# Cyber Assessment Program (CAP)

As DoD cyber defenses continue to improve, the offensive capabilities of potential adversaries are escalating; many DoD cyber defenses and warfighter missions remain vulnerable to offensive cyber capabilities of potential adversaries. DoD is implementing Zero Trust best practices, which are imperative to defend against advanced cyberattacks, but full implementation will take several years, and may require a level of training, expertise, and automation that is not currently planned. Until effective defenses and fight-through capabilities are developed, implemented, and routinely practiced, critical DoD missions will likely be degraded in conflicts with an advanced adversary.

DoD's cyber posture remains at risk from attacks by unconventional threats, such as those posed by radio frequency (RF)-enabled cyberattacks

where cyber payloads in radio emissions disrupt systems, or direct attacks on weapon systems' data busses and control systems that are essential to aircraft, ships, and vehicles. During FY23, relatively simple RF-enabled cyberattacks caused critical mission disruptions. Future DoD cyber strategies, resource allocation, development, and testing must consider such cyber threats.

Many combatant commands (CCMDs) are increasing the threat realism of their exercises, with U.S. Indo-Pacific Command leading the transition from training exercises to mission rehearsals. These operationally realistic events enabled DOT&E's Cyber Assessment Program (CAP) to emulate more advanced adversaries in selected events, affording warfighters and defenders opportunities to fight through more realistic contested environments. With the increasing demand from CCMDs for greater threat realism, additional cyber Red Team resources are needed to emulate increasingly advanced threats in these expanding mission rehearsals. Because every CAP assessment provides recommendations on how to improve defenses, commands almost always demonstrate improved network and mission assurance in subsequent assessments, decreasing the risk of mission disruption due to advanced cyberattacks.

DoD continues to accelerate the migration of critical missions and classified data to commercial clouds, but limited access to proprietary cloud infrastructure has prevented the DoD from independently assessing the cyber survivability of commercial clouds and the DoD missions that they support. Commercial clouds containing classified DoD mission data are a prime target for advanced cyber adversaries, and such assessments are critical to ensure DoD data is protected. The DoD should perform operationally realistic assessments of the proprietary cloud infrastructure needed to support DoD's portion of the cloud, using cyber Red Teams emulating advanced adversaries. The DoD's Joint Warfighting Commercial Cloud contracts require this, as does recent legislation. Both DoD and the commercial cloud vendors would benefit from such assessments, and DoD Components should work with commercial cloud vendors and DOT&E to ensure they are routinely performed.

Cross domain solutions (CDS) are key to the movement of critical DoD mission data. CAP performed reviews of CDS implementation in FY23 and identified the need for further evaluation of the cyber survivability of DoD CDS capabilities. DOT&E has placed CDS on oversight to ensure rigorous testing and full awareness of the operational state of CDS capabilities.

Significant advances in artificial intelligence (AI) and machine learning (ML) occurred in the commercial sector during FY23. In FY23, CAP – in partnership with the Chief Digital and AI Office (CDAO), federally funded research and development centers (FFRDCs), National Labs, academia, and DoD cyber Red Teams – accelerated its efforts to develop and demonstrate assessment methods and tools unique to AI/ML technologies and will continue these efforts in FY24 in anticipation of deployments of AI-enabled capabilities to the CCMDs.

## PROGRAM OVERVIEW

CAP is a congressionally directed program, established in FY03, focused on assessing the cyber survivability of CCMD and Service missions in contested environments. Congress directed DOT&E to plan and conduct these operational evaluations during major exercises.

DOT&E resources cyber Red Teams to emulate realistic adversaries during major CCMD and Service exercises, and to provide assessment venues to help warfighters improve their ability to fight through cyberattacks and accomplish critical missions. DOT&E also provides resources to assessment teams from the Operational Test Agencies and FFRDCs to plan and execute mission-focused assessments and analyze and report on the results at the system, network, and operational levels.

Although exercises are the primary venues for CAP assessments, DOT&E also employs Cyber Readiness Campaigns (CRCs) that include non-exercise events to examine specific elements of warfighter missions

and defenses. These CRC events may include pre-exercise Red Team activities, cyber-stimulation events to help cyber defenders fine-tune their sensors and response actions, tabletop exercises with leadership to explore various contingency plans, and range-based events to examine mission elements and threats that may not be appropriate for operational networks. CRCs provide advanced training opportunities for the CCMDs and Services to rehearse their missions in environments that include realistic adversary emulation. The CRC events that culminate with an exercise capstone event enable CAP to assess cyber warfighting in a realistic mission context.

## MISSION

The CAP mission is to characterize and support improvement of the DoD's ability to defend critical warfighting capability and missions against cyberattacks and to project cyber power in support of national defense and security objectives. CAP assessments focus on fielded warfighting capabilities and encompass the ability of operational warfighters to plan and conduct full-spectrum cyberspace operations in support of overall CCMD missions.

## FY23 KEY ACTIVITIES

In FY23, CAP fused together focused intelligence expertise, pre-exercise Red Teams (see Persistent Cyber Operations below), and exercise Red Teams into a unified cyber opposing force (OPFOR) that affected a wide range of missions and supporting components at U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), U.S. Special Operations Command (USSOCOM), and other venues. These activities set the conditions for rigorous assessments with representative adversary emulation and improved the realism of mission rehearsal for the participating commands.

During these assessment activities, CAP teams identified cyber vulnerabilities and demonstrated potential impacts that could degrade CCMD missions, all of which were fully communicated to system owners and network defenders so that vulnerabilities could be remediated, and missions made more resilient. The assessment teams also identified improvements in cyber defenses, including well-defended enclaves that have been assessed and enhanced through multiple cycles and have incorporated some Zero Trust principles. Room for improvement remains, particularly at Service-level components, which can be targeted through long-duration persistent Red Teams and other more advanced means.

To help keep pace with evolving cyber adversaries, in FY23 CAP developed new cyberattacks targeting cloud technologies and AI/ML capabilities. CAP developed cyberattacks using the RF spectrum, and techniques integrating cyberspace effects with both kinetic and non-kinetic effects. CAP also developed new capabilities for cyber Red Team data automation and improved collection methodologies for cyber-defense data.

### » CCMD AND SERVICE ASSESSMENTS

During FY23, CAP performed cyber assessments at nine CCMDs (U.S. Africa Command [USAFRICOM], U.S. Central Command [USCENTCOM], USEUCOM, U.S. Northern Command [USNORTHCOM], USINDOPACOM, USSOCOM, U.S. Southern Command [USSOUTHCOM], U.S. Strategic Command [USSTRATCOM], and U.S. Transportation Command [USTRANSCOM]), and four Services (Air Force, Army, Navy, and Space Force). As projected in the FY22 Annual Report, DOT&E ramped up assessment activities with the U.S. Space Force and the U.S. Space Command. In FY23, CAP collected data on sensors, manning, and training to inform cyber defense initiatives, and in FY24, CAP will conduct its first assessment of the new Tier 1 APOLLO GRIFFEN exercise.

CAP prepared a classified report for each CCMD and Service assessment that documents the planning, execution, analyses, and recommendations. Cybersecurity perimeter defenses at most assessed CCMDs and Services were effective but defensive capabilities against threats that have penetrated the perimeter were often lacking. This is a concern because a persistent adversary is highly likely to

penetrate any defensive perimeter, given enough time. At several CCMDs, perimeter cyber defenses were improved from prior years, as were abilities to detect and respond to threats rapidly. These improvements resulted in a greater number of events where Red Team activity was stopped before these exercise adversaries could achieve opposing-force objectives. Once inside perimeter defenses, Red Team activities were generally successful, at the expense of warfighter missions and objectives.

In FY23, CAP expanded exercise assessments to include more component commands, Service cyber components, and U.S. allies and partners in recognition that exercises frequently involve components supporting the CCMD. DOT&E observed a range of cyber defense capabilities across the participating components. Some groups of local defenders were better resourced and trained than others, and those defenders tended to be more capable. The CCMDs should ensure that their subordinate components are adequately resourced to counter cyber threats and inform the components of how their cyber vulnerabilities affect CCMD missions.

CAP continued to incorporate cyber opposing-force leads in exercise assessments to help translate cyber effects into mission effects for the exercise control group. Exercise controllers included those mission effects in multiple exercise scenarios, providing dynamic training opportunities for the command staff and exercise participants. This training could be improved by including a wider range of disruptive effects representative of those that potential adversaries could deliver. Exercises with more realistic adversary portrayal would provide warfighters and defenders with improved opportunities to practice their missions in the expected contested environments and help them enhance their fight-through capabilities. In FY23, leadership at several CCMDs emphasized the shift from "training exercises" to more operationally realistic "mission rehearsals," most prominently by USINDOPACOM.

Operationally realistic mission rehearsals simultaneously stress all aspects of CCMD missions and provide the best opportunities for DOT&E to assess CCMD's ability to fight through contested environments and be successful in their missions. The DoD should continue the enhanced realism observed by DOT&E in FY23 during FY24 and beyond.

A significant limitation to enhanced operational realism during CAP assessments is that DoD Red Teams remain under-staffed and under-resourced. Compounding this issue are continuing challenges with retention of Red Team experts who are being stressed by ever-increasing demand, and lack of development pipelines for advanced cyber tools and tradecraft. DoD Red Teams lost many of their journeyman and master-level operators over the last several years, and it will take many years and significantly more resources to remedy these losses. Unless remedied, cyber Red Team shortfalls will lead to inadequate preparation during mission rehearsals, inadequate program acquisition activities, and ultimately critical warfighter capabilities that are not survivable.

DOT&E observed in FY23 that cyber-related information sharing could be improved across the DoD at all levels. Successful cyber defense requires completing prevent, detect, respond, and recover actions, and organizations should ensure they can reliably conduct incident reporting and cyber-threat intelligence sharing. The interconnected nature of networks and systems, trust relationships across commands, and the ability for data to be rapidly disseminated means that an individual CCMD's data security depends on all participating DoD parties. Combatant commanders and DoD leadership should fully understand the mission risks associated with data sharing initiatives across the Department, including the Combined Joint All-Domain Command and Control (CJADC2) initiative.

## » SPECIAL ASSESSMENTS

CAP performed the following special assessments in FY23 in collaboration with U.S. Cyber Command (USCYBERCOM), USSTRATCOM, the DoD Chief Information Officer (CIO), CDAO, Joint Forces Headquarters DoD Information Network (JFHQ-DODIN), the Defense Information Systems Agency (DISA), and the Department of Energy's Sandia National Laboratories:

- Zero Trust architectures in Software-as-a-Service environments
- Transponder-Combat Identification
- Commercial cloud assessments
- Cross-Domain Solution (CDS) assessments
- Nuclear Command, Control, and Communications (NC3)
- Offensive Cyberspace Operations (OCO)
- Preparations for assessments of artificial intelligence (AI) and machine learning (ML) technologies
- Industrial Control Systems
- Radio frequency (RF)-enabled cyber operations
- 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 CRCs, as well as cybersecurity OT&E of acquisition programs. A number of these special assessments are discussed below.

## Zero Trust Environment Assessments

The DoD CIO describes Zero Trust as "protecting critical data and resources, not just the traditional network or perimeter security" (DoD Zero Trust Reference Architecture). In keeping with recommendations made by DOT&E over the past several years to move from boundary-focused to data-focused protections, the DoD CIO has many ongoing efforts to move to a Zero Trust architecture, and CAP has observed positive outcomes because of the adoption of various combinations of the tenets and pillars of Zero Trust, as defined by the DoD CIO.

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. The CIO Zero Trust Portfolio Management Office resourced four commercial providers to develop and deploy Zero Trust environments, and in FY23 CAP completed two assessments of a cloud service provider's Zero Trust environment. Other cloud service provider environments will be examined in FY24.

## Cross-Domain Solution (CDS) Assessments

CDS are integrated hardware/software systems that enable access and exchange of sensitive data across networks at different levels of security classification. CDS capabilities are essential for the movement of data across myriad DoD systems that are critical to warfighting capabilities. CAP reviewed CDS implementation in FY23 and identified the need for further evaluation of the cyber survivability of DoD CDS capabilities. As a result, DOT&E has placed CDS on oversight to ensure rigorous testing and full awareness of the operational state of CDS capabilities.

## Nuclear Command, Control, and Communications (NC3)

CAP and USSTRATCOM continued a partnership for assessing and improving the cyber survivability of NC3. The complex nature of the hybrid legacy and modernized system-of-systems that comprises 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.

CAP is sponsoring the development of a high-fidelity virtualization environment for a subset of NC3 legacy systems. This environment will assist with assessments and Red Team activities that would otherwise be challenging on the operational networks. Once validated, the environment will also help assess and experiment with improved cybersecurity defenses and allocation of sensors deployed across the transitioning NC3 systems-of-systems.

## Offensive Cyberspace Operations (OCO)

DOT&E continued assessments of OCO, defined as missions intended to project power in and through cyberspace. DOT&E conducted OCO capability assessments on capabilities developed and fielded

by the Air Force and by USCYBERCOM. DOT&E also conducted assessments on the integration and synchronization of OCO in major exercises at USINDOPACOM, U.S. Forces Korea (USFK), USEUCOM, and key events with Joint Special Operations Command. In addition to continued assessments supporting USINDOPACOM, USFK, USEUCOM, and Joint Special Operations Command in FY24, DOT&E plans to assess capabilities and events supporting USSOUTHCOM, U.S. Space Command (USSPACECOM), and USSTRATCOM's Joint Electromagnetic Spectrum Operations Center.

In FY24, DOT&E will also expand its ties with the Defense Advanced Research Projects Agency (DARPA) and with OUSD(R&E) to support early operational assessments of unique, "fast-tracked" capabilities. In some cases, this will require broader team accesses to specialized programs, and DOT&E will continue to work with the OUSD(A&S) Special Access Program Central Office (SAPCO) to ensure early operational assessments are conducted to improve development and timely delivery of important capabilities to the warfighter.

The DoD continues to develop most OCO capabilities without formal operational testing. Although CAP provides operationally realistic assessments for a small subset of OCO capabilities, there are many more OCO capabilities being developed in multiple DoD Components with no such assessments. OCO capabilities continue to grow in importance to DoD missions, and insufficient testing in operational environments with representative threats may result in OCO capabilities failing to work as needed, or in a lower confidence regarding the scope and duration of OCO capability effects.

## Artificial Intelligence (AI) and Machine Learning (ML) Assessments

In FY23, CAP expanded efforts to prepare for assessments of AI-enabled technologies, working with the CDAO, FFRDCs, National Labs, academia, and DoD Red Teams on the development and demonstration of assessment methods and tools unique to AI/ML technologies. CAP will continue these efforts in FY24 in anticipation of deployments of AI-enabled capabilities to the CCMDs and ensure good alignment with related DOT&E initiatives addressed under Pillar 4 of the DOT&E Strategy Implementation Plan, especially "Evaluate the operational and ethical performance of AI-based systems."

CAP performed the first phase of a series of tabletop exercises for a technology recommended by the CDAO, which will help develop best practices for future assessments of AI/ML capabilities. In parallel, CAP is identifying the Red Team tools and tradecraft needed to perform counter-AI/ML assessments, and specific requirements for range environments. CAP coordinated with the Joint Information Operations Range to create a persistent range environment where AI/ML assessments can be hosted and is working with CDAO to receive models under development for pilot assessments and training of DoD Red Teams in aggressing AI/ML systems.

## Radio Frequency (RF)-Enabled Cyber Operations

DOT&E recognizes the importance of Joint Electromagnetic Spectrum Operations and its close relationship to offensive and defensive cyber capabilities. The National Defense Strategy notes that electromagnetic spectrum (EMS) and other non-kinetic threat developments are challenging U.S. response capabilities, and rapid and low-cost technology is eroding U.S. technology leads. In close partnership with the Air Force Cyber Resiliency Office for Weapon Systems (CROWS), CAP is expanding its assessments to include RF-enabled cyberattacks to facilitate an enhanced OPFOR that is not solely focused on traditional cyber and Internet Protocol (IP) networks but includes spectrum and apertures to the spectrum. CAP has taken action on the assertion made in last year's Annual Report by integrating effects based on potential RF-enabled cyberattacks (cyber payloads contained in radio emissions). These effects include system degradation due to direct attacks on weapon systems' data buses and other control systems essential to many DoD aircraft, ships, and vehicles.

In FY23, DOT&E consolidated two years of data showing potential mission effects for Transponder – Combat Identification systems and developed tools and methods to safely replicate and insert

these effects into aircraft flying during operational exercises. DOT&E is working with operators and solution providers to assess remedial actions and updates to tactics, techniques, and procedures to mitigate risks posed by these threats. Additionally, these results will be included in planning for future CCMD and Service exercise assessments.

### Cyber Wargames to Expand Mission Assurance Assessments

CAP has designed a set of cyber wargames with an emphasis on the operational level of warfare. These wargames will help extend assessments beyond the limitations of exercises on operational networks and help demonstrate potential mission impact of advanced cyberattacks to warfighters and leaders. To highlight the importance of cyber defenders and expose non-experts to key aspects of cyber warfare, CAP Wargame (CMOCK-W). CMOCK-W will help leaders become more familiar with degraded environments not generally permitted during training exercises and assist in refinement of contingency and response-action planning. CMOCK-W will be implemented in FY24 as part of the CRC for several CCMDs. Rigorous and recurring CMOCK-W engagement will improve warfighter preparations to fight through contested cyber environments and improve mission assurance.

## » SUPPORTING ACTIVITIES

### Persistent Cyber Operations (PCO)

PCO 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. These activities help identify subtler and more pervasive vulnerabilities and provide more realistic training for cyber defenders. The longer dwell time enables PCO Red Teams to escalate privileges and move laterally within target networks to cause effects at the time of their choosing, as an advanced persistent threat would. Accesses gained by PCO are handed off to exercise Red Teams acting as cyber OPFOR during specified exercises.

During FY23, DOT&E expanded PCO to include three DoD-certified Red Teams and improved the process for PCO planning and execution. The new process focuses on campaign-style assessments of selected missions and includes more rigorous planning and reporting. The PCO team was able to support seven CCMDs during FY23, and when the process is fully implemented, all CCMDs will be eligible to receive PCO support for their primary missions on an annual basis.

Also in FY23, the PCO team supported the combined exercises of PACIFIC SENTRY 2023 at USINDOPACOM and TURBO CHALLENGE 2023 at USTRANSCOM. This PCO mission lasted approximately six months and involved three separate Red Teams operating in multiple theaters and on numerous headquarters and component enclaves. Red Teams were assigned to operate in designated enclaves to meet objectives provided by those CCMDs. Specific targets were based on real-world cyber intelligence.

DOT&E and the Missile Defense Agency (MDA) are working to provide a briefing to the congressional committees on plans for a PCO to cover MDA systems and networks, in accordance with congressional direction.

### Advanced Cyber Operations (ACO) Team

CAP continued to cultivate relationships across multiple organizations that can provide master-level cyber operators and serve as members of the CAP's ACO team. CAP utilizes the ACO team to conduct assessments of emerging technologies, provide cutting-edge expertise as part of continuous augmentation to DoD Red Teams, and facilitate the portrayal of more advanced cyber threats. Organizations participating in the ACO team include DoD-certified Red Teams, FFRDCs, National Labs, University-Affiliated Research Center Laboratories, academia, and industry. During FY23, the DOT&E ACO team supported:

- Assessments of several Zero Trust architectures offered by vendors as Software-as-a-Service environments

- Cyber survivability testing of the F-35
- Assessments of data-lake repositories currently in use throughout the DoD to store, process, and secure large amounts of data (both structured and unstructured), to include the Advancing Analytics (Advana) platform
- Assessments of cyber-physical systems such as industrial control systems and aircraft transponders
- Assessments of specialized networks used by special operations forces
- Assessments of Offensive Cyber Operations (OCO) capabilities
- Development of cyber survivability testing procedures for CDS currently in use throughout the DoD
- Development of enhanced Red Team capabilities, tools, and tradecraft
- Expansion of Red Team accesses via PCO
- Preparation for assessments of AI/ML technologies
- Assessments of NC3 networks

Demand for ACO support grew in FY23 and is expected to continue to grow in FY24. Hiring and retention challenges are a primary concern for the Red Team community, which thus far has been unable to keep pace with the opportunities and salaries offered in the private sector for cyber professionals.

## Advanced Cyber-Threat Emulation Capabilities

DOT&E sponsors the Capabilities Development Working Group (CDWG), providing the cyber Red Team community with a collaborative forum to acquire more advanced tools and tradecraft for teams supporting CAP assessments and OT&E. DOT&E also continues to pursue additional resources for tool development and acquisition that include IP, RF, and other special cyber capabilities that will be needed for assessments of new and emerging technologies such as AI-enabled capabilities.

During FY23, the DOT&E CDWG supported:

- Development of a capability that can be used to change Red-Team tool signatures, enabling them to better represent advanced adversaries and evade detection by virus scans
- Standardizing and automating Red Team action maps, data collection, and data visualization
- Development of a command and control framework for Red Teams

In order to address the increasing demand for Red Team participation, DOT&E began a new project in FY23 to identify and acquire tools for Red Teams that automate their current tasks and activities. These enhancements will include tools and tradecraft that expand beyond current Red Team capabilities and may include AI-enablers for Red Teams to plan and execute assessments. In FY24, DOT&E will also explore tools and methods that enable Red Teams and assessment teams to assess and explain the cybersecurity vulnerabilities of AI/ML capabilities in DoD applications and systems.

## Engagement with the Intelligence Community

CAP's collaboration with the Intelligence Community remains an essential element of CCMD mission-focused assessments and OT&E events. High security 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. The lack of opportunity to experience the most representative and known threats may leave warfighters unprepared to defend and sustain their critical missions. DOT&E is working with the Defense Intelligence Agency, the National Security 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 threats portrayed in assessments and OT&E.

## Table 1. CAP FY23 Activity

| Type of Event |
|---|
| **Physical Security Assessment (6 Events)**<br>USEUCOM, USINDOPACOM, USFK, USNORTHCOM, USTRANSCOM (2) |
| **Assessment of Mission Effects during Exercises (15 Events)**<br>USN (2), USAFRICOM, USEUCOM, USFK, USCENTCOM, USINDOPACOM, USNORTHCOM (2), USSOCOM (3), USSOUTHCOM, USSTRATCOM, USTRANSCOM |
| **Assessments of Network Security, Stimulation Exercises, and Tabletop Exercises (8 Events)**<br>USAF, USEUCOM (2), USINDOPACOM, USSOCOM, USSOUTHCOM, USSF, USTRANSCOM |
| **Range Event**<br>USINDOPACOM |
| **Assessment of Cyber Fires Processes for Offensive Cyber Operations (3 Events)**<br>USINDOPACOM, USEUCOM, USFK |
| **Assessment of Special Capabilities and Projects (17 Events)**<br>Capability (5), Non-Kinetic Fires (6), SME Support (3), TCID (3) |
| Acronyms: SME – Subject Matter Expert; TCID – Transponders, Combat Identification; USAF – U.S. Air Force; USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; USN – U.S. Navy; USNORTHCOM – U.S. Northern Command; USSF – U.S. Space Force; USSOCOM – U.S. Special Operations Command; USSOUTHCOM – U.S. Southern Command; USSTRATCOM – U.S. Strategic Command; USTRANSCOM – U.S. Transportation Command |