Information Assurance (IA) and Interoperability Evaluations During Combatant Command and Service Exercises

SUMMARY

- DoD is improving its IA and interoperability postures, but the information operations (IO) threat continues to increase in capability and in ability to rapidly exploit new vulnerabilities.
- Operational assessments of IA/interoperability during Combatant Command (COCOM) and Service exercises promote identification and resolution of problems that could impact warfighter mission accomplishment.
- A full assessment cycle of Blue (vulnerability assessment), Green (train and assist), and Red (threat penetration assessment) teaming provides the most comprehensive assessments and the greatest opportunity to improve IA and interoperability postures.
- Most of the vulnerabilities found to date are basic problems with readily available solutions.
- Exercise authorities appreciate and desire more Operational Test and Evaluation (OT&E) expertise during their exercise planning, execution, and assessment phases. COCOM and Service requests have grown to 28 events for FY05.
- Assessment methodology and metrics continue to mature and be tailored to the exercise environment and the needs of supporting organizations across DoD.

BACKGROUND

The FY03 Appropriations bill directed that the COCOMs and Services conduct operationally realistic IA and interoperability evaluations during major exercises. The bill directed the Service Operational Test Agencies (OTA's), the Service Information Warfare Centers, and the National Security Agency (NSA) assist in the planning, conduct, and evaluations of these exercises. DOT&E's responsibility consists of overseeing these efforts and providing annual updates on DoD's progress based on results of the exercise evaluations and OT&E. DoD has programmed $156M through FY09 for this initiative, $18M of which was funded in FY04.

The bulk of the FY04 funds were distributed to the OTAs, who in turn assembled teams with the expertise to perform IA and interoperability assessments before and during exercises. These teams plan, execute, collect data, analyze, and report the results of all activities associated with IA and interoperability assessments. The following describes the planning and assessment methodology employed by the OTAs for a given exercise:

- Actively participate in all exercise planning conferences beginning with the Concept Development Conference. Early involvement results in greater likelihood that realistic Red Team penetration events will be synchronized with the exercise scenario and data collection requirements are supported.
- Design a comprehensive Red Team scenario overlaid on the exercise scenario to examine the performance of operational networks and operators when subjected to information operations attacks. Red Team events that provide multi-echelon stress with multi-level threats enhance the warfighter's appreciation for the rapidly evolving threat, and solidify their training and capabilities in all aspects of "protect, detect, react, and restore" missions.
- Design an interoperability assessment plan in coordination with the Joint Interoperability Test Command.
- If full Red Team penetration activities are appropriate and approved, activate the Red Team approximately nine months in advance of the exercise.
- Conduct an administrative Blue Team vulnerability assessment approximately six months prior to the exercise, providing feedback to the exercise authority for remedial actions in advance of the exercise; special focus is paid to ensure prior issues have been resolved. Interoperability reviews and certification efforts may also be included during the Blue Team phase.
- Provide Green Team assistance to the exercise authority in understanding the nature, priority, and remedial activities associated with identified vulnerabilities.
- Coordinate external support for solutions beyond the organic capabilities of the exercise authority and assist in the identification of sources for any needed training.
- During the exercise, execute the Red Team events safely, legally, and consistent with the exercise objectives.
- Capture relevant IA and interoperability data, analyze results, and support trend analyses.
- Provide quick-look feedback to the exercise authority and participants, and support after-action reviews.

- Prepare reports that inform exercise participants, system administrators, and leadership.
- Identify problems that require external solutions and provide appropriate results to developers and sponsors who will construct solutions and prioritize efforts.
- Update databases, compare performance with rolling baseline, and perform trend analysis. Provide all results to DOT&E.
- Recommend activities for the next cycle (e.g., more stressing or operationally focused Red Teaming).
- Begin the next cycle.

FY04 ASSESSMENT ACTIVITIES

In this fiscal year, the OTA teams have grown significantly, as have the relationships with COCOMs and other critical partner organizations such as the NSA, the Service Information Warfare Centers, the Defense Intelligence Agency (DIA), and the Defense Information Security Agency (DISA). Accomplishments by the OTA Teams and their partners include the following:

- Performed full Blue/Green/Red Team assessments for 6 exercises (see Table 1).
- Performed Blue/Green Team assessments for 12 exercises. Another four exercises were observed for future assessment.
- Observed and assisted in exercises that have (or offer future opportunity for) Red Teaming.
- Developed IA and interoperability metrics that are observable in the exercise environment, meaningful to the warfighter, and suitable for performing baseline assessments and trend analyses.
- Developed an evaluation-plan template and an exercise-planning checklist to bring appropriate levels of analytical rigor to exercises.
- Coordinated with acquisition elements in their commands to share best practices, metrics, and lessons learned from COCOM and Service exercises.
- Initiated a working group to identify critical mission thread information that will support both IA and interoperability assessment planning.
- Initiated a working group to identify most effective and affordable candidates for Blue Team tool kits.

The NSA and the Service Information Warfare Centers are refining a training and certification program to expand Red Team resources available to support assessment activities. They are also developing new tools and methodologies to stress the exercise participants. DIA continues to provide critical support to this initiative via the Joint Information Operations (IO) Threat Working Group, and has committed to provide a comprehensive IO Threat Capabilities Assessment update every six months. The DIA assessments are essential to proper portrayal of the IO threat for the exercises associated with this effort, and also in all of the formal OT&E for DoD's acquisition programs.

DOT&E has increased the focus on IA as an evaluation issue for systems on the OT&E oversight list. DOT&E identified a dozen acquisition programs in FY04 for an expanded review of the adequacy of IA evaluation planning and to confirm appropriate IA OT&E metrics were in use. This effort included review of Test and Evaluation Master Plans, Test Plans, and Defense Information Technology Security certification and Accreditation Process documentation. The OTAs are performing similarly expanded efforts on selected acquisition programs, and both DOT&E and OTA efforts to heighten IA awareness in acquisition program planning will continue in FY05. The OTA teams also maintain awareness of results across the assessment initiative, and ensure that solutions and lessons learned in one theater are shared across other theaters.

The DOT&E policy for IA evaluations implemented in 1999 remains in effect, with an update currently in final coordination. The update incorporates new metrics and lessons learned from this initiative that are appropriate for acquisition OT&E.

Information Assurance and Interoperability Exercise Events for FY04			
COCOM	**Exercise**	**OTA Lead**	**OTA Support**
CENTCOM	Internal Look 05 Preparation (cancelled)	ATEC	N/A
EUCOM	Agile Response 04	ATEC	OPTEVFOR
	Austere Challenge 04	ATEC	JITC, AFOTEC
JFCOM	United Endeavor 04	OPTEVFOR	JITC, ATEC
	CJTF Exercise 04-02	JITC	OPTEVFOR
NORTHCOM	United Defense 04	ATEC	JITC, MCOTEA
	Salt Lake Shake 04	ATEC	JITC
	Determined Promise 04	ATEC	JITC, MCOTEA, OPTEVFOR
	Joint Warrior Interoperability Demonstration 04	JITC	ATEC
PACOM	Terminal Fury 04	OPTEVFOR	JITC, ATEC
	RSOI 04 (PACOM HQ)	OPTEVFOR	ATEC, AFOTEC
	RSOI 04 (U.S. Forces Korea)	OPTEVFOR	ATEC
	Ulchi Focus Lens 04	OPTEVFOR	ATEC
	Cobra Gold 04	OPTEVFOR	
SOUTHCOM	Fuertas Defensas 04	ATEC	JITC, MCOTEA
SOCOM	TBD	JITC	
STRATCOM	Global Guardian 04	JITC	AFOTEC
	Austere Challenge 04	JITC	ATEC
	Amalgam Virgo 04	JITC	ATEC
TRANSCOM	Turbo Challenge 04	JITC	AFOTEC
Joint / Service	JNTC Horizontal One Exercise	MCOTEA	AFOTEC, ATEC
	Asynchronous Warfare Initiative (AWI)	OPTEVFOR	JITC
	Marine Expeditionary Force Exercise 04	MCOTEA	
	HMX-1 Network Vulnerability Assessment	MCOTEA	JITC
	JNTC Horizontal Two Exercise	MCOTEA	AFOTEC, ATEC

CENTCOM	Central Command
EUCOM	European Command
JFCOM	Joint Forces Command
NORTHCOM	Northern Command
PACOM	Pacific Command
SOUTHCOM	Southern Command
SOCOM	Special Operations Command
STRATCOM	U.S. Strategic Command
TRANSCOM	U.S. Transportation Command

JITC	Joint Interoperability Test Command
AFOTEC	Air Force Operational Test and Evaluation Center
ATEC	Army Test and Evaluation Command
MCOTEA	Marine Corps Operational Test and Evaluation Agency
OPTEVFOR	Operational Test and Evaluation Force

FY05 GOALS AND PLANNED ASSESSMENT ACTIVITIES

FY05 funding for this initiative is programmed at $23M. Assessment plans for FY05 include 15 exercises with active Blue, Green, and Red Teams (full assessment support), and 13 additional exercises with lesser efforts (see Table 2). Based on current projections and planned levels of effort, this funding level appears to be adequate for FY05. However, the

response from exercise authorities continues to be very positive, and additional resources may be required to provide the full assessment support to more than twenty exercises.

In a merger of acquisition and exercise support, the Navy's Operational Test and Evaluation Force will examine several acquisition programs (e.g., Deployable Joint Command and Control IOT&E, Navy Marine Corps Internet FOT&E) during COCOM exercises. We are optimistic that many training and test objectives can be simultaneously satisfied during combined events, and that the efficiencies provided to the Department are potentially significant.

Planned Information Assurance and Interoperability Exercise Events for FY05

COCOM	Exercise	OTA Lead	OTA Support
CENTCOM	Internal Look 05	ATEC	
	United Endeavor 05	ATEC	
EUCOM	Flexible Leader 05	ATEC	OPTEVFOR
	Sharp Focus 05	ATEC	JITC, AFOTEC
JFCOM	United Endeavor 05	OPTEVFOR	JITC, ATEC
	JTF Exercise 05	JITC	OPTEVFOR
NORTHCOM	United Defense 05	ATEC	JITC, MCOTEA
	Northern Edge 05	AFOTEC	JITC
	Joint Warrior Interoperability Demonstration 05	JITC	ATEC
PACOM	Terminal Fury 05	OPTEVFOR	JITC, ATEC
	RSOI 05 (PACOM HQ)	OPTEVFOR	ATEC, AFOTEC
	RSOI 05 (U.S. Forces Korea)	OPTEVFOR	ATEC
	Ulchi Focus Lens 05	OPTEVFOR	ATEC
	Talisman Sabre 05	OPTEVFOR	
	Cobra Gold 05	OPTEVFOR	
SOUTHCOM	Fuertas Defensas 05	ATEC	JITC, MCOTEA
SOCOM	TBD	JITC	
STRATCOM	Global Guardian/Lightning 05	JITC	AFOTEC
	Global Archer 05	JITC	ATEC
TRANSCOM	Turbo Challenge 05	JITC	AFOTEC
Joint / Service	JNTC Exercise 05-01	MCOTEA	AFOTEC, ATEC
	Asynchronous Warfare Initiative (AWI)	OPTEVFOR	JITC
	Marine Expeditionary Force Exercise 05-01	MCOTEA	
	HMX-1 Network Vulnerability Assessment	MCOTEA	JITC
	Positive Force	JITC	ATEC
	JNTC Exercise 05-02	MCOTEA	AFOTEC, ATEC
	Keen Sword	COTF	ATEC
	Roving Sands	JITC	AFOTEC
	Marine Expeditionary Force Exercise 05-02	MCOTEA	

ASSESSMENT

DOT&E is developing a database to capture baseline performance data for events assessed to date. These data will be aggregated to support trend analyses for recurring events and across like events in the future. Emerging trends across FY04 events for which data is available include the following:

- Vulnerabilities have been found by every Blue and Red Team associated with this initiative.
- Most problems found are basic (e.g., unprotected servers and open ports, Intrusion Detection Systems not installed or improperly configured, etc.) and easily remedied by trained system administrators.
- There is unfounded trust that certain networks are inherently secure and remote monitoring is always effective. These combine to reduce vigilance by local operators, and set the stage for penetrations to go undetected.
- Corrective-action management is sometimes lacking; some identified problems are not being fixed, and some that have been fixed get reintroduced when backup or update disks are loaded.
- Tactics, techniques, and procedures for detect, react, and restore missions are generally immature and/or not well understood by operators.
- Responsiveness to solving problems found in networks during operational exercises, or when focused follow-up is provided, is excellent.

These results have been shared both with the exercise authorities and with our initiative partners in the Joint Staff and the Defense IA Program in ASD(NII). Our partners are becoming more closely aligned with this initiative and exploring new ways to use the available results and influence focus areas for future events. They are also employing these results to support further activities and investments to improve DoD IA and interoperability postures.

Exercise authorities have demonstrated strong interest in applying remedies for identified vulnerabilities. We have observed significant improvements in IA posture between Blue and Red Team events for those exercises that have agreed to incorporate the full assessment cycle. We attribute this in part to the increased IA awareness among exercise participants that a full assessment brings to the exercise planning, but also to the increased command emphasis that is generally associated with the decision to have a full assessment. We also believe the focused Green Team and the synergy across all of the teams improves the likelihood that identified problems will be fixed, and repeat observations of the same problem will be minimized.

Although data at this time are limited, we are beginning to see trends for this initiative as portrayed by Figure 1. This chart plots IA Protect Posture as a function of the assessment level; IA Protect Posture is equated to the threat tier that our assessment teams determine a given set of exercise players could defend against. Threat tiers are defined as follows:

- Tier 1 = Basic level comprised of amateur hackers with no real agenda and limited resources
- Tier 2 = Medium level comprised of skilled hackers with an agenda, some resources, and possible sponsorship that includes intelligence support
- Tier 3 = High level comprised of experts with resources associated with nation state sponsorship

The first two assessment levels are based on observations from FY04 exercises, and can be explained as follows: those exercise authorities who agree to be subjected to Blue (and sometimes Red) Teams will more actively prepare their defenses, and as a result will be better able to protect their networks. The third assessment level is an extrapolation, but based on the data that show every Blue Team finds a vulnerability that could be exploited by a Tier 1 threat. And if there is no Red Team planned for the upcoming exercise, there may be little motivation to ready network defenses. These data indicate there is a strong correlation between IA Protect Posture and level of preparation, which is itself correlated to willingness to submit to Red Team attack.

In addition to Protect Posture, all of the OTA teams have also begun collecting data on Detect, React, and Restore Postures. Results for all of these IA mission domains will be addressed in my FY05 Annual Report.

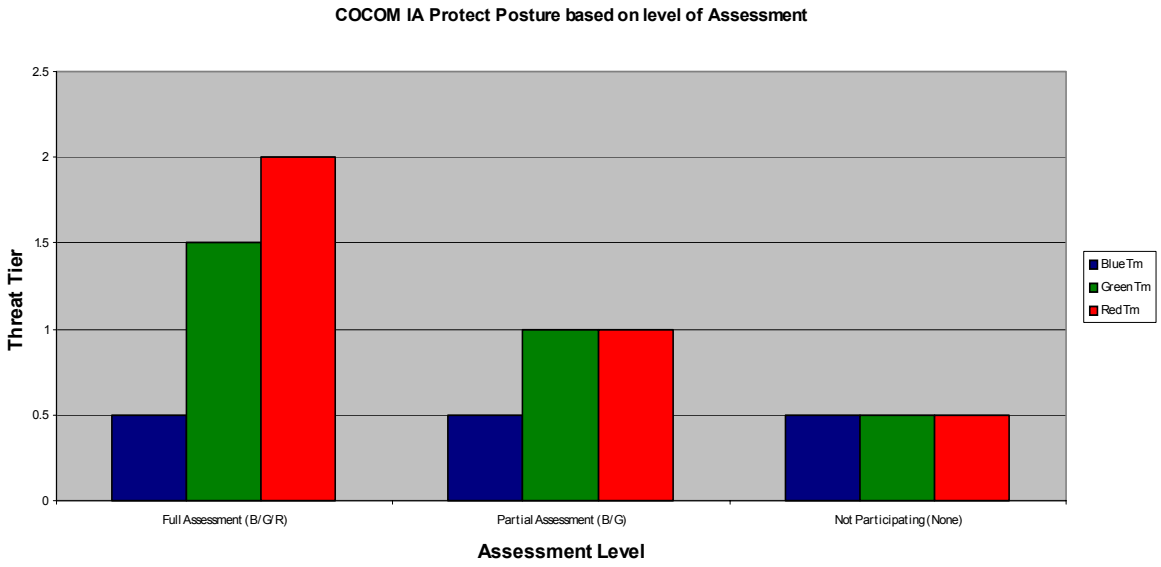

FIGURE 1

CONCLUSION AND RECOMMENDATION

There are many ongoing activities focused on improving DoD's IA and interoperability posture, and in the aggregate they are having positive effect. The OTA-led effort described in the preceding pages has already assisted in integrating and finding synergy among these efforts. Still, more must be done to deliver and maintain systems that are interoperable and information assured. The push to field emerging capabilities and commercial technologies, combined with the rapidly growing IO threat, will be a constant source of friction with the Department's information superiority goals, but one that can be best met with the fully engaged organizations involved in this effort.

The Department should continue to synchronize its many activities and leverage the results of the operational evaluations provided by this assessment initiative. Furthermore, in conjunction with other training objectives, IA should become an exercise objective (i.e., realistic Red Teaming should be present) wherever information is critical to mission accomplishment. Finally, we should accept that threat penetrations may occur when and where we least expect them; as such, more effort must be placed in preparing to detect, react, and restore critical services in the face of a successful attack. As previously discussed, this initiative is prepared to assess the ability of exercise participants in each of these domains.