Cyber Assessments

SUMMARY

DOT&E-sponsored cyber assessments and cybersecurity operational tests in FY20 show that the Department of Defense (DOD) continues to evolve cyber defensive capabilities as well as the means to measure them. DOT&E's Cybersecurity Assessment Program (CAP) has been instrumental in helping warfighters develop defenses against advanced threats. However, development of effective capabilities remains slow and observations for this fiscal year confirm the conclusion from previous years: critical DOD missions remain at high risk of disruption from adversary cyber actions.

Despite coronavirus (COVID-19) pandemic restrictions, DOT&E continued OT&E oversight and CAP activities, although at a reduced pace, to provide insight on the DOD's cyber posture during FY20. The restrictions reduced the number of activities; however, there were still 36 OT&E events and 33 CAP assessment activities executed.

Some DOT&E-sponsored assessment activities continued without impact from COVID-19, most notably the Persistent Cyber Operations (PCO) activities run by the U.S. Army's Threat Systems Management Office (TSMO). TSMO teams continued assessment missions remotely for six Combatant Commands (CCMDs). They also performed several special assessments and acquisition-program testing, with emphasis on providing rapid feedback on identified vulnerabilities, and options to improve sensor configurations and network-defense procedures. The U.S. Air Force 177th Information Aggressor Squadron also provided critical support to PCO assessments during FY20. At the end of the fiscal year, the Missile Defense Agency approved expanded PCO activities for networks supporting Ballistic Missile Defense, and the Defense Information Systems Agency (DISA) approved PCO assessments for the DOD Information Network (DODIN). Plans are maturing to add PCO cells that will focus on Service networks.

DOT&E also supported special requests by U.S. Cyber Command, the DOD Chief Information Officer (CIO), and the Defense Threat Reduction Agency for rapid-response assessments of emerging capabilities and critical network components. Examples of these assessments included a prototype Zero-Trust Network, a concept that demonstrated the potential to markedly improve the security of the DOD's networks, and Nuclear Command and Control networks and systems. DOT&E also provided cyber expertise to assess the cybersecurity of essential technologies such as cloud services, aircraft safety and communications systems, and critical infrastructure.

DOT&E subject matter experts assisted with operational assessments of offensive cyber operations tools and procedures, developed specialized tools and techniques to assess non-internet protocol (IP) communication buses, and integrated cyber-centric intelligence. DOT&E initiatives such as PCO and the Advanced Cyber Operations (ACO) Team made top-notch cyber expertise available for rapid, on-demand assignment to assessment teams.

The operational pause caused by COVID-19 for other planned activities provided DOT&E the opportunity to review and improve CAP procedures and ensure the program can continue to address priority missions in an increasingly austere budget environment. These efforts will ensure CAP remains an extremely cost-effective program. CAP expenditures represent only about 3 percent of the annual DOD exercise program cost. Large exercises typically range from $8 Million to $18 Million to plan and execute, with CAP assessment activities generally costing between $400,000 to $800,000. These activities include the planning, execution, analyses, and reporting by the assessment team; support from Red Teams and in many cases from the PCO teams; and special support from a cyber threat-intelligence team. The return on this small investment is large; CAP activities ensure warfighters train as they will fight, in a realistic environment that includes cyberattacks. DOT&E assessment data show that commands that train routinely in cyber-contested environments provided by the CAP can better sustain their critical missions, with fewer losses, when under attack.

Over the life of the CAP program, assessment teams have assisted in bringing realistic cyber elements into 16 pre-deployment exercise certifications for major Army and Marine Corps forces during combat operations in Iraq and Afghanistan. They similarly supported 11 pre-deployment exercises and certifications for naval strike and amphibious groups. In the course of these and other assessments, DOT&E-sponsored assessment teams identified many vulnerabilities, and beyond the identification phase, helped remediate serious cybersecurity shortfalls in DOD systems and weapons platforms via 65 dedicated events focused on vulnerability remediation.

A unique and critical part of the CAP is a fusion cell which integrates cyber and kinetic opposing-force elements during exercises in order to demonstrate cyber impacts to the command's missions. This fusion cell enables DOT&E to highlight and help mitigate those cyber vulnerabilities that could most seriously impair critical missions. During the COVID-19-induced operational pause, DOT&E identified a number of focus areas that will continue to improve the CAP's ability to emulate advanced nation-state adversaries to help the DOD improve its ability to complete critical missions in the face of cyber threats.

The resources and expertise needed for realistic OT&E and assessments during exercises continue to increase due to the ever-increasing number and variety of cyber threats coupled

with a growing number of events, including events that involve coalition partners and agencies outside of the DOD. DOT&E's efforts to acquire an adequate supply of cyber capabilities are greatly hindered by the chronic deficit of cyber expertise available to the DOD. Emerging technologies that are enabled by artificial intelligence and machine learning will soon call for entirely new assessment tools and methods, and will intensify the expertise gap. To close this gap, the DOD urgently requires a well-funded and widely accessible pipeline of cyber expertise from sources such as academia, Federally Funded Research and Development Centers (FFRDCs), and the national labs.

CYBER ASSESSMENT ACTIVITY

In FY20, as in previous years, DOT&E supervised cybersecurity OT&E for programs on DOT&E oversight, and performed cybersecurity assessments of operational networks and systems leading up to and during CCMD and Service training exercises. DOT&E also supported cyber defender exercises, assessments of offensive cyber capabilities and targeting, and mission-effects analyses to characterize the operational implications of cyber threats.

The number of cyber events was slightly less than two-thirds that of previous years (69 in FY20 compared to 114 in FY19). Postponements and cancellations due to the response to COVID-19 notably contributed to the reduction of events in FY20. DOT&E adjusted operations to accommodate COVID-19 by, for example, using telepresence technologies to monitor and guide assessments while maintaining travel and distancing guidelines.

Operational Test and Evaluation with Cybersecurity

DOT&E continued to emphasize the importance of cybersecurity OT&E for all systems that transmit, receive, or process electronic information by direct, wireless, or removable means. DOT&E focuses cybersecurity OT&E on the evaluation of whether combat forces can complete operational missions in a cyber-contested environment. In FY20, DOT&E monitored more than 36 tests across 23 acquisition programs. This is about half of the number conducted in FY19 because COVID-19 restrictions slowed the progress of many DOD programs.

Over the last several years, the operational test agencies have increased the rigor and scope of cybersecurity OT&E for systems that rely on the IP. A significant gap remains in the development of tools and techniques needed to test specialized protocols, such as those used in industrial control systems, tactical data links, and aircraft transponders. DOT&E is working with the Services and other agencies (such as the Federal Aviation Administration) to address that gap.

Cybersecurity Assessment Program (CAP)

DOT&E's CAP worked with the CCMDs and Services to build and execute Cyber Readiness Campaigns. These campaigns provided DOT&E assessment opportunities via a series of focused events throughout the year, while affording the commands training in realistic environments to improve their cyber capabilities. In FY20, DOT&E provided resources for assessment teams, intelligence subject matter experts, and cyber Red Teams to plan and conduct the 27 cybersecurity-related assessments and support the six PCO efforts listed in Table 1. The number of assessments in FY20 is about three-quarters of the 46 in FY19. The major exercises assessed were Global Lightning 2020, Global Thunder 2020, Juniper Cobra 2020, Littoral Combat Ship (LCS)-Exercise, Pacific Sentry 20-2, USS *Dwight D Eisenhower* Carrier Strike Group, USS *Iwo Jima* Amphibious Ready Group and Marine Expeditionary Unit (ARG/MEU), Trident 2020-2, and Trident 2020-4. Assessment focus areas included:

- Mission assurance in cyber-contested environments
- Performance of network and system defenses when under attack
- Timeliness of attack detections and response actions
- Ability of physical security measures to protect facilities with network or system assets
- Planning and employment of offensive cyber capabilities
- Remediation support to facilitate fixes to identified problems

The CAP Cyber Readiness Campaigns continue to improve both technical and process-oriented measures for cyber defense; this in turn has led to increased demand for cyber expertise to support these campaigns. As CAP expands adversary portrayal and assessments to more dimensions of the cyberattack surface, the program will identify additional cybersecurity risks and risk mitigations related to the internet of things, wireless technologies, industrial control systems, cloud technologies, and artificial intelligence.

Persistent Cyber Operations (PCO)

PCO provide cyber Red Teams with longer dwell time on DOD networks to probe selected areas and to portray advanced adversaries that typically conduct long-duration, stealthy cyber reconnaissance to identify cybersecurity weaknesses without being detected. PCO also afford the opportunity to identify more important and pervasive vulnerabilities, and provide more realistic training for cyber defenders. PCO enabled DOT&E to continue assessment operations during the COVID-19 response, providing assessments to CCMDs on how to best adjust their sensors and tools to facilitate operations by off-site personnel. The ability to continue operating and dynamically respond to evolving requests contributed to FY20 having the highest demand and operational tempo yet for PCO.

In FY20, DOT&E resourced PCO at six CCMDs. PCO activities expanded at the end of the fiscal year to include networks supporting Ballistic Missile Defense and the global DODIN, and plans are maturing to add PCO cells that will focus on all major Service networks.

DOT&E works with TSMO to coordinate PCO activities and report on vulnerabilities that span functional or geographic areas

of responsibility. The demand for PCO support continues to increase, highlighting the interest in cyber activity at times other than during tests and exercises. The limited availability of cyber expertise within the DOD is a factor that limits both the growth of the PCO, and its ability to emulate the most advanced cyber threats.

Advanced Cyber Operations (ACO)
DOT&E resources an ACO team to augment cyber Red Teams with specialized cyber expertise and develop new cyber tools, tactics, techniques, and procedures. During FY20, the ACO supported:

- Assessments of the Joint Regional Security Stacks
- Cybersecurity testing of the F-35
- Assessments of offensive cyber operations capabilities
- Cybersecurity assessment of the IKE planning and execution tool that supports U.S. Cyber Command (USCYBERCOM) operations
- Assessment of Office 365 Zero-Trust Network
- Assessments of industrial control systems
- Development of enhanced Red Team capabilities
- Stand-up of a new Red Team location in Maryland

Demand for ACO support grew dramatically during FY20, and requests for FY21 will likely drive further expansion of the ACO Team, subject to available cyber expertise.

Assessment of Offensive Cyber Capabilities
DOT&E continued collaboration with offensive cyber capability developers and testers, helping to integrate more operationally realistic elements into assessments of these capabilities. DOT&E observed demonstrations or performed assessments of seven offensive cyber events in FY20 and assessed processes for planning cyber fires during exercises with U.S. Indo-Pacific Command (USINDOPACOM). Examples of capabilities examined during FY20 assessments ranged in sophistication from tactical devices used to help defeat terrorists to advanced cyber/electromagnetic spectrum attacks designed for use against nation states.

Engagement with the Intelligence Community
DOT&E continued to partner with the Intelligence Community to employ and improve cyber-related intelligence. Such intelligence ensures the realism of cyber threats portrayed during OT&E and CAP assessments, and is a critical foundation for the development of adequate cyber defenses.

Collaboration with Naval Postgraduate School
DOT&E's outreach to the academic community includes working with the Naval Postgraduate School to sponsor applied research projects in cyber topics, including an Insider Threat detection capability using statistical network-traffic modeling, and tools to increase the fidelity of virtualized networks and components. These efforts have resulted in a toolkit that the Navy has employed, and which is being transitioned for joint use.

Special Project Assessments
DOT&E performed multiple special assessments in FY20 requested by USCYBERCOM, the DOD CIO, OSD's Joint Service Provider, DISA, and U.S. Southern Command (USSOUTHCOM). These assessments provided cyber expertise to assess priority missions and emerging technologies to include:

- Proposed perimeter cybersecurity defenses for the SIPRNET
- Cloud-based models for Zero-Trust network and endpoint security
- Grey space network flow analysis of DODIN components
- Nuclear command, control, and communications

Special assessment methodologies and outcomes were shared with requesting organizations and will inform the broader CCMD and Service Cyber Readiness Campaigns, as well as cybersecurity OT&E of acquisition programs.

EXAMPLES OF FY20 OBSERVATIONS AND ACCOMPLISMENTS

PCO Contributions during COVID-19
During the early days of the COVID-19 response, when travel by DOD personnel was largely stopped, DOT&E expanded PCO assessment activities. When the DOD implemented the Commercial Virtual Remote (CVR) environment as a rapidly deployed solution to enhance telework, the PCO found configuration management vulnerabilities that would enable an adversary to gain unauthorized access to unclassified CCMD networks, reported them to USCYBERCOM, and the DOD CIO issued guidance for remediation. The PCO also worked directly with CCMD network defenders to help them test and secure their networks and security baselines. The PCO's real-time feedback allowed CCMDs and supporting defenders to implement fixes and new security technologies, provided positive training, and resulted in improved cybersecurity.

Joint Regional Security Stack Assessments
DOT&E's ACO team and the DISA Red Team performed an assessment of the SIPRNET-Joint Regional Security Stack (S-JRSS). Assessment results identified multiple poor cybersecurity findings, which contributed to DISA shutting down existing S-JRSSs, and the DOD CIO to delay future S-JRSS deployments until FY23.

DOT&E also worked with DISA to conduct a comparative analysis of operational JRSS cybersecurity logs with network flow information gathered by commercial vendors. These data are helping JRSS operators recognize potential adversarial activity, tune their defensive tools, and remedy gaps in incident response processes.

Zero-Trust Architecture Assessment
DOT&E helped lead the USCYBERCOM-sponsored Microsoft Office 365 Design and Implementation cybersecurity validation events to assess how implementation of Zero-Trust principles in cloud-based environments could improve the DOD's cybersecurity posture. Initial results indicate that a Zero-Trust

design, properly implemented in a DOD network, could provide significantly better cybersecurity than the DOD's current perimeter defense design.

Assessment of Tanium Endpoint Security
In FY19, DOT&E provided ACO assessment support to DISA to examine the ability of Tanium to provide endpoint protection and application control across the DOD. The ACO assessment identified multiple issues, and DOT&E continued assessment support through FY20 as the developer experimented with solutions and ultimately delivered an improved product. Tanium is helping safeguard more than two million DOD computers.

Implications of adversarial exploitation of compromised information
DOT&E conducted research with the Federal Bureau of Investigation's National Cyber Investigative Joint Task Force for several acquisition programs to explore implications of adversarial exploitation of known compromised information. The efforts provided insights into the criticality of supply chain security to cybersecurity posture and operations. DOT&E continues this research to inform planning and conduct of OT&E and training exercises.

WAY AHEAD

For the FY21 CAP, DOT&E will continue to increase the realism of our assessments to accurately test the warfighter's ability to sustain critical missions that are contested and degraded by an advanced cyber adversary. Ready access to a talented cyber workforce and advanced tools are all essential, and DOT&E will continue to advocate that the DOD establish a well-resourced pipeline of cyber talent from academia, the FFRDCs, and the national labs. Overarching CAP assessment objectives developed during FY20 include the following:

Assess Mission Assurance with Network Degradation
Exercise planners are generally reluctant to allow threat-realistic cyberattacks that degrade network operations. This limits DOT&E's ability to help improve warfighters' ability to withstand such attacks. DOT&E will prioritize funding for assessments that permit realistic degradation to networks and the missions they support. Such assessments will enable DOT&E to better assess the DOD's mission-assurance posture and will help warfighters improve their playbooks in order to sustain missions under realistic wartime conditions.

Improve Assessments and Tests of Offensive Cyberspace Operations (OCO) Capabilities and Processes
As OCO capabilities grow in importance, operationally realistic testing of these capabilities is not as routine or rigorous as is needed to provide confidence to commanders that the capabilities will work as designed. DOT&E's OCO Assessment Team will continue to plan and execute operational assessments with Service representatives and the Cyber Mission Force to help improve confidence in OCO capabilities and processes, and inform future operational testing. DOT&E will work to overcome the following challenges to enable adequate assessments and OT&E on OCO capabilities:

- Testers need better access to advanced cyber expertise to plan and execute tests on advanced OCO technologies.
- Testers need improved access to intelligence on threat targets and defensive capabilities surrounding these targets.
- Red Teams need training and capabilities to portray near-peer adversaries for targets of interest.
- Test ranges are needed to assess the effectiveness of cyber capabilities delivered by over-the-air transmissions.

Special Assessments for Cross-Cutting Technology
DOT&E will continue to grow capabilities to assess emerging technologies and other critical warfighting technologies for which threat-realistic cyber assessments are lacking. These will include efforts to explore and stress the security of cloud computing; assess cybersecurity of aircraft transponders; examine the convergence of cyber and electromagnetic spectrum operations; assess specialized communications protocols; and assess cybersecurity of critical infrastructure supporting DOD installations, organizations, and systems.

During FY20, DOT&E established an Industrial Control System Working Group (ICS WG) to assess vulnerabilities and improve cyber defense at the facility-related ICS level and develop a methodology for integrating ICS assessments into CAP. The first assessment is a scheduled ICS Pilot at USSOUTHCOM in early December 2020. The pilot will assess the risks, threats, and vulnerabilities at the convergence point between the ICS/Supervisory Control and Data Acquisition and the Information Technology/IP systems. The data will be mapped to the MITRE ICS ATT&CK framework of attack techniques, and integrated with Sandia National Lab's SCEPTRE to emulate, test, and validate control system security.

Implement Remote Assessment Technologies
The response to the COVID-19 pandemic impacted the planning and execution of many assessments scheduled for FY20 and created the need for options to conduct assessments and tests with reduced on-site presence. DOT&E will continue experimentation with the Test Resource Management Center on available and emerging remote/telepresence capabilities for an array of use cases that represent typical assessment and test venues. The objective is to find a workable balance of virtual and in-person activity to meet the requirements of both OT&E oversight and CAP core missions across the array of classified events and environments where data bandwidth is a challenge.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY20		
EVENT TYPE	**ACQUISITION PROGRAM OR TYPE OF EVENT**	
Programs Completing Operational Tests of Cybersecurity	Aerosol and Vapor Chemical Agent Detector	Global Command and Control System - Joint
	Air Operations Center - Weapon System	Global Positioning System Contingency Operations
	Amphibious Combat Vehicle Family of Vehicles	Interim Mobile Short Range Air Defense
	AN/SQQ-89A(V) Integrated Undersea Warfare Combat Systems Suite	KC-46 - Tanker Replacement Program
	Army Integrated Air & Missile Defense	Limited Interim Missile Warning System
	Bradley	Maneuver-Short Range Air Defense
	Defense Enterprise Accounting and Management System	Military Global Positioning System User Equipment
	Deliberate and Crisis Action Planning and Execution Segments	RQ-7B SHADOW - Tactical Unmanned Aircraft System
	DOD Healthcare Management System Modernization	Space-Based Infrared System Program
	Electronic Warfare Planning and Management Tool	Stryker Anti-tank Guided Missile
	F-35 - Lightning II Joint Strike Fighter Program	Wide Area Surveillance
	Family of Beyond Line-of-Sight Terminals	
Cybersecurity Assessment Program	**Physical Security Assessment (1 Event)** USSOCOM	
	Cooperative Network Vulnerability Assessment (3 Events) USAFRICOM, USINDOPACOM, USFK	
	Assessments of Network Security, Stimulation Exercises, and Phishing Campaigns (5 Events) USAFRICOM, USNORTHCOM, USSOUTHCOM, USFK (2)	
	Assessment of Mission Effects during Exercises (11 Events) USCENTCOM, USNORTHCOM, USSTRATCOM (2), USSOCOM (2), USEUCOM, USINDOPACOM, U.S. Navy (3)	
	TAssessment of Cyber Fires Processes for Offensive Cyber Operations (1 Event) USINDOPACOM	
	Assessments of Offensive Cyber Operations Capabilities (6 Events) USCYBERCOM (3), USINDOPACOM (2), USSOCOM	
	Assessments During Persistent Cyber Operations (6 Efforts) USCENTCOM, USEUCOM, USINDOPACOM, USNORTHCOM, USSTRATCOM, U.S. Air Force	

USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USCYBERCOM – U.S. Cyber Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; USNORTHCOM – U.S. Northern Command; USSOCOM – U.S. Special Operations Command; USSOUTHCOM – U.S. Southern Command; USSTRATCOM – U.S. Strategic Command