Cyber Assessment Program (CAP)

The 49 cyber assessments conducted in FY22 demonstrated that the limited Zero Trust principles and practices emerging within the Department, when executed by well-trained cyber defenders, will help protect critical DOD missions. Radio frequency and other unconventional cyber threats pose new and serious challenges, and the DOD's abilities to assess against Red Teams portraying nation-state adversaries remain limited due to persistent resource and personnel shortfalls.

Summary of Cyber Assessment Program FY22 Assessments

Cyber Assessment Program (CAP) observations show that even partial implementation of Zero Trust principles by Combatant Commands and Services, if supported by well-trained, experienced cyber defenders, could improve their capability to fight through cyberattacks and accomplish critical missions. The Zero Trust concept assumes the DOD's networks have been breached by adversaries, an assumption borne out by years of DOT&E cyber assessments. Instead of trusting perimeter defenses around a network, which are readily evaded by advanced cyber actors and DOD cyber-Red Teams, Zero Trust relies on strict controls on data access and encryption to secure information.

During FY22, the DOD CIO focused on developing a Zero Trust Strategy and Framework and building a Zero Trust portfolio management office; these are appropriate first steps, but effective implementation of Zero Trust for DOD critical missions will require initial investments, a significant culture shift across the DOD, and a sustained focus of resources. Congressional support for Zero Trust, reflected in Section 1528 of the FY22 National Defense Authorization Act (NDAA), has helped drive this change.

A critical element of Zero Trust is well-trained and equipped cyber defenders supporting defense of critical DOD missions. There is no cyber defense without cyber defenders, however many critical DOD missions lack the support of capable cyber defenders, which include dedicated network defenders as well as weapon system operators and mission commanders trained to respond to cyberattacks. In conflict with an advanced adversary, DOD missions are not likely to succeed without effective cyber defenses, operators, and leaders who are familiar with indications of attacks and the response actions they must be prepared to execute in a timely manner. Implementation of Zero Trust will require significant new technologies to support cyber defenders, such as cyberattack warning systems for operators of weapon systems, methods to routinely tag critical mission data to control who can access that data, and automatic ways to monitor the cyber defense status of mission networks.

As the newest Service, the U.S. Space Force is aware of the threat cyberattacks pose to its missions; missions which are foundational to most DOD combat capabilities. The U.S. Space Force plans to

deploy cyber Mission Defense Teams to support all of its missions. As a key component of Zero Trust, the Mission Defense Teams will require sustained support and resources in order to succeed.

The focus of the DOD's current cyber-related strategies and cyber defenses is on protecting data on internet protocol-based networks and systems. While it is essential to improve defenses of these networks and systems, as Zero Trust is designed to do, such defenses are not sufficient to prevent advanced nation-states from threatening critical DOD missions. A significant shortfall in DOD's cyber posture is defense against unconventional cyber threats, such as those posed by radio frequency (RF)-enabled cyberattacks (e.g., disrupting a system's operations using cyber payloads contained in radio emissions), or direct attacks on weapons systems (e.g., the 1553 busses and other control systems that are essential to many DOD aircraft, ships, and vehicles). FY22 CAP events, recent major exercises, as well as a small number of cyber operational tests have revealed major mission disruptions that can be caused by relatively simple RF-enabled cyberattacks. Future DOD cyber strategies, resource allocation, and Research, Development, Test, and Evaluation efforts must all consider such cyber threats.

Another persistent shortfall in the DOD's cyber posture is the lack of adequate cyber test capabilities. Nation-states, notably Russia and China, are devoting significant resources to offensive cyber capabilities directed against the United States. Comparable test capabilities are needed to adequately assess the DOD's ability to withstand cyberattacks by such nations. Previous DOT&E annual reports have noted this problem, and several recent factors have made the problem more acute: 1) the need to assess the capabilities of the Joint Cyber Warfighting Architecture (JCWA), 2) the demand for cyber operators in the Space Force discussed above, and 3) rapid losses of experienced cyber operators to private industry. JCWA is the DOD's effort to develop an advanced, well-integrated set of cyber capabilities spanning the full spectrum of cyber operations. To succeed, JCWA and the Service branches require top level cyber developmental and operational test capabilities. Currently there are not enough skilled cyber operators in the DOD to support these requirements.

While the DOD's requirements for cyber expertise are rapidly growing, the private industry, spurred by coronavirus (COVID-19) pandemic restrictions, is offering increasingly lucrative offers to the best cyber operators in the DOD, including the ability to earn high salaries while working from home. Many of the DOD's cyber operators are taking these offers, further reducing the available pool of cyber talent in the DOD. To reverse this trend and support the DOD with adequate test capabilities will require the DOD to invest in automated test capabilities to relieve the burden from overtaxed cyber operators and test teams. Other helpful changes to current policies would allow for significantly higher pay, more efficient hiring processes, and more flexible work-from-home opportunities for key personnel such as experienced Red Team operators.

Despite improvements facilitated in part by DOT&E's CAP, DOD development of cyber defenses continues to fall behind the growing offensive capabilities of potential adversaries. DOD missions remain at risk of disruption from adversary cyber actions. The most effective way to reduce this risk is for DOD to place increased emphasis on training in contested cyber environments, especially during major exercises. A cyber "fight-through objective" should be established for every major exercise to provide warfighters and cyber defenders the opportunity to experience the full spectrum of cyber threats and effects, and allow them to improve their defenses, detections, and resilience. To highlight the importance of cyber defenders and expose non-experts to key aspects of cyber warfare, the Institute for Defense Analysis, with the support of DOT&E's CAP, piloted a tabletop cyber wargame in FY22. Initial results were promising, and DOT&E plans to include this wargame as part of future Cyber Readiness Campaigns.

The DOD migration of critical missions and classified data to commercial clouds continues to expand, but current contracts with cloud vendors do not allow the DOD to independently assess the security of cloud infrastructure owned by the commercial vendor. Limited access to the

proprietary cloud infrastructure prevents the DOD from fully assessing the security of commercial clouds and the DOD missions that they support.

Advances in artificial intelligence (AI) and machine learning are expanding in the commercial sector and are expected to add new warfighter capabilities as well as cybersecurity challenges. Future assessments with the Combatant Commands (CCMDs) will be expanded to help ensure warfighter awareness of cybersecurity considerations in employing new AI-enabled technologies.

DOT&E CAP Overview

DOT&E's CAP is a unique, congressionally-directed effort focused on emulating realistic nation-state cyber threats during major CCMD and Service exercises to assess and help improve the Department's ability to fight through cyberattacks to accomplish critical missions. Despite limitations from both COVID-19 and Russian activities in Ukraine, both of which contributed to canceled and/or scaled-back exercises, DOT&E's FY22 assessments included persistent cyber operations, assessing unconventional cyber threats (e.g., combined cyber and electronic warfare attacks), evaluating emerging cyber technologies and offensive cyber capabilities, and special projects to support key mission areas and initiatives such as nuclear command and control and advanced data analytics. Table 1 provides a comprehensive list of major FY22 assessment activities.

As part of the CAP, DOT&E employed Cyber Readiness Campaigns, which are a series of assessment events designed to help CCMDs and Services assess and potentially improve their 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 to help train cyber defenders, tabletop exercises, and range-based exercises to assess the ability of an adversary to disrupt critical missions and impact U.S. operational decision-making. DOT&E worked with cyber defenders during these events to identify critical problems and help improve defenders' capabilities.

Program Activities

Combatant Command and Service Assessments

Of the 49 events in FY22, DOT&E assessed multiple Combatant Commands and Services via Cyber Readiness Campaigns to identify both logical and process issues impeding effective cyber defenses. DOT&E and three of the Operational Test Agencies conduct these assessments in collaboration with the Joint Staff, USCYBERCOM, the Joint Force Headquarters for the Defense Information Networks, and coalition allies and partners. While COVID-19 and events in Ukraine imposed limits on global cyber activities in FY22, there were several notable findings associated with these assessments. CCMD staffs have hardened headquarters networks to the point that in at least two commands, DOD Red Teams were unable to penetrate or maneuver when given network accesses. Assessments also covered new special-purpose or coalition networks, and implemented aggressive remediation processes to address the findings. DOT&E oversaw the integration of offensive cyber operations capabilities into the exercises in FY22, which will continue to expand across the CCMDs. Within the Navy service exercises, the CAP continues to provide key cyber assessment and training to deploying carrier and amphibious troops, and confirmed key practices that harden Navy networks, which the Navy is looking to expand in coming years.

Persistent Cyber Operations

Persistent cyber operations (PCO) provide 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. These activities help identify subtler and more pervasive vulnerabilities and provide more realistic training for

cyber defenders. Based on lessons learned in early FY22, DOT&E revamped PCO planning and execution to be less driven by geographic CCMD areas of responsibility, and more focused on campaign-style assessments organized around selected missions. Long-duration assessments of selected DOD missions span multiple CCMDs, and we expect to see the results of the revamped approach in FY23.

Advanced Cyber Operations Team

DOT&E has access to advanced cyber operators (ACO) across multiple organizations to support special assessments, augment Red Teams with specialized cyber expertise, and assist in the portrayal of more advanced adversaries. Organizations with ACO talent include government Red Teams, Federally Funded Research and Development Centers, National Labs, University-Affiliated Research Center Laboratories, academia, and industry. During FY22, the DOT&E ACO supported:

- Cybersecurity testing of the F-35, Ground-Based Strategic Deterrent, and F-22
- 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
- Development of enhanced Red Team capabilities
- Expansion of Red Team accesses via PCO

Demand for ACO support continued to grow in FY22, and DOT&E expects that trend to continue into FY23, with confounding challenges of talent retention due to competing opportunities in the private sector for cyber professionals.

Assessment of Offensive Cyber Capabilities

DOT&E continued assessments of Offensive Cyberspace Operations (OCO), defined as the application of force in or through cyberspace. DOT&E assessments included OCO and their enabling capabilities, such as RF capabilities, as well as OCO planning and integration with other warfare domains. Capability assessments performed in FY22 focused on realism of the representative network, and realism of the threat, which includes a thinking opposing force or adversary. FY22 assessments on the application of OCO in realistic scenarios were performed primarily with USINDOPACOM, U.S. Forces Korea, and Joint Special Operations Command.

Engagement with the Intelligence Community

DOT&E's collaboration with the Intelligence Community remains an essential element of CCMD mission-focused assessments and OT&E events. High classifications assigned to intelligence information on advanced adversary capabilities and intent limit the ability of assessment teams to fully emulate the full-spectrum adversary against which warfighters should routinely practice the execution of their missions. DOT&E is working with the Office of National Intelligence, the Defense Intelligence Agency, DOD Red Teams, the National Ground Intelligence Center, the National Air and Space Intel Center, and the Missile and Space Intelligence Center to improve the information sharing and the resulting realism of the threat portrayed in assessments and OT&E.

Special Project Assessments

DOT&E performed the following special assessments in FY22 in collaboration with USCYBERCOM, USSTRATCOM, the DOD Chief Information Officer (CIO), the Chief Digital and AI Office (CDAO), Joint Forces Headquarters DOD Information Network (JFHQ-DODIN), the Defense Information Systems Agency (DISA), and the Department of Energy Sandia National Labs:

- Zero Trust architectures in Software-as-a-Service environments
- Industrial Control Systems
- RF-enabled cyber operations
- Small Business Innovative Research projects for enhanced cybersecurity of software applications
- Transponder-Combat Identification
- Commercial cloud assessments

- Preparations for assessments of AI and machine learning technologies
- Nuclear command, control, and communications
- Wargames to improve and expand assessments beyond the limits of exercises

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.

Results

Combatant Command and Service Assessments

A decade ago, and with SECDEF endorsement, the Chairman of the Joint Chiefs of Staff directed DOD components to incorporate a realistic operational environment into all major DOD exercises. The stated purpose was to improve the DOD capability to sustain operations in a denied or degraded cyber environment. DOT&E was directed to conduct operational assessments of cyber defenses and mission assurance during these exercises. On the 10-year anniversary of the SECDEF-endorsed Chairman of the Joint Chiefs of Staff Execute Order, DOT&E notes the following trends:

- Most exercise authorities allow some level of cyber adversary portrayal during their exercises
- Some CCMDs support longer-duration cyber-Red Team activities (see section on PCOs)
- Network defenses have improved against low- and mid-level cyber threats
- Some CCMDs are showing increased interest in cyber mission rehearsals to augment traditional training exercises

These are positive trends, with the last one critically needed to make up for exercise cancellations and reductions in FY20-21 due to COVID-19. The negative trends are:

- Adversary play during most exercises falls well below the stresses expected from an advanced persistent threat
- Realistic effects that would stress leadership, operators, and network defenders are seldom permitted
- Training objectives receive higher priority than including representative cyber-threat environments.

As a result, DOT&E has limited data to assess whether warfighters can sustain missions in cyber-contested conditions representative of an advanced adversary. In conflict with an advanced adversary, DOD missions will not succeed without effective cyber defenses or operators and leaders who are familiar with indications of attacks and the response actions they must be prepared to execute in a timely manner. In the absence of routine exercises that practice fighting through advanced cyberattacks, DOD missions are at risk of disruption from adversarial cyber actions.

The remainder of this section covers assessment activities that the DOT&E CAP supported in FY22, ranging from Zero Trust validation events, special assessments of emerging and commercial technologies, and assessments of specific mission areas, such as NC3 challenges and concerns about the ability of DOD Red Teams to portray advanced adversaries.

Zero Trust Validation Events

The DOD CIO describes Zero Trust as "protecting critical data and resources, not just the traditional network or perimeter security" (Department of Defense Zero Trust Reference Architecture). For several years, DOT&E CAP has recommended moving from boundary-focused to data-focused protections. Throughout 2022, DOT&E CAP continued to see failures of the DOD's defense-in-depth architecture due to failures in technologies and defenses at higher levels that lower-tiered organizations are fully dependent on, and yet are unaware of the failures. The complexity of the current architecture creates significant challenges to adequate cyber survivability of critical DOD missions.

The DOD has many ongoing efforts to move to a Zero Trust architecture and DOT&E CAP has observed positive outcomes as a result of adoption

of various combinations of the tenets and pillars of Zero Trust, as defined by the DOD CIO. DOT&E CAP has not yet observed a complete implementation of Zero Trust that includes continuous multi-factor authentication, micro segmentation, encryption, endpoint security, automation, analytics, and robust auditing. Listed below, under the tenets and pillars of Zero Trust, are DOT&E CAP observations so far:

TENETS:

- Assume a Hostile Environment – DOT&E's assessment results support this assumption.
- Presume Breach – DOT&E-sponsored cyber–Red Teams routinely breach network perimeters.
- Never Trust, Always Verify – The concept of least-privilege and locking down access to data continues to be a challenge across the DOD enterprise.
- Scrutinize Explicitly – Cyber defenders with training and capabilities continue to be identified as the most critical attribute to cyber survivability.
- Apply Unified Analytics – Multiple efforts are ongoing across the DOD to improve logging and analytics for every action but the efficacy of these actions is still unclear.

PILLARS:

- Users – Shortfalls in multi-factor authentication and privilege access management remain.
- Device – Device monitoring, comply-to-connect, and continuous monitoring of devices across the DOD has improved but is not yet complete.
- Network – Segmentation and granular access to the multitude of DOD networks remains a challenge.
- Data – Organizations have started to review the criticality of data elements in preparation for Zero Trust.
- Visibility and Analytics – Improvements in visibility have contributed to cyber defenders' successes.
- Automation and Orchestration – Some organizations have implemented automated security processes to orchestrate security changes at a faster pace, but this is not ubiquitous across the DOD.

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

DOT&E observed growing instances in FY22 where critical elements of a DOD capability reside in networks or infrastructure deemed proprietary by the commercial sector; this is especially true with commercial clouds. The DOD migration of critical missions and classified data to commercial clouds continues to expand, but current contracts with cloud vendors do not allow the DOD to independently assess the security of cloud infrastructure owned by the commercial vendor. This prevents the DOD from fully assessing the security of commercial clouds and the DOD missions that they support. Future contracts must provide for threat-realistic, independent security assessments by the DOD of commercial clouds to ensure critical data is protected.

During FY22, DOT&E continued to collaborate with Amazon Web Services, which is providing commercial cloud services that support critical DOD missions. Planning is underway for assessments of cloud infrastructure, and events that will bring DOD network defenders into closer coordination with Amazon Web Services defenders. This will help ensure both sets of defenders gain appreciation for their counterpart's sensors, tools, and approaches to detecting and responding to cyberattacks, and improve responses to attacks. Collaboration between DOT&E and cloud service providers enables DOD and cloud vendors to develop and share best practices and information on emerging technologies and threats, and helps ensure DOD's commercial clouds are secure against advanced cyber adversaries.

DOD Ability to Portray Advanced Cyber Threats

A large gap exists between the cyberattack capabilities of advanced threats and the ability of DOD Red Teams to emulate these threats during exercises assessments and OT&E. One dimension of this gap is insufficient time on network for cyber aggressors;

persistent cyber operations are expected to reduce this component of the capability gap. Other gaps include limited Red Team toolsets, deficiencies in Red Team tactics, techniques, and procedures, unrealistic rules of engagement during exercises, and lack of end-to-end planning for a coherent cyber threat campaign.

DOT&E sponsors a Red Team Development Working Group that identifies requirements for emulating various adversaries and pursues the acquisition of development of tools for Red Teams that will improve the realism of assessments on operational networks. Resources for tool development and acquisition are limited, as are the number of master-level operators needed to portray advanced adversaries.

Aircraft Combat Identification

DOT&E consolidated two years of data showing the mission effects from degraded Transponder Combat Identification (T-CID), including potential effects from an adversary manipulating T-CID messages These results are now included in planning efforts for selected FY23 CCMD and Service exercises.

Artificial Intelligence and Machine Learning

DOT&E continued efforts to prepare for assessments of AI-enabled technologies. This included engagement with CDAO representatives at multiple CCMDs to prepare for deployments of AI-enabled technologies via the DOD's AI and Data Acceleration (ADA) initiative, as well as other efforts already underway at USINDOPACOM and USNORTHCOM. The DOT&E CAP initiated an AI/Machine Learning (AI/ML) working group with Federally Funded Research and Development Centers, National Labs, Academia, and DOD Red Teams. This working group began to identify best practices for AI/ML assessment methods and tools, metrics unique to AI/ML technologies, Red Team tools and tradecraft needed to perform counter-AI/ML assessments, and specific requirements for range environments.

Data Standards, Training, and Automation

DOT&E relies on data from the Red Teams to correlate adversarial activities with mission assurance findings and defensive cyber processes. Historically, Red Team data products required manual collection of their adversarial cyber activities. DOT&E analytical objectives for FY23 and beyond will require improved Red Team data standards and training, and automated collection of Red Team data. DOT&E established a working group to create automated data collection procedures that will assist Red Teams in capturing and reporting required data.

Missile Defense PCO Assessment

The Missile Defense Agency (MDA) continued a PCO assessment of the MDA unclassified and classified networks (UNet/CNet) in FY22. While not the operational networks for the Missile Defense System, the UNet/CNet are paramount to the development effort leading to a combat-capable Missile Defense System. The goal of this PCO is to discover potential cybersecurity vulnerabilities and identify potential fixes to help make UNet/CNet more secure.

Nuclear Command, Control, and Communications (NC3) Hardening

DOT&E and Commander, USSTRATCOM have committed to a partnership for assessing and improving the cyber survivability of the NC3. USSTRATCOM has directed NC3 enterprise organizations to conduct hardening actions on their respective NC3 systems.

In FY22, DOT&E met with 20 NC3 enterprise organizations to discuss how they implemented the requested NC3 hardening actions, observed and reported on challenges in the NC3 hardening process, and provided recommendations to USSTRATCOM for future NC3 hardening efforts. As a result of these efforts, many important improvements have been made to the NC3 mission.

The complex nature of the hybrid legacy and modernized system-of-systems that comprises the NC3 poses challenges to assessments of this mission space, however, progress is being made across the NC3 enterprise as a result of the continued partnership. Barriers to cyber assessments of the NC3 enterprise include a lack of operational capacity

to support operations and testing simultaneously, as well as ongoing modernization efforts.

Offensive Cyber Capability Assessments

The DOD continues to develop offensive cyber capabilities without formal operational testing to ensure such capabilities will work when used against in representative operational conditions. Although DOT&E's CAP supports operationally realistic testing against a small subset of 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. DOT&E collaborated with USCYBERCOM representatives in FY22 with the goal of making such testing more routine and placed the JCWA on the DOT&E oversight list. OT&E of the JCWA will provide the opportunity to assess many smaller OCO capabilities not on oversight.

U.S. Space Force

U.S. Space Force, as the newest Service, recognizes the importance of cybersecurity and cyber survivability as key elements to its ability to perform its missions; this recognition and commitment to improvement has been instilled in the Space Force by the Chief of Space Operations. For example, the Space Force is building units that will assign cyber defense forces to critical space systems. This effort directly aligns with findings from DOT&E assessments that knowledgeable defenders with training and tools are vital to cyber survivability. At the request of the Chief of Space Operations, DOT&E is providing cybersecurity assessments, training opportunities with DOD Red Teams, and lessons learned from other assessments across the DOD in order to speed the establishment and maturation of these critical forces.

Wargames to expand Mission Assurance Assessments

To highlight the importance of cyber defenders and expose non-experts to key aspects of cyber warfare, the Institute for Defense Analysis, with the support of DOT&E's CAP, piloted a tabletop cyber wargame in FY22. Initial results were promising, and DOT&E plans to include this wargame as part of future Cyber Readiness Campaigns. Wargames may also help demonstrate potential mission impacts of advanced cyberattacks to warfighters and leaders.

Way Ahead and Recommendations

Increasing the realism of the assessments to accurately assess the warfighter's ability to sustain missions in environments contested and degraded by an advanced cyber adversary will continue in FY23. Ready access to a talented cyber workforce and advanced tools remains essential, and DOT&E continues 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 FY23 are discussed in the following subsections.

Combatant Command and Service Exercises Should Increase Emphasis on Fighting Through Cyberattacks

The DOD should continue to emphasize improving the skills of cyber defender personnel. Increased focus should encompass not only the technology, but also the doctrine, organization, and training needed to ensure cyber defenders can effectively 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. The DOD should establish a cyber "fight-through objective" for every major exercise to provide warfighters and cyber defenders the opportunity to experience the full spectrum of cyber threats and effects; allow them to improve their defenses, detections, and resilience; and demonstrate they can fight through representative cyberattacks.

Assessment of Zero Trust Implementation

DOT&E will continue performing rigorous assessments of Zero Trust implementation across the DOD.

Commercial Cloud Infrastructure Independent Assessments

DOT&E will continue collaboration with commercial cloud providers to identify risks 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.

Advanced Cyber Threat Emulation

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 areas to achieve a more-realistic portrayal of full-spectrum threats during CCMD and Service assessments:

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

DOT&E will continue to sponsor the Red Team Development Working Group to provide more advanced tools and tradecraft for Red Teams that support CAP assessments and OT&E. DOT&E will also pursue additional resources for tool development and acquisition that include IP, non-IP, and special capabilities that will be needed for assessments of new technologies such as AI-enabled capabilities.

Aircraft Combat ID

DOT&E will assess T-CID in FY23 Northern Edge and Bold Quest exercises. DOT&E will include other cyber-RF threats in CAP events, and transition mature threat emulations into relevant OT&E.

AI- and ML-Enabled Technology Assessments

DOT&E will work with CDAO representatives to assess the cybersecurity of AI-enabled technologies deployed to the CCMDs, in conjunction with the assessment activities that DOT&E already performs at the CCMDs. DOT&E will continue efforts to identify best practices for AI/ML assessment methods and tools, metrics unique to AI/ML technologies, Red Team tools and tradecraft needed to perform counter-AI/ML assessments, and specific requirements for range environments.

Data Standards and Automation

DOT&E will invest in new technology and personnel to achieve improved Red Team data standards and improve automation for collecting Red Team data.

Missile Defense PCO Assessments

The MDA should continue PCO assessments of the MDA unclassified and classified networks (UNet/CNet) in FY23. DOT&E will monitor progress of these assessments, ensure this PCO effort is executed to the same standards as other PCO assessments sponsored by DOT&E, and synchronize findings with missile-defense assessments performed with CCMDs.

Nuclear Command, Control, and Communications (NC3) Hardening

DOT&E will continue close collaboration with Commander, USSTRATCOM and the NC3 enterprise organizations to assess the hardening actions on their respective NC3 systems.

Offensive Cyber Operations Capability Assessments

DOT&E will continue engagement with USCYBERCOM and the Service developers of OCO capabilities to increase test the realism of OCO capabilities and tools not covered under formal OT&E. The DOD should ensure critical offensive cyber capabilities are operationally tested prior to their fielding.

U.S. Space Force

In FY23, DOT&E will continue to ramp up assessment activities with the U.S. Space Force and the U.S. Space Command. New assessment teams will be established and supporting resources identified to support planning and execution of mission-focused exercises with representative threat emulation.

Wargames to Expand Mission Assurance Assessments

DOT&E will use cyber wargames at CCMDs in FY23 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. These wargames should be particularly helpful to extend beyond exercise events that were limited due to competing training objectives, and to explore in focused ways the potential mission impacts of advanced cyberattacks; the indications and warnings of these attacks; and the types of responses that defenders, operators, and leaders should have at the ready to sustain their critical missions in cyber-contested environments.

Table 1. Cybersecurity Assessment Program FY22 Activity

Type of Event
Physical Security Assessment (4 Events) USINDOPACOM, USSOCOM, USSTRATCOM, USFK
Range Event (1 Event) USCENTCOM
Assessments of Network Security, Stimulation Exercises, and Tabletop Exercises (11 Events) USCENTCOM, USCYBERCOM (2), USEUCOM, USINDOPACOM (2), USSOCOM, USSOUTHCOM, USSPACECOM, USSTRATCOM, USFK
Assessment of Mission Effects during Exercises (13 Events) USAFRICOM (2), USINDOPACOM, USNORTHCOM, USSOCOM (2), USSOUTHCOM, USTRATCOM, US Air Force, US Navy (3), USFK
Assessment of Cyber Fires Processes for Offensive Cyber Operations (2 Events) USINDOPACOM, USFK
Assessment of Special Capabilities and Projects (12 Events) Capability Assessment (2), OCO Capability (4), SME Support (2), TCID (4)
Assessments Employing Persistent Cyber Operations (6 Efforts) USCENTCOM, USEUCOM, USINDOPACOM, USSTRATCOM, U.S. Air Force, Missile Defense Agency
OCO – Offensive Cyberspace Operations; SME – Subject Matter Expert; TCID – Transponders, Combat Identification; 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