Shift Left: Inserting Cybersecurity Testing and Evaluation Earlier into the Acquisition Lifecycle

Prepared by MAJ Patrick Major
14 November 2013

U.S. Army Test and Evaluation Command

Agenda

- Challenges and Background
- Army Cybersecurity Evaluation Requirements
- Shift Left – Cybersecurity Test and Evaluation earlier in the acquisition life cycle
- Concept
- Path Forward
- Cybersecurity Challenges & Opportunities in Modeling and Simulation

The Cybersecurity Challenge

- Interconnections are Ever Increasing
- Advantages for both threats and the network
  - Technology advancing at an increasing pace
  - Technology provides an edge to the Warfighter
  - Low Barriers to Entry

- Current T&E Paradigm:

  At IOT&E, testers conduct a vulnerability assessment and use a threat computer network operations team to attack the network and assess system's ability to Protect, Detect, React, and Restore

Background

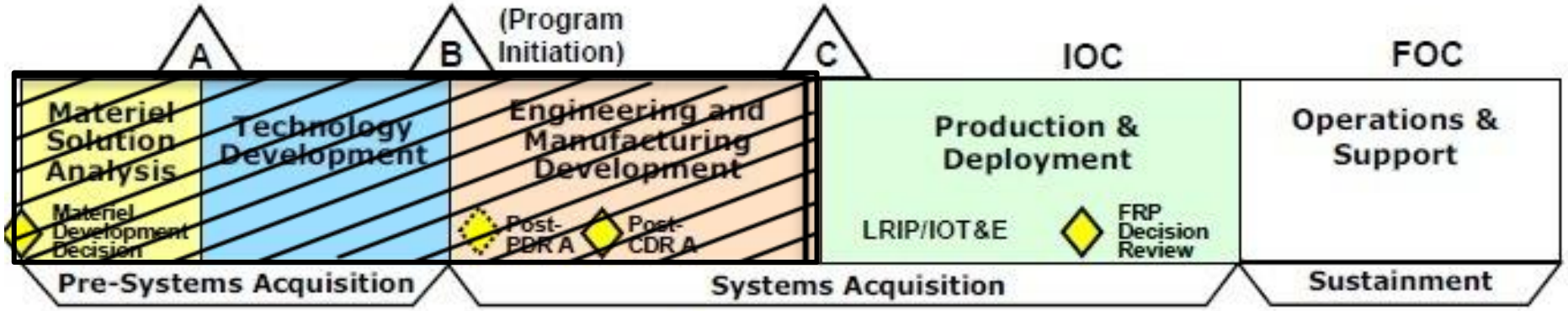
- The cybersecurity environment is growing more complex
  - Growing threats and associated challenges in network security are driving the requirements to understand and inform on cybersecurity much earlier
  - Current Army evaluation strategy, resources and task organization require review in response to the changing environment

Army Cybersecurity Evaluation Requirements

- Army requires protection of Warfighter (weapon and IT) systems against cyber attack and exploitation throughout the lifecycle from program inception to operational use
  - The Army must conduct land warfare and have capabilities to Protect, Detect, React, Restore systems from cyber attack
  - Assessment of the performance of Army systems and infrastructure must be addressed appropriately and early to ensure proper protections are in place

The analysis presented addresses the strategy and event requirements for evaluations conducted by the Army on behalf of the DoD.

Why Shift Left?



Problem: The current approach does not prepare systems adequately for testing against realistic threats until after MS C

Source: Acting DASD(DT&E)/D Briefing ICOTE, March 2013.

Shift Left

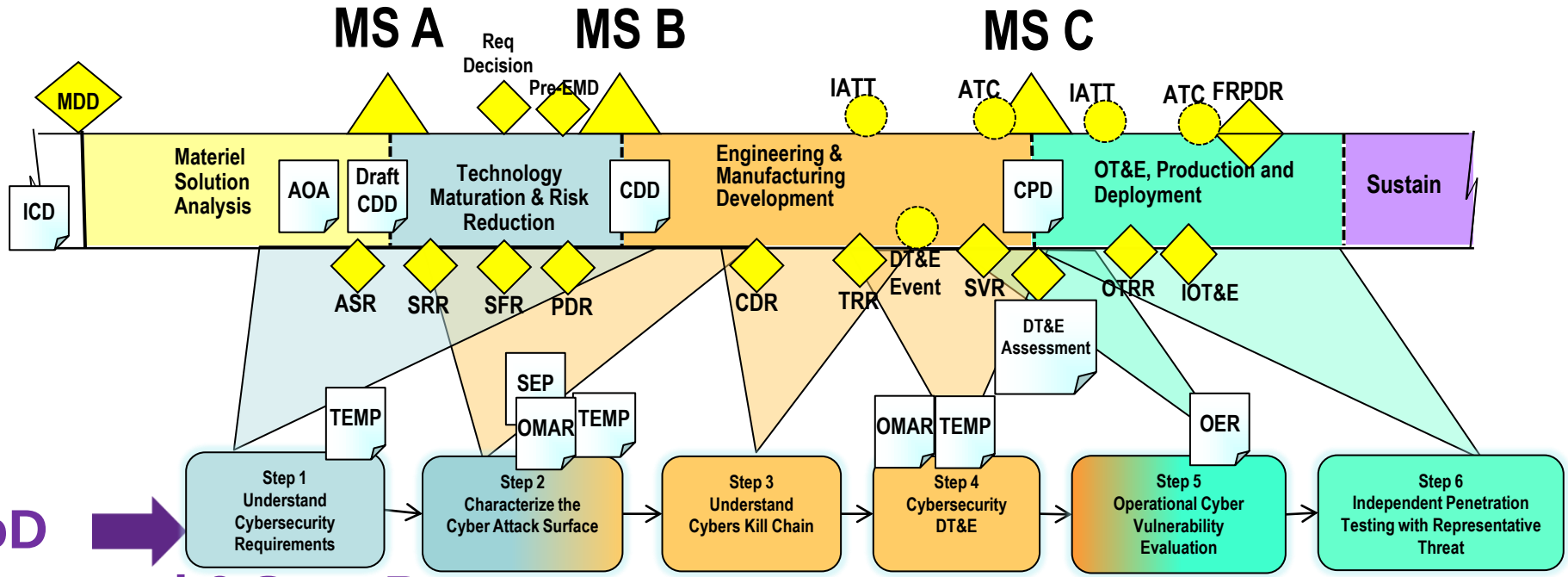
- Compliance with IA controls and interoperability standards and profiles are *necessary but not sufficient*
- Systems found to have interoperability issues and novice IA vulnerabilities during OT, which is problematic and costly

Shift Left

to discover cybersecurity issues earlier in the acquisition lifecycle

Source: Acting DASD(DT&E)/D Briefing ICOTE, March 2013.

Shift Left Strategy



DoD Proposed 6 Step Process earlier in the Acquisition Lifecycle

Draft OSD AT&L DT&E and DOT&E policy, "Procedures for Test and Evaluation of Cybersecurity/Information Assurance in Acquisition Programs", 9 Aug 13

Shift Left Path Forward

- Leverage existing opportunities for T&E
- Establish a cybersecurity sub-IPT
- Improve production readiness
- Reduce discovery of critical vulnerabilities in IOT&E
- Improve acquisition outcomes

Draft OSD AT&L DT&E and DOT&E policy, “Procedures for Test and Evaluation of Cybersecurity/Information Assurance in Acquisition Programs”, 9 Aug 13

Proposed Cybersecurity T&E

Function/ Service	Step 1 Understanding Cybersecurity Requirements	Step 2 Characterize the Cyber Attack Surface	Step 3 Understand the Cyber Kill Chain	Step 4 Cybersecurity DT&E	DT / OT	Step 5 Operational Cyber Vulnerability Evaluation	Step 6 Ind. Pen. Testing with Rep. Threat
Vulnerability Assessment and Penetration Testing	***Network Dependent***						
Systems Engineering Opportunities	***Increasing Complexity of Threat Penetration Testing***					***Validated Accredited Threats***	

Draft OSD AT&L DT&E and DOT&E policy, "Procedures for Test and Evaluation of Cybersecurity/Information Assurance in Acquisition Programs", 9 Aug 13

Shift Left Conclusion

- Improve production readiness for systems earlier in the acquisition lifecycle
- Reduce new discoveries in IOT&E
- Improve the acquisition outcomes to get the system to the Warfighter faster

Cybersecurity T&E Simulation Challenges & Opportunities

- Virtual Machine Emulation
- Networks are:
  - Large (Many Connections and Nodes)
  - Diverse (Many types of hardware and software)

- Network Flow Models

  Over simplify complex processes
- Opportunities for better evaluations using VME and Network Flow models
- Ability to look at cybersecurity performance under different conditions

Test Events are by definition limited assessments of an instantiation of the network with a version of hardware and software at that point in time

Discussion