CYBERSECURITY OT&E

DOT&E Cybersecurity Roles

- Cybersecurity OT&E of systems during acquisition
  - DOT&E Memo "*Procedures for the Operational Test and Evaluation of Cybersecurity in Acquisition Programs*" (1 Aug 2014)
    - Specifies a two-phase OT&E: *Cooperative Vulnerability and Penetration Assessment* followed by an *Adversarial Assessment*
    - Goal: Identify all significant vulnerabilities and operational impact
- Cybersecurity operational assessments
  - Congressional mandate (FY03 Defense Approps Act, Oct 2002)
  - Conduct cybersecurity assessments at CCMDs and Services during major exercises
    - Over 200 assessments conducted since 2003
    - Aggregate results analyzed annually and reported
    - Most recent report (Jan 2017) included summary of demonstrated best practices from CCMDs
- Cybersecurity ranges and training
  - CMF/CPT Training support

DOT&E Cybersecurity Findings

- DOD missions are currently at risk from cyber adversaries
  - Combatant Commands and Service authorities have yet to consistently show that critical missions can be assured in the presence of intermediate or advanced cyber adversaries.

- Cyber adversaries are developing advanced cyber intrusion techniques
  - Determined cyber adversaries can acquire a foothold in most DOD networks

- It is critical that DOD network defenders and system operators learn to "fight through" cyber attacks, just as they are trained to fight through more conventional, kinetic attacks

DOT&E Cybersecurity Findings (2)

- Both acquisition and exercise events point to the same findings:
  - Network defenders are not adequately trained, equipped or available
  - Passwords and other credentials are readily accessible to intruders
  - Software is not up-to-date
  - Software is not configured properly for security
  - Networks and applications have services and capabilities that are easily exploited
- Most cybersecurity vulnerabilities discovered during OT could have / should have been discovered during EMD/DT
  - 90% of all cybersecurity findings FY12-FY14 did not require operational testing to discover

DOT&E Cybersecurity Findings (3)

- Skilled network defenders and conscientious users, supported by a "hygenic," well-protected network, can defeat cyber attacks

- In FY14, the Transportation Command quickly detected and effectively responded to multiple attacks by an intermediate-level cyber red team. TRANSCOM demonstrated key cybersecurity tenets:
  - Implementation and enforcement of strong passwords and password storage
  - Hardening of outward-facing servers
  - Consistent review of network logs using automated scripts to detect possible intrusions
  - Effective incident response and reporting processes

- Because of TRANSCOMs effective defense and response, the red team was unable to impact the missions on TRANSCOM's network.

- Most recent DOT&E cyber report notes good cyber defense demonstrated in some other Combatant Commands

What Makes a Good Test?

A good test results in the resolution of shortfalls and identify the reasons some shortfalls persist. It needs:

- *A Representative System*: the system must be equivalent to the system that will be fielded, and fielded in a way that is consistent with the operational CONOPs
- *The Representative Threat*: the system must be assessed for the ability to "fight through" while exposed to the cyber threats that have been identified for the system and/or network
- *Representative users*: the system must be tested while being operated by typical users with typical levels of training and inherent expertise
- *Deconfliction*: the cybersecurity tests should be deconflicted from other test objectives so that the findings are not constrained or limited.
- *Time*: the test needs to be long enough to meet data requirements

Problems With Representative Systems

- Platform shortages:
  - The typical platform is not available due to operations or a mismatch in delivery schedules
- Configuration issues:
  - The software is not locked (still open to revisions)
  - The software is still a developmental load
  - The software is not the version that will be fielded
- Environmental/Architectural issues:
  - The software is not installed on an operationally representative network (or there is not representative network available)

Threat Challenges

- Asset shortages – not enough Red/Blue Teams available
  - Expansion of operational cyber teams is hurting the availability of skilled cyber teams for acquisition testing
- Intelligence and enumeration:
  - The test teams must conduct extensive discovery of the network and systems to accommodate testing
  - System Threat Assessment Reports (STARs) do not cover
- Execution issues:
  - Permissions: Tests require ground rules for Red Teams; but they cannot be too restrictive.
    - Makes “fighting through” attacks difficult to assess
  - Safety: software decertification risks; open networks

Challenges With Other Resources

- Representative users not available:
  - Appropriate inclusion of higher echelon (Tier 2 and Tier 1) cyber defenders often difficult
  - Many users are not trained to distinguish cyber effects from simple malfunctions or maintenance issues
- Cyber tests can conflict with other test events:
  - Cannot combine flight hours / availability tests with cyber tests that may make the aircraft software unsafe
  - Need to set aside specific opportunities to demonstrate cyber mission effects
- Timing is everything:
  - The best test results in fixing things – cannot accomplish if the testing phases are too close together
  - Duration of the test is too short to depict the full threat

Potential Solutions

- Cyber ranges
  - “Safe sandbox” ranges allow depiction of more aggressive/realistic threats and more realistic cyber defenses
  - Ability to demonstrate cyber mission effects without adversely affecting an operational platform
- Persistent Cyber Threats
  - Extends exposure of Red/Blue activities
  - Allows for re-use of key architecture assessments
  - Requires extensive prior coordination, but less event coordination
- Dedicated test systems / events
  - While more resource-intensive, dedicated cybersecurity test articles and test events allow rapid completion of tests without interference with other objectives