Cyber Assessments

SUMMARY

DOD missions and systems remain at risk from adversarial cyber operations. Operational tests continued to discover mission-critical vulnerabilities in acquisition programs, and assessments during Combatant Command (CCMD) training exercises continued to identify previously undetected vulnerabilities. However, there were an increasing number of instances where the cyber Red Teams employed during DOT&E assessments experienced greater difficulty in penetrating network defenses or maintaining previously acquired accesses. These improvements are both noteworthy and encouraging, but we estimate that the rate of these improvements is not outpacing the growing capabilities of potential adversaries, who continue to find new vulnerabilities and techniques to counter the fixes and countermeasures by DOD defenders.

DOT&E assessment data for this summary are based on more than 50 cybersecurity assessments with CCMDs and Services, and nearly 70 cybersecurity OT&E events (see Table 1 on page 231). Additionally, DOT&E sponsored classified assessments of nuclear command, control, and communications; cross domain solutions; data breaches; and Public Key Infrastructure. The demand for cyber expertise to plan and execute cyber assessments across the DOD, and for the in-depth analyses of the data produced by these events, is rapidly increasing and stressing available resources.

For example, the U.S. Army's Threat Systems Management Office Red Team performed more than 200 events in FY18, meeting or exceeding threat-portrayal objectives in most cases. However, DOT&E observed a growing number of instances where the Red Team needed more time to achieve objectives. This was due in part to improved network defenses, but also due to insufficient time to prepare the array of representative cyber-attacks attributed to the portrayed adversary. There remains a gap between DOD cyber Red Team capabilities and the advanced persistent threat, and assessments that do not include a fully representative threat portrayal may leave warfighters and network owners with a false sense of confidence about the magnitude and scope of cyber-attacks facing the Department. DOT&E is working with the DOD Red Teams to close that gap by helping them acquire additional personnel, more advanced capabilities, and training; however, more resources are urgently needed in this area.

Recent advances in cyber technologies indicate that automation – and even artificial intelligence – are beginning to make profound changes to the cyber domain. Warfighters and network defenders must prepare for the onslaught of multi-pronged cyber-attacks across both critical mission systems and the multitude of supporting systems and networks that enable these missions. Preparations must include realistic demonstrations of fight-through capabilities, resilience, and alternate modes when stressed by Red Teams portraying advanced adversaries. Even though directed by the Chairman of the Joint Chiefs in 2011, these realistic demonstrations have yet to become routine.

DOT&E remains committed to working with the acquisition community and operational commands in discovering and documenting cybersecurity problems, providing information to facilitate their remediation, and verifying the efficacy of solutions or mitigations.

CYBER ASSESSMENT ACTIVITY

DOT&E oversees cybersecurity OT&E for major defense acquisition programs, and performs congressionally-directed cybersecurity assessments of operational networks and systems during CCMD and Service training exercises. DOT&E also supported operational assessments of offensive cyber capabilities, and performed analyses to characterize operational implications if an adversary exploited known compromised information.

Based on results from operational tests and exercise assessments, DOT&E publishes classified reports on overarching cybersecurity topics of interest. One report published this past fiscal year explored the performance of cyber defenses against observed attacks to identify specific changes that have proven to contribute to improved defensive performance.

Operational Test and Evaluation with Cybersecurity

DOT&E continued to emphasize the importance of OT&E of cybersecurity and recommended such testing for all systems that transmit, receive, or process electronic information, by direct, wireless, or removable means. These operational tests focus on confirming that forces and units equipped with the systems can complete operational missions in a cyber-contested environment. In FY18, DOT&E monitored more than 70 such tests across 38 acquisition programs.

DOT&E published updated procedures for planning, conducting, and reporting cybersecurity testing results. DOT&E also continued efforts to improve techniques and tools for testing network gateways, non-Internet Protocol systems, and industrial control systems using the find-fix-verify paradigm.

DOT&E observed rapidly increasing demand for cybersecurity OT&E, with FY18 having the largest number of such tests. The increased demand coupled with the increase in data from the tests is stressing the test community's cybersecurity resources. Table 2 (on page 234) shows the operational test community organizations involved in cybersecurity.

Cybersecurity Assessment Program

DOT&E's Cybersecurity Assessment Program worked with the CCMDs and Services to define tailored Cyber Readiness Campaigns that help address vulnerabilities and improve cyber defense through a series of focused events throughout the year. In FY18, DOT&E provided resources for operational test agencies, intelligence subject matter experts, and DOD cyber Red Teams to plan and conduct the 54 events listed in Table 1 (on page 233). The events included assessments of physical security, focused attack techniques such as phishing, cyber activities causing mission effects, and assistance in understanding and correcting discovered problems. DOT&E published a new Cybersecurity Assessment Program Handbook of best practices and guidance to the assessment teams for planning, conducting, and reporting on the campaigns and events. As in the other areas of cyber-related activity, DOT&E observed increasing CCMD and Service demand for cyber expertise to support these assessment events.

Assessment of Offensive Cyber Capabilities

DOT&E worked with offensive cyber capability developers to integrate operationally realistic testing into the non-traditional acquisition lifecycles of these capabilities, which often involve compressed timelines. DOT&E observed or supported more than 10 such events in FY18. Concurrently, DOT&E worked with the Joint Technical Coordinating Group for Munitions Effectiveness to identify the data required to build analysis tools to predict offensive cyber effects.

Operationally, the processes for planning and employing offensive capabilities is a complex undertaking. DOT&E assessed the synchronization of cyber fires with component schemes of maneuver, integration of intelligence support, and support to commander objectives, and made recommendations to improve these critical procedures.

Persistent and Advanced Cyber Operations

DOT&E employs limited Persistent Cyber Operations (PCO) in assessments for several CCMDs. These assessments with longer dwell time afforded the PCO Red Teams time to probe deeper into network and system vulnerabilities. This approach results in assessments that are both more thorough and more threat-representative.

In addition to identifying vulnerabilities that matter to the warfighter, the PCO facilitates the development of solutions or mitigation strategies that will reduce the effect of demonstrated attacks, and performs follow-on assessments to verify the solutions work as intended. The PCO Find-Fix-Verify model is the most rapid and effective way to achieve a higher degree of cybersecurity and warfighter mission assurance.

The Advanced Cyber Operations (ACO) Team augments other Red Teams with expertise that not all Red Teams possess, leads the development and acquisition of new Red Team capabilities, and supports testing of offensive cyber capabilities as a cyber opposing force.

Cybersecurity Assessments with Coalition Partners and Networks.

DOT&E observed or assessed several events with coalition partners in FY18, and performed several Find-Fix-Verify assessments on the Combined Enterprise Regional Information Exchange System (CENTRIXS) network. During the Australian-led (U.S. Indo-Pacific Command supported) exercise Talisman Saber 19, the Australian exercise lead plans to integrate demonstrations of non-kinetic and kinetic effects to assist Blue Force training objectives. DOT&E is planning to assess bi-lateral cyber activities associated with this coalition exercise.

Cyber Ranges

For the last several years, DOT&E advocated for a cyber range structure that supports both test and training requirements. Because of the similarity of functions in test and training, a common architecture across these ranges is needed to provide efficiency and flexibility to address the increasing demand for cyber range resources, and to effectively respond to rapidly evolving and increasingly sophisticated cyber threats

DOT&E engaged with the Persistent Cyber Training Environment (PCTE) program to monitor their technology assessments, advocate for the acquisition of effective and suitable range capabilities, to collaborate in the development of a test and evaluation approach, and to encourage dual-use across test and training ranges. In 3QFY19, DOT&E will co-sponsor a range demonstration with the PCTE program and the Test Resource Management Center that will examine emerging technologies such as automated opposing force capabilities and continuous monitoring for network defense. DOT&E is also interacting with both test and training communities to promote a clear understanding of cyber-range requirements, common architectures, and standards.

Engagement with the Intelligence Community

DOT&E formed a team of engineers, system designers, system operators, cyber Red Team members, Intelligence Community experts, and program representatives to characterize the operational risk posed by program information that is known to be compromised. The assessments combine the insights from the subject matter experts to identify and then confirm vulnerabilities and attack techniques to inform mitigation efforts. The positive reception to the first reports by senior DOD leadership led to demand for additional efforts for other programs and systems. Here, as with the other cyber efforts, the demand is outpacing and stressing available resources.

Coordination with USD(A&S) on Statutory Cybersecurity Assessments

In FY18, DOT&E continued collaboration with USD(A&S) for cyber assessments of major DOD weapons systems, as directed by section 1647 of the FY16 National Defense Authorization Act (NDAA). DOT&E invited USD(A&S) representatives to participate in cybersecurity assessments with the DOT&E Cybersecurity Assessment Program when the events included systems of mutual interest.

OBSERVATIONS

This section describes noteworthy observations from FY18 exercise assessments and special evaluations. Most of the observations highlight the challenges facing the DOD in securing networks and supporting critical missions with survivable and resilient capabilities, but several include positive themes that network defenses have improved over the past several years. However, the tenuous balance between network defense and adversary capabilities leans heavily in the favor of potential adversaries, and the DOD must continue to emphasize the importance of cyber expertise at all levels and in all mission areas: warfighter, network defenders, leadership, and assessors. The summary areas each warrant continued monitoring and further assessment. DOT&E can provide more detailed classified information on each topic.

Leadership Emphasis on Cybersecurity of Warfighter Networks. DOT&E performed an assessment of a major command which identified several vulnerabilities that could impact mission assurance. Senior leadership at the command self-reported to senior DOD leadership that the command's mission assurance posture was potentially degraded, and made mitigation of these vulnerabilities a top priority. Within 60 days, all identified vulnerabilities had been remedied, were verified by the assessment team, and the command leadership reported that their mission assurance posture had improved. This example of a rapid "Find-Fix-Verify" cycle is an objective of all DOT&E cybersecurity assessments.

Nuclear Command, Control, and Communications (NC3). Protected, assured, and resilient command, control, and communications are essential for all military operations and especially so for the NC3 components of our national capability. At the request of the DOD Chief Information Officer (CIO) and the Defense Threat Reduction Agency (DTRA), DOT&E participated in classified cybersecurity assessments to characterize the status and identify options for improving the mission assurance and cyber-related aspects of the NC3 capability.

Legacy Systems and Cybersecurity. DOT&E performed several preliminary assessments of systems and networks that had been developed and fielded several decades ago, and which were widely believed to be safe from current-era cyber-attacks. However, initial findings identified technology updates that were not part of the original design or security plan and which could provide avenues for a cyber-attack.

Trust Relationships Facilitate Adversary Cyber-Attacks. The network compromises achieved by a Red Team during an assessment at one command allowed a separate Red Team – portraying a common adversary – to attack a different command. Trust relationships are critical to the operational support relationships between separate warfighter commands, but they must be designed and monitored to prevent mission impacts by adversaries.

Physical Security Linkage to Cybersecurity. DOT&E continues to assess physical security of facilities and installations because lapses in these areas can enable cyber-attacks. One assessment in FY18 found a serious set of cyber and physical vulnerabilities that, if exploited, could degrade critical missions. The DOD leadership, supported by DOT&E, took immediate steps to prevent a similar exploit in the future; DOT&E plans to provide independent verification of the efficacy of the remediation actions taken.

Stolen Credentials. Multiple DOT&E assessments – as well as commercially available information – confirm that credential theft is one of the most common cyber-attack actions that leads to data breaches. Credential theft is attractive to both DOD Red Teams and cyber adversaries because of the reduced risk of detection associated with using stolen credentials compared to other hacking tools and techniques. DOT&E works with acquisition programs and operational organizations to identify and amend practices that enable compromise of credentials.

Breaches of Cleared Defense Contractors. DOT&E worked with law enforcement and the intelligence community to understand the potential impacts from past breaches on DOD systems and networks. DOT&E led several multidisciplinary teams in the evaluation of specific systems to assess the potential value to adversaries of known compromised information. These evaluations extended beyond list reviews of compromised documents, and included deeper analyses by Red Team personnel to identify how compromised information could be aggregated to enhance a potential cyber-attack. DOT&E communicated assessment results to appropriate DOD leadership and program officials, with the recommendation that additional resources be provided to expand this important assessment mission.

Operational Cyber Defenses. DOT&E performed analyses on 4 years of exercise assessments (FY14-17) to examine the changing nature of DOD cyber defenses. The analysis identified that defenders demonstrated increasing ability to detect Red Team activity, that Red Teams prefer to employ stolen credentials over software vulnerabilities, and that defenders need to improve speed and accuracy for processing reported incidents. DOT&E identified additional recommendations in this classified report to further improve the defensive posture and DOD mission assurance.

Cyber Expertise of Red Teams. DOT&E employs cyber Red Teams in most assessments, and in FY18, there were several instances where Red Teams were not available to support an assessment. In FY19, DOT&E intends to execute assessments where more advanced threat portrayal will be required, and the ability of Red Teams to meet these requirements is in question.

Currently Red Teams lack the time and funding to develop new tools and capabilities. The manning models for the Service Red Teams vary widely and are not uniformly successful. Reviews

of the capabilities of several Red Teams in FY18 showed that the best teams were overscheduled and overwhelmed by workload.

As demand for cyber Red Teams continues to increase, DOT&E observed numerous losses of master-level Red Teamers in FY18 to commercial jobs that were higher paying or which required less travel. Red Team capacity and retention options must be increased to meet the demands of testing, training, and other assessment activities.

IMPROVING CYBERSPACE OPERATIONS – OPERATORS AND AUTOMATION ARE KEY

Test and assessments in FY18 again found that low-capability attack techniques too often posed a risk for disrupting operational missions, however, DOT&E observed instances of successful cyber defense operations. A common thread running through these successful operations was the presence of a knowledgeable cyber operator with adequate defensive technology and tools.

DOT&E identified five improvement areas to enable cyber defenders to do their jobs well:

- Scope the task by defining the key cyber terrain, operational missions, tasks, and expectations.
- Foster unity of effort amongst participants that have different roles (offensive, defensive) and responsibilities (internal and external to assigned key cyber terrain).
- Know the key cyber terrain, operational concepts, and available tools.
- Match tools and skills to the operational tasks, missions, and key cyber terrain.
- Practice and train in operationally representative conditions against realistic cyber-attacks.

Scope the Task

- Focus defenders on mission-critical cyber terrain and provide appropriate technology such as real-time sensors and monitoring.
- Minimize the attack surface of mission-critical cyber terrain by using technologies such as Virtual Desktop Infrastructure, best practices such as segregated network enclaves, rigorous configuration management, and eliminating non-mission-critical connections.

Foster Unity of Effort

- Establish a centralized and standardized cyber reporting process that includes the necessary analytics and forensics.
- Develop and deploy cyber situational awareness tools.
- Establish specific duties, responsibilities, and tools to coordinate the activities of local defenders, help desks, system managers, and other key cyber defensive teams. A "one-size-fits-all" model does not work well.

Know the Terrain

- Identify and monitor mission-critical cyber terrain.
- Provide terrain-specific tools and training for needed skills such as automated monitoring, analysis, and forensics.
- Provide system and terrain-specific tools to automate configuration management, system backups, system isolation, and restoral.
- Establish mission and terrain specific training for cyber defenders.

Match Tools and Skills to the Task

- Establish a federated approach to cyber defense, vice relying on network boundary defenses, e.g. stop "flattening" the networks and relying on defensive tools at the network boundary.
- Work with academia, the private sector, and national labs to improve defensive cyber techniques, tools, and technologies.
- Pair automated tools to the specific attributes of the systems and networks defended, and provide defenders training on those tools.

Practice and Train

- Establish PCO (both automated and human penetration testing) on all mission-critical DOD cyber terrain to reflect current threats, attack vectors, and known exploits.
- Develop tools to help automate cyber-attacks to supplement and support cyber teams. This automation will help reduce the deficit in Red Team resources, and allow for continuous testing of acquisition programs and continuous monitoring of operational networks.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY18		
EVENT TYPE	**ACQUISITION PROGRAM OR TYPE OF EVENT**	
Programs Completing Operational Tests of Cybersecurity	Amphibious Combat Vehicle	Global Command and Control System – Joint
	AEGIS Modernization (Baseline Upgrades)	Global Positioning System Next Generation Operational Control
	Armored Multipurpose Vehicle	Integrated Personnel and Pay System – Army Increment 2
	AN/APR-39 Radar Warning Receiver	Integrated Strategic Planning and Analysis Network Increment 4
	Air Operations Center – Weapon System 1	Joint Air-to-Ground Missile
	Army Tactical Missile System – Service Life Extension Program	Joint Light Tactical Vehicle
	Ballistic Missile Defense System Program	Joint Precision Approach and Landing System
	Coastal Battlefield Reconnaissance and Analysis System	Joint Warning and Reporting Network
	Command Post Computing Environment	Key Management Infrastructure Increment 2
	Distributed Common Ground System - Army	Mounted Computing Environment
	Defense Enterprise Accounting and Management System	Near Real Time Identity Operations
	DOD Healthcare Management System Modernization	P-8A Poseidon Program
	Enclave Control Node	Paladin/FASSV Integrated Management (PIM)
	Enhanced Polar System	Public Key Infrastructure Increment 2
	F-35 – Lightning II Joint Strike Fighter Program	Stryker Family of Vehicles to include all variants
	Family of Beyond Line-of-Sight Terminals	Teleport, Generation III
	Fire Scout Unmanned Aircraft System	Triton
	Global Hawk Unmanned Aircraft System Multi-Spectrum Sensor	UH-60V BLACKHAWK
	Ground/Air Task Oriented Radar	Unmanned Aircraft System Gray Eagle
Cybersecurity Assessment Program	**Physical Security Assessment (2 Events)** U.S. Navy, U.S. Special Operations Command (USSOCOM)	
	Cooperative Network Vulnerability Assessment (4 Events) U.S. Air Force, U.S. Africa Command (USAFRICOM), U.S. Central Command (USCENTCOM) (2)	
	Cyber Operations (7 Events) U.S. Navy, USAFRICOM (2), U.S. Indo-Pacific Command (USINDOPACOM) (3), U.S. Northern Command (USNORTHCOM)	
	Mission Effects with Cyber Operations (29 Events) U.S. Air Force (2), U.S. Army (2), U.S. Forces Kores (2), U.S. Navy (2), USAFRICOM, USCENTCOM, USINDOPACOM (7), USNORTHCOM (2), USSOCOM (3), U.S. Southern Command (USSOUTHCOM), U.S. Strategic Command (USSTRATCOM) (3), U.S. Transportation Command (USTRANSCOM)	
	Targeting Processes for Offensive Cyber Operations USINDOPACOM	
	Dedicated Phishing Campaign USAFRICOM	
	Range Event U.S. Army	
	Sharing Solutions Fix Event (8 Events) U.S. Air Force (2), U.S. Forces Korea (2), U.S. Cyber Command (USCYBERCOM) (2), USINDOPACOM (2)	
	Table Top Exercise U.S. Navy	

TABLE 2. CYBERSECURITY TEST COMMUNITY	
OPERATIONAL TEST AGENCIES	
Military Services	Air Force Operational Test and Evaluation Center
	Army Test and Evaluation Command
	Navy Operational Test and Evaluation Force
	Marine Corps Operational Test and Evaluation Activity
Defense Agencies	Joint Interoperability Test Command
CYBER TEAMS	
Air Force	57th Information Aggressor Squadron
	177th Information Aggressor Squadron
	92nd Cyberspace Operations Squadron
	46th Test Squadron
	18th Flight Test Squadron
	Air Force Information Operations Center
	688 Information Operations Wing
Army	1st Information Operations Command
	Threat Systems Management Office
	Army Research Laboratory, Survivability/Lethality Analysis Directorate
Navy	Navy Red Team
	Space and Naval Warfare Systems Command Red Team
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Red Team