Information Assurance and Interoperability Evaluations During Combatant Command and Service Exercises

The FY03 Appropriations bill directed that the Combatant Commands (COCOMs) and Services conduct operationally realistic information assurance (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) to assist in the planning, conduct, and evaluations of these exercises. DOT&E's responsibility consists of providing annual updates on DoD's progress based on results of the exercise evaluations and acquisition. The FY03 bill provided DOT&E $7.6M to initiate this effort and DoD was directed to fund this effort in future budget submissions.

DOT&E's initial steps have been focused on identifying exercise opportunities (see table), joining with those who plan and execute these exercises, and working to enhance the operational realism and relevance of Red Team events during planned exercises. These activities will set the stage for both the IA and interoperability evaluations in the future.

Although this is the initial year of this effort, there are many positive comments. This effort has been well received across DoD. Soon after the FY03 Appropriations bill was finalized, DOT&E partnered to implement this language with the Joint Staff and the Assistant Secretary of Defense for Command, Control, and Communications (now Network Integration and Information). Each of these offices issued a memorandum to respective communities soliciting full support for this initiative. Three workshops have been held to identify exercise opportunities, develop concepts of operations, and form teams to plan and execute the evaluations. Each workshop was well attended by representatives from the COCOMs and other organizations identified in the language of the bill.

With all of these activities and communications, there has been a perceptible increase in the awareness of IA issues by senior leaders, including significant interest in conducting more realistic evaluations in the exercise environment. Furthermore, the OTAs are reporting that their involvement in this effort is enhancing the support of acquisition programs.

There are many ongoing efforts that are individually focused for the improvement or examination of some portion of DoD's IA posture. NSA's extensive Blue and Red Team Programs are very active with most of the COCOMs; Blue Team events are detailed vulnerability assessments performed generally in an administrative environment and in advance of an exercise, while Red Team events are overlaid on exercises to examine the performance of operational networks when subjected to information operations attacks. The relationships between NSA teams and the COCOMs have proven extremely beneficial to this initiative and will be instrumental to future efforts and IA improvements.

The Service Information Warfare Centers also have active Blue and Red Teams. These teams focus on tactical and operational events and systems, and support Service exercises and other operations. Their expertise complements that of the NSA, and there are frequent events where NSA and Service teams partner to leverage each other's capabilities and share best practices. There are existing databases of vulnerability assessment results that have been collected by NSA and the Defense Information Systems Agency. These databases are undergoing review for relevant lessons learned and metrics to help establish the current IA performance baseline.

The Service OTAs and the Joint Interoperability Test Command (JITC) routinely perform IA and interoperability evaluations on acquisition programs in accordance with DOT&E policy. Both are well acquainted with the operational challenges and rapidly evolving threats. Their efforts are instrumental in raising the IA posture and interoperability of fielded systems (to a limited extent, they examine significant upgrades to fielded systems).

In this fiscal year, teams led by the OTAs have postured for improved Red Teaming via the following activities:

- Observation of exercises that have (or offer future opportunity for) Red Teaming.
- Development of IA and interoperability metrics that are observable in the exercise environment, meaningful to the warfighter, and suitable for performing baseline assessments and trend analyses.
- Development of an evaluation plan template and an exercise planning checklist to bring appropriate levels of analytical rigor to exercises.

- Participation in FY04 exercise conferences to improve the synchronization and relevance of Red Teaming with the exercise objectives.

In FY04, the OTAs will assemble teams with the proper expertise to plan, execute, collect data, analyze, and report the results of exercises. They will endeavor to optimize the realism of the Red Team events, the utility of the evaluation and feedback, and the overall benefits to the warfighter for a given exercise cycle. The following is a sample of the OTA cycle:

- Actively participate in all exercise planning conferences beginning with the Concept Development Conference. Early involvement by the OTA teams will result in greater likelihood that the exercise scenario will be synchronized with realistic Red Team events and given access to data collection.
- Conduct an administrative Blue Team evaluation approximately six months prior to the exercise, providing feedback to the exercise authority for remedial actions in advance of the exercise; special focus will be paid to ensure prior issues have been resolved.
- Assist the exercise authority in acquiring any needed training.
- Design a comprehensive Red Team scenario that provides multi-echelon stress with multilevel threats across the spectrum of information operations; this approach will improve the warfighter's appreciation for the rapidly evolving threat and solidify their training and capabilities in all aspects of "protect, detect, and react."
- Execute the Red Team events safely, legally, and consistent with the exercise objectives.
- Capture relevant IA and interoperability data, analyze results, and develop a baseline to support future trend analyses.
- Provide quick-look feedback to the exercise authority and participants, and support after-action reviews.
- Identify problems that require external solutions and provide appropriate results to developers and sponsors who will construct solutions and prioritize efforts.
- Update databases, compare performances with rolling baseline, and perform trend analysis. All results will be provided to DOT&E.
- Participate in the NSA Vulnerability Trends Forum. This forum brings together those organizations involved in vulnerability assessments and system research and development, and fosters sharing of the latest assessment results, vulnerability concerns, and IA products.
- Begin the cycle again

The NSA and the Service Information Warfare Centers have been actively developing a training and certification program to support the above activities and the expansion of required resources. Their efforts will support the planning process and the selection and introduction of the appropriate Red Team threat into all facets of the exercise. The Defense Intelligence Agency has also been very supportive of this effort by standing up the Joint Information Operations (IO) Threat Working Group and committing to providing a comprehensive IO Threat Capabilities Assessment update every six months. This assessment will be critical 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.

The OTA teams received a bulk of the funding provided in FY03, as they will every year. The OTAs are expected to assemble the appropriate teams and contract out for those capabilities that they do not have in-house (e.g., Red Teams). DoD programmed $156M for continuation of this effort through FY09, with $18M planned for FY04. Based on current projections and planned levels of effort, these funding levels appear to be adequate. However, the response from exercise authorities has been positive, and additional resources may be required to provide the full support outlined above to more than 20 exercises. The plans for FY04 include four exercises with active Blue and Red Teams and associated support, and 18 additional exercises with lesser efforts. These exercises are identified in the table, as are the lead OTAs and supporting OTAs. Most of these exercises are expected to have full Blue and Red Team events in FY05.

Information Assurance and Interoperability Exercise Events FY04			
COCOM	**Exercise**	**OTA Lead**	**OTA Support**
CENTCOM	Internal Look 05 Prep	ATEC	N/A
EUCOM	Agile Response 04	ATEC	OPTEVFOR
	Austere Challenge 04	ATEC	JITC, AFOTEC
JFCOM	United Endeavor 04 (JNTC)	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	OPTEVFOR	ATEC
	Cobra Gold	OPTEVFOR	
SOUTHCOM	Fuertas Defensas 04	ATEC	JITC, MCOTEA
SOCOM	TBD	JITC	N/A
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 04	MCOTEA	AFOTEC, ATEC
	Asynchronous Warfare Initiative (AWI)	OPTEVFOR	JITC
	Marine Expeditionary Force Exercise 04	MCOTEA	N/A

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
JNTC	Joint National Training Capability
ATEC	Army Test and Evaluation Command
MCOTEA	Marine Corps Operational Test and Evaluation Agency
OPTEVFOR	Operational Test and Evaluation Force

The Army and Navy OTAs have been extensively involved in the planning effort for U.S. European Command's "Agile Response 04 (AR04)" and U.S. Pacific Command's "Terminal Fury 04 (TF04)." The lessons learned from these two exercises will set precedents for future exercises, and inform the efforts of other teams. The first to execute will be TF04 in December 2003. TF04 is an annual Pacific Command exercise focused on both headquarters and deployed forces. The primary objective in TF04 will be the integration of the Standing Joint Force Headquarters into the operational scenario. IA events have been planned to support and integrate with the exercise scenario, support the exercise objectives, and permit assessment and analysis of the PACOM network security. The next exercise will be AR04, which will provide

both training and operational rehearsal to EUCOM and NATO forces preparing for contingency support to the Athens Olympics. Integration of the Standing Joint Force Headquarters is also a major goal of this exercise, and IA events have been planned and coordinated to support the scenario. Final planning for this exercise will take place by the end of 2003, and the exercise will execute in March 04.

DOT&E has increased the focus on IA as an evaluation issue for systems on the OT&E oversight list. The DOT&E policy for IA evaluations that was implemented in 1999 remains in effect. A dozen programs were identified in FY03 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 OTA's 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 FY04. In addition, DOT&E IA policy is being revised to reflect the latest information in IA practices and metrics and will also address the evaluation of legacy systems during COCOM and Service exercises.

There are many ongoing activities focused on improving DoD's IA and interoperability posture. The OTA-led effort described in the preceding pages will assist 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.