Cybersecurity

SUMMARY

DOT&E provides cybersecurity evaluations of DOD acquisition programs as part of the programs' operational test and evaluation. In addition, Congress directed DOT&E to perform cybersecurity assessments of live, operational DOD networks and systems during Combatant Command (CCMD) and Service training exercises. This report includes results from FY16 assessments, but pays particular attention to the trends and changes that have occurred since 2009, when DOT&E updated and improved the requirements and procedures for cybersecurity test and evaluation. Key observations follow, and additional details are in the classified cybersecurity report DOT&E issued in July 2016:

- Over the last 7 years, the Department has increased its focus on cybersecurity, and allocated additional resources to cyber capabilities, expertise, and associated activities. As a result, in recent years some DOD programs and networks have demonstrated, for the first time, effective defenses against attacks from cyber Red Teams emulating threats with limited cyber capabilities. In recent years, DOT&E's cybersecurity assessment program has helped CCMDs address major cybersecurity vulnerabilities through its focus on finding vulnerabilities, helping the CCMD to fix the vulnerabilities, and independently verifying that the vulnerabilities have indeed been fixed. This "find-fix-verify" approach has proven to be an effective way to rapidly improve the cybersecurity of DOD programs and networks.
- Despite this progress, during major exercises critical CCMD missions remain at risk when subjected to cyber-attacks emulating an advanced nation-state adversary. Cyber-attacks are clearly a part of modern warfare, and DOD networks are constantly under attack. However, DOD personnel too often treat network defense as an administrative function, not a warfighting capability. Until this paradigm changes, and the change is reflected in the Department's approach to cybersecurity personnel, resource allocation, training, accountability, and program and network management, the Department will continue to struggle to adequately defend its systems and networks from advanced cyber-attacks.
- DOT&E issued more explicit policy and guidance regarding cybersecurity testing over the past 7 years, resulting in a significant increase in the cybersecurity component of OT&E for major programs. Most operational tests have found significant vulnerabilities and limitations in the system's ability to sustain missions or rapidly restore capabilities when compromised.
- Over the past 7 years, Red Team operators have become high-demand, low-density assets, and requests for Red Team services increasingly go unsatisfied. DOD had an enviable share of master-level operators 7 years ago, but a significant number of these cyber experts accepted positions in the private sector in the ensuing years, often because of the increased wages and more relaxed work environment. Simultaneously, demand within DOD for Red Team services has more than doubled. The new congressional requirement to conduct cybersecurity assessments of all major DOD programs (Section 1647 of the FY16 NDAA) will increase further the demand on DOD Red Teams. Additionally, Red Team capabilities and expertise must increase so that the teams can emulate more advanced and realistic adversaries during testing and training.
- Over the last 3 years, DOT&E refined and expanded the use of long-duration cyber Red Teaming in CCMD networks, including U.S. Pacific Command (USPACOM) and U.S. Northern Command (USNORTHCOM). Such long-duration Red Teaming, conducted by a Persistent Cyber Opposing Force (PCO), is far better at emulating advanced, persistent nation-state cyber threats, while at the same time more efficiently utilizing scarce Red Team resources. PCO activities have identified, and rapidly addressed, serious vulnerabilities that had not previously been discovered during more than a decade of short-duration, less realistic exercise events.
- To effectively fight a war in cyberspace, the focus of cyber defense needs to expand beyond the traditional approaches of system protection and intrusion detection to encompass a broader view of system resilience. DOD has focused a great deal of attention and resources on the defense of outward-facing boundaries. As a result, these boundaries have shown significant improvement in protecting against nascent- and limited-level attacks. However, Red Teams emulating a moderate-level adversary – or below – routinely demonstrate the ability to intrude DOD networks and operate undetected within DOD networks for extended periods of time. The Department needs to put more emphasis on preventing lateral movement by network intruders and improved detection of anomalous network activity.
- In recent years, CCMDs and Services have provided better opportunities for DOT&E-sponsored assessments to inject limited cyber-attacks and observe the resulting effects and responses. However, exercise and network authorities seldom allow fully representative cyber-attacks, and complete assessments of protection, detection, and response capabilities.
- Cyber ranges can be effective venues to fully evaluate realistic cyber-attacks and defenses in a safe and secure environment, without any risk to DOD operations and missions. Cyber ranges may be the only acceptable environment where Red Teams can fully execute attacks representative of an advanced nation-state cyber adversary. Over the last 7 years, DOD has matured its cyber range capabilities, but existing ranges will not be able to fully support the anticipated near-term requirements, including: needed training for the Cyber Mission Forces (CMF), more realistic CCMD and Service exercises and assessments, and rapidly increasing acquisition

program cyber testing requirements. Recent investments in the Persistent Training Environment and Cyber Test Ranges should help remedy these shortfalls, but improvements are likely to remain sub-optimized due to lack of a single Executive Agent for cyber ranges.

- While some Cyber Protection Team (CPT) elements have successfully defended DOD networks during our assessments, many of the 68 CPTs have not received adequate training or equipment to provide effective and timely support to defend networks and critical missions. The initial staffing of the CPT included personnel without the requisite skills and training, and with many current CPT members scheduled to depart in the next year, DOD needs to focus on attracting, training, and retaining skilled individuals for the CPT. DOT&E has provided excellent training opportunities for CPT members during our assessments, and we plan to work with U.S. Cyber Command (USCYBERCOM) to identify more opportunities to do so in the future.
- Over the last 7 years, CCMDs have become increasingly interested in Offensive Cyber Operations (OCO) capabilities. However, CCMDs often have little confidence in available OCO capabilities because the OCO developers have not tested the capabilities in a realistic environment. DOT&E sponsored several test events in FY16 to demonstrate that more realistic testing of OCO capabilities can be both expeditious and low-cost. These events demonstrated that realistic testing of OCO can reveal significant operational problems which do not surface during limited lab testing. The OCO developers can then address these problems to make the capability more likely to succeed when it is deployed. Realistic OCO testing also enabled DOT&E to provide CCMDs with an improved understanding of the scope and duration of OCO effects.
- In recent operational tests, DOT&E has frequently encountered two components that are prevalent across many DOD acquisition programs: Programmable Logic Controllers (PLC), and Cross-Domain Solutions (CDSs). These components can introduce cyber vulnerabilities to the system under test and the associated network(s). DOT&E provided guidance in 2015 and 2016 for testing industrial control systems that contain PLCs and CDSs. DOT&E also sponsored testing to help identify vulnerabilities, potential mitigation strategies, and rigorous methods for testing these components.

Table 1 below shows the operational tests involving cybersecurity, and the DOT&E-funded cybersecurity assessments conducted during FY16. Table 2 shows the cybersecurity test organizations that supported the conduct of the activities shown in Table 1.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY16		
EVENT TYPE	**SYSTEM OR ORGANIZATION**	
Cybersecurity Operational Test	Automated Biometric Information System	F-35 Joint Strike Fighter – Central Point of Entry
	AC130-J Ghostrider	F-35 Joint Strike Fighter – Squadron Kit
	Aegis Ashore	Joint Stand-Off Weapon
	Advanced Field Artillery Tactical Data System	Joint Warning and Reporting Network
	Army Integrated Air and Missile Defense	Littoral Combat Ship
	Acoustic Rapid Commercial-off-the-Shelf Insertion	LHA 6 - America Class - Amphibious Assault Ship
	Airborne Warning and Control System	MQ-9 Reaper
	Aegis Weapons System	Mobile User Objective System
	Common Aviation Command and Control System	Next Generation Diagnostic System
	Consolidated Afloat Network and Enterprise Services	Network Integration Event
	CV-22 Osprey	Navy Advanced Extremely High Frequency Multi-band Term.
	Defense Agency Initiative	Near Real Time Identity Operations
	Distributed Common Ground System – Navy	Pueblo Chemical Agent Destruction Pilot Plant
	Defense Medical Information Exchange	Paladin Integrated Management
	E-2D Advanced Hawkeye	Public Key Infrastructure
	Expeditionary Sea Base	RQ-4 Global Hawk
	Global Broadcast Service	Space-Based Infrared System
	Global Command and Control System - Joint	Spider XM7 Network Command Munition
	High Mobility Artillery Rocket System	Theater Medical Information Program – Joint
	F-35 Joint Strike Fighter – Air Vehicle	Warfighter Information Network – Tactical
	F-35 Joint Strike Fighter – Autonomic Logistics Operating Unit	
Exercise Assessments	U.S. Africa Command Epic Guardian 2016	U.S. Special Operations Command Jackal Stone 2016
	U.S. Central Command Marine Forces Central	USMC Large Scale Exercise 2016
	U.S. European Command Jackal Stone 2016	U.S. Strategic Command Global Thunder 2016
	U.S. Pacific Command Pacific Sentry 2016	U.S. Strategic Command Global Lightning 2016
	U.S. Southern Command PANAMAX 2016	U.S. Navy Valiant Shield 2016
Cyber Readiness Campaigns	U.S. Northern Command	
	U.S. Pacific Command	

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 Corp 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 and Lethality Analysis Division
Navy	Navy Information Operations Command
	Space and Naval Warfare Systems Command
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Information Assurance Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Risk Management Executive Red Team

RECOMMENDATIONS

- The Combatant Commands and Services should reduce restrictions that prevent testing and training against realistic cyber threats, and perform "fight-through" events to demonstrate that their critical missions are resilient in contested cyber environments.
- The Joint Staff should sponsor a cyber-focused exercise with a different CCMD each year, where cyber training and mission resiliency are the primary training objectives.
- The Services should upgrade their cyber Red Teams with additional capacity, capabilities, training, and threat assessments to ensure that the certified Red Teams can portray relevant and representative adversaries, including advanced nation-state threats.
- The DOD Chief Information Officer and USCYBERCOM should issue policy and instructions to require implementation of the following as soon as possible; vulnerabilities in these areas often jeopardize CCMD and acquisition program missions during cybersecurity assessments and operational tests:
  - Secure credential use and storage
  - Segregation of network privileges, to include role-based allocation of privileged accounts and responsibilities, and network segmentation based on the segments' mission criticality
  - Reduction of cross-connections between networks, and effective, active defense of cross-connections which cannot be eliminated
  - Encryption of data at rest and in transit
  - Centralized logging and audit log correlation to enable rapid detection and tracking of threats inside a system or network
  - Effective anomalous behavior detection, and cyber-attack response tactics and procedures for attacks inside the system or network, as well as at the system/network boundary
  - A consolidated reporting and analysis tool for cyber incidents
  - Locking down SharePoint websites based on "need-to-know"
  - Authentication and verification procedures for chat room participants
- The Joint Staff and USD(AT&L) should require systems and networks to support essential missions even when compromised, and cyber defenders should be able to quickly reset and restore systems and networks following a successful cyber-attack.
- DOD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel

for all DOD-funded ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate. The leadership for the Persistent Training Environment and the Cyber Test Range should collaborate to identify priority requirements for range environments in support of testing, training, as well as CCMD and Service exercise assessments.
- DOD should field new cyber capabilities (e.g., Joint Regional Security Stacks, OCO capabilities) only after realistic operational testing confirms the capabilities will be effective and suitable for use by representative users.
- CCMDs and Services should routinely conduct long-duration cyber assessments using a PCO, to enable more threat-representative cyber Red Team activities on DOD networks and to more rapidly discover and address critical cyber vulnerabilities.
- USCYBERCOM, the Services, and Defense Information Systems Agency should conduct "hands-on" training in realistic networks using realistic cyber threats, and effective tools and procedures, for Cyber Mission Force (CMF) personnel and Cybersecurity Service Providers.
- USD(AT&L) and DOD CIO should sponsor the development of test tools and procedures for evaluating cybersecurity in non-Internet Protocol applications, including CDSs, PLCs, system-unique data buses and protocols, radio and acoustic frequencies, and tactical datalinks.

EVOLVING GUIDANCE AND TEST/ASSESSMENT TRENDS

In FY03, the Congress directed DOT&E to perform annual operational evaluations of information assurance with each of the CCMDs and Services; develop a process to similarly consider systems on the DOT&E oversight list; and report to Congress on the Information Assurance (IA) posture of the DOD. DOT&E has performed the required assessments annually since that time, and has in recent years issued and enforced new policy for cybersecurity OT&E.

Early assessments were generally network-focused, with extensive limitations on the supporting Red Teams. Today DOT&E observes fewer limits and restrictions on cybersecurity testing and assessments, but actual impacts to networks and systems are still limited due to safety, security, or other training requirements. The result is that warfighters generally train and conduct cyber assessments in a relatively benign cyber environment.

DOT&E issued the first guidance on cybersecurity requirements for OT&E in 2009, establishing requirements and procedures for testing cybersecurity. Over the past 7 years, that focus has expanded from information-handling systems to encompass a variety of weapons and weapons platforms, and the missions they support.

In 2011, ADM Mullen, the CJCS, issued an Execute Order (EXORD) that directed all CCMDs perform threat-representative assessments of critical CCMD missions in cyber-contested environments within a 3-year period. This EXORD charged exercise authorities and CCMD leadership to conduct major training exercises in a non-benign cyber environment. Exercise authorities now expected cyber Red Teams to participate during exercises, but CCMDs did not consider cyber to be a training objective, and hence cyber activities were severely limited. The Secretary of Defense Leon Panetta re-emphasized the CJCS EXORD in 2012, but this emphasis was soon diluted due to the downsizing and cancelation of exercises due to sequestration.

In 2013, DOT&E and USPACOM agreed that the Department needed to break from the notion that cyber training and assessment performed once a year was acceptable. As a result, DOT&E developed a new approach that includes multiple building-block events in a given year – a Cyber Readiness Campaign – that leads to a culminating event (e.g., a full CCMD exercise), and employs a PCO to emulate a realistic nation-state cyber adversary.

In 2013, USCYBERCOM created the Cyber Mission Force (CMF), consisting of 133 teams. USCYBERCOM and the Services did not have mature plans for training and equipping the CMF. This became evident during DOT&E-sponsored cyber assessments when CCMDs requested Cyber Protection Team (CPT) support, and CPTs were often slow to deploy and unable to provide much support when they arrived. This is still the case for many of the CPTs; however, more recently, DOT&E observed several instances where the CPTs working with hunt teams performed well in detecting and responding to Red Team intrusions. DOT&E will continue to encourage participation of CPT personnel in DOT&E-sponsored Cyber Readiness Campaigns and cybersecurity assessments, where CPTs receive much-needed "hands-on" network training while defending against a realistic cyber adversary.

Concerned with the lack of cybersecurity guidance for acquisition programs, in 2014 DOT&E recommended that the Department develop a cybersecurity requirement. In response, in November 2014 the Deputy Secretary directed the Joint Staff to develop such a requirement within 90 days. Over the past 2 years, the Joint Staff drafted a Cybersecurity Endorsement to the Survivability Key Performance Parameter. The Joint Staff also developed an implementation guide, which identifies a number of key attributes pertaining to cybersecurity that the Services must address in the requirements documentation for systems that handle digital data transfers. These attributes include the ability of the system to control access, reduce detectability, harden attack surfaces, encrypt data, detect anomalies, and recover from a cybersecurity incident. Although the cybersecurity endorsement has been in a draft form for months, the JROC has not yet formally approved and issued it.

In 2015, Secretary Carter issued the DOD Cyber Strategy. This coincided with a number of well-publicized cyber-attacks of government and private organizations, including the breach of

the Office of Personnel Management records involving millions of federal personnel. These cyber-attacks helped DOD senior leadership understand the importance of cybersecurity and created opportunities for DOT&E to portray more realistic cyber adversaries during operational tests and exercises.

Despite progress, operational test and exercise planners need to encourage the use of realistic cyber actions that could require restoration of systems or implementation of alternative means of operations. The reluctance to permit debilitating cyber-attacks is appropriate when there are personnel safety concerns, but the DOD needs to routinely assess the ability of missions and systems to either operate through cyber-attacks or restore operations afterwards. Training in a benign environment is not acceptable in any other warfighting domain, nor should it be for cyber.

The DOD should continue to lessen restrictions that prevent testing and training against realistic cyber threats in order to improve the resistance and resilience of mission and systems under conditions that increasingly are part of the daily operational environment.

PROGRESS AND CHALLENGES

Cyber Defenses Continue to Lag Cyber Threats

Over the last 7 years, DOT&E observed and reported on the gradual improvement of defensive capabilities within the Department. The levels of compliance with key cybersecurity practices and controls improved steadily for several years, and test events show that the majority of DOT&E-assessed systems and networks meet key cybersecurity compliance criteria. Nonetheless, DOD cyber Red Teams continue to compromise DOD systems and networks and jeopardize critical DOD missions during exercises. This is because mere compliance with cybersecurity controls is not enough to provide an effective cyber defense. An effective cyber defense requires well-trained, well-equipped cyber defenders, operating in a secure network environment, in conjunction with other warfighters, to maintain critical missions.

Focus Shift to Cyber Resilience: "Assume Breach"

Most cyber defense tools and systems focus on hardening network and system boundaries. When network configurations are up to standard and patches are current, DOD networks can usually withstand cyber-attacks from Red Teams using limited cyber-attack capabilities. Over the past 7 years, the DOD has hardened many of its networks and systems against cyber-attacks by more rapidly installing security patches and improving the security of credentials (such as passwords). This has helped prevent Red Teams using novice techniques from penetrating network and system boundary defenses and disrupting missions during exercises. However, Red Teams using more advanced techniques continue to demonstrate the ability to bypass boundary protections, intrude into DOD networks, and operate undetected for extended periods.

Once they have gained access to a network, Red Teams frequently use tools native to the network and stolen credentials. These two tactics seriously challenge defenders, as they do not currently have sensors or tools to determine that an adversary is using tools or credentials approved for that network; in order to identify an adversary presence, they must detect some anomalous activity or behavior. Anomalous behavior detection is a critical element of cybersecurity, but few DOD cyber defenders have the tools needed to accomplish this.

Coordination and communication among the many agencies and activities charged with providing cyber defenses is often inefficient or ineffective. This lack of coordination contributed to missed opportunities to detect Red Team activities.

DOD should prepare for potential adversaries who may employ advanced capabilities and techniques by developing "fight-through" capabilities. CCMDs and Services should perform frequent training in cyber-contested environments that emphasizes well-coordinated cyber responses, the ability to reset or restore networks and systems to operation following an attack, and the ability of the warfighter to complete assigned missions while under cyber-attack.

Maturing the 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 enhancements for these cyber ranges and the establishment of an Executive Agent in 2012; as a result, the cyber ranges received additional funding during the FY13 Program Review, but there was no decision for an Executive Agent.

The FY15 NDAA directed DOD to establish an Executive Agent for cyber training ranges and an Executive Agent for cyber testing ranges. In FY16, the DOD allocated funds separately for a Persistent Training Environment, and for cyber test ranges. As combined testing and training are necessary for efficient use of the ranges, and to help address the rapidly increasing demand for cyber range resources, the creation of two separate Executive Agents—with separate responsibilities and funding—may hinder the Department's ability to effectively respond to rapidly evolving and increasingly sophisticated cyber threats. The DOD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel for all DOD-funded ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate.

Over the past 2 years, the Test Resources Management Center (TRMC) delivered multiple Regional Service Delivery Points (RSDPs) to key geographical locations, including USPACOM and MIT Lincoln Labs. RSDPs bring cyber range capabilities to local users to permit cost effective testing and training, and they provide a variety of capabilities (instrumentation, traffic

generation, environments, etc.) on the local "mini cloud" to reduce the bandwidth requirements for distributed range events. The TRMC also upgraded the National Cyber Range (NCR), and plans to build additional NCR facilities to help meet the rapidly growing demand for cyber test and training resources.

Assisted by DOT&E funding, over the last few years several of the National Labs demonstrated advances in the creation of realistic range environments, including environments that can be quickly built and deployed to an RSDP, the NCR, or other suitable range locations to support testing, training, and CCMD assessments that are not suitable for operational networks. DOD needs more of these environments to adequately test and train against advanced cyber threats.

Joint Information Environment Testing Shortfalls

In 2013, the Chairman of the Joint Chiefs of Staff signed a white paper entitled "Joint Information Environment" identifying "IT efficiencies" as a key goal. This white paper proposed a "shared Information Technology (IT) infrastructure with a common set of enterprise services, under a single security architecture." Subsequently, the DOD CIO established the Joint Information Environment (JIE) as a "concept." The DOD CIO intends all DOD networks to eventually conform to the JIE concept. Hence, the cybersecurity of the JIE concept is critical to the future security of the entire Department. Unfortunately, there is little evidence that JIE will improve cybersecurity, especially if Services field JIE components without adequate preparation in order to meet IT efficiency targets.

JIE is not a formal program of record, and it lacks a unified program executive to manage cost and schedule, monitor performance metrics, and plan and conduct testing. Furthermore, DISA and the Services are pursuing a non-traditional acquisition approach for major JIE components such as the Joint Regional Security Stack (JRSS), and both the Army and Air Force have fielded JRSS without conducting operational testing, despite developmental tests that showed cyber defenders could not use JRSS effectively to defend their network. See the JIE section elsewhere in this annual report for more details.

Although cyber defenders need improved tools to meet the evolving cyber threats, the DOD should not field tools such as JRSS until testing confirms that the tools are effective and usable by representative defenders.

Testing Offensive Cyber Capabilities

Combatant Commands are increasingly interested in Offensive Cyber Operations (OCO) capabilities either as a complement or as an alternative to traditional military capabilities. Factors that prevent CCMDs from adopting OCO capabilities into plans and operations include:

- Timelines for OCO approval that are unacceptably long;
- Waived testing or tests with limited operational realism, and;
- Lack of confirmed and well-characterized knowledge of OCO effects and potential risks.

OCO developers may waive tests because they consider testing as an unacceptable cost in terms of time and money. Waiving such tests occurs despite the fact that extended approval timelines for OCO result in part from the failure to conduct testing to rigorously characterize OCO effects and risks. What policy and guidance does exist for OCO capabilities emphasizes technical specifications, rather than the operational performance and suitability of the tool in a realistic environment. Many OCO capabilities undergo only limited testing, and seldom do any of these tests approach the rigor or realism of an operational test.

DOT&E sponsored several test events in FY16 for selected OCO capabilities at the request of Combatant Commands who had interest in advertised capabilities, but were unsure how much confidence to place in the scope and duration of the desired effects. These events demonstrated that testing of OCO capabilities can be both expeditious and low-cost. The test findings based on end-to-end employment with a cognitive cyber adversary differed greatly from the limited lab testing results. DOT&E-sponsored test results motivated improvements to OCO capability performance and reductions in undesirable second- and third-order effects.

OCO development and release authorities should conduct rigorous operational testing on OCO capabilities when the capabilities are complex and likely to be employed, and/or the risks of failure are unacceptable. DOD should take advantage of the recent advances in high-fidelity cyber ranges to perform more rigorous testing of OCO capabilities. OCO development teams should include test experts in the capability development phase to help validate requirements, focus performance metrics, and expedite a range environment that can support development, testing, and mission rehearsal.

DOT&E will continue to work with US Cyber Command, the Joint Staff, and the Services to enable rigorous OT&E of OCO capabilities. DOT&E will also stand up a cyber element within the Joint Technical Coordinating Group to perform subsequent analysis and reporting of test results to warfighters and DOD leadership.

PATH FORWARD FOR CYBERSECURITY TESTING

Improve Strategic Test Planning

DOT&E has reviewed over 800 documents related to cybersecurity OT&E in the last four years, including Test and Evaluation Master Plans, Operational Test Plans, Emerging Results, and test reports. DOT&E reviewed 240 of these documents in the last calendar year, supporting operational test and evaluation of over 100 systems.

While the quality of cybersecurity test planning continues to improve, program offices and operational test agencies need to place greater emphasis on the following areas in preparing test plans:

- Development and documentation of complete system architectures

- The means for testing non-Internet Protocol technologies
- A description of how cybersecurity tests will demonstrate active defense from attacks, measure the effectiveness of the cyber defenses, and assess the mission impacts resulting from cyber-attacks
- End-to-end testing, to include key subsystems, peripherals, and plug-ins
- Identification of resources (including cyber ranges) to be used for testing
- The role of cybersecurity service providers.

Similarly, test agencies and CCMDs require better master plans to improve the management and objectives of exercise assessments. An acquisition program's TEMP should include and describe the overall plan for cybersecurity test and evaluation. A Cyber Assessment Master Plan (CAMP) is a multi-year plan that identifies the strategic cybersecurity priorities for each CCMD or Service participating in the DOT&E Cybersecurity Assessment Program. CAMPs should focus assessment activities on critical missions that CCMDs must be able to sustain in contested cyber environments, and should motivate fight-through demonstrations in exercises or high-fidelity range events.

As the capabilities of cyber adversaries continue to grow, so must our ability to accurately portray and account for cyber threats in our OT&E and CCMD assessments. To achieve this we will work with the Combatant Commands and Services, and in particular USCYBERCOM, to develop long-term Standing Ground Rules that enable PCO activities. These standing agreements are key to the realistic threat portrayal of advanced adversaries, and offer efficiencies in the application of limited Red Team assets.

Meeting the Need for Cyber Red Teams

The DOD Cyber Strategy and DOT&E policy mandate that operational tests and exercise assessments include representative cyber-threat portrayal. Attainment of this mandate requires sufficient numbers of expert Cyber Red Team operators and supporting cyber planners to assist in the development and execution of operationally realistic cybersecurity tests, the planning and assessment of CCMD exercises and missions, and to support remediation efforts for identified vulnerabilities. The demand on DOD Cyber Red Teams has increased significantly in the past 3 years, and in the same timeframe, the private sector has hired away many members of Cyber Red Teams. As a result, Red Teams are unable to meet current DOD demand. This shortage has caused delays in cybersecurity operational testing, and reduced Red Team capabilities during some CCMD assessments. More critically, the personnel shortage has drastically increased the operational tempo of Red Team members, reducing their training opportunities to the extent that they are not able to keep pace with the tool and skill sets of advanced cyber adversaries. To address this critical situation, the Services should increase the hiring and retention of qualified Red Team personnel, and upgrade their Red Teams with new tools and training to ensure that their teams can portray advanced nation-state adversaries.

DOT&E has created two initiatives to mitigate the impact of Red Team personnel shortages and address the need for more advanced Cyber Red Team support. The PCO organizes existing DOD-certified Red Teams to support long-duration cyber activities that more closely resemble advanced persistent cyber adversaries. USPACOM and USNORTHCOM have signed Standing Ground Rules to implement the PCO construct to provide year-round cyber opposing force support for training and assessment events. The PCO has helped USPACOM find and remediate significant cyber vulnerabilities that might have otherwise gone undetected. Other Combatant Commands are developing agreements to permit PCO activities in their theaters, and DOT&E is coordinating with USCYBERCOM to develop the process and authorities for a global PCO.

DOT&E also created the Advanced Cyber OPFOR (ACO) concept to augment DOD Red Teams with more advanced nation-state capabilities. The ACO enables developers of advanced cyber capabilities and practitioners of advanced techniques to assist in planning and execution of PCO operations.

Testing Fielded Operational Systems

The cybersecurity posture of systems reflects aspects inherent to the system itself, but also aspects that reflect the surrounding operational environment, systems, and cyberspace. Operational testing of acquisition programs enables the evaluation of cybersecurity for systems in development, but fielding of the system following operational testing can result in changes to its cybersecurity posture.

Cybersecurity is a continuing and iterative process, but the DOD has no established mechanism for examining cybersecurity posture of systems following fielding. The DOT&E Cybersecurity Assessment Program examines fielded systems during CCMD and Service exercises, but most are headquarters command and control systems.

Congress recognized this cybersecurity shortfall with the FY16 NDAA Section 1647 language that directed USD AT&L to examine the cybersecurity posture of fielded systems. DOT&E is assisting this effort by providing access to all assessment results and partnerships, and identifying opportunities to conduct Section 1647 assessments in conjunction with CCMD and Service assessments and range events. To develop the Section 1647 assessment plans, the 1647 team used best practices DOT&E developed for cybersecurity operational testing and network assessments.

Resolving Legacy Problems

In conducting tests of already-fielded systems as well as new systems under acquisition oversight, DOT&E has encountered several classes of components (e.g., Programmable Logic Controllers (PLC), and Cross-Domain Solutions (CDS)), which could introduce cyber vulnerabilities to the system. Focused cybersecurity testing of such components will identify methods and analytical approaches to apply test results across multiple

acquisition programs and achieve potentially significant test efficiencies.

DOT&E provided guidance in 2015 and 2016 for testing industrial control systems that contain PLCs and CDSs. DOT&E also sponsored testing at Sandia National Laboratory, Pacific Northwest National Laboratory, and the MITRE Corporation to help identify rigorous methods for cyber testing these components, vulnerabilities, and potential mitigation strategies for developers and users of systems with these components.

Additionally, DOT&E provided guidance to the Operational Test Agencies regarding areas where cybersecurity OT&E should expand. These include:

- Non-Internet Protocol data buses and formats, to include the Military Standard 1553 bus, the Aeronautical Radio Standard 429, the Controller Area Network bus, and the 700 and 800-series avionics data buses
- Radio frequency, acoustic, radar data, and tactical datalink formats

TABLE 3. PLANNED CYBERSECURITY ASSESSMENT PROGRAM ASSESSMENTS IN FY17

EVENT TYPE	ORGANIZATION	
Exercise Assessments	U.S. Africa Command Judicious Response 2017	U.S. Pacific Command Pacific Sentry 2017
	U.S. European Command Austere Challenge 2017	USMC Large Scale Exercise 2017
Cyber Readiness Campaigns	U.S. Central Command	U.S Air Force Air Operations Centers (to be selected)
	U.S. Northern Command	U.S. Navy Amphibious Ready Group/Marine Expeditionary Group
	U.S. Southern Command	U.S. Army Reserve Command
	U.S. Special Operations Command	U.S. Army Civil Affairs Physiological Operations Command
	U.S. Strategic Command	White Sands Missile Range
	U.S. Transportation Command	