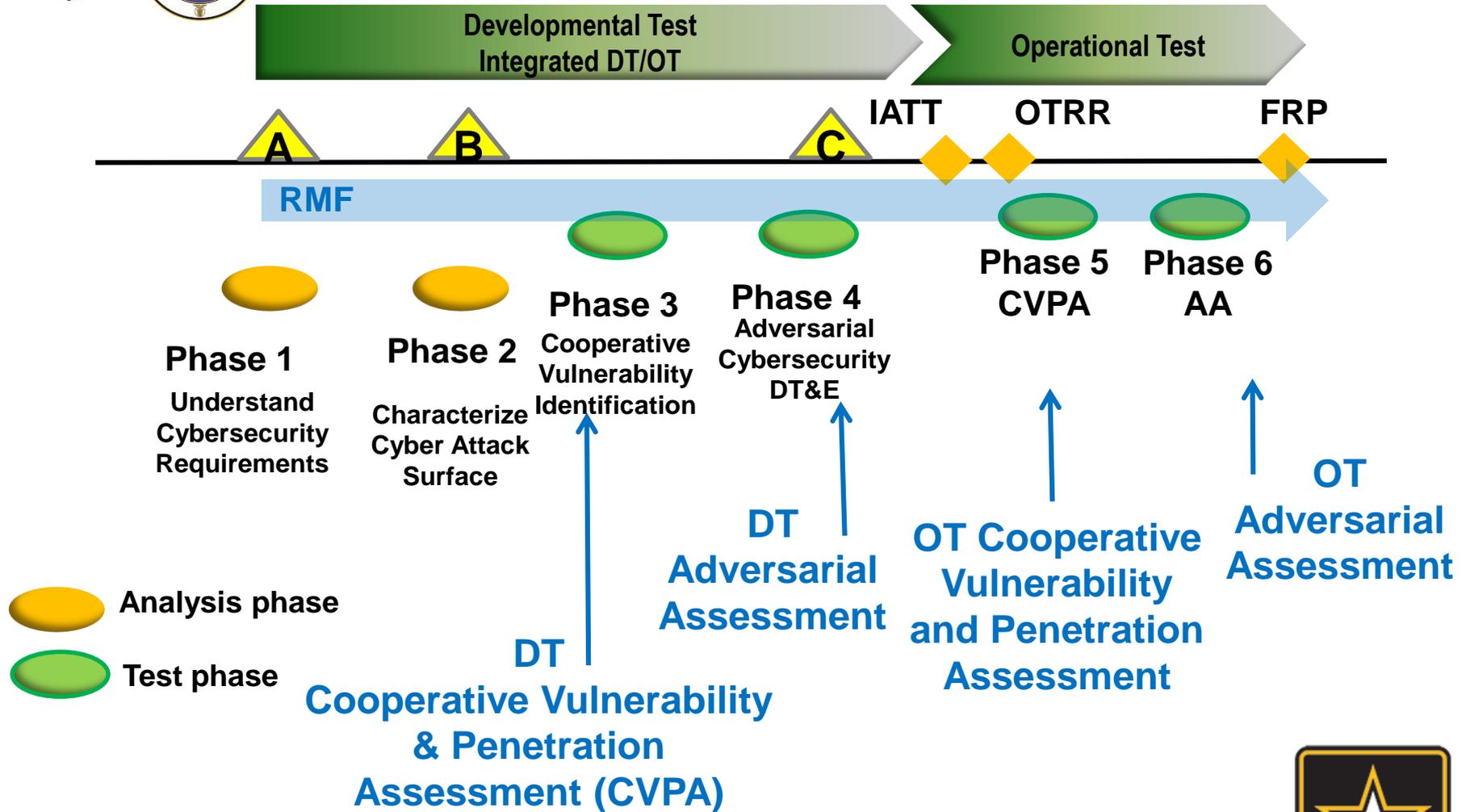
Event	Score	Comments
TEMP	G Y R	Date; Unresolved Issues, related to DOT&E Attachment D
Draft TTSP Part I	G Y R	Date; Unresolved Issues
OTRR 1, T-240	G Y R	Date, Venue, ARL Lead; Unresolved Issues
TAWG	G Y R	Date; Unresolved Issues
Core System Protection, and Core Cyber Defense Performance – Data and Metrics	G Y R	Unresolved Issues, related to DOT&E Attachment C
Operational Test Plan	G Y R	Unresolved Issues, related to DOT&E Attachment E
1 <sup>st</sup> (DT) Blue Team Assessment	G Y R	Date; Unresolved Issues
1 <sup>st</sup> (DT) Red Team Assessment	G Y R	Date, Venue, TSMO Lead; Unresolved Issues
OTRR 2, T-60	G Y R	Date; Unresolved Issues
Verification of Fixes	G Y R	Date, Venue, Provider; Unresolved Issues
OTRR 3, T-5	G Y R	Date; Unresolved Issues
2 <sup>nd</sup> (OT) Blue Team Assessment	G Y R	Date, Venue, ARL Lead; Unresolved Issues
2 <sup>nd</sup> (OT) Red Team Assessment	G Y R	Date, Venue, TSMO Lead; Unresolved Issues



Cybersecurity T&E Scorecard Presented at Each PEO Executive Test Day



# Proposed Cybersecurity T&E Events



Events derived from draft DASD(DT&E) DoD Cybersecurity Test and Evaluation Guidebook, and DOT&E Cybersecurity Operational Test and Evaluation Guidance Memo (01 August 2014)



# Challenges

- **Cybersecurity as Systems Engineering Discipline**
- **Contractual Language for systems with IT**
- **Cyber Test Ranges – “Plug and Play” Tactical Network**
- **M&S – Virtual Machine Emulation & Simulation**
  - **System of Systems Risk Assessment for Investment Decisions**
- **Operational Requirements**
  - “If there is a computer in something, it *can* be [cyber-attacked](#), and we need to be able to harden it and defend it,” the Pentagon’s [Deputy Chief Information Officer for Cybersecurity](#) Mr. Richard Hale
    - “The Joint Staff has recently put out a formal requirement document that includes cybersecurity as a key part of the survivability key performance parameter [KPP]” for every new system”
- **Addressing DOTMLPF-P**
- **Metrics**

**Defensible  
Systems**

