Cyber Assessment Program

In FY21, DOT&E resourced assessment teams, cyber Red Teams, cyber intelligence support, and other subject matter expertise to plan and conduct 45 assessments of operational networks, systems, and missions during Combatant Command (CCMD) and Service exercises.

FY21 assessments included persistent cyber operations, advanced cyber operations, assessments of emerging cyber technologies, to include offensive cyber capabilities, and special project assessments. Table 1 provides a comprehensive list, with major exercises being Global Thunder 21, Global Lightning 21, Mobility Guardian 21, Pacific Fury 21, Pacific Sentry 21, Judicious Response 21, Combined Command Post Exercise 21-2, Trident 21-3 and 21-4, and Copper Ring 21.

To improve the readiness for these exercise assessments, DOT&E continued to expand Cyber Readiness Campaigns, which are designed to help the Combatant Command (CCMD) or Service improve and assess operational-level cyber operations and decision-making. Cyber Readiness Campaigns use a CCMD exercise as the capstone event to assess cyber warfighting in a realistic mission context. Precursor Cyber Readiness Campaign events include cyber-stimulation events, table-top exercises, range-based exercises, and other events (that include full-spectrum threats) to credibly and comprehensively assess the ability of an adversary to deliver mission effects and impact U.S. operational decision-making. DOT&E works with cyber defenders during these events to identify critical problems and help improve defenders' capabilities.

DOT&E analyzed CCMD and Service exercises from FY14 through FY20 to identify strengths, deficiencies, and trends in DOD defensive capabilities. The analysis resulted in the following observations and recommendations.

There is no cyber defense without cyber defenders. In conflict with an advanced adversary, DOD missions will not succeed without effective cyber defenses. Cybersecurity must be built into system design, and the human defender should be included early on in cyber defense engineering and programmatic priorities for both system usability and training. Cyber defenders can and should include dedicated mission defense teams, system users, response-action teams, commanders, and network operators, all of whom should be trained and equipped to fight though cyberattacks to complete critical missions. DOT&E cyber assessments and operational tests continue to show that where systems or networks are actively defended by well-trained personnel in environments employing Zero Trust concepts, Red Teams emulating cyber actors have difficulty degrading critical DOD missions.

The DOD continues to develop and field cyber technologies, such as endpoint security systems and offensive cyber capabilities, without adequate programmatic support or operationally-realistic threat testing. Current DOD acquisition practices avoid the funding of dedicated program offices; such offices would help ensure the effectiveness of cyber technologies and that cyber operators are prepared with the degree of training commensurate with kinetic warfare operators. Lack of trained and resourced program offices is a root cause of many cybersecurity problems DOT&E discovers in the field, such as insecure system design, inadequate training of cyber defense personnel, and insufficient test planning and conduct. DOD development of cyber defenses continues to lag behind our adversaries' growing offensive capabilities, and critical DOD missions remain at risk of disruption from adversary cyber actions.

With DOD missions at risk, DOT&E recommends that warfighter exercises place increased emphasis on training in contested cyber environments. Although all exercises that DOT&E participates in include a DOT&E-sponsored Red Team, exercise authorities seldom permit warfighters to experience representative adversarial cyber effects because of the risk of degrading other training objectives. The net result of this limitation is a false sense of confidence by warfighters and leadership alike: failure to train in realistic cyber environments leaves warfighter skills and playbooks immature, and they will be unable to quickly detect cyberattacks or perform effective response actions.

DOT&E is engaging with the Joint Staff to promote the inclusion of realistic cyber stresses in every major training exercise. A cyber "fight-through objective" will provide warfighters and network defenders the opportunity to experience the spectrum of cyber threats and effects, and allow them to improve their defenses, detections, and resilience.

DOT&E assesses that DOD cyber concerns increasingly mirror those in the commercial sector due to increasing DOD reliance on commercial products and infrastructure. As a result, cyberattacks and vulnerabilities in the

commercial sector also affect the DOD's cyber posture. The FY21, SolarWinds attackers used novel hacking techniques to gain accesses to commercial networks and erase signs of their presence, enabling months of enduring access for research, exfiltration, and preparations for future operations. The DOD must prepare for these types of attack, and confirm the adequacy of preparations with cyber Red Team assessments.

DOT&E relies on Service-led cyber Red Teams to emulate nation-state threats during exercises and operational tests. DOD Red Teams, however, are stretched thin by high demand, and do not have the resources or personnel needed to routinely emulate sophisticated near-peer attacks. The cyber Red Teams need additional resources, as well as automation capabilities, to ease their workload. DOT&E will continue to urge the DOD to address critical Red Team capability gaps to improve CCMD assessments and cyber operational testing.

The DOD increasingly uses commercial cloud services to store highly sensitive, classified data, but current contracts with cloud vendors do not allow the DOD to independently assess the security of cloud infrastructure owned by the commercial vendor, preventing the DOD from fully assessing the security of commercial clouds. Current and future contracts must provide for threat-realistic, independent security assessments by the DOD of commercial clouds, to ensure critical data is protected.

Advances in artificial intelligence (AI) and machine learning will likely add new warfighter capabilities and cybersecurity challenges. The DOD plans to deploy AI capabilities to the CCMDs in FY22, and DOT&E has begun engagement with the Joint AI Center, the DOD Chief Data Officer, and supporting elements who are part of the AI and Data Accelerator Initiative. DOT&E will expand future assessments to help ensure new AI technologies are secure.

Program Activities

Persistent Cyber Operations

Persistent cyber operations provide cyber Red Teams with longer dwell time on DOD networks to probe selected areas and portray more advanced adversaries. As opposed to one- to two- week exercises or tests, long-duration activities offer Red Teams time for stealthier cyber reconnaissance to identify cybersecurity weaknesses and access points that might otherwise go undetected. After obtaining accesses, Red Teams can continue more stealthy operations to move laterally or escalate privileges. These activities may identify subtler and more pervasive vulnerabilities, and provide more realistic training for cyber defenders.

In FY21, DOT&E resourced such operations at six CCMDs, but due to the limited availability of planners and operators, these operations were more "part-time" than persistent. Requests for such activities expanded at the end of the fiscal year, to include networks supporting Ballistic Missile Defense and the global Department of Defense Information Network (DODIN); persistent cyber operations resources will have to continue to grow to adequately evaluate the DOD cybersecurity posture.

Advanced Cyber Operation Team

DOT&E resourced an advanced cyber operations team to augment cyber Red Teams with specialized cyber expertise and assist in the portrayal of more advanced adversaries. The advanced cyber operations team supported persistent cyber operations activities and the development of new cyber tools and tactics, techniques, and procedures (TTPs). During FY21, the advanced cyber operations team supported:

- Cybersecurity testing of the F-35
- Assessments of offensive cyber operations capabilities
- Assessment of Zero Trust architectures in Microsoft Software-as-a-Service environments
- Assessments of military aircraft transponders and critical aircraft systems
- Assessments of industrial control systems

- Development of enhanced Red Team capabilities
- Stand-up of a new Red Team location in Maryland
- Expansion of Red Team accesses via persistent cyber operations
- Review of evolving cybersecurity architectures and defensive measures

Demand for advanced cyber operations support continued to grow in FY21, and DOT&E expects requests for this support to continue into FY22, with efforts 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, including more representative environments, systematic variation of operational conditions, and inclusion of a thinking opposing force. Programs often overlook these critical elements because they focus on expediting development and delivery without completing rigorous OT&E.

Engagement with the Intelligence Community

DOT&E's collaboration and integration with the Defense Intelligence Agency continues to prove critical to our CCMD-focused assessments and OT&E events, and will remain so in the coming year. We continue to face challenges in conducting threat-representative cyber assessments, due in part to information-sharing challenges originating from multiple communities within the Department.

Special Project Assessments

DOT&E performed the following special assessments in FY21 in collaboration with USCYBERCOM, the DOD Chief Information Officer (CIO), Joint Forces Headquarters DOD Information Network (JFHQ-DODIN), the Defense Information Systems Agency (DISA), the Defense Threat Reduction Agency, and the Department of Energy Sandia National Labs:

- Zero Trust architectures in software-as-a-service environments
- DOD Office 365
- Usability of mid-tier defensive cyber operations tools
- DISA Internet Access Point that connects the DOD Information Networks to the commercial Internet
- Internet Protocol version 6 implementation
- 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.

Assessment

The DOD continues to develop and field cybersecurity technologies, such as endpoint security systems and network monitoring tools, without adequate programmatic support or operationally-realistic threat testing. DOD Components often fail to provide dedicated program offices and adequate funding to support the development and fielding of cybersecurity technologies. The lack of trained and resourced program offices is a root cause of many cybersecurity problems DOT&E discovers in the field, such as insecure system design, inadequate training of cyber defense personnel, and insufficient test planning and conduct. In order to improve its cybersecurity posture and avoid costly cybersecurity technology failures, which DOT&E too-often encounters during our cyber assessments, the DOD must ensure that cybersecurity technology development is always conducted by well-resourced program offices; this should include cyber engineering expertise and cyber defense expertise of

the highest caliber. Moreover, training for cyber operators should be commensurate with the degree of training provided to kinetic warfare operators, and should include routine exercises against realistic cyber threats.

There is no Cyber Defense without Cyber Defenders

DOT&E analyzed CCMD and Service exercises from FY14 through FY20 to identify strengths, deficiencies, and trends in DOD defensive capabilities. The analysis showed the importance of defending each phase of a cyberattack, especially the phase during which an adversary maneuvers within a network or system to find their objective. DOT&E found that this phase presents unique detection challenges for cyber defenders. DOT&E also assessed emerging technologies that promise to increase defender visibility to such attacks. These include DOD's Office365 cloud-based environment and the Zero Trust Architecture model, discussed below.

Zero Trust Validation Events

In FY21, DOT&E took part in the DOD's implementation of Office365 and executed 15 cybersecurity assessments to inform decisions by senior leaders in DOD CIO, DISA, and U.S. Cyber Command on various aspects, options, and risks associated with the DOD's O365 employment. These assessments indicated that a data-centric security model implementing Zero Trust principles improves protection of DOD data. Furthermore, given the proper tools, manning, and training, the Zero Trust model can help cyber defenders actively defend mission-critical cyber terrain and enable improved cybersecurity over traditional perimeter-based defenses.

Remote Assessment of Security Stack Usability

DOT&E, in collaboration with a DOD Security Operations Center, conducted a usability assessment of the NIPRNET Joint Regional Security Stacks in FY21. For this project, DOT&E developed a methodology to remotely collect usability information from DOD network defenders. DOT&E intends to share this methodology with the test community to promote more rigorous and routine collection of usability information on fielded systems.

Collaboration with Commercial Sector to Assess Cybersecurity of Infrastructure Supporting DOD Operations

DOT&E observed increasing instances in FY21 where critical elements or even the whole of a DOD capability reside in networks or infrastructure deemed proprietary by the commercial sector, such as commercial clouds. Contractual language often prevents adequate operational test and evaluation of commercial networks and infrastructure within the scope of OT&E, resulting in incomplete evaluations. In the case of cybersecurity testing, independent assessments by DOD Red Teams are essential to assessing the security of DOD's data within the commercial infrastructure; contracts need to permit such assessments for the DOD to be able to understand how well critical mission data is protected.

Several major defense and commercial contractors have recently indicated willingness to allow DOT&E and select DOD Red Team personnel to collaborate with their contractor Red Teams on joint assessments of key elements residing on commercial networks and infrastructure. While not equivalent to independent OT&E, these collaborations represent positive first steps to remedy the current barriers to more complete OT&E and assessment of the myriad networks and capabilities that support all DOD missions.

DOD Ability to Portray Advanced Cyber Threats

In FY21, DOT&E conducted an assessment highlighting the gaps between the cyber capability of advanced threats, as reported by the intelligence community, and the existing DOD ability to emulate such capabilities during cybersecurity exercises and assessments. The most frequent gaps included insufficient time on network for cyber aggressors, limited toolsets, deficiencies in TTPs, unrealistic rules of engagement, and lack of end-to-end planning for a coherent cyber threat campaign. DOD Red Teams do not have the capacity or automation tools to routinely emulate sophisticated near-peer attacks. Such limitations preclude an ability to

stress systems, networks, and warfighters during CCMD exercise assessments and during OT&E to the extent expected in a real-world conflict.

Internet Access Points

Internet Access Points (IAPs) are intended to provide a protected security boundary between the Internet and NIPRNET. DOT&E supported a JFHQ-DODIN assessment of the DISA IAPs, sponsoring a DOD Cyber Red Team to conduct operationally realistic attacks against the IAPs to assess their cybersecurity capabilities. DOT&E provided findings and recommendations, and DISA is developing an implementation plan for a number of the recommendations.

Aircraft Combat Identification

DOT&E, with the Commander, Operational Test and Evaluation Force, analyzed the mission effects from degraded Transponder Combat Identification (T-CID) at the Northern Edge 2021 exercise. Working with DOT&E, the Air Force Life Cycle Management Center conducted a cybersecurity risk-reduction of Mode 5 Level-2 to demonstrate capabilities and effects from an adversary manipulating T-CID messages, and the Air Force Joint Test and Evaluation Program Office assessed air surveillance mission risk from T-CID-based capabilities and developed corresponding TTPs.

Artificial Intelligence

Advances in AI and machine learning will likely add new warfighter capabilities and cybersecurity challenges. During FY21, DOT&E led a team of cyber analysts at the request of the DOD CIO to develop machine learning tools and TTPs for the analysis of DOD network traffic data. The DOT&E team analyzed extremely large data sets using these techniques, allowing a deeper review of the technical data than previously possible using only human capabilities. These tools supported unique cybersecurity analyses and the identification of previously undetected problems. DOT&E briefed the results to the Office of the Secretary of Defense, the DOD CIO, and mission partners.

Assessments of Offensive Cyber Capabilities

The DOD continues to develop offensive cyber capabilities without formal operational testing to ensure such capabilities will work when used against an adversary. Although DOT&E's Cyber Assessment Program is conducting operationally realistic testing against a small subset of critical offensive cyber capabilities, there are many more offensive cyber capabilities being developed in multiple DOD Components with no such testing. This risks such capabilities failing to work when needed, and lowers commanders' confidence in the capabilities. The DOD should ensure offensive cyber capabilities are always operationally tested prior to their fielding.

Endpoint Security Tools

Endpoint security is a critical component of cyber defense-in-depth. For enterprise endpoints, the selection of the endpoint tools has been mandated through DOD CIO policy (e.g., Host Based Security System) with the DOD Components needing exceptions to policy to adopt alternative solutions for their networks.

In FY21, DOT&E conducted an assessment of Microsoft's Defender for Endpoint (MDE) as part of the U.S. Navy's proposed architecture for the enterprise Office365. The positive cybersecurity results of this assessment informed the DOD's decision to use MDE on all Navy endpoints.

Way Ahead and Recommendations

DOT&E will continue to increase the realism of our assessments to accurately assess the warfighter's ability to sustain missions in environments contested and degraded by an advanced cyber adversary. Ready access to a talented cyber workforce and advanced tools remain essential, and DOT&E will continue to advocate that the DOD

establish a well-resourced pipeline of cyber talent from academia, federally funded research and development centers, national labs, and the commercial sector. Overarching recommendations and assessment objectives for FY22 are discussed in the following subsections.

Increase Emphasis on Defenders

The DOD should refocus its cybersecurity efforts on cyber defender personnel, instead of focusing primarily on the technology associated with cyber tools, networks, and systems. Such a focus necessarily encompasses not only the technology, but the doctrine, organization, and training needed to ensure cyber defenders can effectively use technology to thwart cyber adversaries' attempts to disrupt DOD missions. All personnel performing DOD missions – including commanders and system and network operators – should be trained and equipped to recognize and help fight through cyberattacks commensurate with the degree of training provided to kinetic warfare operators. This will require the development of, and training for, new technologies capable of identifying potential cyberattacks to system operators and mission commanders. Such "cyberattack warning" technologies must be developed in order to identify and react to cyberattacks on mobile platforms such as aircraft, ships, and combat vehicles. Critical DOD missions should always be supported by trained teams dedicated to providing cyber defense for those missions.

Independent Assessment of Cloud Infrastructure

DOT&E will continue engagement to improve collaboration with commercial cloud providers in understanding and identifying the cyber risks from commercial cloud infrastructure to DOD critical missions, and ways to mitigate these risks.

The DOD should renegotiate contracts and establish requirements for future contracts with commercial cloud providers that enable the DOD to perform independent and threat-representative cybersecurity assessments of cloud infrastructure which hosts critical DOD capabilities.

Operational Testing of Cyber Tools

The DOD should operationally test cyber capabilities, such as endpoint security tools, prior to their wide-scale deployment to assess their cyber vulnerabilities, operational effectiveness, usability, and interoperability with other tools. The DOD should also assess the effectiveness and usability of existing endpoint security tools to help understand current returns on investment.

Adequate testing of cyber capabilities will require operational environments for both on-premises and cloud-based architectures, with up-to-date catalogs of threats and malware, fielded versions of the endpoint systems, and well-planned tests. Rigorous testing would allow the use of new malware with existing software to determine how well a current defensive cyber tool reacts to zero-day vulnerabilities. Such an infrastructure would also allow for DOD Cyber Red Teams to aggress candidate systems to discover unknown vulnerabilities, defensive cyber experts to fine-tune configurations, and cyber instructors to develop training materials and approved TTPs for selected systems.

Implementing Presidential Directive on Zero Trust

DOT&E will continue supporting Zero Trust efforts with rigorous assessments across the DOD as the Federal Government responds to the May 2021 Presidential Directive to adopt Zero Trust architectures.

Cyber Assessment Support to the ADA Initiative

In May 2021, the Deputy Secretary of Defense launched the Artificial Intelligence and Data Acceleration (ADA) Initiative to expedite deployment of AI-enabled technologies to the CCMDs, starting at the end of FY21. In FY22, DOT&E will proactively work with these teams to identify opportunities to assess the cybersecurity of these technologies in conjunction with the assessment activities that DOT&E already performs at the CCMDs.

Increase Assessment Realism for Offensive Cyber Operations (OCO) Capabilities

DOT&E has placed the Joint Cyber Warfighting Architecture on the DOT&E oversight list. OT&E of the Joint Cyber Warfighting Architecture will provide the opportunity to assess many smaller OCO capabilities not on oversight. DOT&E will coordinate with U.S. Cyber Command and the Service developers of OCO capabilities to increase involvement and test the realism of OCO capabilities and tools not covered under formal OT&E.

Full-Spectrum Cyber Assessments

Cyber operations increasingly involve interactions with the other warfighting domains (air, land, sea, space) and electromagnetic spectrum operations. DOT&E will increase focus on the following during CCMD and Service assessments:

- Cyber-physical systems such as industrial control systems and aircraft transponders
- Cyber-electromagnetic spectrum operations that use the radio frequency itself to cause cyber effects
- Cyber operations at tactical levels for better integration into military maneuvers in other domains

Evolve Persistent Cyber Operations to Campaign Mindset

DOT&E plans to evolve and mature persistent cyber operations to a campaign mindset conducted by a team of specialists to better capture the evolution of cyber actors, from criminal groups to nation-state adversaries. By integrating a campaign-planning element that integrates intelligence and other support components into persistent cyber operations, DOT&E plans to strengthen the persistent cyber operations concept to better portray advanced cyber threats and expand persistent cyber operations to additional CCMDs, as resources permit. DOT&E is developing a cyber campaign pilot partnership with the Air Force.

Mission Assurance Assessments via Wargames

DOT&E intends to offer cyber wargames to the CCMDs and Services as a complementary approach to assessing their cyberspace capabilities and processes. DOT&E will tailor each wargame using the applicable cyberspace terrain, participating cyber units, adversarial objectives and tactics, and overall scenario to enable stakeholders to explore cyberspace decisions and their relationship to improved mission assurance.

Table 1. Cybersecurity Assessments in FY21	
Event Type	**Acquisition Program or Type of Event**
Cyber Assessment Program Events	**Physical Security Assessment (2 Events)** USSPACECOM, USTRANSCOM
	Cooperative Network Vulnerability Assessments (3 Events) USINDOPACOM, USNORTHCOM, USTRANSCOM
	Assessments of Network Security, Stimulation Exercises, and Table Top Exercises (10 Events) USAFRICOM (2), USCENTCOM (3), USEUCOM (2), USSOUTHCOM (2), USSTRATCOM
	Assessment of Mission Effects during Exercises (12 Events) USAFRICOM (2), USINDOPACOM, USSOCOM (2), USSPACECOM, USTRATCOM (2), US Air Force, US Navy (2), USFK
	Assessment of Cyber Fires Processes for Offensive Cyber Operations (4 Events) USINDOPACOM
	Assessment of Special Capabilities and Projects (8 Events) Cyber Red Team Tools, SME Case Studies, DOD O365, DOD SOC Usability Study, USCC ZT Pilots, and USN MDE Assessment
	Assessments Employing 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; USSPACECOM – U.S. Space Command; USSTRATCOM – U.S. Strategic Command; USTRANSCOM – U.S. Transportation Command	