“Fighting Through” the Contested Cyber Domain

Bradley O Thomason
2 May 2013
“The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy.”

- Department of Defense Strategy for Operating in Cyberspace
DoD Approach

• **Protect – Detect – React – Restore** model

• When all else fails – write a policy........
Information Assurance Policy

Build and Operate a Trusted GIG

Cybersecurity (CS)-Related Policies and Issuances
Developed by the DoD CIO, CS Deputy
Last Updated: January 1, 2013
Send questions/suggestions to info@theodian.com
Reality of the World

• 700% increase in number of adversaries capable of significant cyber activities against the US in last 5 years

• Adversary investment in cyber capabilities has risen >900% in last 3 years

• Global information environment provides access to broad spectrum of capabilities.

• Effective mission execution through “Hired Guns”
Levels of Threat

- **Level 1**
  - Lone or small group actors
  - Common tools, techniques
  - Unsophisticated without significant support

- **Level 2**
  - Individuals or small groups supported by commercial entities, criminal syndicates, or other transnational groups such as terrorist networks
  - Common tools used in a sophisticated manner
  - Activities include espionage, data collection, network mapping/recon, and data theft

- **Level 3**
  - Individuals or small groups supported by state-sponsored institutions (military or civilian)
  - Significant resources and sophisticated tools
  - Activities include espionage, data collection, network mapping/recon, and data theft

- **Level 4**
  - State-sponsored offensive IO, especially CNA
  - State-of-the-art tools and covert techniques
  - Activities conducted in coordination with military operations
Cost ($)/Usability

Threat Level - Army FM 3-13

Current complexity required for 98% success

Current complexity required for 98% success

Cost ($) Usability

1 2 3 4
Relevant Guidance

- DOT&E, *Test and Evaluation of Information Assurance in Acquisition Programs*, Feb 13

- Secretary of Defense, *Maintaining Readiness to Operate in the Cyberspace Domain*, Dec 12

- CJCS Execute Order to *Incorporate Realistic Cyberspace Conditions into Major DoD Exercises*, Feb 11
Take Away From Guidance

• “Protect-Detect” will **NEVER** stop the threat from impacting systems
  – Not “if” but “when” your system will be impacted (directly or indirectly) by adversary cyber operations

• **ALWAYS** will have a need for robust “React- Restore”
  – “React” must include understanding Operational Impact
  – “Restore” costly and must include short term mitigation strategy

• Future focus should emphasize understanding impacts of cyber activities on military (and national) operations

• Ultimate measure of success is ability to rapidly restore systems efficiently and effectively – i.e. Fighting through a contested cyber domain......
QUESTIONS

There I was, stuck in a Chinese firewall, when suddenly our router lit up like the Fourth of July... Bots to the left of me, Trojans to the right... We lost some good servers that day.

Future War Stories
DT&E Supports DOT&E Six Step Process

DT&E Four Step Process

- **Step 1**: Characterize Attack Surfaces and Develop Cybersecurity DT&E Strategy
- **Step 2**: Cybersecurity Component and System Integration Test and Evaluation
- **Step 3**: Evaluate Cybersecurity Kill Chain
- **Step 4**: Cybersecurity Developmental Test and Evaluation

DOT&E Six Step Process

- **Step 1**: Is the candidate acquisition program covered by DOT&E Cyber Policy
- **Step 2**: Initial review (MAC, CL, IA Controls)
- **Step 3**: OT&E Risk Assessment
- **Step 4**: Operational Cyber Vulnerability Evaluation (IOT&E)
- **Step 5**: Protect, Detect, React, and Restore Operational Evaluation
- **Step 6**: Continuity of Operations Evaluation

Coordination with DOT&E ongoing
MEMORANDUM FOR COMMANDER, ARMY TEST AND EVALUATION COMMAND
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY
COMMANDER, OPERATIONAL TEST AND EVALUATION FORCE
COMMANDER, AIR FORCE OPERATIONAL TEST AND EVALUATION CENTER
COMMANDER, JOINT INTEROPERABILITY TEST CENTER

SUBJECT: Test and Evaluation of Information Assurance in Acquisition Programs

DOT&E has provided detailed guidance for the test and evaluation of information assurance in acquisition programs and I recently reviewed the implementation of this guidance in FY12 across a number of test reports.¹ I have attached a copy of that review. While we have collectively improved information assurance testing and evaluation, my review identified a number of areas where we can further improve, as follows:

- **Independent Penetration Testing** – Due to limited test durations, sharing system information and interconnections between the cooperative cyber vulnerability assessment teams (usually a “Blue Team”) and the independent cyber penetration/exploitation teams (usually a “Red Team”) is acceptable. However, shared information should not include specific vulnerabilities or system shortfalls. The effort of the cyber penetration/exploitation team should go beyond merely validating prior findings, and focus on examining the system under test in an operational and threat representative event. Additionally, separate teams preferably should perform vulnerability assessments and penetration/exploitation assessments to enhance independence and opportunities for assessing protect, detect, react and respond components. Finally, the correction of vulnerabilities discovered in the cooperative assessments should be an entrance criterion for subsequent penetration/exploitation testing.

- **Network Defense Analysis** – The test environment should encompass those network defense elements (including trained personnel, standard tools, and normal network defense procedures) that may not be locally resident and are increasingly provided at higher tiers by other activities. The test should quantitatively examine not only the inherent system/network protections for the system under test, but also the network defense ability to detect penetration or

¹ Director, Operational Test and Evaluation, Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs, 21 January 2009; Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs, 4 November 2010.
exploitation, react to those events (either procedurally or automatically), and restore the system to full capability following the event. Where appropriate, continuity of operations should be demonstrated or assessed for enterprise system programs; weapons system programs should coordinate with my office to confirm the requirement for continuity of operations testing.

- **Operational Effects Analysis** – Testing should include an assessment of operational risk presented by vulnerabilities and shortfalls exploited by a representative threat, and the most direct way to assess that risk is to demonstrate and record relevant operational effects. When operational threat representative effects cannot be conducted on live-networks, alternate evaluation approaches (including the use of cyber range facilities) should be employed and included in the test planning.

We must routinely review information assurance test and evaluation procedures and outcomes as the cyber environment in the Department evolves. I request your support in continuing to improve these information assurance tests to be not only as rigorous as every other test you conduct, but as rigorous and challenging as the cyber threats these systems will confront.

J. Michael Gilmore
Director

Attachment:
As stated