Cyber Assessments

SUMMARY

DOT&E cyber assessments in FY19 confirmed that critical DOD missions remain at high risk of disruption from adversary cyber actions. Furthermore, DOT&E observed very few instances where cyber penetrations or disruptions were followed by rapid detections and effective response actions necessary for mission resiliency. These two observations remain consistent with reports from prior years, as does the fact that the DOD is applying significant resources towards improvements, some of which are making a positive difference.

However, many cybersecurity capabilities continue to be fielded without adequate maturation and assessment of the key technologies. DOT&E observed multiple suboptimal acquisition outcomes in FY19, such as system fielding without adequate cybersecurity, inadequate defender skills and training, and slow detections or poor reactions to cyber-attacks. The root cause of these poor outcomes is the inability of the DOD to acquire and apply sufficient cyber expertise to improve leadership decisions, system development and test, and network operation and defense.

Leadership decisions regarding cybersecurity improvements frequently focus more on what can be achieved quickly and cheaply, with less emphasis on actual performance and the confirmation that desired performance has been achieved. Many efforts in recent years at "agile acquisition" and "tech refresh" have expeditiously spent a great deal of money towards capabilities that did little to enhance cybersecurity. These less accountable approaches often fail to consider the Doctrine, Organization, Training, Materiel, Logistics, Personnel, Facilities and Policies (DOTMLPF-P) needed to ensure that the capabilities actually work, and that cyber defenders can use the capabilities effectively. Leaders with greater access to cyber expertise will make better decisions about which technologies need more programmatic rigor, which should be more thoroughly assessed against representative threats before deployment, and what can cyber defenders with chronic high turnover reasonably be expected to do.

A wealth of cyber expertise is available in the Nation's academic sector, but the DOD has yet to apply significant resources to harness the capabilities of U.S. universities. Cyber adversaries, such as China have been harnessing U.S. academic cyber capabilities for decades by sending their students to U.S. universities; the DOD should make a concerted effort to employ more of the cyber experts in academia in the defense of our Nation.

Assessment data for this summary are based on nearly 40 cybersecurity assessments with Combatant Commands (CCMDs) and Services, and more than 60 cybersecurity OT&E events (see Table 1 on page 232). Additionally, DOT&E performed special assessments of nuclear command, control, and communications (NC3); data breaches; and Public Key Infrastructure. In the aggregate, these assessments reveal that the DOD is expanding its focus from the tactical tasks of defending organizations, networks, and systems to examining the operational concerns of completing missions in the face of adversarial cyber operations. DOT&E will attempt to focus assessment efforts with CCMDs and Services in FY20 to rigorously assess mission assurance and warfighter abilities to fight through cyber-attacks.

The DOD is larger than any Fortune 500 company, and "out-of-the-box" solutions that may work for corporate enterprise networks may not scale well to meet DOD missions. The rapid fielding of emerging technology is not delivering desired benefits because of immature integration strategies, incomplete training of user personnel, and inadequate assessment prior to deployment. Better attention to these three challenge areas is necessary to avoid aggressive schedule-driven deployments of capabilities that fail to significantly improve cybersecurity. Rapid fielding of unproven technologies, with the intention of adding cybersecurity afterwards, provides adversaries the opportunity to gain network footholds, which are difficult to detect and remove. The schedule-driven deployment of the Joint Regional Security Stacks on the DOD unclassified NIPRNET, despite multiple assessments that indicate they do not help defend against realistic cyber threats, is a recent example of this (see page 41).

The DOD's relentless expansion of internet protocol (IP) networks has greatly improved our peacetime ability to communicate. But it has often been accomplished with little regard for cybersecurity, and has created an ever-growing network boundary that the DOD has limited ability to defend. To address this problem, the DOD needs to rethink the policies and processes associated with information technology (IT) to reflect that IT is not merely a commodity to be purchased at the lowest cost and fielded as quickly as possible; it is a critical warfighting capability that directly affects the security of the Nation.

One of the hallmarks of DOT&E cyber assessments is the emphasis on going beyond simply finding vulnerabilities: all DOT&E-led assessment teams provide full disclosure about how vulnerabilities were identified and exploited, and offer "Green Team" support to develop fixes and mitigation strategies. DOT&E also performs follow-up assessments to verify that improvements preclude repeat attacks.

This "find-fix-verify" approach has created a rapidly increasing demand for DOT&E cyber assessments across the DOD, and for the in-depth analyses of assessment data, which continues to stress available resources. The ability of DOT&E-sponsored assessment teams to perform these assessments is at risk as capacity of available cyber teams to meet the rising demand becomes ever more limited.

Furthermore, a widening gap exists between DOD cyber Red Team capabilities and those of nation-state threats. Assessments that do not include a fully representative threat portrayal may leave warfighters and network owners with a false sense of confidence about the magnitude and scope of cyber-attacks facing the Department. DOT&E is working with the DOD Red Teams to close that gap by helping them acquire additional personnel, more advanced capabilities, and training; however, significantly more resources are needed in this area.

Automated capability, to support cyber tools and data collection, is needed to help meet ever-growing cybersecurity and cyber assessment demands. The most promising approaches for the near-term involve semi-automated solutions that combine the strengths of human understanding and innovation with the speed of automation and artificial intelligence, and DOT&E has initiated development efforts towards these enhancements.

Resources alone will not solve the DOD's cyber problems; the DOD needs the best cyber expertise available. The DOD's cyber intellect must exceed that of our adversaries'. In FY20, the DOD allocated funding for DOT&E to expand access to cyber expertise for advanced and persistent cyber operations, and to set the groundwork for a Cyber University Affiliated Research Center (UARC) that would open a critical pipeline to the cyber talent resident within academia. The Cyber UARC will not only help the T&E community meet the increasing demand for cyber assessments and ensure that nation-state threats are adequately portrayed, it will provide the entire Department access to cutting-edge cyber tools, including those enabled with automation and artificial intelligence. Once the Cyber UARC is established, additional funding will be needed to grow and sustain it.

CYBER ASSESSMENT ACTIVITY

In FY19, as in previous years, DOT&E performed oversight of 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 network defender exercises, operational assessments of offensive cyber capabilities and targeting, and mission effects analyses to characterize the operational implications of cyber threats.

Based on results from tests and exercise assessments, DOT&E periodically publishes classified reports on overarching cyber topics of interest. In FY19, DOT&E published a report in December 2018 responding to direction from the U.S. Senate Committee on Appropriations that discussed efforts in the DOD to prevent cyber intrusions, mitigate compromises, and recover from losses in capability to networks, systems, and platforms.

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. These operational tests focused on determining whether combat forces can complete operational missions in a cyber-contested environment. In FY19, DOT&E monitored more than 60 such tests across 36 acquisition programs, and noted a common shortfall: most tests included cyber threats that were significantly more limited than would be expected from an advanced adversary. This limitation reflects a growing trend that must be remedied so that adequate, threat-representative OT&E can be performed for DOD acquisition programs.

Cybersecurity Assessment Program

DOT&E's Cybersecurity Assessment Program 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 FY19, DOT&E provided resources for assessment teams, intelligence subject matter experts, and DOD cyber Red Teams to plan and conduct the 38 events and support the 6 Persistent Cyber Operations (PCO) efforts listed in Table 1. Assessment focus areas included:

- Effectiveness of network defenses when under attack
- Timeliness of attack detections and response actions
- Effectiveness of physical security measures to protect facilities with network assets
- Effectiveness in the planning and employment of offensive cyber capabilities
- Remediation support to facilitate fixes to identified problems

Because the Cyber Readiness Campaigns have consistently helped improve the cyber posture of the CCMDs and Services, DOT&E has continued to see increasing CCMD and Service demand for cyber expertise to support these campaigns.

Persistent Cyber Operations (PCO)

PCO provides Red Teams longer dwell time on DOD networks to deeply probe selected areas, to more realistically portray nation-state adversaries, and to provide more realistic training for cyber defenders. PCO assessments have found a number of critical vulnerabilities that were not previously detected, resulting in fixes that have reduced the potential for adverse mission effects.

In FY19, DOT&E resourced PCO at six CCMDs, and is working towards PCO assessments with four additional CCMDs, Services, or Agencies in FY20. DOT&E has worked with the U.S. Army Threat Systems Management Office to coordinate PCO activities, and appropriately report on vulnerabilities that span functional or geographic areas of responsibility.

Advanced Cyber Operations (ACO)

DOT&E resources the ACO team to augment cyber Red Teams with specialized cyber expertise, and to develop new cyber tools and procedures. The ACO also supported special assessments for

nuclear command and control systems, emerging network defense capabilities, and offensive cyber operations.

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. DOT&E observed demonstrations or performed assessments of more than a dozen offensive cyber events in FY19. In addition, DOT&E worked with the Joint Technical Coordinating Group for Munitions Effectiveness to identify the data necessary to build analysis tools to predict offensive cyber effects.

Joint Cyber Warfighting Architecture (JCWA)
Because of its criticality to the future of the DOD's cyber posture, DOT&E placed the JCWA on oversight, including the Unified Platform, Joint Cyber Command and Control, and the Persistent Cyber Training Environment programs. DOT&E is working with the Program Offices to ensure that capabilities delivered to U.S. Cyber Command (USCYBERCOM), other functional and geographic CCMDs, the Cyber National Mission Force, the Service cyber components, and the rest of the DOD are operationally effective, suitable, and secure.

Cybersecurity Assessments with Coalition Partners and Networks
DOT&E observed or assessed several events with coalition partners and networks, including assessments of the Combined Enterprise Regional Information Exchange System (CENTRIXS), Multi-National Information System, and bilateral networks, such as Seagull. DOT&E observed that most coalition networks do not have assigned Cybersecurity Service Providers (CSSPs), and most are not instrumented with sensors that a CSSP would require to monitor network performance and security. DOT&E is supporting experimentation with a zero-trust network concept that employs virtual machine environments and encrypted peering to limit exposure and lateral movement of potential attackers between mission partner environments.

Engagement with the Intelligence Community
DOT&E continued to work with the Intelligence Community to employ and improve cyber-related intelligence. Intelligence on adversarial cyber capabilities and intent is vital to ensuring both rigorous testing and defensive measures. DOT&E partnered with the National Cyber Investigative Joint Task Force (NCIJTF), the Defense Intelligence Agency, the National Reconnaissance Office, and the National Ground Intelligence Center to verify that both the operational test community and the DOD have a consolidated understanding of cyber threats. The partnership with NCIJTF allowed for the assessment of threats to major weapons systems and to understand the breadth of the expanding risk to DOD missions. DOT&E worked with the Intelligence Community to improve the realism of threat representation in CCMD and Service exercises.

Joint Cyber Insider Threat Joint Test and Evaluation
During FY19, DOT&E developed the Joint Cyber Insider Threat Joint Test and Evaluation tactics, techniques, and procedures (TTPs) for cyber insider threat detection and reporting. These TTPs guide cyber detection, analysis, and reporting efforts to monitor user actions and report potential cyber insider threats to the appropriate authorities. The procedures also include network management considerations, resource and personnel implications, detection and reporting procedures, and training recommendations. These products provide cyber defenders a set of tools to thwart the insider threat.

Collaboration with Naval Postgraduate School
DOT&E's outreach to the academic community includes working with the Naval Postgraduate School to sponsor research projects in cyber topics. Research efforts in FY19 included development of algorithm-based insider threat prediction capabilities, and tools to enable cyber testing of different communications protocols.

Coordination with USD(R&E) on Statutory Cybersecurity Assessments
In FY19, DOT&E continued collaboration with USD(R&E) for cyber assessments of major DOD weapons systems, as directed by section 1640 of the FY18 National Defense Authorization Act (NDAA).

OBSERVATIONS

This section describes noteworthy observations from FY19 operational tests, exercise assessments, and special evaluations. DOT&E can provide more detailed classified information on each topic.

Good Cybersecurity Requires Holistic Approach.
DOT&E observations indicate that effective cybersecurity includes active and passive measures, in both the physical and cyber domains, to prevent intrusion, mitigate compromises, and recover capability. Red Teams demonstrated again in FY19 that physical intrusions can provide attackers access to compromised IT for follow-on exploitation by cyber adversaries.

Stolen Credentials Can Be Catastrophic.
DOT&E assessments – as well as publicly available analyses of commercial networks – confirm that credential theft remains one of the most common cyber-attack actions that leads to data breaches. DOT&E continues to find that of 11 general categories of system vulnerabilities, three are more prevalent in the DOD than the others: authentication and credential; software configuration; and host network. In FY19, Red Teams used stolen credentials to move across networks, escalate network privileges, and steal critical warfighter information at will. Red Teams were able to help the exercise opposing force weaponize

stolen information during exercises and demonstrate how DOD warfighter missions could be severely degraded.

Breaches of Contractors Give Advantage to Adversary. Breaches of cleared defense contractors provide adversaries with information that enables the development of cutting-edge weapons to be used against us, paves the way for cyber-attacks that could compromise critical DOD missions, and degrades our technical and commercial advantages.

DOT&E analyzed past breaches of defense contractors for several major programs and found that these breaches exposed extensive information that empowers our adversaries to degrade key DOD systems and missions. DOT&E also observed several supply-chain table top exercises where significant efforts were being implemented to help shield critical design information and software from adversaries. Efforts such as these should be implemented for all critical programs, and operational assessments and monitoring of contractor networks, tools, facilities, and software factories should become routine for critical programs.

Nuclear Command, Control, and Communications (NC3). Protected, assured, and resilient command, control, and communications are essential for all military operations and especially so for the NC3 components of our national capability. At the request of U.S. Strategic Command (USSTRATCOM), the DOD Chief Information Officer, and the Defense Threat Reduction Agency, throughout FY19, DOT&E participated in classified cybersecurity assessments to characterize the status and identify options for improving the mission assurance and cyber-related aspects of the NC3 capability. The results of these assessments were briefed to the highest levels of DOD leadership and have resulted in a significant increase in focus in this vital area.

New Vulnerabilities Outpace Patching Responses. The volume of new vulnerabilities exceeds the ability of the DOD to identify and comprehensively patch them before an adversary can exploit them. As most vulnerabilities can be weaponized within 30 days, comprehensive patching is probably unachievable, and DOD efforts should use threat-realistic cyber assessments to focus mitigation efforts on mission-critical vulnerabilities. The fact that there will always be unpatched vulnerabilities means that the likelihood of cyber intrusions is high, and should be assumed for every system and network.

Cyber Intrusions Demand Ability to Recover and Restore. Since cyber intrusions are always possible, missions can only be assured if warfighters and network defenders have developed and practiced recover and restore operations. DOT&E observed very few instances of recovery following a cyber-attack in FY19, in part because detection and recovery timelines are either nonexistent or are too long to be effective during wartime, and exceed the duration of an exercise or acquisition test. Another reason is that most exercises and tests do not allow Red Teams to deliver major cyber effects, so there is no opportunity for warfighters to demonstrate their ability to fight through a mission failure that would call for recovery actions. DOT&E has reported on the lack of such realistic cyber realism in DOD exercises and tests for more than a decade.

Big Data Platforms May Improve Network Defenses. USCYBERCOM and the Service cyber components have aggregated extensive network logs and implemented search functionality for this large amount of data. This functionality allows cyber defenders and hunt teams to look for indicators of adversary presence across disparate networks over much greater timespans than were previously possible. DOT&E will assess the effectiveness of this new capability during FY20 assessments.

Project IKE Offers Improvements, But Needs to be Cyber Secure. As the Cyber National Mission Force (CNMF) evolves to a unified command structure, it needs tools to track the readiness, status, and activities of cyber operators. Additionally, CNMF leaders need a consolidated situational awareness picture of cyber threat indicators and known compromises, and associated aids in course of action development. The OSD Strategic Capabilities Office identified the potential to achieve these goals with the Defense Advanced Research Projects Agency's Plan X, and has initiated a prototype called Project IKE.

DOT&E observed Project IKE pilots during several CCMD exercises during FY19. Project IKE demonstrated the potential to provide situational awareness when timely and properly formatted data are provided to its databases. To date, these demonstrations have depended on large amounts of manual data entry. For these tools to be operationally useful and scaled to support the larger CNMF, the underlying data sets must exist and be populated and maintained via automated feeds. Additionally, it will be critical that the CNMF integrate effective cybersecurity into the implementation of Project IKE. Failure to do so may allow an adversary to mask penetrations and network degradation by inserting false reporting into CNMF leadership displays.

Threat Portrayal is Not Fully Representative. DOT&E employs National Security Agency (NSA)-certified , Service-owned Red Teams during OT&E and assessments to emulate the type of advanced cyber-attacks that DOD warfighters will experience. Several of these teams simulate adversary malware and TTPs well, but most teams operate at only the moderate-threat level or below, and none can routinely operate at the advanced nation-state level. Their portrayal of moderate threats is useful to identify numerous vulnerabilities present on DOD networks and to stress defenders and mission resiliency; however, moderate threats are not the driving force behind the DOD's most expensive acquisition programs. Furthermore, no-fail missions that the CCMDs must execute should be stressed by the best approximation of advanced adversaries.

Staying abreast of the rapid advances in cyber technologies, and the companion vulnerabilities, is a challenging and expensive proposition. Due to a lack of expertise and resources, the skills and expertise of several NSA-certified Red Teams have atrophied to such an extent that DOT&E can no longer effectively employ them on assessments, and the retention of their certification is in question. In FY19, DOT&E initiated an effort to provide cyber

experts to these Red Teams with the goal of returning them to a mission-ready status in FY20; however, this will only be possible if the Services supporting these teams significantly increase their support to them.

Non-Internet Protocol (IP) Attack Surfaces. Electronic exchange of information uses a number of transmission protocols including the familiar IP. Other protocols often support specialized applications, such as moving information among aircraft and vehicle control devices (e.g. Military Standard (MIL-STD)-1553) or specialized data links (e.g. Link 16). Many of the non-IP protocols bridge the cyber-physical system gap to enable cyber-attacks to have destructive physical effects on vehicles and equipment. The test community and the cyber teams continue to develop the tools and ability to assess the cyber posture of non-IP protocols. DOT&E is working with multiple Service and contractor partners to develop threat-realistic assessment tools for non-IP protocols.

Confirm Cybersecurity of Defensive Tools. The DOD must consistently consider both the performance (ability to protect others) and security (ability to protect itself) of defensive cybersecurity tools. Emerging commercial tools, such as agent-based technologies, can help with cyber defense, but they introduce additional cyber risks that must be assessed via threat-realistic operational testing to inform decisions to acquire and deploy the tools on DOD networks.

Cyber/Electronic Warfare (EW) Convergence. Combining capabilities in the cyber and EW domains enable the engagement of targets that are not connected to the internet or subject to cyber-attacks via IP means. DOT&E is monitoring these developments and will support developers and testers in the planning and execution of tests of these capabilities.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY19		
EVENT TYPE	**ACQUISITION PROGRAM OR TYPE OF EVENT**	
Programs Completing Operational Tests of Cybersecurity	Advanced Airborne Sensor	Ground/Air Task Oriented Radar
	AEGIS Modernization	Integrated Personnel and Pay System – Army Increment 2
	AH-64E Apache	Joint Assault Bridge
	AN/SQQ-89A(V) Integrated Undersea Warfare (USW) Combat Systems Suite	Joint Air-to-Ground Missile
	Air Operations Center – Weapon System 10.1	Key Management Infrastructure Increment 2
	Acoustic Rapid Commercial Off-the-Shelf (COTS) Insertion for SONAR	Abrams M1A1 SA; M1A2 SEP; Active Protection Systems (APS)
	B61 Mod 12 Life Extension Program Tail Kit Assembly	MK 54 torpedo/MK 54 Vertical Launch Anti-Submarine Rocket (VLA)/MK 54 Upgrades Including High Altitude Anti-Submarine Warfare (ASW) Weapon Capability (HAAWC)
	Ballistic Missile Defense System Program	MK 48 Common Broadband Advanced Sonar System (CBASS) Torpedo including all upgrades
	C-130J – HERCULES Cargo Aircraft Program	Mounted Computing Environment
	Command Post Computing Environment	Mobile User Objective System
	Defense Agency Initiative	Patriot Advanced Capability 3 (PATRIOT PAC-3)
	Distributed Common Ground System – Army	Public Key Infrastructure Increment 2
	Distributed Common Ground System – Navy	Small Diameter Bomb, Increment II
	DOD Healthcare Management System Modernization	Space Fence
	Enhanced Polar System	Spider XM7 Network Command Munition
	Electronic Warfare Planning and Management Tool	Teleport, Generation III
	F-35 - Lightning II Joint Strike Fighter Program	UH-60V BLACK HAWK
	Family of Beyond Line-of-Sight Terminals	VH-92A Presidential Helicopter
Cybersecurity Assessment Program	**Physical Security Assessment (8 Events)** U.S. Indo-Pacific Command (USINDOPACOM), USSTRATCOM, U.S. Africa Command (USAFRICOM), U.S. Special Operations Command (USSOCOM), U.S. Navy (2), U.S. Northern Command (USNORTHCOM) (2)	
	Cooperative Network Vulnerability Assessment (2 Events) USAFRICOM, U.S. Central Command (USCENTCOM)	
	Cyber Operations (7 Events) U.S. European Command (USEUCOM) (2), USAFRICOM (3), USCENTCOM, USNORTHCOM	
	Mission Effects with Cyber Operations (12 Events) USSTRATCOM (2), USSOCOM (2), USEUCOM, U.S. Forces Korea (2), USINDOPACOM (2), U.S. Air Force, U.S. Navy (2)	
	Targeting Processes for Offensive Cyber Operations (2 Events) USINDOPACOM (2)	
	Sharing Solutions Fix Event (5 Events) USINDOPACOM (2), USEUCOM, USTRATCOM (2)	
	Offensive Cyberspace Operations Capability (2 Events) USINDOPACOM (2)	
	Persistent Cyber Operations (6 Efforts) USINDOPACOM, USSTRATCOM, USNORTHCOM, USCENTCOM, U.S. Air Force, USEUCOM	

TABLE 2. CYBER OPERATIONAL TEST AND ASSESSMENT COMMUNITY INVOLVED IN OT&E AND CYBER ASSESSMENT PROGRAM EVENTS	
OPERATIONAL TEST AGENCIES	
Military Services	Air Force Operational Test and Evaluation Center
	Army Test and Evaluation Command
	Navy Operational Test and Evaluation Force
	Marine Corps Operational Test and Evaluation Activity
Defense Agencies	Joint Interoperability Test Command
NATIONAL SECURITY AGENCY (NSA)-CERTIFIED CYBER RED TEAMS	
Air Force	57th Information Aggressor Squadron
	177th Information Aggressor Squadron
Army	1st Information Operations Command
	Threat Systems Management Office
Navy	Navy Red Team
Marine Corps	Marine Corps Red Team
Defense Agencies	Defense Information Systems Agency Red Team
	NSA Cyber Red Team
CYBER TEAMS	
Air Force	47th Cyber Test Squadron
	92nd Cyberspace Operations Squadron
	461st Flight Test Squadron
	747th Test Squadron
	Air Force Research Laboratory Sensors Directorate
	Combat Capabilities Development Command, Data and Analyses Center
Navy	Naval Air Systems Command Cyber Detachment
	Naval Air Systems Command Point Mugu Cyber Test and Evaluation Branch
	Naval Air Systems Command Air Test and Evaluation Squadron 23 (VX-23)
Department of Energy	Sandia National Laboratory Red Team