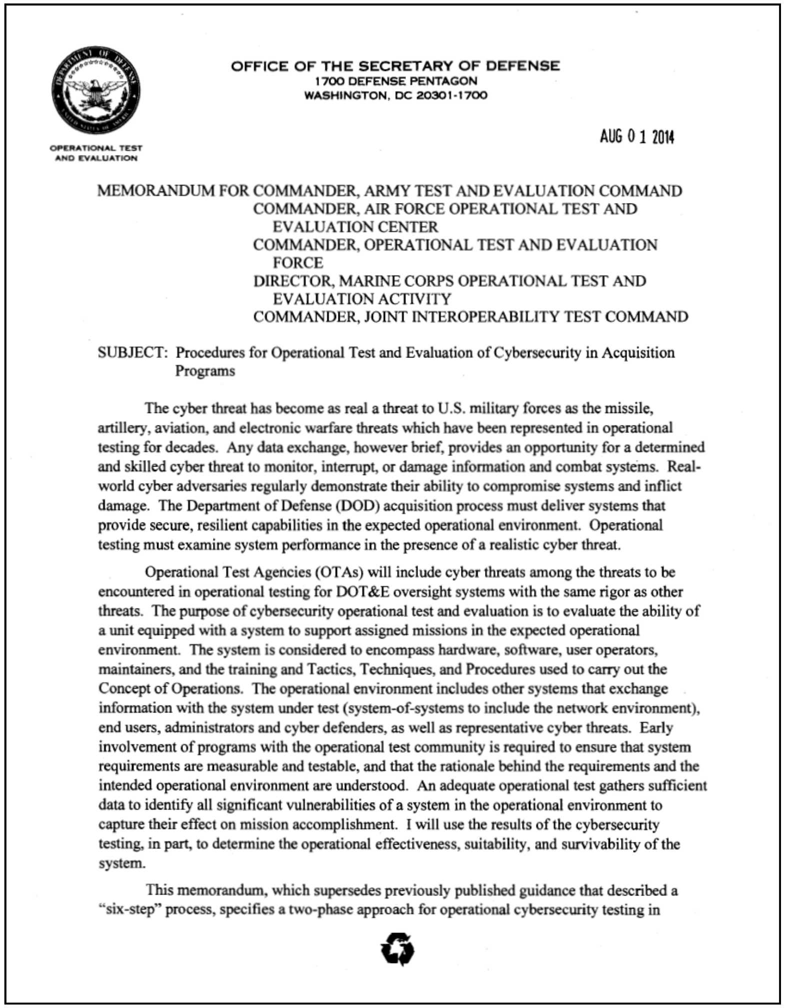
Cybersecurity Training in OT&E for DOT&E Action Officers

Dr. Catherine Warner

Science Advisor to the Director,
Operational Test and Evaluation (DOT&E)

DOT&E Guidance

Dr. Gilmore’s August 1, 2014 Memo to OTAs



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

OPERATIONAL TEST
AND EVALUATION

AUG 0 1 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), end 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

- ❑ Identifies the cyber threat as a real and present danger for modern warfare systems
- ❑ Requires that any oversight system capable of sending or receiving digital information undergo cybersecurity testing as part of OT&E
- ❑ Defines adequate cybersecurity testing as testing that:
  - ❑ Identifies all significant vulnerabilities in the operational environment
  - ❑ Captures their effect on mission accomplishment
- ❑ Prescribes a two-phased approach to cybersecurity OT&E:
  - ❑ Cooperative Vulnerability and Penetration Assessment
  - ❑ Threat-representative Adversarial Assessment

Reviewing TEMPs and Test Plans

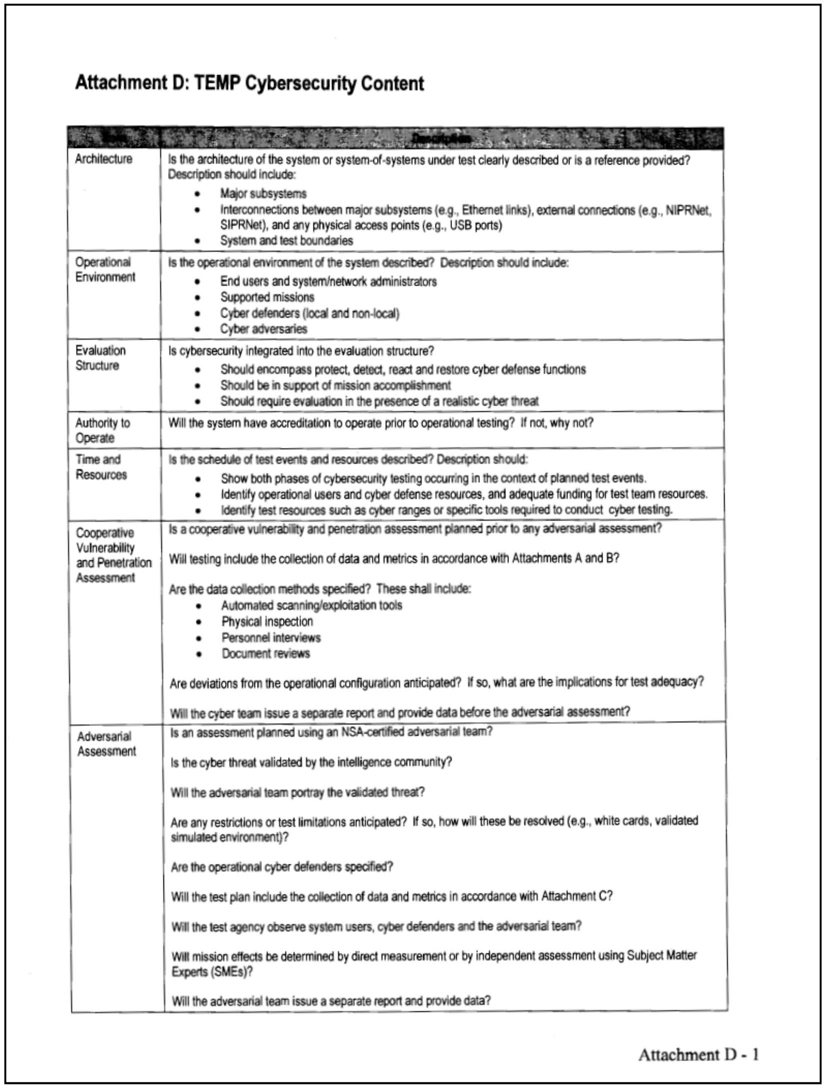
- **DOT&E guidance highlights expected contents for TEMPs and Test Plans**

- **All cyber OT&E events should have a DOT&E-approved plan**

- **DOT&E AO should coordinate with Cyber OT&E POC (Dave Aland)**

- **At IDA, Cyber OT&E group will review all incoming TEMPs and Test Plans**

- **Send documents for review early – while changes can still be made!**

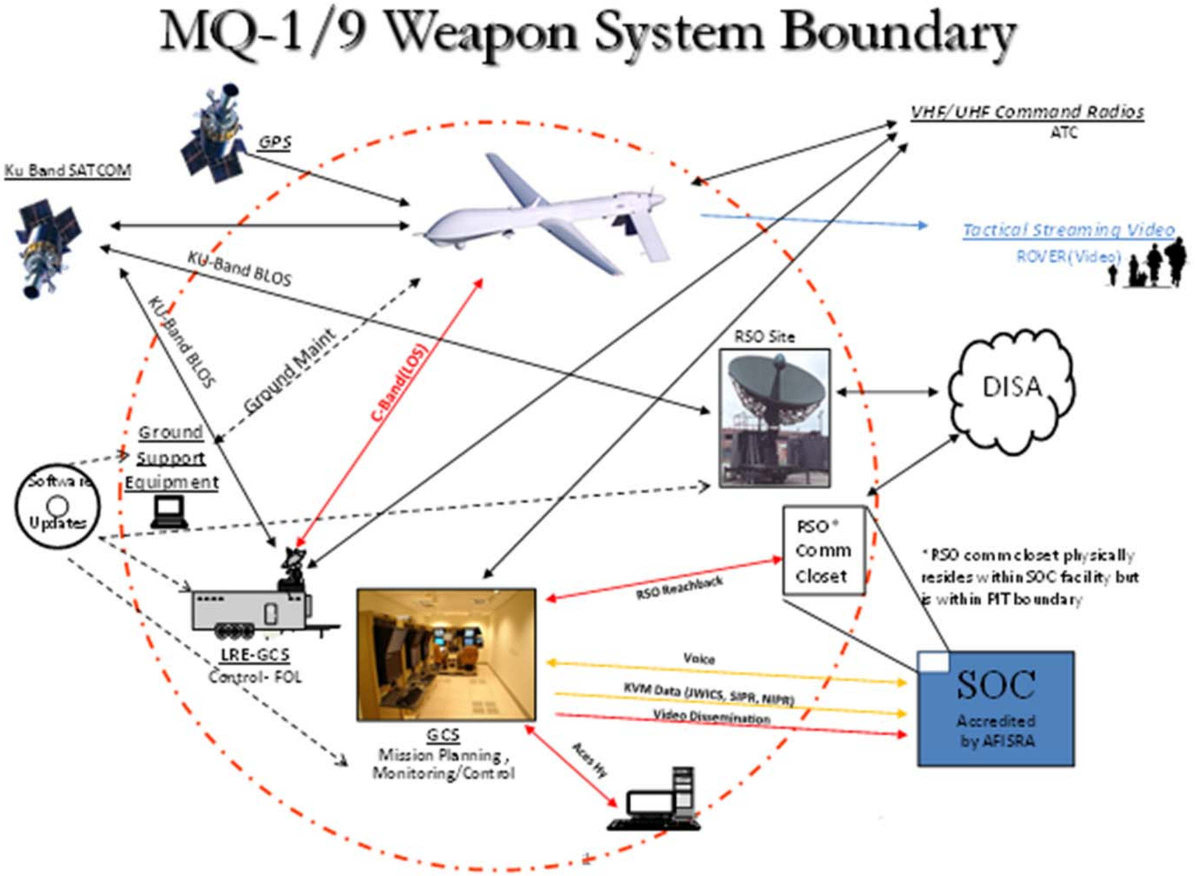


Attachment D: TEMP Cybersecurity Content

[illegible]	Description
Architecture	Is the architecture of the system or system-of-systems under test clearly described or is a reference provided? Description should include: • Major subsystems • Interconnections between major subsystems (e.g., Ethernet links), external connections (e.g., NIPRNet, SIPRNet), and any physical access points (e.g., USB ports) • System and test boundaries
Operational Environment	Is the operational environment of the system described? Description should include: • End users and system/network administrators • Supported missions • Cyber defenders (local and non-local) • Cyber adversaries
Evaluation Structure	Is cybersecurity integrated into the evaluation structure? • Should encompass protect, detect, react and restore cyber defense functions • Should be in support of mission accomplishment • Should require evaluation in the presence of a realistic cyber threat
Authority to Operate	Will the system have accreditation to operate prior to operational testing? If not, why not?
Time and Resources	Is the schedule of test events and resources described? Description should: • Show both phases of cybersecurity testing occurring in the context of planned test events. • Identify operational users and cyber defense resources, and adequate funding for test team resources. • Identify test resources such as cyber ranges or specific tools required to conduct cyber testing.
Cooperative Vulnerability and Penetration Assessment	Is a cooperative vulnerability and penetration assessment planned prior to any adversarial assessment? Will testing include the collection of data and metrics in accordance with Attachments A and B? Are the data collection methods specified? These shall include: • Automated scanning/exploitation tools • Physical inspection • Personnel interviews • Document reviews Are deviations from the operational configuration anticipated? If so, what are the implications for test adequacy? Will the cyber team issue a separate report and provide data before the adversarial assessment?
Adversarial Assessment	Is an assessment planned using an NSA-certified adversarial team? Is the cyber threat validated by the intelligence community? Will the adversarial team portray the validated threat? Are any restrictions or test limitations anticipated? If so, how will these be resolved (e.g., white cards, validated simulated environment)? Are the operational cyber defenders specified? Will the test plan include the collection of data and metrics in accordance with Attachment C? Will the test agency observe system users, cyber defenders and the adversarial team? Will mission effects be determined by direct measurement or by independent assessment using Subject Matter Experts (SMEs)? Will the adversarial team issue a separate report and provide data?

Attachment D - 1

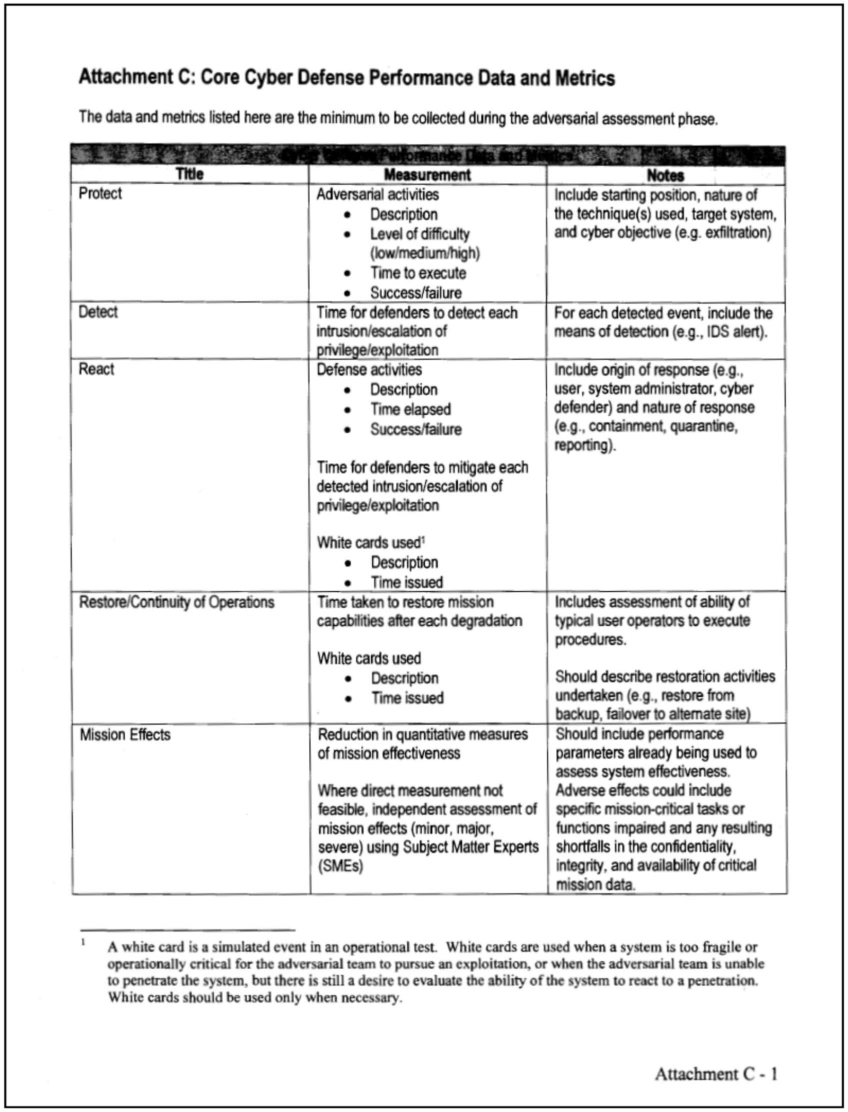
Elements of Cyber OT&E Planning



Taken from MQ-1/9 Architecture Analysis
(Every program should have a diagram like this one to help define the scope of testing)

- Almost every modern weapons system sends or receives digital information, and therefore needs cyber testing in OT&E
- Air-gapped systems are still vulnerable and must be tested

Data Collection



Attachment C: Core Cyber Defense Performance Data and Metrics

The data and metrics listed here are the minimum to be collected during the adversarial assessment phase.

Cyber Defense Performance Data and Metrics

Title	Measurement	Notes
Protect	Adversarial activities • Description • Level of difficulty (low/medium/high) • Time to execute • Success/failure	Include starting position, nature of the technique(s) used, target system, and cyber objective (e.g. exfiltration)
Detect	Time for defenders to detect each intrusion/escalation of privilege/exploitation	For each detected event, include the means of detection (e.g., IDS alert).
React	Defense activities • Description • Time elapsed • Success/failure Time for defenders to mitigate each detected intrusion/escalation of privilege/exploitation White cards used[1] • Description • Time issued	Include origin of response (e.g., user, system administrator, cyber defender) and nature of response (e.g., containment, quarantine, reporting).
Restore/Continuity of Operations	Time taken to restore mission capabilities after each degradation White cards used • Description • Time issued	Includes assessment of ability of typical user operators to execute procedures. Should describe restoration activities undertaken (e.g., restore from backup, failover to alternate site)
Mission Effects	Reduction in quantitative measures of mission effectiveness Where direct measurement not feasible, independent assessment of mission effects (minor, major, severe) using Subject Matter Experts (SMEs)	Should include performance parameters already being used to assess system effectiveness. Adverse effects could include specific mission-critical tasks or functions impaired and any resulting shortfalls in the confidentiality, integrity, and availability of critical mission data.

[1] A white card is a simulated event in an operational test. White cards are used when a system is too fragile or operationally critical for the adversarial team to pursue an exploitation, or when the adversarial team is unable to penetrate the system, but there is still a desire to evaluate the ability of the system to react to a penetration. White cards should be used only when necessary.

Attachment C - 1

- **1 August 2014 memo defines minimum set of data to be collected for both Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Phases**
- **Emphasis needs to be on detection, reaction, and response**
  - Not just identifying vulnerabilities
- **Goal is to understand how well the system can perform in the *presence of a cyber adversary***

Reporting

- **DOT&E uses the results of cybersecurity testing when determining operational effectiveness, suitability, and survivability**

- **Results can be caveated**
  - E.g. survivable in the presence of an outsider cyber threat but not survivable in the presence of a nearsider or insider cyber threat

- **DOT&E reports should incorporate:**
  - Vulnerability results from CVPA
  - Vulnerabilities discovered during adversarial testing
  - Detection, reaction, and response performance of cyber defenders
  - Mission effects through cyber
    - » Through direct demonstration in OT&E, or
    - » Inferred from SME expertise when necessary due to safety or other risks

Cyber OT&E Challenges

- **The list of NSA-certified cyber threat teams (Red Team) is small compared to the number of events they need to cover**
  - 177th and 57th Information Aggressor Squadrons
  - Threat Systems Management Office
  - 1st Information Operations Command
  - Naval Information Operations Command / Commander, Operational Test and Evaluation Force
  - DISA Red Team

- **In FY14, there were 21 oversight OT&E cyber events and 16 exercise assessments – this is only what's under DOT&E oversight!**
  - All of the teams receive Service-level tasking as well

- **Many programs perceive a lack of clear requirements**
  - DepSecDef directed examining the feasibility of a Cyber KPP
  - JROC is examining incorporating Cyber into a Survivability KPP
  - DOT&E has been working with JROC, but also exploring alternatives including a standalone Cyber KPP

DOT&E Exercise Assessment Program

- **Separately from the OT&E oversight role, DOT&E also administers the Congressionally-mandated CCMD cybersecurity exercise assessment program**
- **Assesses cybersecurity posture of CCMDs in the context of pre-existing training exercises**
- **Training audience learns to fight through a *hostile cyber environment***
- **Although most of today will focus on OT&E, two briefings this afternoon will introduce the assessment program**
  - Focus will be on sophisticated analysis of attack threads and defender responses
  - Demonstrates why operational cybersecurity testing is vital prior to fielding

Today's Schedule

- DOT&E Procedures
- Case Study #1 Q-53
- Common Myths and Refutations
- Cyber OT&E Overarching
- Case Study #2 LCS
- Best Practices
- FY14 Exercise Overarching
- Valiant Shield 2014