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

Summary

- DoD is improving its Information Assurance (IA) and Interoperability (IOP) postures, but the information operations threat continues to increase in capability and in ability to rapidly exploit new vulnerabilities.
- Operational assessments of IA/IOP 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, Green, and Red teaming provides the most comprehensive assessments and the greatest opportunity to improve IA and IOP postures.
- Many of the vulnerabilities found to date are basic problems with readily available solutions; however, some will require more extensive enterprise solutions.
- Exercise authorities appreciate and desire more OT&E expertise during their exercise planning, execution, and assessment phases. There has been more senior-leadership emphasis on IA during selected exercises this fiscal year, resulting in improved IA performance.
- Assessments and remediation efforts in support of units deploying to Iraq and Afghanistan were tailored and conducted during four exercises this fiscal year; three such assessments are planned for FY06.
- 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 IOP evaluations during major exercises. The bill directed the Service Operational Test Agencies (OTAs), the Service Information Warfare Centers, and the National Security Agency (NSA) to assist in the planning, conduct, and evaluations of these exercises. DOT&E oversees these efforts and provides annual updates on DoD's progress based on results of the exercise evaluations and acquisition OT&E.

The bulk of the FY05 IA/IOP funds were distributed to the OTAs, who in turn assembled teams with the proper expertise to perform IA and IOP assessments before and during exercises. These teams plan, execute, collect data, analyze, and report the results of all activities associated with IA and IOP assessments. Primary execution elements include:

- Blue Teams -- Perform network scans and surveys of network personnel and policy
- Green Teams -- Assist the exercise authority in understanding the nature, priority, and remedial activities needed for identified vulnerabilities; provide remediation support and training, where appropriate
- Red Teams -- Design a comprehensive Red Team scenario overlaid on an exercise scenario to examine the performance of operational networks and operators when subjected to information operations attacks

The following improvements were made this fiscal year to the planning, assessment, and reporting methodology:

- Plan Red Team events that provide multi-echelon stress with multi-level threats to enhance the warfighter's appreciation for the rapidly evolving threat, and solidify their training and abilities in all aspects of the "protect, detect, react, and restore" missions.
- Design IOP assessment plans in coordination with the Joint Interoperability Test Command (JITC).
- 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. Interoperability certification reviews may also occur during the Blue Team phase.
- Provide Green Team assistance after both Blue and Red Team events.
- Coordinate external support for solutions beyond the organic capabilities of the exercise authority and assist in the identification of sources for any needed training.

FY05 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 Systems Agency (DISA). Accomplishments by the OT&E community and our partners include the following:

- Performed full Blue/Green/Red Team assessments for 15 exercises (see Table 1).
- Performed Blue/Green Team assessments for eight additional exercises.
- Observed and assisted in exercises that have future assessment opportunity.
- Performed four assessments for units preparing to deploy to Iraq and Afghanistan.
- Developed IA and IOP 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.

Table 1 - Information Assurance and Interoperability Exercise Events in FY05

Exercise Authority	Exercise	OTA Lead	OTA Support
CENTCOM	No Exercises this FY	N/A	N/A
EUCOM	Lion Challenge 05	ATEC	N/A
	Flexible Leader 05	ATEC	JITC, AFOTEC
JFCOM	Joint Task Force Exercise 05	JITC	N/A
	Unified Endeavor 05-01*, 05-02*, and 05-03*	ATEC	JITC, MCOTEA
	Roving Sands/Joint Red Flag 05	JITC	N/A
	Coalition Warrior Interoperability Demo 05	JITC	MCOTEA
NORTHCOM	Unified Defense 05	ATEC	JITC, MCOTEA
	Ardent Sentry 05	ATEC	N/A
	Northern Edge/Alaska Shield 05	AFOTEC	JITC
PACOM	Terminal Fury 05	OPTEVFOR	JITC, ATEC, AFOTEC
	Reception, Staging, Onward Movement, and Integration (U.S. Forces, Korea) 05	OPTEVFOR	JITC, ATEC, AFOTEC
	Ulchi Focus Lens 05	OPTEVFOR	JITC, ATEC
SOUTHCOM	Joint Task Force - Bravo 05	ATEC	JITC, MCOTEA
	Fuertas Defensas 05	ATEC	N/A
	Ellipse Echo 05	ATEC	N/A
SOCOM	No Exercises this FY	N/A	N/A
STRATCOM	Global Guardian/Lightning 05	JITC	AFOTEC
TRANSCOM	Turbo Challenge 05	JITC	AFOTEC
Joint / Service	Joint National Training HMX	MCOTEA	N/A
	Marine Expeditionary Force Exercise 05*	MCOTEA	N/A
	Urgent Victory 05	ATEC	JITC
RDT&E	Army Battle Command System Research, Development, Test, and Evaluation (RDT&E)	ATEC	N/A
	Deployable Joint Command and Control RDT&E	ATEC	N/A

*Denotes Mission Rehearsal Exercise (MRX) event for deploying unit

CENTCOM	Central Command
EUCOM	European Command
JFCOM	Joint Forces Command
NORTHCOM	Northern Command
PACOM	Pacific Command
SOUTHCOM	Southern Command
SOCOM	Special Operations Command
STRATCOM	Strategic Command
TRANSCOM	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 Activity
OPTEVFOR	Operational Test and Evaluation Force

- Coordinated with acquisition elements in the OT&E community to share best practices, metrics, and lessons learned from COCOM and Service exercises.
- Initiated a Capability Improvement Integration Team with Joint Forces Command to identify critical mission thread information that will support both IA and IOP assessment planning. This team will also focus on identified shortfalls and lead efforts to determine appropriate solutions.
- Initiated a Coordination and Solutions Team to perform trend analyses and ensure that solutions and lessons learned in one theater are shared across other theaters, and with appropriate DoD sponsors.
- Continued efforts to identify the 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 the resources required in support of assessment activities. They are also developing new tools and methods to stress the exercise participants. DIA continues to provide critical support to this initiative via the Joint Information Operations (IO) Threat Working Group, and provides a comprehensive IO Capstone Threat Assessment update every six months. This assessment is essential to proper portrayal of the IO threat, not only for the exercises associated with this effort, but 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 FY05 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 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 FY06. In a merger of acquisition testing and exercise support, several acquisition programs (e.g., Deployable Joint Command and Control IOT&E, and Army Battle Command Systems) were evaluated during COCOM exercises.

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, while maintaining compatibility with DoD policies for IA and IOP.

In May 2005, the Chairman of the Joint Chiefs released a message outlining immediate and long-term efforts to enable sustained, operationally ready networks. The Commander, Joint Forces Command (JFCOM) was directed to establish IA training objectives for at least half of the FY06 JFCOM-supported exercises. Commander, JFCOM was further directed to expand IA as a training objective into all JFCOM-supported exercises in FY07.

Table 2 – Planned Information Assurance and Interoperability Exercise Events for FY06

Exercise Authority	Exercise	OTA Lead	OTA Support
CENTCOM	Internal Look 07 Planning	ATEC	N/A
EUCOM	Flexible Response 06	ATEC	AFOTEC, MCOTEA
	Austere Challenge 06	ATEC	N/A
JFCOM	Unified Endeavor 06-01* and 06-02*	ATEC	JITC, MCOTEA
	Coalition Warrior Interoperability Demo 06	JITC	MCOTEA, OPTEVFOR
NORTHCOM	Ardent Sentry 06	AFOTEC	N/A
	Vigilant Shield 06	AFOTEC	JITC
PACOM	Terminal Fury 06	OPTEVFOR	JITC, ATEC, AFOTEC, MCOTEA
	RSOI 06 (U.S. Forces, Korea)	OPTEVFOR	JITC, ATEC, AFOTEC
	Ulchi Focus Lens 06	OPTEVFOR	ATEC
SOUTHCOM	Fuertas Defensas 06	ATEC	N/A
	Blue Advance 06	ATEC	N/A
SOCOM	TBD	MCOTEA	N/A
STRATCOM	Global Shield/Lightning 06	JITC	AFOTEC, MCOTEA
	Global Thunder 06	JITC	AFOTEC, MCOTEA, OPTEVFOR
TRANSCOM	Turbo Distribution 06	JITC	AFOTEC, MCOTEA
Joint / Service	Marine Expeditionary Force Exercise 06*	MCOTEA	Joint Multi-Disciplinary Vulnerability Assessment
	Bullwark Defender 06	JITC	ATEC, AFOTEC, MCOTEA, OPTEVFOR
	I Corps Exercise	ATEC	N/A
	Federation of Systems Exercise 06	MCOTEA	JITC
	Joint Task Force Exercise - 2	OPTEVFOR	N/A

*Pre-deployment assessment events planned for FY06

FY06 Goals and Planned Assessment Activities

Assessment plans for FY06 include 15 exercises with active Blue, Green, and Red Teams (full assessment support), and six additional exercises with lesser efforts (see Table 2). Based on current projections and planned levels of effort, funding appears adequate for FY06. However, the response from COCOM and Service exercise authorities continues to be very positive, and additional resources may be required to provide the full assessment support to more than 15 exercises. In particular, assessment and remediation support to units preparing to deploy to Iraq/Afghanistan has been very well received, and three of these assessment events are planned for FY06 (these events are designated with an asterick in Table 2).

Interoperability problems will usually be observed during exercises via failures to achieve critical mission requirements. The assessment team will seldom have instrumentation in place to capture system performance data so the exact cause of a problem may not be known. In FY06, we plan to develop a process with JFCOM and JITC for follow-up events to identify specific causes of interoperability problems identified during exercises.

Acquisition program support will continue to expand during FY06, and will include planning for an IA assessment during an upcoming Missile Defense Agency (MDA) wargame covering several MDA acquisition programs. We are optimistic that many training and test objectives can be simultaneously satisfied during combined events, and believe that the efficiencies and cost savings to the Department will be significant.

Assessment

High-level trends across FY05 events 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 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.

Specific trends in more detailed assessment areas include the following:

- **Personnel and Training** - A common standard for network manning, reflecting the complexity or operational criticality of the networks, does not exist. Many personnel working IA tasks are not designated as IA personnel, and as a result do not receive necessary training or achieve skill standards appropriate for their duties. DoD is revising IA training standards to address many of these issues.
- **Configuration Management** – Standards are inconsistently followed, and often too complex for local personnel to achieve. Poor configuration management results in undesirable network variance, making the detection of unauthorized modifications or access difficult. DoD has programmed additional development to an enterprise network scanning and remediation suite to address these shortfalls.
- **Continuity of Operations Plans (COOP) or Recovery Plans** – Many commands lack effective incident response guidelines, and seldom exercise COOP plans. Existing response and continuity plans are being rapidly overtaken by new technology options, such as Voice-over-Internet Protocol (IP), online IP-based chat, and intercom channels. These and other technologies provide popular services that leave few alternative options in their absence. The Joint Task Force for Global Network Operations is developing a template for these plans.
- **Firewalls and Intrusion Detection Systems (IDS)** - Many units have no firewalls and no IDS in place, particularly on classified networks. Where firewalls and IDS are employed, host-based and internal firewalls and IDS capabilities are more effective than those provided at only enterprise boundaries or by higher echelon.
- **Information Assurance Vulnerability Advisory (IAVA) Compliance** - Many systems are not compliant with IAVAs, and some cannot be brought into compliance due to incompatibility with recommended patches. Units have little or no control over Program of Record software, which must be patched by the program manager. Within the U.S. Army Battle Command System, steps have been taken to more rapidly test and field new patches and protections. Additionally, DoD has purchased enterprise licenses for certain software tools to identify and remediate IAVA shortfalls locally.
- **Organizational Roles and Responsibilities** - Many organizations rely on higher echelons to perform critical network management tasks. The lack of local responsibility causes reduced awareness of and attention to critical IA practices. It also results in reduced ability to locally protect networks from attack and perform proper detection, reaction, and restoration actions in the face of an attack.

- **Physical Security** - Exercise opposition forces routinely demonstrate the ability to penetrate badging and gate/door security. Sensitive information that facilitates both physical and electronic penetration is often found in unguarded trash. Additionally, computer screen locks and time outs are inconsistently applied, allowing intruders access to logged-on systems.

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 the office of the Assistant Secretary of Defense (Network Information and Integration). 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. The Coordination and Solutions Team (CST) at DOT&E has established a method for harvesting information concerning critical vulnerabilities and shortfalls. It is intended that COCOM-specific vulnerabilities and shortfalls will be reviewed by the COCOM at least bi-monthly, supported by the CST efforts to obtain outside agency assistance. The CST has additionally provided briefings and other information via the Joint Staff to the senior leadership on interoperability issues, with the intent of establishing a "clearing house" for remediation similar to that which exists via the Enterprise Solutions Steering Group for IA vulnerabilities.

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 reduced.

The U.S. Strategic Command subordinate command, the Joint Information Operations Command (JIOC), and the Marine Corps collaborated on the conduct of the first Joint Multi-Disciplinary Vulnerability Assessment. This effort expands the assessment previously planned for 1st Marine Expeditionary Force to include other elements, such as radio frequency and telephone monitoring. DOT&E, in partnership with NSA and other DoD entities, will continue to work closely with the JIOC to help shape this initiative in a fashion that will not duplicate or obviate other efforts that are already executing successfully.

Although a variety of methods for managing vulnerabilities and shortfalls exists within DoD, DOT&E has instituted the use of a Vulnerability and Shortfall Matrix. This matrix identifies the vulnerability or interoperability shortfall, proposes a remedy, and includes a statement of the operational impact if remedies are not applied. The matrix is updated following every Blue, Green, or Red Team assessment to reflect the current state of observed vulnerabilities and shortfalls. This tool is used to monitor correction of vulnerabilities and shortfalls, support trend analyses across theaters, and assist in the identification of issues to be reviewed or validated in subsequent events. Several COCOMs have chosen to employ this matrix as their own tracking tool.

Conclusion and Recommendation

There are many ongoing activities focused on improving DoD's IA and IOP posture, and in the aggregate they are having a positive effect. The efforts described in the preceding pages have already assisted in integrating and finding synergy among these efforts, resulting in improved IA postures and awareness wherever the full cycle of Blue-Green-Red Teaming is performed. The assessments enable rapid identification of vulnerabilities and interoperability/training shortfalls, and frequently result in immediate correction of identified problems. DoD has refocused and charged several senior review groups to receive assessment information produced by this initiative, prioritize issues for correction, and identify appropriate agencies to address those solutions for all of DoD.

The Department should continue to synchronize its many activities and leverage the results of the operational evaluations provided by this assessment initiative. In last year's report, we recommended that IA should become an exercise objective (i.e., realistic Red Teaming should be present) wherever information is critical to mission accomplishment. The Chairman of the Joint Chiefs' message in May 2005, to the Commander, Joint Forces Command is a step in the right direction, but should be expanded to include all COCOMs. In recognition of the continued success by Red Teams, we believe that every major exercise should have IA as a critical operational training objective. Consistent with other training objectives, Red Teams should be permitted to conduct threat representative activities, and exercise participants should have mature continuity of operations plans and be prepated to execute them.

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.