Information Assurance (IA) and Interoperability (IOP)

In FY10, the assessing organizations performed IA and IOP assessments during 21 Combatant Command (COCOM) and Service exercises; eight assessments involved units preparing to deploy – or already deployed – to Iraq or Afghanistan.

The IA posture observed during FY10 exercise assessments is not sufficient to prevent an advanced adversary from adversely affecting the missions that were being exercised. Improvements in certain areas of network defense were observed, but Red Teams generally overcame defenses during exercises by increasing their level of effort. The cyber threat portrayed during assessed exercises was consistently below that expected from a nation-state. The level of cyber-threat portrayal in future exercises is expected to increase significantly in response to a memorandum signed by the Chairman, Joint Chiefs of Staff in September 2010. This memorandum augments Secretary of Defense Guidance to the Development of the Force, which stated "All DoD Components shall reduce the risk of degraded or failed missions by regularly exercising the capability to fight through cyber or kinetic attacks that degrade the Global Information Grid."

The FY10 IOP assessments found that interoperability issues encountered by the training audience typically hindered, rather than prevented, mission accomplishment; this is due primarily to operators who developed and executed workarounds. Even though missions were generally accomplished, the workarounds usually increased operator workload, and often resulted in degraded efficiency of completing tasks.

In FY11 DOT&E will continue to emphasize and report results of improved portrayal of cyber threats, assessment of operational impact from cyber activity and interoperability shortfalls, and utility of extending assessment opportunities to times outside of exercise execution periods.

PARTNERSHIPS AND COORDINATION

DOT&E remained partnered with the Joint Staff and Assistant Secretary of Defense for Networks, Information, and Integration (ASD (NII)) in the oversight and coordination of the Information Assurance and Interoperability Assessment Program.

DOT&E continued the partnership with the Joint Forces Command (JFCOM) Joint System Integration and Interoperability Laboratory that is intended to enhance assessments conducted by both organizations during training exercises through coordinated sharing of information and expertise. The partnership was involved in three FY10 assessment venues (Austere Challenge, Terminal Fury, and Angel Thunder).

DOT&E has coordinated closely with the intelligence community, National Security Agency, and the Service information warfare centers to improve the characterization of the representative cyber threat and its portrayal during exercises. The Defense Intelligence Agency (DIA) has made significant progress in the definition of advanced and emerging methods of cyber attack. DIA assessments will be instrumental in the identification of the Red Team assets needed to portray the cyber threats used in all exercises where IA assessments will be performed. DOT&E also coordinated with the JFCOM Opposing Force cell to achieve more realistic cyber play during the numerous COCOM exercises they support each fiscal year.

A Memorandum of Understanding with U.S. Cyber Command is also in final staffing that will create a Cyber Assessment Synchronization Working Group. This group is working to synchronize planning, execution, and reporting activities among exercises. Enhanced training and certification for Blue and Red Teams will contribute to more threat-representative cyber play and assessments, as will a newly created Cyber Command exercise support cell.

DOT&E has initiated a partnership with the Naval Postgraduate School to improve and expand the capabilities of network test tools and analysis methods. This partnership includes the design and development of network test tools, instrumentation, and methods; analysis of compliance and performance findings to postulate cause/effect models for use in simulation; and mapping of direct operational effects arising from network performance issues.

Additionally, DOT&E has partnered with the Defense Information Systems Agency to improve and expand the level of assistance available to assessed organizations. This partnership will focus on improved training resources, community feedback, and operator training tools to help remediate vulnerabilities and shortfalls identified during assessments.

FY10 ASSESSMENT ACTIVITIES

In FY10, Information Assurance (IA) and Interoperability (IOP) assessments were performed during 13 COCOM and eight Service exercises. There were also three sets of assessments performed during current operations, with two sets performed in the CENTCOM theater. Six of the Service assessments involved units preparing to deploy to Iraq or Afghanistan (see Table 1).

DOT&E continued the practice of providing formal memoranda of specific system/process findings to cognizant Service and Agency senior leadership. Finding Memoranda detail specific IA and IOP issues identified during assessments that have the potential to significantly degrade operations and either warrant immediate or long-term response. Findings may include system-to-system issues, process/procedure issues, or cross-DoD issues (such as universal use of commercial products).

DOT&E published four Finding Memoranda in FY10 regarding:

- Use of Microsoft Active Directory in DoD
- Use of joint cyber intelligence fusion practices
- Need for additional configuration guidance for certain commercial products
- Interoperability issues with aviation readiness systems

DOT&E is currently preparing an additional seven Finding Memoranda based on assessment conducted during FY10 that address the following issues:

- System upgrade incompatibilities
- Centralized network management
- Allied system interoperability
- Joint system interoperability
- Use of commercial softwares within DoD

ASSESSMENT

Interoperability

The FY10 IOP assessments found that interoperability issues encountered by the training audience typically hindered, rather than prevented, mission accomplishment; this is due primarily to operators who developed and executed effective workarounds. Even though missions were generally accomplished, the workarounds usually increased operator workload, and often resulted in degraded efficiency of completing tasks.

Of the eleven Finding Memoranda prepared based on assessments performed in FY10, four are related to interoperability findings, including system-to-system exchanges between DoD software, as well as ally-to-ally exchanges between coalition partners. In each case, staffing with the cognizant program offices indicates that these issues are being addressed with priority.

Overall, the FY10 interoperability findings may be categorized in three general areas:

1. IOP problems with coalition partners due to system incompatibility that prevented automated information exchanges.
2. IOP problems due to the existence of multiple systems with similar functionality; the increased number of interfaces adds complexity, and causes a higher likelihood of information exchange problems.
3. IOP problems due to personnel who lack adequate training to effectively operate critical information technology.

Information Assurance

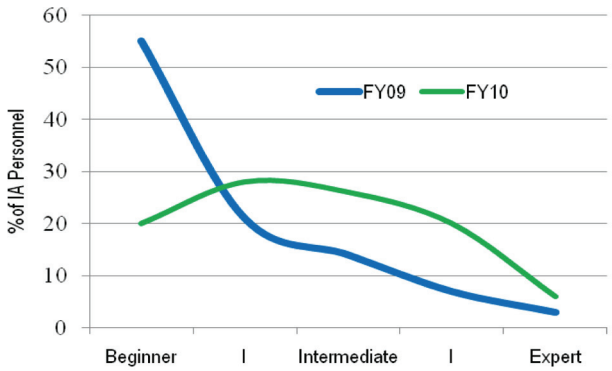
Information assurance assessments continued to highlight the relationships between cyber security and other areas such as physical security and operations security. Despite the finding that overall physical preparation and safeguards have improved over the last 3-5 years, the assessments found that a compromise in any one of these areas generally results in compromises in the other areas.

The assessments confirmed improvements in the ability to protect networks from penetration. All Red Teams reported increasing difficulty in penetrating network defenses, but results show that with sufficient time, Red Teams typically managed to penetrate networks and systems. In several cases, Red Teams were successfully blocked from employing certain attacks due to specific preparations or precautions on the part of network defenders. While this rarely resulted in complete denial of Red Team intrusion attempts, it did increase the level of difficulty for the Red Teams.

The ability of network defenders to detect and react to intrusions remained poor. There has been some preliminary evidence of increased detections noted since the roll-out of the enterprise Host-Based Security System.

Compliance measures and scanning results indicated improvement since FY09, and over the longer period of FY05-FY10, in areas including enclave boundary protection, continuity of operations, incident management, and personnel training. Patch management and policies for wireless devices remain areas of concern where improvement has been modest. Experience levels and formal training levels for network defenders have increased. As shown in Figure 1, the aggregate skill levels of network personnel assessed in several FY09 and FY10 venues indicate an increase in "intermediate" and "expert" skills across the Department and fewer "beginner" level operators.

Figure 1: Skill levels of IA personnel in FY09 and FY10



Assessments have documented a steady improvement in the following areas:

- Compliance testing and system auditing
- Host-based intrusion detection systems
- Processes for network access
- Vulnerability management practices
- Incident response activities

Implementation of the Federal Desktop Standard for DoD computers has increased uniformity and simplified configuration of these assets.

Exercise authorities in several COCOMs have supported greater cyber-threat play in scenarios, and having Red Teams work more closely with the exercise opposition force. Although this is a positive trend, exercise leadership more often than not restricted Red Team activity from disrupting operations to ensure that training objectives were met.

The overall assessment is that information assurance remains a significant operational concern across the Department of Defense. Red Teams were able to overcome even the improved areas of network and systems defense during exercises, although they admittedly had to work harder to do so. The operational concern is further highlighted by noting that the cyber threat portrayed during assessed exercises was consistently below that expected for a nation-state.

Status of Prior Year Recommendations

A recurring recommendation from prior fiscal years (FY07-FY08) was for exercise authorities to incorporate more threat-representative network attacks to stress detection capabilities, network Continuity of Operations, and network recovery plans; and that a Joint Staff recommendation would be helpful. On September 28, 2010, the Chairman of the Joint Chiefs of Staff issued such a memorandum; this memorandum will provide significant support to the execution of rigorous assessments of IA and IOP in representative cyber-threat environments.

FY11 PLANNED ASSESSMENTS AND GOALS

DOT&E has proposals for assessing 22 COCOM and Service exercises in FY11, with the goal of performing at least one interoperability and one information assurance assessment at each COCOM and Service during the fiscal year (see Table 2). Seven of the proposed assessments involve units preparing to deploy (or already deployed) to Iraq and Afghanistan. The FY11 assessment program will focus on the following:

- Improving portrayal of advanced cyber threats during assessments to include providing Red Teams longer time to conduct network reconnaissance, integrating Red Team activities into the exercise scenario, and increasing red team collaboration with the (simulated) opposing force.
- Assessing the ability of network defenders to detect and react to penetrations and intrusions.
- Assessing operational effects and mission impacts from cyber activities.
- Performing assessments at times other than during the conduct of training exercises.

TABLE 1. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS IN FY10

EXERCISE AUTHORITY	EXERCISE	ASSESSMENT AGENCIES
AFRICOM	CJTF Horn of Africa 10	ATEC
	Direct Reporting Unit - Naval Forces Africa	ATEC
CENTCOM	AOR Visit (Air Operations Center for Iraq)	ATEC
	AOR Visit (Qatar)	ATEC
EUCOM	Austere Challenge 10	ATEC
JFCOM	Empire Challenge 10	JITC
NORAD/NORTHCOM	Ardent Sentry 10	688 IOW
PACOM	Terminal Fury 10	OPTEVFOR, MCOTEA, JITC
SOUTHCOM	JTF GITMO	ATEC
	Panamax 10	ATEC
STRATCOM	Global Lightning/Bulwark Defender 10	JITC, MCOTEA
	Global Thunder 10	JITC, MCOTEA
TRANSCOM	Turbo Distribution 10	JITC, MCOTEA
USFK	Key Resolve 10	ATEC, MCOTEA
USA	Unified Endeavor 09-03-VI	ATEC
	Unified Endeavor 10-1	ATEC
	Unified Endeavor 11-1-I	ATEC
	Unified Endeavor 11-1-III	ATEC
USN	Planned Exercise Delayed to FY11	OPTEVFOR
USAF	Black Demon 10	688 IOW, MCOTEA
	Angel Thunder 10	JITC
USMC	II MEF COMMEX	MCOTEA
	III MEF (in Key Resolve)	MCOTEA
Other	Coalition Warrior Interoperability Demonstration 2010	JITC

AFRICOM – African Command
AOR – Area of Responsibility
ATEC – Army Test and Evaluation Command
CENTCOM – Central Command
CJTF – Combined Joint Task Force
COMMEX – Communications Exercise
EUCOM – European Command
GITMO – Guantanamo Bay
IOW – Information Operations Wing
JFCOM – Joint Forces Command
JITC – Joint Interoperability Test Command
JTF – Joint Task Force
MCOTEA – Marine Corps Operational Test and Evaluation Activity
MEF – Marine Expeditionary Force
NORAD – North American Defense Command
NORTHCOM – Northern Command
OPTEVFOR – Operational Test and Evaluation Force
PACOM – Pacific Command
SOUTHCOM –Southern Command
STRATCOM – Strategic Command
TRANSCOM – Transportation Command
USFK – United States Forces Korea
USA – United States Army
USN – United States Navy
USAF – United States Air Force
USMC – United States Marine Corps

TABLE 2. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS PROPOSED FOR FY11

EXERCISE AUTHORITY	EXERCISE	ASSESSMENT AGENCIES
AFRICOM	Judicious Response 2011-2	ATEC
	Direct Reporting Unit Assessment	ATEC
CENTCOM	AOR Site Assessment #1	ATEC
	AOR Site Assessment #2	ATEC
EUCOM	Austere Challenge 2011	ATEC
JFCOM	Angel Thunder 2011	JITC
NORAD/NORTHCOM	Vigilant Shield 2011	688 IOW
	Ardent Sentry 2011	688 IOW
PACOM	Terminal Fury 2011	COTF
	Keen Edge 2011	COTF
SOCOM	Emerald Warrior 2011	ATEC
SOUTHCOM	Integrated Advance 2011	ATEC
	Trade Winds 2011	ATEC
STRATCOM	Bulwark Defender 2011	JITC
TRANSCOM	Assessment During Operations	JITC
USFK	Key Resolve 2011	ATEC, MCOTEA
USA	Unified Endeavor 11-1-IV	ATEC
	Unified Endeavor 11-2	ATEC
	Unified Endeavor 11-3	ATEC
	Unified Endeavor 11-1-VI	ATEC
USN	JTFEX 11-1	COTF
	JTFEX 11-4	COTF
USAF	Black Demon 2011	688 IOW
	Dragon 2011/Red Flag 11-3	688 IOW
USMC	Unified Endeavor 11-2 (II MEF)	MCOTEA

AFRICOM – African Command
AOR – Area of Responsibility
ATEC – Army Test and Evaluation Command
CENTCOM – Central Command
COTF – Commander, Operational Test and Evaluation Force
EUCOM – European Command
IOW – Information Operations Wing
JFCOM – Joint Forces Command
JITC – Joint Interoperability Test Command
JTFEX – Joint Task Force Exercise
MCOTEA – Marine Corps Operational Test and Evaluation Activity
MEF – Marine Expeditionary Force
NORAD – North American Defense Command
NORTHCOM – Northern Command
PACOM – Pacific Command
SOCOM – Special Operations Command
SOUTHCOM –Southern Command
STRATCOM – Strategic Command
TRANSCOM – Transportation Command
USFK – United States Forces Korea
USA – United States Army
USN – United States Navy
USAF – United States Air Force
USMC – United States Marine Corps