Cybersecurity

SUMMARY

DOT&E observed improvements in several cybersecurity areas within the Department of Defense (DOD) this past year; however, the Department's warfighting missions and systems remain vulnerable to cyber-attack. Observed improvements include enhanced protection of some network elements, greater challenges for cyber opposing forces (OPFOR) attempting to gain access to networks, and greater awareness by DOD leadership of the potential impact that cyber attacks could have on key systems and the critical missions they support. However, these improvements are not enough to ensure mission success.

In FY15 operational tests and exercise assessments, the cyber OPFOR was frequently in a position to deliver cyber effects that could degrade the performance of operational missions. Exercise authorities seldom permitted cyber attacks from being conducted to the full extent that an advanced adversary would likely employ during conflict, so actual data on the scope and duration of cyber attacks are limited. Additionally, exercise authorities often declined to allow kinetic effects based on data exfiltrated by the cyber OPFOR.

DOT&E believes the reluctance by Combatant Commands (CCMDs) and Services to permit realistic cyber effects during major exercises is due to the requirement to achieve numerous other training objectives in those exercises. Additionally, exercise authorities have stated they fear that cyber attacks could distract from—and possibly preclude—achieving these objectives. However, based on the increasing frequency of cyber attacks throughout the world, CCMDs should expect cyber attacks to be present for all critical missions they may be ordered to execute. In order to attain a high state of mission readiness, CCMDs and supporting defenders should conduct realistic tests and training that include cyber attacks and effects representative of those that advanced nation states would execute.

Identified Cyber Vulnerabilities

As in previous years, assessment teams consistently found four categories of vulnerabilities in both system tests and exercise assessments:

- Exposed or poorly managed credentials
- Systems not configured to identified standards
- Systems not patched for known vulnerabilities
- System/network services and trust relationships that provide avenues for cyber compromise

Noteworthy Successes by Network Defenders

Although defenses need improvement, there were specific instances where defenses worked, including the following:

- The cyber OPFOR found that vulnerabilities routinely available in many networks were not present in some networks due to timely upgrades and software patches.
- A layered approach to stop primary attack vectors, such as phishing, proved effective at defending networks and forced the cyber OPFOR to expend more time and deploy more advanced capabilities. Layered defenses that occupy the adversary's time away from a target may buy sufficient time for the Blue Force to sustain its critical missions.
- Application whitelisting, where network defenders allow only "known good" applications to operate on a network, precluded the cyber OPFOR from expanding its foothold in the network.
- A local hunt team supported by a Cyber Protection Team (CPT) was effective at log reviews that resulted in detection of the cyber OPFOR's presence.

Detection tools used by network defenders were primarily signature-based and dependent upon commercial tools adapted for DOD use. However, the majority of adversarial accesses involved the use of "native" software normally available within the networks and operating systems. Since misuse of native software is less easily detected and eliminated than malware, the DOD should augment current network defenses with behavior-based and heuristic-type sensors.

Cyber Red Teams

The demand on DOD-certified Red Teams, which are the core of the cyber OPFOR teams, has increased significantly in the past 3 years. In the same timeframe, the private sector has hired away members of Red Teams, resulting in staffing shortfalls during a time when demand is likely to continue to increase. This trend must be reversed if the DOD is to retain the ability to effectively train and assess DOD systems and Service members against realistic cyber threats.

Persistent Cyber OPFOR (PCO) and Continuous Assessments

In FY15, U.S. Pacific Command (USPACOM) leadership approved year-round activities of a Persistent Cyber OPFOR (PCO) in order to portray a more realistic cyber adversary in training and assessment events, and make the most efficient use of scarce Red Team personnel. The PCO employs DOD-certified Red Teams in longer-duration activities to be more representative of enduring threat actors than can be portrayed in a brief exercise period. This PCO has already helped USPACOM find and remediate mission-critical vulnerabilities that might have otherwise gone undetected.

USPACOM also agreed to a Theater Cyber Readiness Campaign (TCRC) in FY15. The TCRC included more frequent cyber assessment activities and allowed USPACOM to optimize cybersecurity preparations in smaller events throughout the year, and then examine a larger array of challenges in a capstone exercise event. U.S. European Command (USEUCOM) and U.S. Northern Command (NORTHCOM) are also developing

TCRCs. In theaters where the PCO and continuous assessments are active, DOD is better positioned to find cybersecurity problems, develop solutions or mitigation strategies, and verify that fixes are in place and effective.

Cyber Protection Team (CPT) Assessments

In FY15, DOT&E continued a partnership with U.S. Cyber Command (USCYBERCOM) to experiment with evolving cyber range capabilities and the potential benefits of team-training for representatives from CPTs. Most participants stated the opportunity to experience cyber attacks as a team on a realistic range network that included a live OPFOR, and then engage with the OPFOR during after-action reviews, constituted the best training they had received to date. They also expressed a strong desire for this type of training at their individual duty stations. DOT&E observed CPTs with team training performed better than CPTs without team training, and expects that significant time on realistic ranges will be instrumental to CPTs attaining an effective operational capability. DOT&E also observed some individuals assigned to CPTs do not possess the proper training, background, or motivation to become effective CPT members. DOT&E acquired and enhanced survey tools that can help determine individual suitability for CPTs, and has offered these tools to USCYBERCOM and Service cyber components.

Cyber Ranges

The FY15 National Defense Authorization Act (NDAA) directed DOD to establish an Executive Agent (EA) for cyber training ranges and an EA for cyber testing ranges. DOT&E has often used cyber ranges for events that combine testing and training. Such combined events make efficient use of scarce cyber range resources. The creation of two separate EAs—with separate responsibilities and incentives—would make it difficult to conduct combined activities in a timely manner. A single EA should be designated with the authority to oversee funding and personnel for all DOD-owned cyber ranges.

Conclusions

During exercises, DOD network defenders continue to demonstrate low detection rates of cyber OPFOR activities. The Microsoft Corporation has recently adopted the assumption that all systems are compromised ("Assume Breach"), which is an appropriate posture for the Department as well. The DOD should experiment with and perfect—with rigorous test and evaluation—the tools, tactics, and operational procedures that can quickly identify and stop ongoing cyber attacks.

Combatant Commands should make serious preparations to conduct all critical missions in a cyber-contested environment, and perform periodic operational demonstrations to ensure mission success. These demonstrations should include operational units, all network defenders, and CPT elements that would be expected in support of each mission. DOT&E is prepared to provide support to plan, conduct, and evaluate such demonstrations on both operational networks and in appropriate cyber range environments.

Recommendations

DOT&E recommends the CCMDs and Services:

- Demonstrate the ability to sustain critical missions in a contested cyber environment, consistent with Secretary of Defense and Chairman, Joint Chiefs of Staff guidance.[1]
- Develop tools, tactics, and operational procedures and perform regular battle drills with playbooks to ensure mission accomplishment in the contested cyber environment.
- Allow threat-representative cyber effects, using a persistent cyber OPFOR, during all major exercises.
- Request the leadership of the DOD Enterprise Cyber Range Environment and programs of record create range environments to support the demonstration of cyber effects that are not suitable for operational networks, and the development and testing of remediation options for cyber vulnerabilities.

DOT&E recommends the DOD:

- Accelerate the implementation of key, cybersecurity best practices to include application whitelisting; secure system configurations; and rapid patch application.
- Reduce the number of users with administrative privileges.
- Increase cybersecurity training and accountability for all personnel who use DOD networks.
- Designate a single EA for cyber ranges with the authority to oversee funding and personnel for all DOD-owned cyber ranges.
- Develop options to attract and retain experienced cybersecurity personnel, especially personnel with Red Team and cyber test experience.

DOT&E recommends DOD network defenders implement the following critical cybersecurity measures:

- Limit the availability of native administrative tools that adversaries can exploit to only key personnel.
- Limit access to password and operational data only to authorized users with need-to-know.
- Increase network segmentation and remote authentication policies to create a layered defense of critical assets.
- Deploy heuristic and behavior-based intrusion-detection systems and procedures to assist in the identification of suspicious network and system activity.

DOT&E recommends the Services and EAs for the DOD cyber ranges:

- Provide all CPTs with ready access to range-network environments for routine training and tactics development.
- Employ survey and other testing means to identify candidates for the Cyber Mission Force and to determine their readiness to move into advanced training and mission status.

[1] For example, the DOD Cyber Strategy dated April 2015, and the DOD Cybersecurity Culture and Compliance Initiative memorandum, signed by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, dated September 30, 2015, and agency cyber commands), and Tier 1 (DOD-wide, e.g., U.S. Cyber Command)

DOT&E recommends that the Undersecretary of Defense for Acquisition, Technology and Logistics, require programs of record to demonstrate they have no critical cybersecurity vulnerabilities prior to proceeding to the next acquisition milestone and prior to fielding.

DOT&E recommends the Chief Information Officer (CIO) update DOD Instruction 8330.01 (Interoperability of Information Technology) to require performance of a cybersecurity risk assessment prior to connecting systems or networks for interoperability reasons.

FY15 ACTIVITIES AND OBSERVATIONS

DOT&E conducted 33 cybersecurity operational tests of acquisition programs and 13 assessments during CCMD and Service training exercises, as shown in Table 1.

Cybersecurity OT&E of Acquisition Programs

Cybersecurity operational testing has two phases, as prescribed by DOT&E in August 2014:

- Cooperative Vulnerability and Penetration Assessments (CVPA). Operational test agencies conduct overt and comprehensive vulnerability and penetration assessments in cooperation with the acquisition program manager to characterize the cybersecurity status of a system. CVPAs include all major system interfaces and operational environments.
- Adversarial Assessments (AA). Operational test agencies conduct AAs to determine the operational impact of system cyber vulnerabilities. AAs evaluate the ability of a unit equipped with the system to conduct assigned missions in the expected operational environment in the presence of a realistic cyber threat. The operational environment includes the local and higher-echelon cyber defenders that support the system under test during its mission.

In FY15, DOT&E reviewed and provided cybersecurity test input for 105 Service and DOD systems, including 65 Test and Evaluation Master Plans and 40 operational test plans.

The four common cybersecurity shortfalls found during tests of acquisition systems were:

- Exposed or poorly managed credentials
- Systems not configured to identified standards
- Systems not patched for known vulnerabilities
- System/network services and trust relationships that provide avenues for cyber compromise

The types of systems at risk from cyber threats include non-Internet Protocol networks such as the 1553 and Controller Area Network data buses. A number of programs incorporate sensitive industrial control systems and programmable logic controllers, or deploy capabilities on commercial clouds. The diversity of systems and services susceptible to cyber attack will require new test capabilities and environments for networks at all levels of security classification.

In order to plan and conduct adequate OT&E of these types of systems and networks, test teams will require in-depth knowledge about their operations and unique vulnerabilities. As the Services begin to use commercial cloud services for data storage, it is critical that DOD develop contracts, policies, and regulations that permit independent DOD cybersecurity testing of commercial services and sites.

Cybersecurity Assessments during CCMD and Service Exercises

DOT&E's Cybersecurity Assessment Program observes and reports on DOD efforts to improve cybersecurity and cyber functionality through assessments of the CCMDs and Services. With DOT&E oversight, the five DOD Operational Test Agencies and the Standing Test, Assessment, and Rehearsal Team (START) completed cybersecurity assessments during eight CCMD exercises, two Service exercises, and three assessments of operational sites. The START is the inclusive term for DOT&E partnerships with organizations and individuals who possess unique skills and experience across the cybersecurity, cyber range, and operational test domains. DOT&E used the START in FY15 to plan and conduct cyber assessments in USPACOM, to jump-start the testing of programmable logic controllers, to plan and conduct tests of offensive cyber capabilities, and develop and conduct cyber range events.

To ensure operational realism and standardization of assessments, in FY15, DOT&E also published an Assessment Handbook that outlines procedures; identifies required data elements; and states expectations for the planning, conduct, and reporting of cybersecurity assessments.

Cyber Assessment Master Plan (CAMP)

The Cyber Assessment Master Plan (CAMP) is a 3-year plan that identifies a CCMD's priority missions and specifies when the CCMD plans to assess those missions in a contested cyber environment. CAMPs are signed by CCMD and DOT&E leadership to focus resources and planning of assessments that will meet the requirements of the DOD cyber strategy. For each mission identified in the CAMP, DOT&E will plan a TCRC that will include multiple building block events that lead to a stressing capstone event for the mission to be assessed. A TCRC may span multiple years until the CCMD has demonstrated the TCRC mission will be effective when stressed by an advanced cyber adversary, and that key supporting networks and systems are sufficiently secure or resilient. In FY15, DOT&E began development of CAMPs with USPACOM, USEUCOM, and USNORTHCOM.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY15		
EVENT TYPE	**SYSTEM OR EXERCISE AUTHORITY**	
CVPA and AA	DOD Automated Biometric Information System	F-35 Lightning II Joint Strike Fighter
	Aegis Weapons System	Integrated Personnel and Pay System - Army
	Aegis Ballistic Missile Defense	Joint Warning and Reporting Network
	Air Force Distributed Common Ground System	KC-46 Pegasus – Tanker Replacement Program
	Consolidated Afloat Network and Enterprise Services	Littoral Combat Ship
	Defense Agencies Initiative	Logistics Modernization Program
	Distributed Common Ground System – Army	Mid-Tier Networking Vehicular Radio
	Defense Enterprise Accounting and Management System	MV-22 Osprey – Joint Advanced Vertical Lift Aircraft
	Defense Medical Information Exchange	Pueblo Chemical-Agent Destruction Pilot Plant
	Department of Navy Large Aircraft Infrared Countermeasures	XM1156 Precision Guidance Kit
	Defense Readiness Reporting System	AN/TPQ-53 Radar System
	F-22 – RAPTOR Advanced Tactical Fighter	Surface Electronic Warfare Improvement Program
	Global Combat Support System – Army	RQ-21A Small Tactical Unmanned Aerial System
	Global Combat Support System – Joint	Surveillance Towed Array Sensor System Low Frequency Active
	Guided Multiple Launch Rocket System – Alternative Warhead	Theater Medical Information Program –Joint
	MQ-1C Gray Eagle Unmanned Aircraft System	Space Classified Program
	Integrated Electronic Health Record	
Exercise Assessment	U.S. Africa Command Judicious Response 2015	U.S. Special Operations Command Tempest Wind 2015
	U.S. Northern Command Vigilant Shield 2015	U.S. Strategic Command Global Lightning 2015
	U.S. European Command Austere Challenge 2015	U.S. Transportation Command Turbo Challenge 2015
	U.S. Pacific Command Pacific Sentry 2015	U.S. Army Warfighter 2015-4
	U.S. Southern Command Integrated Advance 2015	U.S. Navy USS *Harry S. Truman* Sustainment Exercise
Site Assessment	U.S. Central Command Air Forces Central Command	U.S. Forces Korea Headquarters and Osan Air Base
	U.S. Air Force 613 Air Operations Center	
CVPA – Cooperative Vulnerability and Penetration Assessment; AA – Adversarial Assessment		

Cyber Blue and Red Teams

DOD cyber teams include organizations that provide OPFOR aggressors (Red Teams) as well as penetration testers and teams that perform other cybersecurity assessments (Blue Teams). DOT&E guidance establishes data and reporting requirements for cyber team involvement in both operational tests of acquisition systems and exercise assessments.

The demand on DOD-certified Red Teams, which are the core of the cyber OPFOR teams, has increased significantly in the past 3 years. In the same timeframe, the Cyber Mission Force and private sector have hired away members of Red Teams, resulting in staffing shortfalls at a time when demand is likely to continue to increase. This trend must be reversed if the DOD is to retain the ability to effectively train and assess DOD systems and Service members against realistic cyber threats.

In FY15, the almost non-stop pace of events for all cyber teams challenged their ability to provide complete data sets and complete reports. Without these data and reports, network defenders and trainers will not have the critical inputs they need to develop effective mitigations or perform effective training on new procedures. DOT&E worked with the Cyber Red Teams to improve data collection and reporting efforts, and is examining new capabilities such as graphical free-form databases and automated collection tools intended to reduce the burden on the teams while providing the required information for analysis.

Persistent Cyber Opposing Force (PCO)

Red Teams or cyber OPFOR require authority, typically called "ground rules" or "rules of engagement," to operate on DOD networks and systems for operational tests and training exercises. The creation and staffing of separate ground rules for each event, network, and participating cyber Red Team is an administrative burden that has delayed cybersecurity operational tests and the start of activities in support of training exercises. The PCO is intended to help overcome these problems and enhance cybersecurity assessments.

The PCO is the DOT&E-sponsored collection of Cyber Red Teams that perform long-duration adversarial

activities in approved CCMD and Service theaters. These threat-representative activities are designed to make more efficient use of Red Team personnel, provide more realistic cybersecurity assessment opportunities throughout the year, and provide better training opportunities for the CCMDs and the Cyber Mission Force. DOT&E believes that such training throughout the year will improve CCMD defensive and offensive cyberspace operations and readiness to conduct critical missions.

The U.S. Army Threat Systems Management Office provides day-to-day management of PCO activities and helps ensure that operations are threat-representative and that reporting and data collection are to standard. USPACOM and USNORTHCOM have established Standing Ground Rules that allow for PCO activities in their theaters.

In addition to ongoing assessment activities in FY15, the PCO supported cybersecurity operational tests of acquisition programs, and an Office of Cost Assessment and Program Evaluation study. The PCO provided this support in less time than a traditional Red Team could have due to the continual reconnaissance and network accesses that had already been authorized and established. This approach reduced the workload for Red Teams that are in high demand. During FY15, the PCO, operating outside of a formal test or exercise period, also identified an important vulnerability in networks supporting USPACOM. The PCO provided network authorities the technical details and operational implications of the vulnerability, worked with those authorities to identify solutions, and verified the vulnerability had been resolved in subsequent observations.

The PCO provides frequent and detailed reporting on PCO operations and identified vulnerabilities, and works with network authorities and CPTs to identify and implement solutions or mitigations. The PCO will verify the solutions or mitigations have been effectively implemented during follow-on operations. DOT&E has urged the leadership at other CCMDs to establish Standing Ground Rules to enable PCO operations in their theaters.

Advanced Cyber OPFOR (ACO)

The tool and skill sets of the Cyber Red Teams are not keeping pace with state-of-the-art, nation-state threats, and their operations tempo provides little time for operators to gain expertise with new tools or to learn exploits against non-standard systems. Furthermore, it is difficult for them to obtain advanced cyber tools through normal procurement processes.

DOT&E created the Advanced Cyber OPFOR (ACO) concept to augment DOD Red Teams and the PCO with advanced capabilities our cyber adversaries likely possess. The ACO enables developers of advanced cyber capabilities and practitioners of advanced techniques to assist in planning and execution of PCO operations. For example, during one FY15 exercise, the ACO provided capabilities from two developers to enable the PCO to traverse defensive infrastructure, which had been impeding PCO network attacks. The ACO assist was warranted because network defenses improved, previous exploits from the public domain no longer worked, and the intelligence community assessed the representative adversary to possess more advanced tools and techniques. DOT&E will employ the ACO routinely during FY16 in support of the PCO in similar situations.

Cyber Threat Assessments

DOT&E remains engaged with key intelligence agencies to ensure the latest cyber intelligence is incorporated into the planning for operational tests and cybersecurity assessments. The Defense Intelligence Agency's Exercise Support Team provides cyber adversary threat assessments, writes realistic cyber scenarios to support CCMD exercises, and provides the cyber threat lead during these exercises.

As network defenses continue to improve, the Intelligence Community will need to credit advanced cyber adversaries with capabilities that have not been observed in employment, but which are known to exist. Additionally, the Intelligence Community will need to improve the characterization of adversary cyber actions, which are expected during wartime. An adversary may reasonably limit cyber activities to development of accesses and exfiltration of information during peacetime, but more aggressive cyber activities may be expected when major combat platforms are committed and force-on-force operations are underway.

Testing of Industrial Control Systems

DOT&E is preparing to assess acquisition programs that employ commercial industrial control systems. DOT&E commissioned testing of four common industrial control systems with the help of Sandia National Labs, Pacific Northwest National Labs, and the Johns Hopkins University Applied Physics Lab. When complete, DOT&E will use the results from these tests to recommend test procedures, and will provide the results to programs to support development of mitigation strategies for discovered cyber vulnerabilities. DOT&E will also make the test environments and virtual instantiations available to the Cyber Mission Force and supporting cyber ranges.

DOD Cyber Strategy

DOT&E is participating in three Lines of Effort from the DOD Cyber Strategy:

- Exercise Assessments. In coordination with the Joint Staff, DOT&E will assess the ability of CCMDs to sustain critical missions in a cyber-contested environment. Activities led by DOT&E such as the PCO and CAMP development (discussed above) will assist in providing assessment opportunities and results.
- Computer Network Defense Metrics and Evaluation. Most systems rely on the host network or environment for cybersecurity protection. Additionally, in most cases, the Cybersecurity Defense Service Providers (CDSP) assumes the majority of key cyber defensive responsibilities and tasks. Therefore, measuring the effectiveness of CDSP capabilities is essential to evaluating the cybersecurity posture of every system. To that end, DOT&E will participate in the development of metrics and test methods to measure CDSP performance.

- Red Team Oversight. DOT&E, in coordination with the Chairman, Joint Chiefs of Staff, will establish an oversight system of all DOD Cyber Red Teams; these include opposing force aggressors, cyber system penetration testers, and teams that perform operational cybersecurity assessments. The demand for Cyber Red Teams in all three of these primary roles has grown over the past several years, and DOT&E projects the demand will continue to grow. This effort will help ensure that cyber Red Teams are resourced, organized, trained, and equipped to effectively meet the increasing mission requirements.

Cyber Protection Team (CPT) Training and Experimentation

DOT&E, in partnership with USCYBERCOM J7, conducted a pilot Collective Team Training course for CPTs from April 13 through May 19, 2015, at Camp Dawson, West Virginia. Participants included three, 15-man Quick Reaction Force (QRF) cyber teams from both Army and Navy CPT units. Students were initially trained in four functional cyber defensive groups (Harden, Monitor, Coordinate, and Pursue) and then brought together into a QRF team construct. DOT&E evaluated the performance of the three QRF teams during force-on-force cyber engagements designed to simulate typical CPT mission deployments.

DOT&E conducted a follow-up CPT Performance Assessment Experiment in July and August 2015 to compare performance of CPTs that received collective team training with CPTs that had no team training. Emerging results indicate CPTs that received team training performed significantly better than those without training. DOT&E also observed that some individuals assigned to CPTs do not possess the proper training, background, or motivation to become effective CPT members. DOT&E acquired and enhanced survey tools that can help determine individual suitability for CPTs, and offered these tools to USCYBERCOM and Service cyber components.

DOT&E will provide the aggregated results to USCYBERCOM and the Service cyber components to help inform decisions regarding future CPT training. DOT&E expects that significant time on realistic ranges will be instrumental to CPTs attaining an effective operational capability. This effort also demonstrated that an unclassified range has cost, schedule, and availability advantages over a classified range for a subset of CPT training needs.

Cyber Ranges

The DOD Enterprise Cyber Range Environment is a collection of four independent cyber range assets where classified training and testing can occur. In 2011, these ranges were experiencing budget cuts and were becoming unsustainable. DOT&E proposed critical enhancements for these cyber ranges and the establishment of an EA in 2012; additional funding was programmed in the FY13 Program Review, but there was no decision for an EA.

The FY15 NDAA directed DOD to establish an EA for cyber training ranges and an EA for cyber testing ranges; the NDAA does not preclude the EAs from being a single entity. As combined testing and training are mandatory for the ranges' efficient use, and more importantly for keeping pace with the rapidly evolving cyber threats, the creation of two separate EAs—with separate responsibilities and incentives—would make it difficult to continue to conduct combined activities in a timely manner. Despite this, the Department appears to be on a path to create two separate EAs. This will likely hinder the Department's ability to respond to rapidly evolving and increasingly sophisticated cyber threats. In order to provide the optimal cyber range posture for the DOD, a single EA should be designated for cyber ranges with the authority to oversee funding and personnel for all DOD-owned cyber ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate.

Observations

In FY15, cybersecurity assessment teams consistently identified vulnerabilities which place DOD missions at high risk from cyber compromise, exploitation, and disruption. Although mission impacts are not always permitted during exercises, DOT&E assesses the likelihood and magnitude of impacts to missions based on accesses achieved by the Cyber OPFOR. In many cases, DOT&E has assessed that catastrophic kinetic impacts could be enabled by the information the Cyber OPFOR has accessed.

The limitations imposed upon the Cyber OPFOR by exercise authorities continue to reduce the value of both cybersecurity assessments and training of the Service member and network defenders. Exercise authorities for several CCMDs are working with DOT&E and assessment teams to identify or develop better venues in which cyber effects can be demonstrated to stress networks, defenses, and missions. In light of well-publicized intrusions into U.S. Government networks this fiscal year, exercise authorities should move aggressively to maximize training in realistic cyber-threat environments.

DOT&E observed a continued increase in the participation of CDSPs during FY15 exercises, and also noted growing involvement by CPTs. Although local network defenders, CDSPs, and CPTs need to work to optimize their combined efforts, DOT&E has observed that some cyber attacks were less effective in FY15 than in previous years. The following paragraphs discuss protective measures and reactive capabilities that were observed in FY15.

Protective Cyber Defense – Hindering Attacks. The first line of cyber defenses involves configuring networks and systems to prevent or hinder access by unauthorized parties. In FY15, assessment teams continued to find problems with software configuration and outdated patches, but also confirmed that networks with up-to-date patches and configuration best-practices noticeably hindered the Cyber OPFOR from gaining network access. Assessment teams also reported that successful attacks tended to exploit common information infrastructure via stolen or default credentials, and services such as email, SharePoint, and web portals.

Compared to previous years, assessment teams observed an increasing number of events where protective defenses thwarted lower-capability attacks. Phishing attacks were less successful in networks where email links to internet addresses were disabled; another reason for improvements is likely the heightened awareness and focused training that followed the publicized intrusions on U.S. Government networks.

Network defenders and CCMDs should continue to improve their defensive posture and recognize that more advanced threat capabilities exist. DOT&E is working with the PCO to develop more advanced tools and techniques that are representative of advanced adversary capabilities, which will begin to be employed during FY16 assessments.

Reactive Defense – Responding to Attacks. Reactive defense involves the detection and response to cyber adversaries that have penetrated the protective defenses and are operating within the networks and systems. Defenders typically rely on detecting the signatures of known exploits, noticing unusual activities, or responding to the effects of an attack after it occurs. In one exercise example, defenders identified an intrusion and conducted a coordinated response to shut down a Cyber OPFOR access point. The actions were effective against the original access point, but not sufficiently timely as the cyber OPFOR had already maneuvered to another foothold.

Early detections are critical to reduce the adversary's opportunity to obtain additional network privileges and move to additional network footholds. In another exercise, the assessment team observed effective and timely collaboration across operators and network defenders: an operator noticed an unusual change to a situational-awareness data display, reported the discovery while correcting the errors, and rapidly notified the network defenders who were able to thwart the cyber attack.

DOT&E engaged extensively with CPTs in FY15, developing a better understanding of their mission, how they will support network defense, and metrics for assessment of their performance. DOT&E also began assessment of CCMD processes associated with supporting offensive cyber operations.

Key Findings

CCMDs need an integrated and reactive cyber defense that supplements proper configurations, up-to-date software, and signature-based tools. In order to be effective against an advanced persistent threat, CCMDs will need to be supported by:

- Improved detection of non-signature-based activities such as exfiltration and unauthorized authenticated access
- Accurate cyber situational awareness and timely reporting to enable correlation of information to identify trends and attacks
- Effective response capabilities and playbooks to quickly upgrade defenses via local defenders, CDSPs, or CPTs
- Timely response actions by counter-cyber elements of the Cyber Mission Force

In the course of both operational tests and exercise or site assessments, the assessing organizations often identify vulnerabilities, practices (good and bad), and tools that may have enterprise implications and merit senior leadership review and action. For these vulnerabilities and enhancements, DOT&E publishes finding memoranda to the DOD entities best able to address the situation. In FY15, DOT&E initiated or published research on the following topics:

- Host Based Security System – DOT&E identified newly found shortfalls in the use of this enterprise-wide tool. The Defense Information Systems Agency (DISA) has acknowledged and addressed these findings.
- Special Handling Documents – DOT&E identified shortfalls in the procedures for electronically transmitting special-handling documents. The Joint Staff and Undersecretary of Defense for Policy have acknowledged and addressed these findings.
- Shipboard Tactical Systems – DOT&E identified vulnerabilities with the tactical datalinks supporting afloat platforms. The Navy has acknowledged and addressed these findings.
- Java Beans Open Systems Software – DOT&E identified a number of common vulnerabilities in this widely used software platform. The DOD CIO and DISA are reviewing solutions.
- Industrial Control Systems – DOT&E identified common vulnerabilities in key components of these systems. The Joint Staff, DOD CIO, DISA, and the Services are investigating solutions to the issues identified. DOT&E is sharing test data with the Office of Naval Research on new technology developments related to protecting key control system components.
- Information Condition (INFOCON) Guidance – DOT&E is researching contradictory or incomplete guidance for implementing INFOCON changes that reflect heightened cybersecurity states based on detected or anticipated cyber-adversary actions.
- Cyber tools – DOT&E is researching problems found with the use of Kerberos authentication, the availability of PowerShell utilities, and the effectiveness of software whitelisting and management tools such as AppLocker and Bit9.

Future Assessments

DOT&E plans to focus its FY16 assessment resources on those CCMDs who are willing to permit realistic cyber effects during major exercises and commit to the development of CAMPs and TCRCs. Table 2 provides a list of currently planned FY16 assessments.

TABLE 2. PLANNED CYBERSECURITY ASSESSMENTS IN FY16		
EVENT TYPE	**SYSTEM OR EXERCISE AUTHORITY**	
Exercise Assessment	U.S. Africa Command Epic Guardian 2016	U.S. Pacific Command Pacific Sentry 2016
	U.S. Air Force Red Flag 16-3	U.S. Southern Command PANAMAX 2016
	U.S. European Command Jackal Stone 2016	U.S. Special Operations Command Jackal Stone 2016
	U.S. Cyber Command Cyber Flag/Cyber Guard 2016	U.S. Strategic Command Global Lightning 2016
	U.S. Northern Command Vigilant Shield 2016	U.S. Strategic Command Global Thunder 2016
	U.S. Navy Valiant Shield 16	U.S. Transportation Command Turbo Challenge 2016
Site Assessment	U.S. Central Command Marine Corps Central Command	
	U.S. Marine Corps – II Marine Expeditionary Force Large Scale Exercise	
	U.S. Southern Command – Joint Task Force-Guantanamo	