MAKING THE THREAT REAL

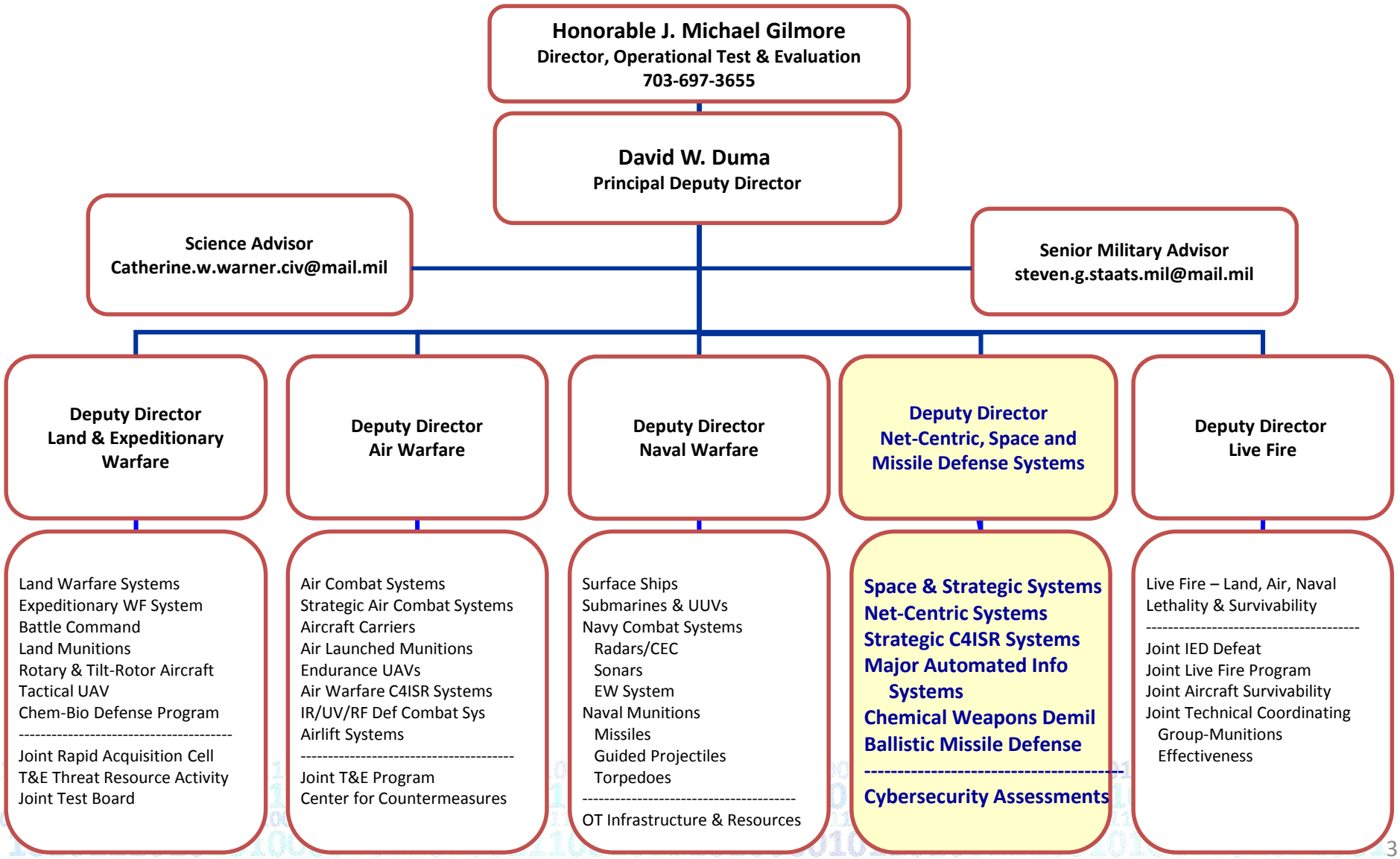
Briefing for the ITEA 2nd Cyber Security Workshop:
"Test and Evaluation to Meet the Advanced Persistent Threat"

Dave Aland
Cybersecurity Assessments


ANONYMOUS


i lov
CyberCaliphate
I love you isis
you isis
TWEETS
3,676
1,268
U.S. Central Command
@CENTCOM

DOT&E Organization



Cybersecurity Assessments

- Cybersecurity OT&E of systems during acquisition
  - DOT&E provides oversight for OT&E of all systems under oversight
  - "*Procedures for the Operational Test and Evaluation of Cybersecurity in Acquisition Programs*" (1 Aug 2014)
- Cybersecurity operational assessments
  - Congressional mandate (FY03 DAA, October 2002)
  - Conduct cybersecurity assessment at each CCMD and Service during a major exercise

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

AUG 01 2014

MEMORANDUM FOR COMMANDER, ARMY TEST AND EVALUATION COMMAND
COMMANDER, AIR FORCE OPERATIONAL TEST AND EVALUATION CENTER
COMMANDER, OPERATIONAL TEST AND EVALUATION FORCE
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY
COMMANDER, JOINT INTEROPERABILITY TEST COMMAND

SUBJECT: Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs

The cyber threat has become as real a threat to U.S. military forces as the missile, artillery, aviation, and electronic warfare threats which have been represented in operational testing for decades. Any data exchange, however brief, provides an opportunity for a determined and skilled cyber threat to monitor, interrupt, or damage information and combat systems. Real-world cyber adversaries regularly demonstrate their ability to compromise systems and inflict damage. The Department of Defense (DOD) acquisition process must deliver systems that provide secure, resilient capabilities in the expected operational environment. Operational testing must examine system performance in the presence of a realistic cyber threat.

Operational Test Agencies (OTAs) will include cyber threats among the threats to be encountered in operational testing for DOT&E oversight systems with the same rigor as other threats. The purpose of cybersecurity operational test and evaluation is to evaluate the ability of a unit equipped with a system to support assigned missions in the expected operational environment. The system is considered to encompass hardware, software, user operators, maintainers, and the training and Tactics, Techniques, and Procedures used to carry out the Concept of Operations. The operational environment includes other systems that exchange information with the system under test (system-of-systems to include the network environment), and users, administrators and cyber defenders, as well as representative cyber threats. Early involvement of programs with the operational test community is required to ensure that system requirements are measurable and testable, and that the rationale behind the requirements and the intended operational environment are understood. An adequate operational test gathers sufficient data to identify all significant vulnerabilities of a system in the operational environment to capture their effect on mission accomplishment. I will use the results of the cybersecurity testing, in part, to determine the operational effectiveness, suitability, and survivability of the system.

This memorandum, which supersedes previously published guidance that described a "six-step" process, specifies a two-phase approach for operational cybersecurity testing in

Common Cybersecurity Findings

- Both acquisition and exercise events reveal:
  - Passwords and other credentials are readily available to intruders
  - Software is often not up-to-date
  - Software is frequently not configured properly for security
  - Networks and applications have services and capabilities enabled that are easily exploited
  - Detection of unauthorized activity is rare
- Cybersecurity testing is frequently incomplete
  - Not all significant vulnerabilities are identified
  - Not all significant vulnerabilities are characterized
  - Testing itself is not adequate
- 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

Operational Test Requirements

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

- A Representative System
- **The Representative Threat**
- Representative users
- Enough Resources and Time

What is a "Representative Threat"

- Identification
  - The threat actors and capabilities are validated by DIA
- Authorization
  - The team is certified in skills and personnel by NSA
  - STRATCOM and US CYBER COM have accredited the team for live network operations.
  - Rules of engagement are established for Red Team activities
- Execution
  - The team has adequate system/network knowledge
  - The team can demonstrate intrusion techniques
  - The team is permitted to induce cyber effects
  - The data is recorded and analyzed

How Hard Can That Be?

- Identification
  - Threats and capabilities are unknown or changing rapidly
- Authorization
  - There are shortages of Red and Blue Teams across DoD
  - Rules of engagement are often restrictive/prohibitive
- Execution
  - The test is too short to allow system insight
  - The team is not allowed to induce effects
  - “Safety of flight” issues
  - Poor data capture by the teams
  - Poor data sharing amongst the teams

What Level Threat Is That?

Beginner	Novice	Intermediate	Advanced
• Lacks funding • Uses readily available Freeware or cheap • "Googles" known vulnerabilities • Easily detected • Single/no layer compromise • Lacks post distribution C2 • Uses personal IP • Does NOT use encryption • Little knowledge of target • Noisy scanning • Poorly designed phishes using attachments • Usually acts alone • Easily attributable (leaves tracks behind)	• Has some resources • Readily available malware; may alter code • "Googles" known vulnerabilities; access to hacker forums • Uses hop points • May deceive some AV/IDSs • Has simple C2 structure • Uses simple encryption • Understands primary target • Not usually persistent • Correct wording of phishes using attachments • Small team working the effort • Can be attributed	• Well funded/developed p • Ppurchased malware; may significantly alter • "Googles" known vulnerabilities; access to special hacker forums; has internal developers • Uses multiple hop points • Scanning paths obscured • Multiple teams coordinated • Uses persistent access; very good target knowledge • May have insiders • Complex phishing using broader relationships (e.g. social network, organization) with attachments and drive-by links • Sometimes difficult to attribute	• Extremely well-funded • Unique malware; use of zero-day exploits • Has team of developers for vulnerabilities • Uses multiple hop points through a TOR cloud • Scanning enabled by intelligence • Multiple specialized teams • Uses persistent access • Employs full-spectrum techniques, including insiders and close-access • When spear-phishing, impersonates a highly trusted source • Very difficult to detect or attribute; may causes mis-attribution

Way Ahead

- Identification
  - Dynamic STAR and frequently updated threat data
- Authorization
  - Combined assessments in exercises and other venues
  - Persistent presence authorizations
- Execution
  - Plan for longer tests if necessary, but plan for cyber
  - Include the possibility of “destructive” cyber testing
  - Use cyber ranges where safety is an issue
  - Instrument, instrument, instrument
  - Don’t treat test data as proprietary