Information Assurance (IA) and Interoperability (IOP)

In FY11, the DOT&E IA and IOP Assessment Program performed 23 assessments during combatant command (COCOM) and Service exercises; four of these assessments involved units preparing to deploy (or already deployed) to Iraq or Afghanistan.

The IA posture observed during the assessed FY11 exercises is not sufficient to prevent an advanced adversary from adversely affecting the missions that were being exercised. DOT&E observed modest improvements in certain areas of network defense, but there were also several areas in which prior progress has declined. In general, information technology and personnel were not fully prepared to operate in realistic and contested cyberspace conditions. Red Teams generally overcame defenses during exercises by only moderately increasing their level of effort over previous years.

The cyber threat portrayed during assessed exercises remains consistently below that expected from a nation-state level adversary. Exercise authorities often restricted cyber activities from affecting exercise-training objectives, thus limiting the ability to fully assess operational/fielded network performance against realistic threats. The Chairman, Joint Chiefs of Staff, issued a Red Team Execute Order (EXORD) in February 2011 that directs a more realistic cyber adversary in all major COCOM and Service exercises. Although this expanded play has yet to be observed, a number of COCOMs are developing EXORD implementation plans. DOT&E will work closely with the exercise authorities, U.S. Cyber Command (CYBERCOM), and the Joint Staff to ensure the best possible implementation of the EXORD occurs, and assessments in more representative cyber environments become the norm.

Recognizing that some advanced adversary actions and the effects they may cause are not suitable for live networks, DOT&E is developing methods and pursuing options to examine these effects during offline demonstrations and in appropriate range environments. DOT&E proposed enhancements to cyber assessment capabilities, including enhancements to the infrastructure of the Joint Information Operations Range (JIOR) and the operational and cyber-threat environments that must be available via the JIOR. These enhancements met with a positive reception by senior DoD leadership, but fiscal constraints are likely to limit the speed with which these important capabilities are acquired.

The FY11 IOP assessments found that interoperability issues encountered by the training audience typically hindered, but rarely prevented, mission accomplishment; this is due primarily to operators who developed and executed workarounds that may have preserved the timeliness and accuracy of mission data at the cost of the efficiency or level of effort required. Even though missions were generally accomplished, the workarounds usually increased operator workload, and often resulted in degraded effectiveness in completing mission tasks. Assessment teams documented measurable impacts to the timeliness, accuracy, and efficiency of operational data handling in these assessments.

The majority of problems identified for investigation and reporting via Finding Memoranda in FY11 involved interoperability concerns. While only three Findings Memoranda were published in FY11, DOT&E is currently investigating findings focused on interoperability issues with the use of third-party software (such as JAVA) on DoD networks, as well as unsynchronized system upgrades in federated (i.e. system-of-sytems) environments. The majority of systems observed during exercise assessments lack interoperability certifications.

In summary, unresolved interoperability issues, coupled with low-to-moderate level threats, were observed to be sufficient to adversely affect the quality and security of mission critical information in a way that could, and did degrade, mission accomplishment. Interoperability and IA problems are rarely observed in isolation from each other, but are frequently interrelated. In FY12, DOT&E will continue to support the implementation of more realistic cyber threats in exercises and will report both the IA and IOP results of these assessments.

PARTNERSHIPS AND COORDINATION

DOT&E remains partnered with the Joint Staff and DoD Deputy Chief Information Officer (CIO) on the oversight and coordination of the IA and IOP Assessment Program. Metrics and observations generated from these assessments are provided to the DoD CIO for use in enterprise-wide IA estimates and programs. In addition, DOT&E coordinates program efforts with the USD(AT&L) and the Director, Developmental Test and Evaluation as a means of informing the acquisition and development of information handling systems.

DOT&E has a memorandum of understanding with CYBERCOM that directs a Cyber Assessment Synchronization Working Group. This group is working to synchronize planning, execution, and reporting activities among all cyber assessment activities, and especially those supporting exercise assessments. Enhanced training and certification for "Blue" (cooperative technical/administrative compliance) and "Red" (proxy-adversary penetration) Teams will contribute to more threat-representative cyber activities and assessments, better standardization of measures and methods, as well as enhancing a CYBERCOM exercise support cell.

DOT&E continues the partnership initiated with the Joint Forces Command (JFCOM), Joint System Integration, and Interoperability Laboratory (now Joint Staff activities) to enhance assessments conducted by both organizations during training exercises through coordinated sharing of information and expertise. The partnership collaborated in two assessments in FY11, and further joint assessments are anticipated for FY12.

DOT&E coordinates closely with the intelligence community, the National Security Agency, and the Service Information Warfare centers to improve both the scheduling and portrayal of the representative cyber threats during exercises. The Defense Intelligence Agency (DIA) has made significant progress in the definition of advanced and emerging methods of cyber attack, and was instrumental in mapping known adversary activities to the threat portrayals for several FY11 exercises. DIA will be instrumental in helping implement the Red Team EXORD through the identification of the Red Team assets needed – and the level of cyber threat actually portrayed – in all major exercises.

DOT&E continues to partner with the Naval Postgraduate School to research and develop improved capabilities for network analyses. This partnership includes the design and development of network test tools; instrumentation; training resources and test/evaluation 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 shortfalls.

Additionally, DOT&E collaborates with the Defense Information Systems Agency to improve and expand the level of assistance and training available to assessed organizations, to include the implementation of a cyber-defense training and assessment suite at several COCOMs. This collaboration will focus on improved training resources, community feedback, and operator training tools to help remediate vulnerabilities and shortfalls identified during assessments.

FY11 ASSESSMENT ACTIVITIES

In FY11, the five assessing organizations included the Army Test and Evaluation Command (ATEC), Commander, Operational Test and Evaluation Force, the Marine Corps Test and Evaluation Activity (MCOTEA), the Joint Interoperability Test Command (JITC), and the Air Force 688th Test and Evaluation Squadron. These five assessing organizations completed 23 exercise assessments under the IA and Interoperability Assessment Program. These assessments included 15 COCOM and 8 Service exercise assessments (see Table 1). Four assessments involved units preparing to deploy (or already deployed) to Iraq and Afghanistan.

DOT&E published three Finding Memoranda in FY11, all of which involved IA problems that also had significant interoperability dimensions:

- Joint Task Force Guantanamo support system (classified) – an outdated software version being maintained to ensure interoperability resulted in IA vulnerabilities.
- U.S. Navy/Marine Corps aviation readiness systems – a manual data exchange protocol between two systems resulted in both interoperability shortfalls and IA risks.
- Microsoft SharePoint Server software configuration – a lack of configuration standards resulted in both interoperability shortfalls and IA vulnerabilities.

Finding Memoranda detail specific IA and interoperability concerns that have the potential to significantly degrade operations and warrant senior-level attention. Findings may include system-to-system issues, process/procedure issues, or cross-DoD issues (such as universal use of commercial products). DOT&E identifies shortfalls and vulnerabilities to the cognizant Service or DoD leadership, whose replies detail their proposed or ongoing mitigation efforts; such upgrades and mitigations are subject to subsequent re-evaluation and validation in future assessments.

Additionally, one FY10 Finding Memorandum concerning network trust architectures was answered in FY11, following an extensive DoD effort to re-design the optimal reference architecture for this fundamental process/service. DOT&E is currently developing seven additional Finding Memoranda based on assessments conducted during FY11 that include: management of allied/coalition networks (both IA vulnerabilities and IOP shortfalls); major headquarter software baselines (a system-of-systems interoperability shortfall); security architectures for public key infrastructure use (both IA and IOP); and an array of Service and joint command-and-control systems (both IA and IOP).

In order to enhance the IA posture of acquisitions, DOT&E has prepared templates and established a process for assessing the adequacy of IA testing in acquisition test and evaluation master plans and test plans. These templates facilitate an early review and development of these documents to ensure that IA is addressed prior to approval of these documents. IA testing was specifically addressed in the test and evaluation master plans for the following six systems:

- CVN 78 *Gerald R. Ford* class
- Littoral Combat Ship (LCS)
- Patriot Post-Deployment Build 7 (PDB-7)
- Broad Area Maritime Surveillance (BAMS)
- B-2 Extremely High Frequency (EHF)
- E-2D Advanced Hawkeye

DOT&E reviewed the IA portion of the following operational test plans:

- Patriot PDB-7
- AEGIS 7.1R/Cooperative Engagement Capability (CEC)
- Global Combat Support System – Army
- *Lewis and Clark* Class of Auxiliary Dry Cargo Ships (T-AKE)

DOT&E reviewed completed tests and resulting data for the following six systems:

- General Fund Enterprise Business System (GFEBS)
- Patriot PDB-6.8
- Tomahawk
- Aegis Weapons System
- Ballistic Missile Defense System/Command, Control, Battle Management, and Communications (BMDS/C2BMC)
- Financial Information Resource System Budget Formulation (FIRST BF)

ASSESSMENT

Several developments in FY11 indicate increasing efforts across the DoD to prepare to conduct exercises – and operations – in a contested cyberspace environment. The Chairman, Joint Chiefs of Staff issued an execute order to increase realistic cyberspace conditions in training exercises, and CYBERCOM published operations orders for securing, operating, and defending the Global Information Grid, while increasing support to the COCOMs. Finally, the OSD released a DoD Strategy for Operations in Cyberspace.

As all of these processes have phased implementation, FY11 saw relatively low levels of improvement in threat depictions during training and operations. Most exercise assessments and tests involved operations largely against low- and mid-level cyber threats that created only partially compromised or marginally degraded network conditions. The exercises infrequently portrayed high-level threats, and no operations were seriously disrupted. While data were gathered concerning the actual performance of networks in a hostile cyber environment, and the impacts of this performance were assessed, the majority of data gathered in FY11 concerned the level of preparation and compliance to standards by DoD networks.

Interoperability

The FY11 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 operators generally accomplished missions, the workarounds usually increased operator workload, and often resulted in degraded efficiency of completing tasks, or degraded timeliness/accuracy of the information generated.

Overall, it was found that less than one-third of all systems observed during assessments had been fully certified for interoperability, although configuration management and documentation was satisfactory in almost 9 of 10 systems reviewed. Despite the lack of interoperability testing/certification, local authorities certified these systems for network operation. In some instances, major software suites were found to be in operational use despite having not completed operational testing or interoperability certification. Several of the findings under research by DOT&E are centered specifically on interoperability shortfalls, including:

- A major headquarters federated network (system-of-systems), which has demonstrated multiple operationally significant interoperability shortfalls due to unsynchronized upgrades to individual systems.
- System and echelon interoperability for cyber situational awareness architectures intended to provide coordination for cyber defense and configuration.
- Lack of network configuration standards for coalition and community-of-interest networks, resulting in both IA vulnerabilities and IOP shortfalls.
- DoD network configuration and interoperability standards for the use of public key infrastructure, resulting in IA vulnerabilities.
- Lack of centralized coordination for updates and upgrades to third-party software (such as JAVA, Adobe, and other commercial software commonly used by DoD), resulting in frequent interoperability and IA problems.

These items, reported to DOT&E from FY11 assessments, are currently under review and validation before being formally reported to the cognizant agencies/Services.

Information Assurance

Overall, control of user access to DoD networks improved in FY11, to include the use of proper identification and authentication for users, physical security of network components and access points, and correct configuration management of systems. Nonetheless, IA assessments continued to highlight the relationships between cyber security and other areas such as physical security and operations security. Physical intrusions, as well as online deception/social engineering, continued to be effective avenues of attack.

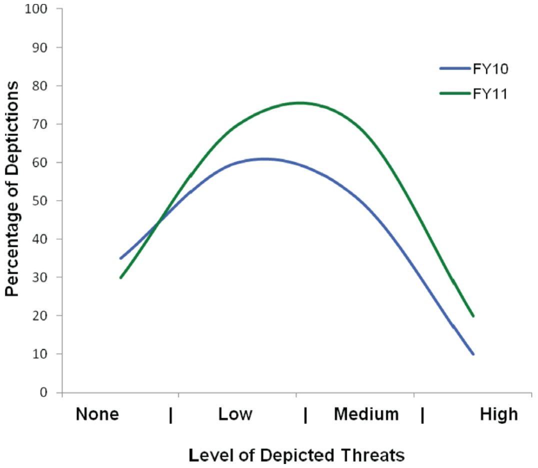

Figure 1: Distribution of threat depictions in assessed exercises.

Most Red Teams reported increased difficulty in penetrating network defenses, but results show that with sufficient time, Red Teams routinely managed to penetrate networks and systems. Detection rates of network intrusions remained low, and the ability of network defenders to detect subsequent exploitations of network data was minimal; most assessments witnessed large exfiltrations of operationally significant data. The extracted data was available, in only a few cases, to the exercise opposition force for tactical/strategic exploitation, which in effect created a more benign exercise environment than postulated by DIA and the intelligence community.

The assessments showed a decrease in the use of backup files and systems, proper audit logging and reviews, logical access controls, incident planning, and vulnerability management. There was an overall increase in high-risk vulnerabilities observed (indicating a decrease in effective patch management), as well as a decrease in effective use of anti-virus tools and software (including failures to routinely update virus signatures). Although the ongoing fielding of the Host Based Security System (HBSS) has resulted in many local improvements in network protection from intrusion as well as intrusion detection, the majority of HBSS suites observed were found to be incorrectly or ineffectively configured.

Experience and formal training levels for network defenders have increased. As shown in Figure 2, the aggregate skill levels of network personnel assessed in several FY09 through FY11 venues indicate an increase in intermediate skills across the DoD and fewer beginner level operators overall. User awareness of IA threats and protections increased in FY11.

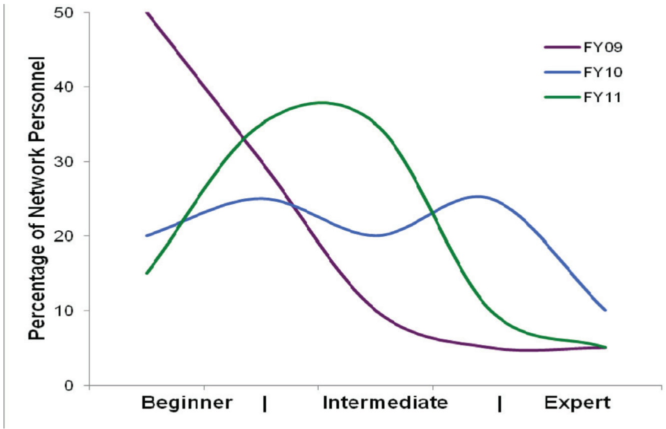

Figure 2: Distribution of skill levels in assessed populations.

Mission Assurance

During approximately half of FY11 assessments, assessment teams further the IA and IOP findings to characterize the operational impacts – or potential operational impacts – to specific missions being exercised. Although cyber-adversary activities posed a high risk to critical operations, exercise authorities seldom permitted any disruptions to be fully exercised; the priority to achieve other exercise training objectives remains at odds with exercising in an environment with representative cyber adversaries. Implementation of the Chairman, Joint Chiefs of Staff Execute Order should result in exercises and assessments with more realistic cyber environments and more useful results, regarding mission accomplishment, and mission impact should become available.

Examples of mission impact that were observed included degradation to the timeliness, accuracy, and efficiency of the networks; adverse impacts to the confidentiality, availability, and integrity of operational data were also documented. In many cases, these adverse effects were not due to IA vulnerabilities, but to poor interoperation between systems. A major source of poor interoperability is often found to be an incomplete set of interface requirements, or uncoordinated upgrades and updates to interdependent systems. Some of the observed mission impacts include:

- Delays in critical battlefield situational awareness
- Reductions in forces available for operational tasking due to delays or inaccuracies in planning systems
- Re-allocation of personnel from less critical tasks to support increased manual efforts for critical ones
- Large-scale exfiltration of operationally significant data from force planning systems
- Modification of blue-force operational data by opposition force actors
- Manual transfers of information between systems unable to automatically interoperate.

FY12 PLANNED ASSESSMENT AND GOALS

DOT&E will continue to assess approximately 20 COCOM and Service exercises in FY12, with the goal of performing at least one interoperability and one IA assessment at each COCOM and Service during the fiscal year (see Table 2). One of the planned FY12 assessments will involve units already deployed to Afghanistan. The FY12 assessment program will focus on the following:

- Supporting the three-year implementation of the Chairman, Joint Chiefs of Staff Red Team EXORD, and continuing to improve portrayal of advanced cyber threats during assessments
- Increased coordination with CYBERCOM and other agencies in the scheduling and conduct of assessments
- Improved methods for gathering and assessing mission impacts
- Expanded use of the Joint IO Range and other test facilities in support of exercise assessments
- Linkages to T&E through research and results sharing

TABLE 1. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS IN FY11

EXERCISE AUTHORITY	EXERCISE	ASSESSMENT AGENCIES
AFRICOM	Judicious Response 2011 (Exercise Cancelled)	ATEC
CENTCOM	AOR Site Assessment #1	ATEC
EUCOM	Austere Challenge 2011	ATEC
JFCOM	Empire Challenge 2011	JITC
NORAD/NORTHCOM	Vigilant Shield 2011	688 IOW
	Vibrant Response 2011	JITC
PACOM	Terminal Fury 2011	COTF
SOUTHCOM	Integrated Advance 2011	ATEC
	Joint Task Force Bravo 2011	ATEC
SOCOM	Emerald Warrior 2011	ATEC
STRATCOM	Bulwark Defender 2011	JITC
	Global Lightning 2011	JITC
TRANSCOM	Assessment During Operations	JITC
	Turbo Challenge 2011	JITC
USFK	Key Resolve 2011	ATEC
	Ulchi Freedom Guardian 2011	ATEC
USA	Unified Endeavor 11-1-III	ATEC
	Unified Endeavor 11-2	ATEC
	Unified Endeavor 11-1-VI	ATEC
USN	JTFEX 11-1	COTF
USAF	Black Demon 2011	688 IOW
	Red Flag 11-3	688 IOW
USMC	Unified Endeavor 11-2 (II MEF)	MCOTEA
	Ulchi Freedom Guardian 2011	MCOTEA

AFRICOM – Africa 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
JTF – Joint Task Force
MCOTEA – Marine Corps Operational Test and Evaluation Activity
MEF – Marine Expeditionary Force

NORAD – North American Aerospace Defense Command
NORTHCOM – Northern Command
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 FY12

EXERCISE AUTHORITY	EXERCISE	ASSESSMENT AGENCIES
AFRICOM	Judicious Response 2012	ATEC
CENTCOM	AOR Site Assessment #1 (Bahrain)	ATEC
	AOR Site Assessment #2 (Afghanistan)	ATEC
CYBERCOM	Cyber Flag 2012	ATEC
EUCOM	Austere Challenge 2012	ATEC
NORAD/NORTHCOM	Vigilant Shield 2012	688 IOW
	Ardent Sentry 2012	688 IOW
	Vibrant Response 2012	JITC
PACOM	Terminal Fury 2012	COTF
SOUTHCOM	PANAMAX 2012	ATEC
SOCOM	Emerald Warrior 2012	ATEC
STRATCOM	Global Lightning 2012	JITC
TRANSCOM	Turbo Challenge 2012	JITC
	Assessment During Operations	JITC
USFK	Key Resolve 2012	ATEC
	Ulchi Freedom Guardian 2012	ATEC
USA	Full Scope Exercise 12-4	ATEC
USN	Bold Alligator 2012	COTF
USAF	Red Flag 12-3	688 IOW
	Ulchi Freedom Guardian 2010 (III MEF)	MCOTEA
USMC	Bold Alligator 2012	MCOTEA

AFRICOM – Africa 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
JITC – Joint Interoperability Test Command
MCOTEA – Marine Corps Operational Test and Evaluation Activity
MEF – Marine Expeditionary Force
NORAD – North American Aerospace 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