Department of Defense
Cyber Table Top Guide

Version 3.0

October 14, 2025

Office of the Director,
Developmental Test, Evaluation, and Assessments

Office of the Under Secretary of War
for Research and Engineering

Washington, D.C.

The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products, or services contained therein. DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

Department of Defense Cyber Table Top Guide

Office of the Director, Developmental Test, Evaluation, and Assessments
Office of the Under Secretary of War for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301-3030
osd.r-e.comm@mail.mil
https://www.cto.mil/dtea/cyber

Distribution Statement A. Approved for public release. Distribution is unlimited.
DOPSR Case # 26-T-0047.

✔

Approved by
Mr. Orlando F. Flores
Director, Developmental Test, Evaluation, and Assessments (Acting)

October 14, 2025

DoD Cyber Table Top Guide Change Record

Date	Version	Rationale
2 July 2018	1.0	Initial Release
16 September 2021	2.0	Updated to align with current practices.
14 October 2025	3.0	Updated to align with the forthcoming DoD Manual 5000.UY and the DoD Cyber DT&E Guidebook, Version 3.0.

This page is intentionally blank.

Executive Summary

The Department of Defense (DoD) recognizes cyberspace as a warfighting domain and expects cyberspace attacks to be part of current and future wars. All DoD systems operate in an increasingly complex, networked environment. Systems engineers, system security engineers, and cyber testers must design, verify, and validate cybersecurity and cyber resilience requirements for all national security systems; weapons systems; and systems that interface with networks, platforms, sensors, maintenance systems, and other elements in the operational environment.

The acquisition and engineering communities need methods and tools to implement effective and affordable cyber survivability, which includes cybersecurity and cyber resilience as a component of operational resilience. The test and evaluation community and developers need procedures, methods, and tools to verify and validate these requirements earlier in the acquisition life cycle. Late discovery of vulnerabilities results in costly design changes or in fielding vulnerable systems, or both. This guide describes methods for the early identification and categorization of cyber risks, as well as the identification of associated critical mission and system functions.

The Cyber Table Top (CTT) is a focused, intellectually intensive mission based cyber risk assessment exercise that explores the effects of cyber offensive operations on the capability of U.S. systems to carry out their missions. A CTT is a wargame-like exercise that centers on three teams: a leadership team and two teams with opposing missions—the operational team charged with executing a realistic operational mission and the cyber opposing forces attempting to prevent the operational mission from being successful.

The CTT provides program managers, systems engineers, information systems security managers, information systems security engineers, testers, users, operators, and other analysts with actionable information on cyber threats to mission execution. Actionable information includes potential system vulnerabilities, demonstrated means of exploitation of those vulnerabilities, and an assessment of the resulting mission impacts. This information enables leaders to allocate their limited resources more effectively toward delivering a system that will operate successfully in contested cyberspace.

The CTT, in conjunction with other tools and processes, provides the program manager (or equivalent), developers, engineering and test teams with opportunities for risk reduction throughout the life cycle of the system under analysis and reduces the likelihood of discovering exploitable mission-impacting vulnerabilities during cyber testing.

This page is intentionally blank.

Contents

Figures

Tables

This page is intentionally blank.

1 Introduction

Department of Defense (DoD) systems increasingly depend on complex interconnected cyberspace environments. These environments are inherently vulnerable, providing opportunities for adversaries to compromise systems and negatively impact DoD operations and missions. Cyber vulnerabilities, if exploited by a determined and capable cyber threat, may pose significant security and warfighting risks to DoD and its warfighters. The Cyber Table Top (CTT) process is a mission based cyber risk assessment (MBCRA) methodology and a best practice which includes an intellectual wargame-like exercise followed by analysis. The CTT exercise and analysis facilitate the identification and comprehension of risks from potential cyber vulnerabilities. The CTT process satisfies the minimum requirements of an MBCRA in accordance with the forthcoming DoD Manual (DoDM) 5000.UY "Cyber Developmental Test and Evaluation." Appendix G of the DoD Cyber Developmental Test and Evaluation (DT&E) Guidebook, Version 3.0, provides guidance for MBCRA methodology selection and how to conduct MBCRAs. CTTs are lightweight and cost less than other MBCRA methodologies. The CTT is highly effective at scoping cyber test and evaluation (T&E).

1.1 Purpose

This guide provides an overview of the CTT process, guidance on performing a CTT, and instructions for generating actionable information on potential cyber threats for decision makers. Organizations may tailor this process and the templates to meet individual organizational needs.

1.2 Organization

This guide contains three sections, including this Section 1 overview. Section 2 provides background information, and Section 3 explains the four steps in the CTT process. The guide includes the following appendices.

- Appendix A: CTT Exercise Preparation Resources
- Appendix B: CTT Exercise Execution Resources
- Appendix C: CTT Post-Exercise Analysis Resources
- Appendix D: CTT Checklists
- Appendix E: Common CTT Challenges and Mitigations

This guide also provides a glossary, an acronym list, and references.

Dynamic and tailorable electronic resources are available in the DoD OSDRE-DoD-Cyber-Table-Tops Team (team code *zlramzr*), and on the CTT Intelink Website in the "Cyber Table

Top Guidance" folder, within the "0-Mission Based Cyber Risk Assessment Methodologies" folder in the page's "Shared Documents" (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx).

1.3 Audience

The intended audience for this guide includes program managers (or equivalent); project leads; science and technology managers (or equivalent); T&E leads; lead systems engineers; system security engineers; information systems security engineers (ISSEs); information systems security managers (ISSMs); chief developmental testers; lead DT&E organizations; operational test agencies (OTAs); other operational test and evaluation (OT&E) organizations; systems developers; analysts performing the cyber analysis and the test planning and scoping or preparing for the testing of any system, subsystem, or system component; as well as anyone conducting or participating in a CTT.

2 Background

Cyberspace is a critical warfare domain that includes the Internet; telecommunications networks; computer systems; embedded processors and controllers; and ubiquitous, rapidly evolving threats. A full-scale conflict with a nation-state adversary will include cyberspace attacks from insiders, supply chain manipulation, attacks over the network, and exploitation through radio frequency (RF) apertures (cyber warfare enabling electromagnetic warfare (EW) or EW enabling cyber warfare). Adversaries could design attacks to cause mission effects via disruption, denial of service (DoS), data manipulation, data corruption, data exfiltration, sabotage, and data or system destruction in a coordinated fashion with kinetic and EW attacks.

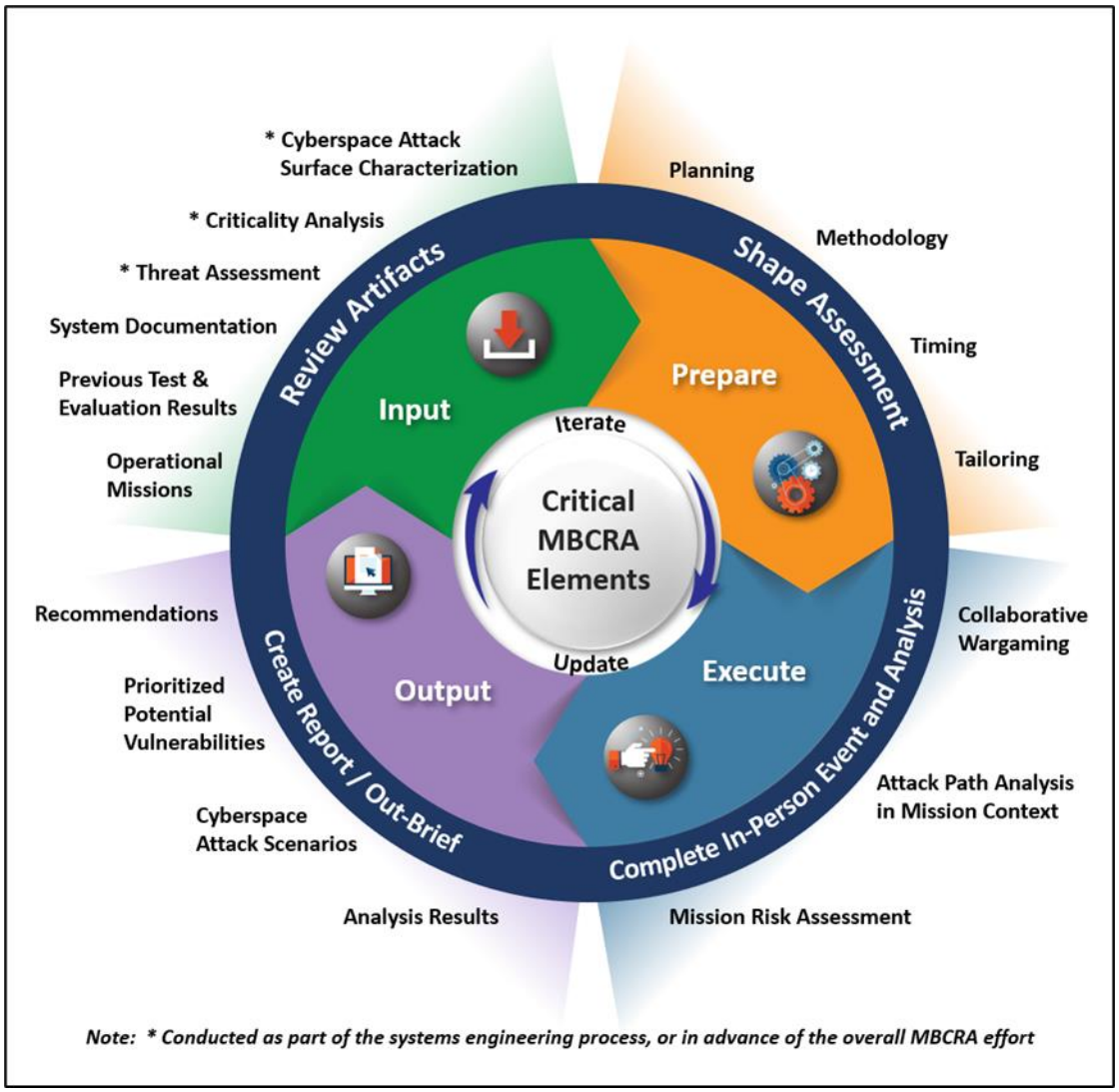
2.1 DoD Cyber Strategy, Objectives, and Policy

The Summary of the 2023 Cyber Strategy of the DoD outlines the four lines of effort to address current and future cyber threats: Defend the Nation; Prepare to Fight and Win the Nation's Wars; Protect the Cyber Domain with Allies and Partners; and Build Enduring Advantages in Cyberspace. The strategy briefly discusses the nation-state cyber threat actors using cyber as a force multiplier and states, "U.S. adversaries seek to use malicious cyber to achieve asymmetric advantages, targeting U.S. critical infrastructure and degrading U.S. military superiority. These activities threaten the safety, security, and prosperity of the American people." CTTs are a process that should enable all these lines of effort but most closely contributes to Defend the Nation by generating useful insights about cyber threats to DoD organizations and systems. DoD Instruction (DoDI) 8500.01, "Cybersecurity," defines and outlines the requirements to achieve operational resilience. Those requirements include performing DT&E and OT&E activities to assess resilience and inform acquisition decisions. Cyber testing is more than vulnerability discovery—testing measures the progress of requirements verification; identifies problems; and characterizes cyber survivability in the context of cybersecurity capabilities, cyber resilience performance, and limitations. Acquisition policy requires conformance to DoDI 8500.01 and encourages effective cybersecurity, cyber survivability, and operational resilience throughout a system's life cycle.

2.1.1 Mission Based Cyber Risk Assessments

DoDI 5000.89, "Test and Evaluation," requires MBCRAs. The forthcoming DoDM 5000.UY provides the minimum requirements, depicted in Figure 2-1, for iterative MBCRAs regarding "what to do." Every MBCRA depends on the latest versions of the depicted artifacts, regardless of the maturity of the system under analysis (SUA). The CTT is one of the MBCRA methodologies consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Guide for Conducting Risk Assessments." The CTT process does not include specific steps to develop the essential artifacts noted by the asterisk (*) in

Figure 2-1: cyberspace attack surface characterization, criticality analysis, and threat assessment. The CTT planners should work closely with the systems engineering (SE) team to develop and update these artifacts in support of each CTT. The DoD Cyber DT&E Guidebook, Version 3.0, provides additional guidance for these artifacts. CTTs are useful for the early characterization of cyber vulnerabilities and associated mission impacts and are adaptable as DoD updates policy. DoD solicits feedback and lessons learned from CTT practitioners and incorporates the best practices into this guide.



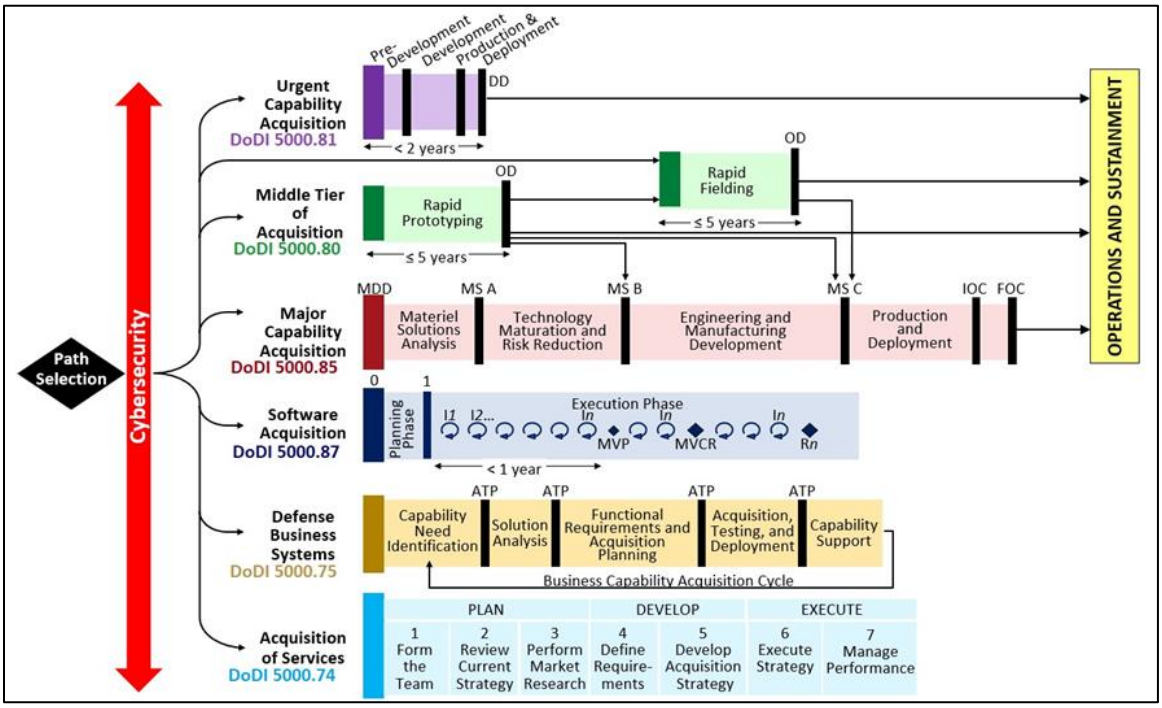
Source: Forthcoming DoDM 5000.UY

Figure 2-1. MBCRA Elements

Because cyber T&E should focus heavily on the mission-relevant terrain in cyberspace for the system under test (i.e., the most critical components of the system under test), the criticality analysis and cyberspace attack surface characterization, shown in Figure 2-1, serve as a vital input to a CTT. To identify the terrain and understand the attack surface, the cyber working

group (CyWG) must support the criticality analysis or perform the analysis before the CTT. This criticality analysis includes decomposing the operational mission and determining critical mission tasks and then decomposing the system and identifying those physical (e.g., a controller) and logical (e.g., a database) assets directly or indirectly supporting those most critical mission tasks. In some cases, the program's criticality analysis may not adequately support the CTT, and the CyWG or the CTT team may need to perform additional analysis to ensure inputs will enable the CTT.

The DoD Cyber DT&E Guidebook, Version 3.0, describes how to conduct iterative MBCRAs. The forthcoming DoDM 5000.UY and the DoD Cyber DT&E Guidebook, Version 3.0, support the DoD Adaptive Acquisition Framework, depicted in Figure 2-2 and described in DoDI 5000.02, "Operation of the Adaptive Acquisition Framework."



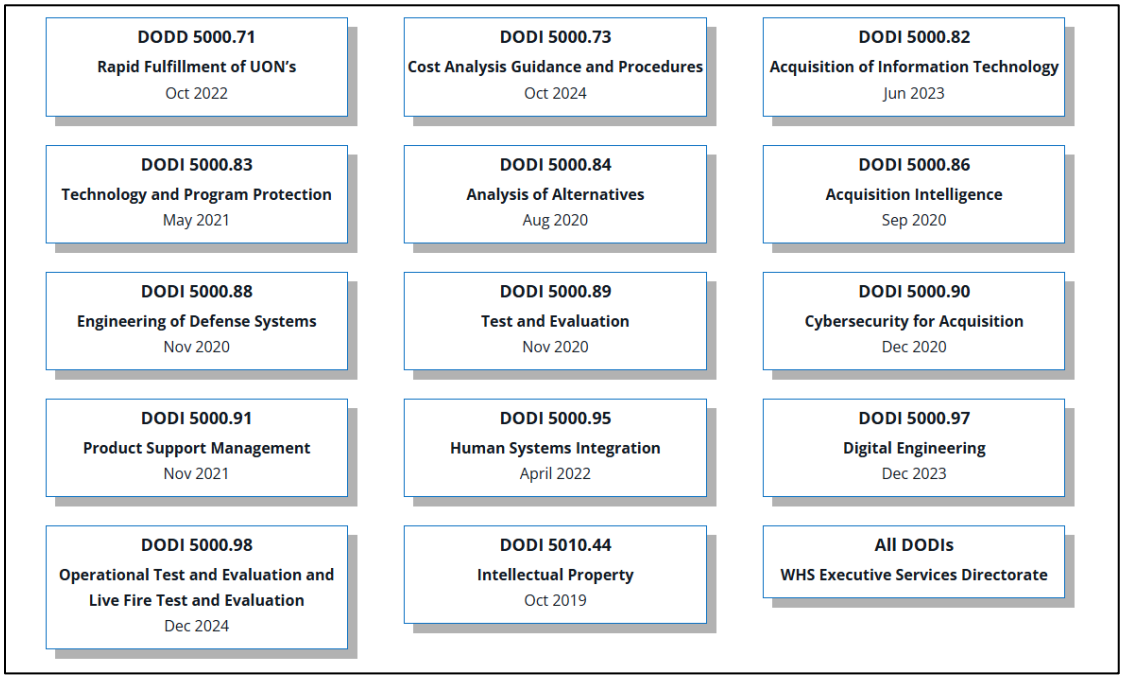
ATP: Authority to Proceed	DD: Disposition Decision	FOC: Full Operational Capability
I: Iteration	IOC: Initial Operational Capability	MDD: Materiel Development Decision
MS: Milestone	MVCR: Minimum Viable Capability Release	MVP: Minimum Viable Product
OD: Outcome Determination	R: Release	

Source: DoDI 5000.02

Figure 2-2. Adaptive Acquisition Framework and Corresponding Pathway Policy

Figure 2-3 depicts the functional policies (e.g., DoDI 5000.89) mandating acquisition programs evaluate cybersecurity, cyber survivability, and operational resilience in the conduct of risk management activities. The forthcoming DoDM 5000.UY extends MBCRAs and the cyber DT&E process to all DoD systems, including non-acquisition prototyping and development; pre-acquisition program technologies and systems; acquisition systems in accordance with DoD

Directive 5205.07, “Special Access Program Policy”; systems acquired via the Defense Acquisition System; and systems in sustainment.



Source: DAU Acquisition Policies Website (https://aaf.dau.edu/aaf/policies/)

Figure 2-3. Functional Policies

CTT planners should be intimately familiar with the forthcoming DoDM 5000.UY and the DoD Cyber DT&E Guidebook, Version 3.0, to maximize CTT planning and harmonize the CTT with cyber T&E processes. DoD policy and guidance require assessing cyber risks at engineering technical reviews to understand system cyber threats and operational impacts. Risk assessment methodologies should be consistent with NIST SP 800-30. Because NIST SP 800-30 is adaptable by design, the publication provides a framework for MBCRA methodologies in use throughout DoD.

The organization should select the MBCRA methodology most aligned to its needs (e.g., information, resources, and schedule). The 2017 Institute for Defense Analyses (IDA) Paper P-8736, “Comparative Review of DoD Mission-Based Cyber Risk Assessment Methodologies” (Ambroso and Hutton 2017), reviews many MBCRA methodologies and provides a decision diagram to help select an appropriate MBCRA methodology. IDA Document P-14309, “Comparative Review of DoD MBCRAs: 2020 Updates and New Methodologies” (de Naray and Galvin 2020), is the 2020 update to the initial MBCRA review that specifies inactive or replaced methodologies and describes several new methodologies. Some of the Service methodologies are limited distribution, and as a result, the IDA papers are not publicly released but are available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and in Shared

Documents on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx).

2.1.2 MBCRA Automation Tool

The MBCRA Automation Tool (MAT) provides planning features that help organize events by automating and accelerating the execution of MBCRAs. The CTT module provides the capability to perform synchronized note-taking, automate report generation, support task management and logistics planning, conduct threat analysis, maintain digital recordkeeping, calculate risk scores, and generate the post-event briefing. The U.S. Army Redstone Test Center (RTC) and the U.S. Air Force 96th Cyberspace Test Group partnered to develop MAT, with sponsorships from RTC, the Cyber Resiliency Office for Weapon Systems, the U.S. Air Force Air Combat Command, and the Office of the Under Secretary of War for Research and Engineering.

Additional upgrades sponsored by the Test Resource Management Center and Air Combat Command are underway to automate, accelerate, and better integrate MBCRAs with system security engineering, cyber supply chain risk management, ontologies, operational risk management, cyber operations lethality and effectiveness analysis, controls-based threat risk analyses, and intelligence-based analysis. MAT upgrades will provide a single integrated risk assessment tool that aligns, streamlines, and integrates risk assessment efforts. The resulting MAT capability will also provide a means to share MAT data and artifacts with other tools that support model-based systems engineering (MBSE) and other risk assessment efforts and to automate cyber T&E event plan generation.

MAT software is available at no cost to DoD users through RTC. RTC requires a signed user agreement before releasing the software. Users can find software request information for MAT in the MAT details (under the Cyber T&E Group) on the Joint Engineering and Test Enterprise Portal website (https://jetep.apps.dso.mil/tools/cards/all). MBCRA event support (using MAT) is also available through RTC and the 96th Cyberspace Test Group's 48th Cyberspace Test Squadron for a fee, based on the level of service requested. Currently, MAT software is primarily on stand-alone laptops (typically procured by the supported program) to enable MBCRA support of all classification levels for programs up to special access program levels. The 48th Cyberspace Test Squadron is actively seeking a MAT software certification to enable use of the tool on classified networks.

2.1.3 MBCRA Scenario Library

Section 8 of the DoD Cyber DT&E Guidebook, Version 3.0, advocates the use of digital engineering and ontologies in MBSE. The Ontology for Attacks in Cyber Risk Assessments

(OACRA) (still at a low technology readiness level), for example, could serve as a library of attacks and enable reusing those CTT attacks across DoD when an SUA or attack surface contains the same elements exploited in the attack. OACRA is currently available on the Secret Internet Protocol Router Network (SIPRNET) via the Army Research Laboratory high-performance computer. For information on OACRA, including gaining access, go to the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) and look for the OACRA folder in Shared Documents. OACRA requires specifying the associated MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework tactic and technique for each attack using version 11.3 of MITRE ATT&CK (https://attack.mitre.org/versions/v11).

Table G-6 in Appendix G of the DoD Cyber DT&E Guidebook, Version 3.0, provides a recommendation for creating or updating MITRE Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND) Cyber Attack-Defense models of the cyberspace attack scenarios. D3FEND Cyber Attack-Defense is free to use, is currently available on the Internet and the Joint Worldwide Intelligence Communications System (JWICS) and will soon be available on the SIPRNET. To inform and enhance MBCRA attack scenario development and reuse, organizations should sanitize the MBCRA scenarios enabling reuse and add the reusable scenarios to a library of attacks, such as OACRA or Cyber Attack-Defense models, enabling cross-DoD reuse and building new scenarios. Maintain attack scenarios information in the library, available on the SIPRNET, as controlled unclassified information (CUI) to enable the reuse of attacks or scenarios across platforms without linking or exposing sensitive system vulnerabilities to specific systems. The library could exist either in the D3FEND sites, in OACRA on the SIPRNET, or in another DoD repository. The approach to providing a centralized DoD library or repository of reusable scenarios is still under development at the time of this guide's publication.

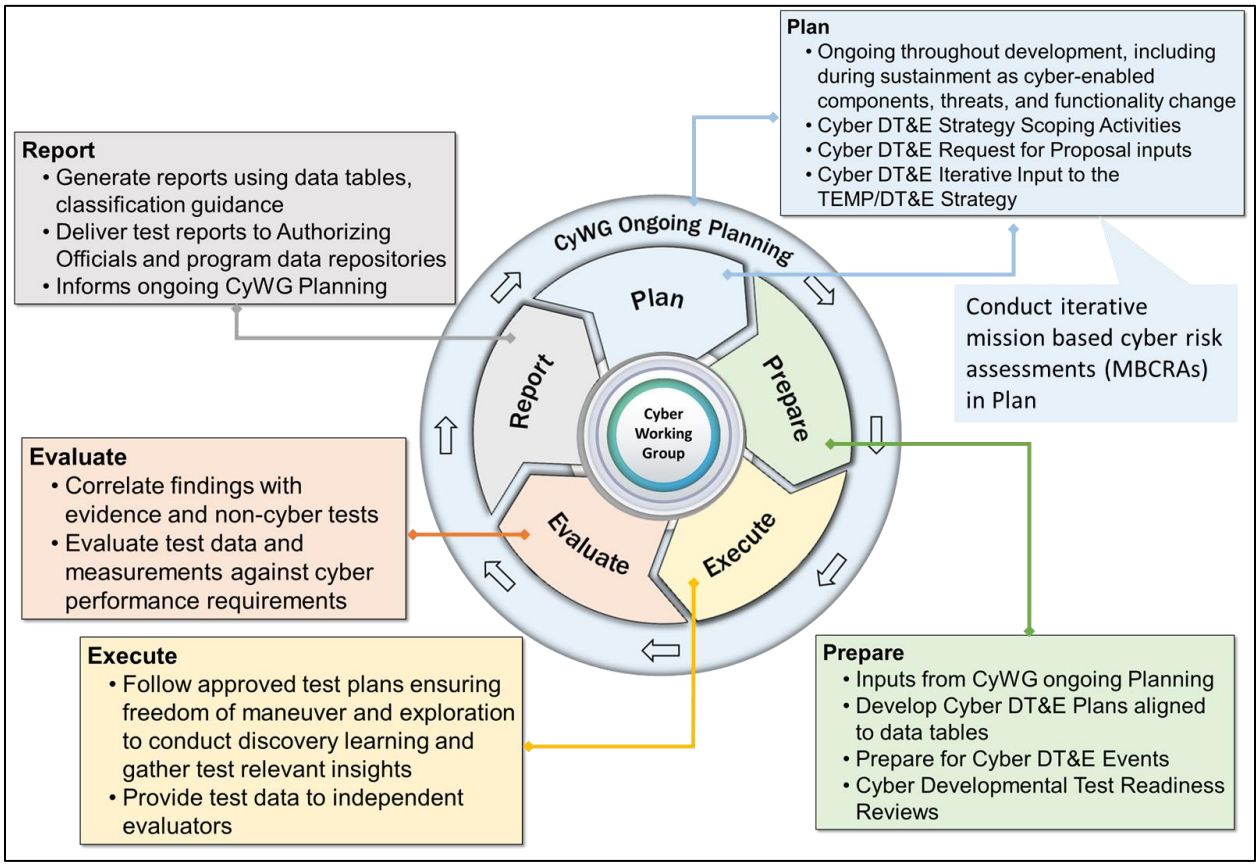
Model-based systems engineers could also import the D3FEND ontology and models into a system modeling tool to facilitate comprehensive analysis, and MAT facilitators can import the library into the MAT tool. These approaches support efficient, consistent, and comprehensive MBCRAs across the life cycle. For more information, see the MITRE D3FEND website (https://d3fend.mitre.org/).

This approach enables teams to quickly identify recurring patterns, vulnerabilities, and previously analyzed attack paths that others have validated, reducing the time required to create attacks and scenarios from scratch. Moreover, these existing scenarios provide a consistent foundation for applying D3FEND Ontology classes and countermeasures, ensuring methodological uniformity and accuracy in new designs. Thus, D3FEND can also support identifying defensive techniques as mitigations (see Figure 3-10) during the CTT *Post-Exercise Analysis*, covered in Section 3.4.

Teams can adapt and extend these attacks and scenarios to align with the specific mission and threat context or system architecture. Each CTT would refer to the library of sanitized attacks and scenarios from prior MBCRAs and select those with digital components similar to the current CTT SUA. The attacks or scenarios may or may not be relevant to the current CTT mission and scenario. The analysis participants will still need to apply the likelihood and mission impact methodologies. Utilizing sanitized attacks and scenarios may enable standardization across assessments and helps the collaboration among stakeholders by providing a common framework for addressing cyberspace risks. By using a well-maintained attack and scenario library, a comprehensive knowledge base informs new scenarios, thus improving the quality, relevance, and efficiency of attack path analysis.

2.2 CTTs Across the Acquisition Life Cycle

The updated DoD Cyber DT&E Guidebook, Version 3.0, describes five iterative activities for cyber DT&E, depicted in Figure 2-4, that the CyWG is responsible for managing, as depicted in the center of the figure's activities.



Source: DoD Cyber DT&E Guidebook, Version 3.0

Figure 2-4. DoD Cyber DT&E Process

This updated iterative cyber T&E process supports the varying cadences of the acquisition pathways depicted in Figure 2-2. Unlike some MBCRA methodologies, an organization can use CTTs at any time in a system's life cycle. CyWGs should update or conduct CTTs during the planning activity. The CTT does not require high fidelity in system designs. As an example, for Major Capability Acquisitions, a program can use CTTs as a tool to understand the cybersecurity and cyber resilience requirements before Milestone A; expanded to support the characterization of the attack surface before Milestone B; used to scope cyber DT&E events by the developer and the government before Milestone C; used to inform OT&E; and used to inform continuous monitoring after Milestone C.

In the event the organization planning for a CTT does not have a CyWG, the organization should substitute the name of its team responsible for cyber T&E planning or for system security engineering for this guide's use of "CyWG."

When conducting CTTs over the system life cycle, it is important for the CyWG to treat iterative CTTs as complementary events that inform and build upon each other, not as discrete events. For example, analysis and outputs from a CTT should be inputs for a follow-on CTT later in the life cycle. CTTs can supplement risk assessment reporting for the DoD Risk Management Framework (RMF) in support of obtaining an authorization to operate. The results allow program managers (or equivalent), ISSMs, ISSEs, engineers, and testers to assess the risk of cyber threats to an SUA, a system, a system of systems (SoS), platforms of systems (e.g., ship, aircraft, vehicle) or families of systems (FoS). Through an understanding of mission-based cyber risk, decision makers can then prioritize what to test (and why), what risks to accept, to mitigate, and what requires further investigation in the engineering process.

2.3 CTT Purpose and Benefits

The CTT process provides program managers (or equivalent), ISSMs, ISSEs, systems engineers, testers, and other analysts with actionable information on cyber threats to mission execution.

Actionable information includes potential system vulnerabilities, demonstrated means of exploitation of those vulnerabilities, and an assessment of the resulting mission impacts. The organization's leaders determine the required actions to reduce, mitigate, or counter the risks identified in the CTT. This information enables leaders to allocate their limited resources more effectively in delivering a system that will operate successfully in contested cyberspace.

Intelligence can play a critical role in the CTT, but intelligence community (IC) representatives often face limitations in providing applicable threat intelligence. Although determining enemy intentions can be challenging, the CTT focuses on assessing an adversary's potential capabilities. This approach enables the identification and prioritization of the most exploitable attack surfaces

and the attack methods that, if successful, could pose the greatest risk to mission success. It is important to emphasize a subtle yet critical distinction:

The primary goal of the CTT is to identify systems, technologies, and capabilities cyber opposition forces *could* target to significantly impact the success of an operational mission, rather than focusing on what analysts believe a specific adversary *is* targeting.

The activities in the four successive steps of the CTT—*Exercise Preparation*, *Exercise Execution*, *Post-Exercise Analysis*, *Reporting*—build on one another to generate the following:

- Risk matrices based on expected mission effects.
- Recommended actions that may increase resistance and resilience to cyberspace attacks.

Section 3 provides more details about the activities and products in each step and provides estimates for how long each step may take. CTTs are not meant to produce an exhaustive list of every possible action that an attacker could take against the system. Instead, the CTT focuses on generating a representative set of plausible attacks that exploit potential vulnerabilities, grounded in the information available during the exercise. Iterative cyber DT&E builds on CTT results by verifying cyber performance requirements, validating the findings from the CTT, and addressing any gaps in coverage to ensure a more comprehensive assessment of the system's cyber resilience.

Cyber T&E objectives should focus test resources on adversary actions that (1) are likely/ possible (i.e., there is a threat with the capability and intent and an exploitable vulnerability) and (2) could generate significant consequences (loss of life, mission failure, etc.). A properly executed CTT will provide testers with the necessary insights to derive the most meaningful test objectives.

The CTT team should ensure that access and pivot points align with the architecture under development to support actionable test cases based on CTT results. This alignment allows test teams to simulate real-world scenarios effectively and to accurately assess vulnerabilities and risks identified during the CTT. The CTT team should ensure realistic command and control (C2) access and pivot points in the SUA that support analysis of attacks affecting the operational mission. The ports, susceptibilities, misconfigurations, services, and protocols that the CTT team identifies enable the test teams to identify additional cyber vulnerabilities and analyze kill chains comprehensively, ensuring that the test cases are relevant and meaningful and contribute to the system's resilience evaluation in its operational context. Without this realism, the test team cannot derive actionable test points for a test plan, rendering the CTT ineffective.

The CTT process offers multiple benefits:

- Socializes the concept of cyberspace as a warfare domain with the organization's leaders.
- Bridges the gap between the information technology (IT) and functional mission viewpoints through a disciplined approach to foster mutual understanding.
- Looks beyond a single system to the cyber vulnerabilities of SoS and FoS within the disciplined context of a specific mission thread.
- Informs architectural decision making early in the development process.
- Promotes the early understanding of operator, defender, and maintainer training needs to support architecting, designing and implementing appropriate human-machine interfaces while identifying areas to improve operator, defender, and maintainer training.
- Aids in identifying vulnerable components and interfaces that can help focus supply chain risk management efforts.
- Informs planning for early testing to collect empirical data to answer key questions aimed at the most critical unknowns.
- Enables knowledge and action that lead to more effective developmental test (DT) events and more successful operational test (OT) events.
- Provides test teams with test points where programs lack cyber test requirements.
- Identifies areas for improved operator, defender, and maintainer training.
- Identifies and characterizes potential mission risk from cyber effects.
- Identifies and characterizes potential mission risks from cyber effects, including how vulnerabilities in supporting platforms, systems, and stakeholders could escalate into broader impacts on mission success.

Stakeholders can utilize CTT results to improve cyber defenses early, ultimately saving time and budget while delivering superior capabilities.

2.3.1 Intelligence Support

Cyber threat intelligence plays a vital role in informing each stage of the SE process. By analyzing known adversary capabilities and intentions, gaps within the available threat intelligence and identifying exploitable areas in the system, the CyWG establishes a feedback loop with the IC representative. This iterative process enables the CyWG to request critical information from the IC or share CTT findings to refine future assessments. The IC, in turn, can focus on the areas explored during the CTT to provide targeted insights that further inform the

CyWG. Requests made to the IC for threat information specific to cyber operations involving certain platforms and missions usually result in the need for the IC to initiate a task, so it is important to file such requests well before the required date. Also see Appendix D in the DoD Cyber DT&E Guidebook, Version 3.0, for more information on cyber threat assessments. DoD Cyber Red Teams can supplement this information via reports providing the latest information from the field and from other red team assessments of similar platforms and missions. With this enhanced intelligence, the CyWG can proactively reduce risk and provide actionable guidance to SE and T&E teams on emerging threats. Additionally, the CTT strengthens the CyWG's collaboration with the IC, supporting the development of Validated Online Lifecycle Threat Reports and relevant cyber threat assessments.

To help ensure a successful CTT that produces actionable information, it is important to specify the system characteristics and type of data required when requesting intelligence information. An intelligence analyst may not know the functionality of the system and architecture, which could hinder the scope of parameters to query and limit the amount of information collected. Including intelligence analysts early in the CTT process in discussions about the system provides an opportunity for the analysts to ask questions and have a better understanding of what type of information is valuable to the risk and threat assessment. System characteristics in an intelligence request should include the following:

- Technology: hardware, software, manufacturer, version.
- Architecture: subsystems, dataflow, interfaces, functionality.
- Mission: system purpose, intent, area of responsibility, operational dependencies, intended environments.

See the DoD Cyber DT&E Guidebook, Version 3.0, for additional guidance on intelligence support.

2.3.2 Risk Reporting

Before executing a CTT, the CyWG must select or determine a risk methodology to guide the final reporting. Traditionally, the CyWG reports risk using a five-by-five matrix, as described in NIST SP 800-30. The analysis associated with producing the matrices may involve varying levels of rigor that includes analysis of threats, vulnerabilities, and impact. If the CyWG decides to execute a streamlined CTT, it may choose to simplify the threat analysis by estimating or hypothesizing threat capability and intent (e.g., assuming that the threat is a highly capable adversary with expert system knowledge). However, because the process is tailorable, the CyWG may also decide to integrate validated threat information. Ultimately, participants need to understand the analysis approach before starting a CTT. By "beginning with the end in mind,"

the CyWG will ensure that decision makers understand and are able to report actionable information in an approved manner.

This guide assumes the use of a traditional five-by-five risk matrix, as depicted in Figure , which is based on Table I-2 in Appendix I of NIST SP 800-30. The NIST publication does not include the colors shown in Figure .

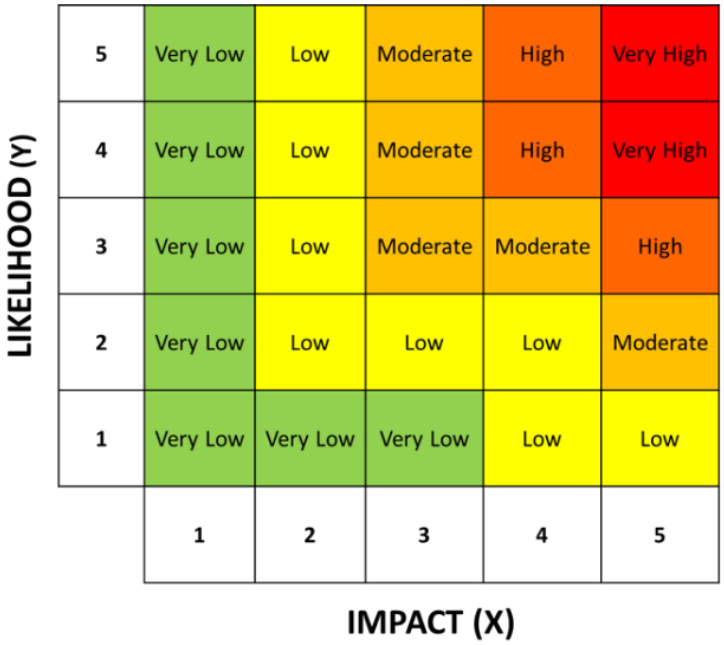


Figure 2-5. Five-by-Five Risk Matrix

3 Cyber Table Top Process

This section presents the recommended method for planning, executing, analyzing, and reporting the results of a CTT.

Figure 3-1 depicts the four steps in a CTT:

1. Exercise Preparation
2. Exercise Execution
3. Post-Exercise Analysis
4. Reporting

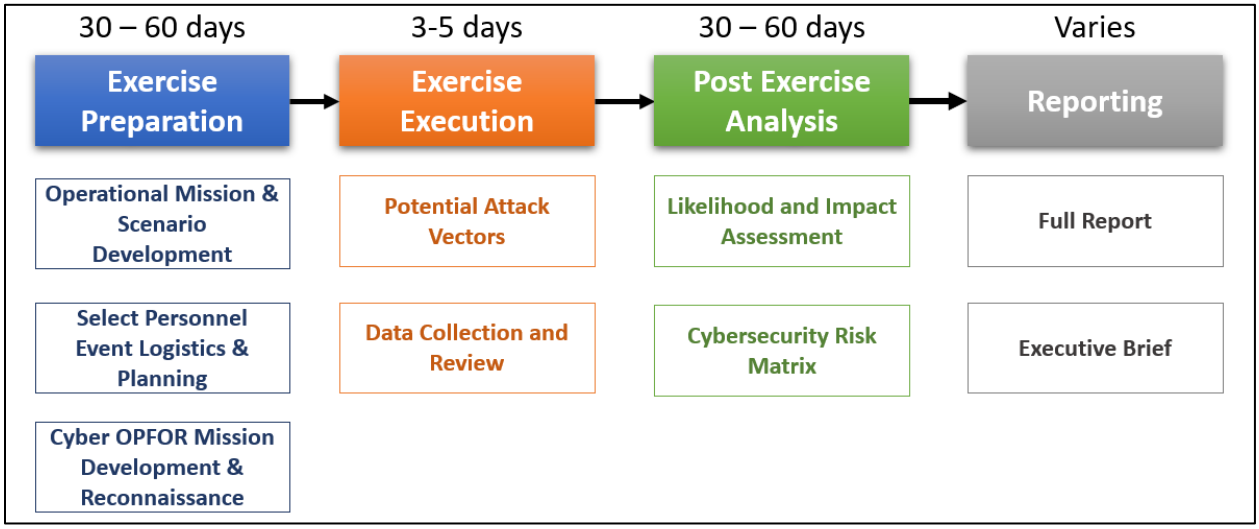


Figure 3-1. CTT Steps

Figure 3-1 also illustrates the major activities in each step and the average number of calendar days to complete a CTT (based on past CTTs). Timelines can vary based on the SUA scope, number of participants, and use of automation as described in Section 2.1.2. Additional factors may have an impact on the timeline; for example, *Exercise Preparation* could take much longer if SUA documentation is not available or the prerequisites described in Section 3.1 are not satisfied.

The CTT steps align with the MBCRA elements in Figure 2-1: *Exercise Preparation* aligns with Input and Prepare; *Exercise Execution* and *Post-Exercise Analysis* align with Execute; and *Reporting* aligns with Output. CTTs require a small team of personnel committed to performing all four steps of the CTT process and a larger group of participants (from the CyWG and other organizations) who are involved mainly in *Exercise Execution*. Throughout this section, "exercise" will refer to all Step 2 activities.

Smaller SUAs will likely have shorter timelines. See Appendix A for several examples of how organizations can use CTTs. The critical step for generating actionable information is *Post-Exercise Analysis* (Step 3). The activities in *Exercise Preparation* (Step 1) and *Exercise Execution* (Step 2) are essential to set the environment and foundation that will ensure that the data needed during *Post-Exercise Analysis* yield a successful outcome for the CyWG when presenting the results during *Reporting* (Step 4). DoD intends for the CTT process to be adaptable and to fit the needs of many different users regardless of SUA size.

3.1 Prerequisites Before Starting a CTT

The CyWG will initiate planning for an MBCRA. If the CyWG selects a CTT as the MBCRA methodology, then the CyWG chair(s) will advocate for the CTT to the organization's leaders to begin the process. The CTT advocate(s) should ensure that the CyWG has met several conditions before beginning Step 1:

Obtained buy-in from leaders. To earn leader buy-in, the CTT advocate(s) should emphasize the benefits of the process and motivate stakeholders. Typically, buy-in efforts involve giving an overview of the process and the expected results to leaders across the organization's functional areas. Leadership buy-in ensures that resourcing (time, personnel) for the CTT is available.

Obtained organizational approval, ownership of the process, and understanding of resource expectations. The organization leads the CTT by making major decisions; allocating resources; providing the artifacts and necessary information about the SUA; and determining the schedule, staffing, and funding constraints. Advance planning will ensure funding for CTTs and the necessary developer support if a systems developer is under contract. The CyWG may need the developer to provide essential SUA information. See Appendix I in the DoD Cyber DT&E Guidebook, Version 3.0, for notional MBCRA contract language enabling systems developer support.

Recruited an experienced CTT facilitator (optional but encouraged). An experienced CTT facilitator (part of the control team described in Section 3.2.1.1) is someone who has taken part in previous CTTs. The CTT facilitator is prepared to guide the CyWG leaders and CTT participants through the process by explaining the expectations of the exercise and ensuring the completion of the activities and products in each step.

Defined the operational mission(s). The CyWG will select one or more missions from the known missions that the SUA supports or from SUA provided functions. Mission selection depends on critical components of interest in the SUA. The possibilities range from an isolated mission for a single system to multiple missions executed in coordination with other platforms.

(See Section 3.2.1.2 for more information on selecting systems in scope for the operational mission).

Obtained commitment of key personnel. Critical personnel involved in conducting a CTT must be enabled and directed to participate in the CTT as explained in this guide. If not, the organization risks CTT schedule slippage, scope modification, and inaccurate results in the report. Deputy team leads for all three teams—control team, operational team, cyber opposing force (OPFOR) team—help mitigate the challenges with meeting conflicts. The team lead must empower deputies to represent the lead, and deputies must have near-equivalent knowledge.

Defined the intended subset of systems and interfaces that make up the SUA in support of an identified operational mission (systems in scope). For example, will the focus be on an entire avionics platform system, a subsystem of the platform, or an FoS executing a common mission? SUA selection determines factors such as the duration, resources, and expertise of the participants in the CTT.

Collected or developed the required CTT input artifacts. A CyWG can perform a CTT at any point in the system development life cycle. If the system design is still immature, then comprehensive system documentation will likely not be available. In this case, the CyWG may need to define some assumptions or provide surrogate designs to use during the CTT. Review Appendix G of the DoD Cyber DT&E Guidebook, Version 3.0, for more details. See also Section 3.2.4 of this guide for more information on system documentation and system reconnaissance.

Determined the classification level of the CTT. The classification level constrains what cyber threat intelligence the CTT team can use, examine, and discuss which intelligence is most relevant based on the objectives for the CTT and the applicable security classification guide(s) (SCGs). The CyWG should consider whether the classification level will exclude some essential participants. For mature systems, the SCG, which may or may not be part of the Program Protection Plan (PPP), describes the level of classification, the distribution statement, the ability to release the findings to foreign partners, and how to address cyber vulnerabilities discussed in the CTT and eventually documented in the report. However, early in a system's life cycle when planning and conducting the initial CTT, the program protection lead may not have finalized the SCG, or the SUA may not require an SCG. The CyWG will need to determine the CTT classification level; the distribution statement; and who will receive the CTT data, results, and related information. Holding a CTT at the Secret level, even if the SE and T&E artifacts are CUI or unclassified, protects the potential cyber vulnerabilities while their sensitivity is uncertain. The CyWG should also consider the classification of the aggregation of potential vulnerabilities. The OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) have

overarching SCGs available in the Cyber Table Top Guidance folder that generally describe how to handle cyber vulnerabilities to provide guidance to CyWGs that do not have an SCG.

Established agreed-upon and well-defined objectives (deliverables, timeline) for the CTT. The CyWG needs to define the objectives, risk reporting methodology, and schedule to guide the preparation and conduct of the event. Without clear objectives, participants will have mismatched expectations and divergent paths. This lack of unity can lead to delays or even the need to repeat part of the CTT.

Applied scientific test and analysis techniques (STAT) (optional). Including STAT subject matter experts (SMEs) who have expertise in techniques such as design of experiments can aid in structuring the CTT, analyzing its results, and assessing risk; see the STAT Center of Excellence (COE) Website (https://www.afit.edu/STAT/) for additional information. Recruiting STAT SMEs early in CTT planning can ensure that STAT best practices inform the activities and products. Contact the STAT COE via its website.

Completed training for key personnel. The organization's CTT lead and other key personnel should attend the Defense Acquisition University (DAU) virtual CTT workshop (CYB 5630V) to become familiar with the process. See the DAU CTT Course Website (https://www.dau.edu/courses/cyb-5630v) for more information.

3.2 Step 1: Exercise Preparation

Typically, Step 1 takes between 30 and 60 days. The major activities during *Exercise Preparation* include the following:

- Select the team leads, deputy team leads, and team members.
- Finalize the systems, subsystems, or components that are in scope and out of scope for the CTT.
- Define the team missions and enabling scenarios for the SUA.
- Prepare the initial mission impact assessment methodology.
- Define the likelihood assessment methodology.
- Collect and review the SUA documentation or initiate open-source reconnaissance for documentation, or both.
- Define and develop the plans and products.

3.2.1 Exercise Preparation: Select Teams

Personnel participating in a CTT are part of one (or more) of the following three teams, illustrated in Figure 3-2:

- Control team
- Operational team
- Cyber OPFOR team

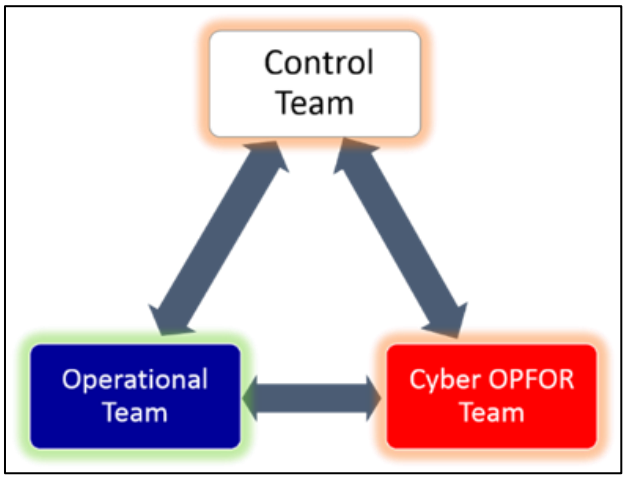


Figure 3-2. CTT Collaboration Diagram

The three teams collaborate to achieve the CTT objectives, and team members may support more than one team to conserve resources. Each team has a different set of responsibilities in the CTT. Team member participation may differ between steps and is adjustable as needed.

The following subsections describe the CTT roles and the optimal personnel to consider for each team. See Appendix A for a quick-reference guide on the CTT team roles and responsibilities. All participants must have the proper level of security clearance determined by the control team.

3.2.1.1 Control Team

The control team advances the CTT from the initial concept through the final report and is responsible for the logistical support for each step. The CyWG should assemble the control team early in *Exercise Preparation* because the team is responsible for recruiting all the other CTT participants. The control team is also responsible for meeting the CTT objectives and deadlines. During *Exercise Preparation*, the control team members are in continual communication while they construct the necessary plans and information before the exercise.

The control team should, at a minimum, be composed of the control team lead, CTT facilitator, operational team lead, cyber OPFOR team lead (also known as the OPFOR lead), and notetakers. Section 3.2.1 describes these roles in more detail.

Other control team roles include deputy team leads, security lead, intelligence lead, data analyst, and analysis lead. To keep the number of personnel at the minimum required; the control team members can serve multiple roles, as desired. Use the control team checklist provided in Appendix D: Cyber Table Top Checklists and the CTT Plan of Action and Milestones (POA&M) to avoid common challenges in conducting CTTs. Review the common CTT challenges and mitigations in Appendix E: Common Cyber Table Top Challenges and Mitigations.

Control Team Lead

The control team lead has the overall authority and responsibility for the CTT. The control team lead also represents the organization and typically has a leadership role in sponsoring the CTT. For a DoD acquisition program–led CTT, the lead systems engineer, lead system security engineer, or the T&E lead should be the control team lead. When industry is leading the CTT for a DoD acquisition program, the industry program manager determines the appropriate lead.

The control team lead needs to have broad knowledge of the system and insight into the SUA development, engineering, and testing schedule. The control team lead understands the operational mission and possesses the authority to ensure personnel assigned to a CTT team can and do support the CTT.

CTT Facilitator

For the initial CTT, a CTT facilitator is helpful in supporting the control team lead. The control team lead can also be dual hatted as the CTT facilitator. An experienced CTT facilitator possesses knowledge about the entire CTT process and brings best practices from previous CTTs. During *Exercise Preparation*, the CTT facilitator tracks the CTT products, helps recruit individuals with the appropriate expertise to participate, educates the control team on the CTT products, and guides the CTT toward satisfying the CyWG objectives. The CTT facilitator is responsible for training the notetakers. During *Exercise Execution* (Step 2), an experienced CTT facilitator ensures the discussions are at the proper depth and breadth and helps to manage time. During *Post-Exercise Analysis* (Step 3), the CTT facilitator continues to manage expectations and ensure ongoing communication and task completion. During *Reporting* (Step 4), the CTT facilitator attends the presentations and answers questions on CTT processes, as requested.

Notetakers

Notetakers have an important role in collecting data during CTTs. Notetakers document all relevant discussions during the exercise, including who said what[1], notional criticality ratings, and ad hoc solutions. Notetakers should understand computer systems and cybersecurity concepts and have some exposure to the SUA. The control team should select notetakers early enough to include them in control team planning meetings, cyber OPFOR lead and team technical exchange meetings (TEMs), and other meetings to build SUA familiarization. Notetakers have the power during *Exercise Execution* (Step 2) to halt the discussion whenever required to clarify unclear data, stop distracting side conversations, confirm the accuracy of data collected, or request additional details.

This guide recommends CTTs with more than 25 participants use at least four notetakers. This guide also recommends having the notetakers attend at least the first *Post-Exercise Analysis* (Step 3) meeting because of their in-depth understanding of the discussions.

Appendix A: Cyber Table Top Exercise Preparation Resourcesprovides an outline of notetaker best practices.

Analysis Lead

The analysis lead manages *Post-Exercise Analysis* (Step 3) and is responsible for developing the actionable information generated during *Exercise Execution* (Step 2) (i.e., analytical spreadsheet) by consolidating the presented documents and notes, ensuring the products are within the CTT scope and time constraints. The analysis lead is a member of the control team and may dually support the cyber OPFOR or operational team. The analysis lead can also be the data analyst described below.

Other Control Team Duties or Roles

The control team lead might need additional help depending on the size of the CTT and may need to delegate additional tasks or bring additional people to the team to complete these duties.

Data analyst: Helps organize the raw notes collected in the exercise into the data used in *Post-Exercise Analysis* (Step 3). For this role, this guide recommends an analytic, detail-oriented, and organized individual who understands cyberspace attacks. Assign the data analyst to both the control team and the cyber OPFOR team. The data analyst creates and maintains configuration control of the analysis table in *Post-Exercise Analysis*.

[1] Best Practice: The control team assigns all CTT participants a unique identification number they can call out when speaking during the exercise to aid the notetakers.

Control team deputy lead: Handles management, logistics, and administrative tasks throughout the CTT.

Security lead: Maintains the derivative classification records, performs the transmission of data, handles the storage of data, assists with identifying the *Exercise Execution* space, managing facility security requirements, and manages participant visit requests.

Intelligence lead: Supports the collection and coordination of intelligence information on known nation-state offensive cyberspace capabilities and known cyber tactics against the SUA.

Additional personnel: Additional technical personnel critical to support the control team who can advise on the operational mission or vulnerabilities and mitigations in the system design include the following:

- Chief developmental tester.
- Lead test engineer.
- System lead engineer.
- System security engineer.
- Other engineers able to answer technical questions about the system's "as-is" and "to-be" requirements and capabilities.
- Active duty or reserve officers with operational experience in the mission area of interest or with the SUAs, or both.
- OTAs.
- Cybersecurity SMEs.
- Prime contractor representatives, systems developers.
- STAT SMEs.

3.2.1.2 Operational Team

The operational team consists of the planned users, defenders, and maintainers of the SUA responsible for executing the team's tasks (including defensive cyberspace operations and system maintenance). This team also includes the engineers and developers who will describe the technical design features and SUA capabilities for the cyber OPFOR team. The operational team lead may ask these SMEs to support developing the operational mission (see Section 3.2.3.1), assembling the system documentation (see Section 3.2.4), and delivering the system(s) overview brief(s) (described in Section 3.2.5.2) for the CTT. To plan a realistic and effective operational mission, the operational team should collectively have knowledge spanning the following areas:

- The system design or concept, interfaces or expected interfaces, and communication paths or dataflows (or anticipated) in support of the operational mission.
- The current or planned tactics, techniques, and procedures (TTPs) for the operators, the operator's tasks in support of the selected mission, and the known or expected capabilities for the SUA necessary to accomplish the mission.
- The current "as-is" system capabilities and future "to-be" system capabilities, if applicable.
- The known, expected, or common pre-mission planning, post-mission debrief, and maintenance activities and systems, as applicable.
- The current SUA development, engineering, and testing schedule.

Identify the operational team members during *Exercise Preparation*. The size of the operational team will depend on the system(s), network(s), sensor(s), etc., in scope for the CTT. Use the operational team checklist provided in Appendix D: Cyber Table Top Checklists for guidance.

Operational Team Lead

The operational team lead, designated by the control team lead, supports all four steps of the CTT process and is responsible for planning the operational mission (see Section 3.2.3.1), gathering system documentation (see Section 3.2.4), and providing operational team deliverables within CTT time constraints. The operational team lead is a member of both the operational and control teams. The operational team lead should have operational knowledge and experience relevant to the systems, the systems' functionality, and the missions under consideration during the CTT.

Operational Team Members

The scope of the systems involved in the CTT should drive the selection of CTT personnel for the operational team. The operational team lead should consider the following personnel for the operational team:

- Military and civilian personnel with the required operational or functional experience from DT and OT organizations, reserve organizations, or operational user and test communities.
- System operators or end users.
- Personnel with weapons and tactics experience relevant to the mission.

- Individuals from organizations involved with the program and SUA development including the program office, prime or lead contractor, and relevant subcontractors.
- Maintainers (e.g., intermediate, organizational, and depot level).
- Engineers who are familiar with the differences between the current "as-is" and "to-be" state of the system(s) of interest (hardware, software, and support equipment).
- Subsystem SMEs (e.g., radar, networks, satellite communications (SATCOM).
- Anti-tamper SMEs.
- Secure supply chain SMEs with knowledge of secure supply chain development practices.
- System security engineers and program protection SMEs.
- Safety SMEs.
- Logistics and sustainment SMEs.
- Cybersecurity service providers (CSSPs) or network defense personnel for the SUA.
- Cybersecurity SME, ISSM.

The cybersecurity SME or ISSM can help ensure the operational mission execution details (see Section 3.2.3.1), operational team products (e.g., SUA briefs, SUA architecture and design or concept, interfaces or expected interfaces, communication paths or dataflows (or anticipated) in support of the operational mission, list of stakeholders of the SUA), and expected system security controls include sufficient technical details for subsequent discussions in *Exercise Preparation* with the cyber OPFOR team. The participants listed above can include personnel from industry (e.g., prime contractors or subcontractors).

This guide recommends the CyWG select the "mandatory" set of operational SME representatives early. Identifying the required SMEs prevents second-guessing the CTT results after the event is over by ensuring the CTT includes the "right" people.

3.2.1.3 Cyber Opposing Force Team

The cyber OPFOR team develops attacks to achieve the OPFOR mission (see Section 3.2.3.3) for the exercise. The cyber OPFOR team does not have to be large to be effective. The cyber OPFOR team (including the cyber OPFOR team lead) should include diverse and broad offensive and defensive cyber testing or cyber operational warfare backgrounds ideally relevant to the technologies in (or anticipated in) the SUA and external interfaces, which could include tactical data links, cloud, RF, or real-time operating systems. This diversity provides the opportunity for proposing a variety of potential attacks. The cyber OPFOR team should be

familiar with publicly known software weaknesses: common attack patterns (MITRE Common Attack Pattern Enumeration and Classification (CAPEC)), information security vulnerabilities (MITRE Common Vulnerabilities and Exposures (CVE)), MITRE Common Weakness Enumeration (CWE), and the NIST National Vulnerability Database (NVD).

The cyber OPFOR team lead should be a versatile professional—a true jack-of-all-trades—capable of managing and integrating the team's diverse talents to achieve mission objectives. The cyber OPFOR team lead may choose to coordinate with the cyber OPFOR team members during *Exercise Preparation* to perform open-source reconnaissance (see Section 3.2.4), mission planning, and attack surface analysis activities. The recommended size of the cyber OPFOR team is four to eight members, but the size may depend on the availability of people with the desired cybersecurity expertise and the technologies in scope. Use the cyber OPFOR team checklist provided in Appendix D: Cyber Table Top Checklists for guidance.

Cyber Opposing Force Team Lead

The cyber OPFOR team lead (also known as the OPFOR lead), designated by the control team lead, supports all four steps of the CTT process, is responsible for planning the OPFOR mission (see Section 3.2.3.3) and the cyberspace attacks driving the exercise. The cyber OPFOR team lead is the most important role in the CTT, and choosing the right person is critical to ensure the CTT results are high quality and useful to the CyWG. The cyber OPFOR team lead should have previous CTT experience serving on cyber OPFOR teams. Appendix A describes the importance of the cyber OPFOR team lead in the CTT and specifies the lead's responsibilities throughout all four steps of the CTT process. The OPFOR team lead must have a background in defensive and offensive cyber and have participated in previous CTTs. The cyber OPFOR team lead also needs to be an effective communicator who can explain cyberspace attacks from the perspective of an operational user. The cyber OPFOR team lead should seek to educate CTT participants by helping them to understand cyber from an offensive perspective and by explaining methods to counter attacks. The cyber OPFOR team lead is a member of both the cyber OPFOR and control teams.

Cyber Opposing Force Team Members

Personnel to consider for the cyber OPFOR team include the following:

- Authorized cyber team penetration testers and OTA representatives (e.g., DoD Cyber Red Team).
- Contractors or government personnel with offensive cyberspace operations certifications.
- Offensive cyberspace operations specialists.

- Penetration testing experts.
- Cybersecurity offensive analysts.
- Adversarial cyber operations professionals.
- Defensive and offensive cybersecurity SMEs.
- Cyber developmental testers or analysts (those expected to perform testing for the SUA and other similar systems).
- Cyber range (DoD, national, or commercial) personnel.
- EW testers.
- Interoperability engineers.
- Cryptography and communication security SMEs (as appropriate).
- CSSPs or network defense personnel for the SUA.
- Systems engineers or testers.

Including personnel from academia if available (such as professors or graduate students at Military Service postgraduate schools or war colleges, the Service academies, or research universities) with relevant offensive and defensive cyber certifications may have the added benefit of familiarity with DoD systems.

SE and T&E members (government organization or systems developer, as available) should also be part of the cyber OPFOR team (or dually assigned from the operational team) to assist cyber OPFOR team members with understanding the SUA and subsystems necessary to execute the operational mission (see Section 3.2.3.1) and to help during the exercise when the cyber OPFOR team is explaining cyberspace attacks.

3.2.2 Exercise Preparation: Finalize Scope

As noted in Section 3.1, the organization defines the intended subset of systems and interfaces that make up the SUA in support of an identified operational mission. However, various factors may contribute to modifying the scope during *Preparation*. The scope may increase or decrease. See Section 3.2.3.1 for additional scoping guidance.

3.2.3 Exercise Preparation: Define Team Missions

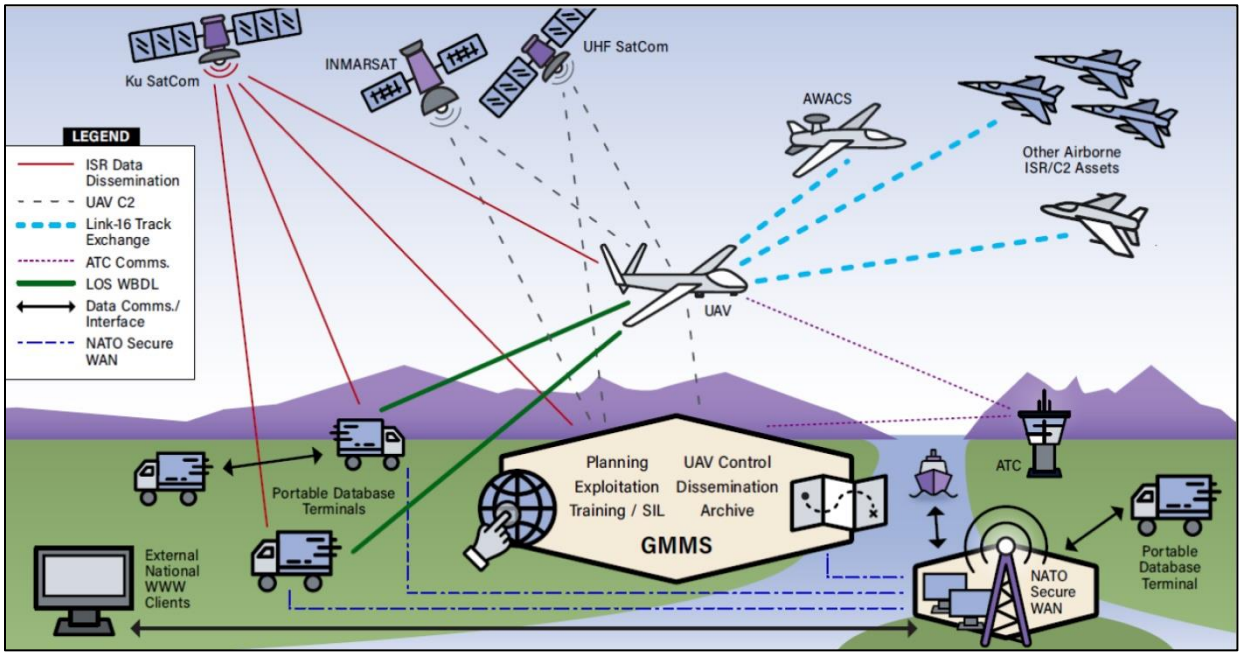
The operational and cyber OPFOR team leads define and document their respective missions for the CTT, and then the control team reviews and approves the missions. The operational team

lead develops the operational mission before the OPFOR mission because the cyber OPFOR team mission will target the operational team mission.

3.2.3.1 Operational Mission

The operational mission is a specific mission featuring the SUA. Most systems support multiple missions and perform multiple mission-critical functions in support of those missions. Missions may range from an isolated mission with just one single system (e.g., transporting equipment and personnel between locations); to missions executed in coordination with other platforms, sensors, or weapons (e.g., ground warfare, air warfare); to logistics and support function missions (e.g., human resources, maintenance, mission development, C2).

Artifacts, such as the requirements documents, concept of operations (CONOPS) or concept of employment, engineering plans, PPP, Test and Evaluation Master Plan (TEMP) or other T&E strategy, network diagrams or network design diagrams, and architectures such as DoD Architecture Framework (DoDAF) views (e.g., the Operational Viewpoint (OV)-1, which is the High-Level Operational Concept Graphic; Capability Viewpoints (CVs); and Standards Viewpoints (StdVs)), as available, all support mission development. These documents holistically provide a description of the subset of systems and interfaces for the various missions the SUA supports. See system reconnaissance in Section 3.2.4 for more information about system documentation. Figure 3-3 is an example OV-1.



Source: Defense Acquisition University Course CYB 5630V

Figure 3-3. Example OV-1 Graphic

The range of operational missions can include the following:

- A simple mission with a limited set of systems, sensors, weapons, and communication pathways. (May be useful as a learning experience.)
- A challenging mission that involves numerous systems, sensors, and communication pathways with complex exchanges to best explore vulnerability pathways.
- A common mission across the SoS or FoS of interest for the CTT.

Example Operational Mission (Based on the OV-1 in Figure 3-3)

The Unmanned Soldier Support System–Airborne (USSS-A) unit will conduct a time-critical 24-hour intelligence, surveillance, and reconnaissance (ISR) mission over a hostile terrorist training camp, Mordor, to provide real-time ISR data to allied forces regarding a high-value target, Sauron, possibly visiting the camp. The mission will include pre-mission planning, in-mission ISR data processing, and post-flight maintenance activities on each air vehicle to sustain operations for the full 24 hours.

The control team supports the operational team lead in developing the operational mission early in *Exercise Preparation* well before the kickoff because the OPFOR mission depends on the mission specified for the SUA. The scope of systems included in the CTT will dictate the number of people needed on the operational team and may drive larger control and cyber OPFOR teams because of the expertise needed and stakeholder interest. Delays in developing the operational mission or delays due to significant changes before kickoff will degrade *Exercise Execution* and may cause schedule delays.

Prepare the Initial Mission Impact Methodology

In preparation for guiding the discussions of mission impact during *Execution* (Step 2), the control team should develop an initial mission impact methodology during *Preparation* (Step 1) to provide time to discuss and refine the criteria before *Exercise Execution*. The operational team will further analyze and refine the methodology during the team's breakout session in *Execution* (Step 2), and the control team will finalize the methodology during *Post-Exercise Analysis* (Step 3). The methodology will document a scoring that aligns to the risk matrix or risk assessment methodology (selected by the CyWG before *Preparation*) to use for *Reporting* (Step 4) the CTT results. The typical scoring is on a 1 to 5 scale. The methodology ensures a consistent and repeatable assessment of mission impact for every cyberspace attack.

Figure 3-4 is an example of a high-level mission impact methodology focusing on critical data, critical functionality, and critical mission timing requirements. These mission impact categories

and associated details are notional and do not apply to all CTTs. There is no requirement to have a specific number of columns or to complete criteria for every row for impacts 1–5.

Impact	Mission Impact	Data Loss (Mission Critical)	System Performance (Mission Essential Function)	Delay (Operational Mission)
5	Non-Mission Capable	Classified	System Performance Severely Impacted/ Total Loss of Functionality	Greater than 2.5 hours
4	Non to Partially Mission Capable	CUI/New Technology	Major Loss of Functionality	Greater than 1 hour, less than 2.5 hours
3	Partially Mission Capable	CUI	Partial Loss of Functionality	Greater than 30 Minutes and less than 1 hour
2	Partial to Fully Mission Capable	Public Access Level	System Performance Marginally Impacted	Greater than 5 Minutes and less than 30 Minutes
1	Fully Mission Capable	No data compromised	System Performance Not Impacted	Less than 5 Minutes

Figure 3-4. Mission Impact Methodology Notional Example

To develop the initial mission impact methodology, the control team should analyze the mission and functionality decomposition from the criticality analysis and other system or mission artifacts to identify the mission-critical functions relevant to the SUA and to identify gaps or errors. The control team needs to understand the mission-critical tasks and critical data associated with the mission-critical functions and apply this knowledge to identify the appropriate impact columns.

The mission impact methodology enables consistency when assessing the mission impact. The control team will attempt to determine what columns are most appropriate in the initial draft based on CyWG objectives while considering critical systems and essential activities for a successful mission. The operational team lead should present the first draft of the mission impact methodology during the mission and scenario brief in *Exercise Execution* (Step 2). During the operational team breakout session in Step 2 (see Section 3.3.1.3), the team should review and refine the columns and the corresponding criteria for what constitutes at least fully mission capable, partially mission capable, and non-mission capable according to the SUA and the associated mission and scenario. The control team finalizes the methodology in *Post-Exercise Analysis* (Step 3) (see Section 3.4.2.2).

Select Systems in Scope for the Operational Mission

The choice of the subsystems included in the SUA limits potential cyberspace attacks to select interfaces, subsystems, FoS, or SoS under consideration in the CTT. Although the CyWG should decide the scope of the SUA before starting a CTT, the control team may identify additional systems during the operational mission development to include or exclude in the CTT. Exploring interfaces beyond the SUA authorization boundary and span of control may not be feasible. The control team must consult the system SMEs to ensure the correct interpretation of all the system information when narrowing down the critical components of interest in the SUA. In some cases, the selection of the systems in scope is a compromise dictated by the design maturity of the various subsystems, the available subsystem SMEs, and the amount of time to complete an assessment of reasonable depth. Some interfaces and subsystems not included in the scope of the first CTT may require additional CTTs to address them. The control team must thoroughly explain assumptions regarding interfacing systems outside of the SUA authorization boundaries.

Example Systems in Scope and Assumptions
(Based on the OV-1 in Figure 3-3)

The unmanned aerial vehicle (UAV), ground mission management system (GMMS), portable database terminal (PDT), and tactical aircraft landing system (TALS) are in the scope of the CTT, but the Airborne Warning and Control System (AWACS) and air traffic control (ATC) are not in scope. Assume the North Atlantic Treaty Organization (NATO) secure wide-area network (WAN), external national World Wide Web clients, and all SATCOM systems are fully operational.

When an SUA includes specialized assets, for example, control systems, anti-tamper, communications security, cross-domain solutions, embedded real-time operating systems, and other embedded components, the CTT team should consult CUI Appendix L of the DoD Cyber DT&E Guidebook, Version 3.0.

3.2.3.2 Operational Scenario

The operational scenario acts as the backdrop for the CTT exercise and contains a realistic set of conditions and circumstances that suggest how an operation might unfold, from the pre-mission planning to the post-mission maintenance phases. The operational scenario should be straightforward, with enough context to address the question of mission impact in contested cyberspace. As with the operational mission, the operational scenario should be ready well before kickoff to enable the cyber OPFOR team to prepare. The operational scenario may help structure attack timing or techniques. The operational team may need to finalize details for the operational scenario during the team's breakout session after kickoff.

Not all systems have a direct DoD warfighting environment. For example, logistics or business systems often operate behind the scenes of a conflict and mostly operate in non-conflict situations. However, these systems may have to support operational units and are legitimate targets, so the supported operational units and mission can provide the scenario backdrop for the logistics or business system operations. Supplying forward-deployed troops, deploying military units for a routine or urgent mission, providing human resources or financial management support, planning a mission, maintaining a critical system, etc., are examples of ways to focus the operational scenario for a system located far from the kinetic part of the conflict. For such systems, consider how the operational team would prepare for conflict well before the conflict breaks out and how threats may have effects in such a circumstance. Alternatively, related SUAs (non-warfighting and warfighting systems) or routine operations can form the basis of a relevant scenario for a CTT.

Factors to Consider for the Operational Scenario

Area of operations. The scenario can be set in a real geographic area (e.g., in the United States, outside the United States) or fictitious geographic area(s). Fictitious locations avoid any political sensitivities of warfare planning that involves potential adversaries but may require extensive preparation in developing the fictitious area compared with using an actual location.

Real geographic areas make it easier to identify actual distances, choke points, facility sites such as airfields and bases, current task force organizations, the location of the potential enemy forces, and specific intelligence information. However, using too specific of an area could result in a set of cyberspace attacks and outcomes not extensible to other real-world locations.

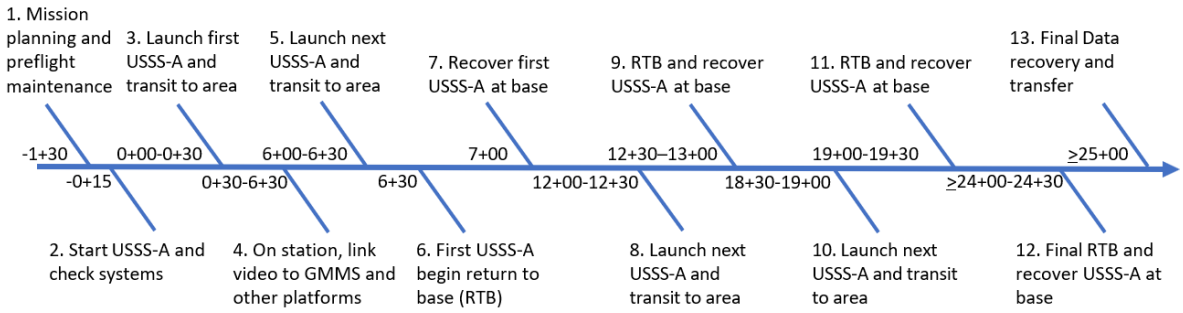
Example Scenario with an Area of Operations
(Based on the OV-1 in Figure 3-3)

The USSS-A unit will operate two UAVs in 6-hour rotations to maintain the 24-hour ISR over Mordor. Mordor is in a mountainous high-altitude (10,000 feet) area. Each UAV will depart from the forward operating base, the Shire, and proceed for approximately 30 minutes to the terrorist training camp airspace. The ISR mission will begin when the first UAV has reached 20,000 feet in altitude over the camp and is delivering ISR data to the GMMS and PDT via established data links. After a maximum 6 hours on station, the current on-station UAV will depart and return to the forward operating base after the second UAV enters the airspace and takes over ISR data collection and transmission. A minimum of four flights will occur to support the 24-hour surveillance period. Upon returning to the camp, each UAV will undergo post-flight maintenance as needed to prepare for its second flight. The mission will end when the last UAV successfully returns

to the forward operating base, and the USSS-A unit completes final ISR data recovery and transfer.

Schedule or time of day. Defining the time of day or involving multiple days may show how different times enhance or degrade the impact of successful cyberspace attacks on the operational mission. Troop movement at specific times of day, system maintenance, logistics, and support activities are potentially all part of the planning within the scenario schedule.

Example Operational Scenario Schedule (Based on the OV-1 in Figure 3-3)



Source: Defense Acquisition University Course CYB 5630V

Personnel. The scenario must account for the diverse range of personnel who may interact with or have access to the SUA during the specific mission thread under analysis. The personnel in the scenario should include all operators, maintainers, defenders, developers, external stakeholders such as contractors or supply chain partners, and other mission-critical personnel who directly or indirectly influence the system's functionality and security during the scenario. Each group introduces unique access points and potential vulnerabilities, whether through direct system interaction, maintenance activities, inadvertent actions, or continuous monitoring. For example, maintainers may require privileged access to perform updates, while operators rely on the system for mission-critical tasks. Additionally, external contractors may handle sensitive components, creating potential supply chain risks.

Example Operational Scenario Personnel (Based on the OV-1 in Figure 3-3)

Operators rely on the GMMS, data links, Global Positioning System (GPS), and supporting airborne assets to navigate to the airspace over camp Mordor and execute the mission. Maintainers perform pre-mission checks and post-mission maintenance to ensure that the UAV is fully operational for subsequent missions. Cyber defenders monitor the GMMS and PDT communication systems for potential adversarial activity during the flights.

Duration. Execution across hours, days, or months may reveal other cybersecurity vulnerabilities or opportunities for previously unidentified cyberspace attack vectors. Scenarios can be a single, short-duration task; multiple tasks spanning more than one crew cycle; tasks during watch standing (day or night); or tasks during system maintenance.

Example Operational Scenario Duration (Based on the OV-1 in Figure 3-3)

The mission will last approximately 25 hours through final data recovery and transfer. Each sortie will last approximately 7 hours from launch to recovery. The maintenance window after each flight is a maximum of 5 hours.

Weather. The scenario can include varying weather conditions such as rain, sleet, fog, chemical attacks, and airborne pollutants. If required, the operational team may need a detailed weather overlay as part of the preparation of the battlefield for mission planning. This overlay could help the operational and cyber OPFOR teams discuss the potentially magnifying effects different weather conditions could have on successful cyberspace attacks.

Example Operational Scenario Weather (Based on the OV-1 in Figure 3-3)

The scenario assumes moderate temperatures and clear skies.

Operational Assumptions. State any assumptions bounding the scenario and the discussions about the system(s). These assumptions may include the level of readiness of the systems (such as level of maintenance and personnel training), the political climate, the importance of the mission, and whether a state of war exists. Assumptions may also provide hypothetical intelligence about the area of operations, threat capabilities, and threat activity. The scenario may begin with an order from a higher authority, which follows a chain of command flow down to the unit represented by the operational team.

Example Operational Scenario Assumptions
(Based on the OV-1 in Figure 3-3)

Only two out of four USSS-A UAVs are operational. The UAVs can fly all night but not during severe weather. The UAVs have limited ability to work out of mission planning system–assigned areas (requiring a 2-day notice to support new areas). In the case of a maintenance failure on one USSS-A UAV, the unit requires 18 hours to return the UAV to service. Only fully qualified and cleared personnel operate the GMMS. USSS-A operators have full trust in the system and data links. Camp Mordor uses lookout teams on-site and at surrounding villages

en route. A recent combined EW (jamming) and an allied nation reported an attempted cyberspace attack against its similar UAV system. Only one PDT can be in active control of a single UAV at any time. Other PDTs may monitor the UAV in the line of sight at any time.

3.2.3.3 Opposing Force Mission

The cyber OPFOR team lead defines the OPFOR mission as an overarching objective to prevent the success of the operational mission and ideally support the control team objectives.

Example OPFOR Mission

Employ offensive cyber operations to prevent the adversary from capturing useful video of the visiting terrorist leader.

The cyber OPFOR team lead defines a series of specific missions across a typical cyberspace attack kill chain intended to deny, disrupt, or degrade the operational mission (see Section 3.2.3.1) for the SUA directly or indirectly (e.g., through deception or destruction). The cyber OPFOR team lead may also define various other objectives. See Appendix A for a description of a cyber kill chain. See system reconnaissance (Section 3.2.4) for more details about the documentation provided for the SUA.

The objective of each cyberspace attack mission usually focuses on a class of attack methods and their effects. The cyber OPFOR team lead should analyze the attack surface characterization and the threat assessment to inform the mission development and to guide the cyber OPFOR team in its attack development once assembled. The cyber OPFOR team lead should report to the control team any identified gaps or modifications. The following list provides non-exhaustive or non-universal examples of tailorable cyber OPFOR mission objectives. Tailoring may be to the specific SUA, the operational mission, or the objectives for the CTT. Later in the CTT, the cyber OPFOR team will develop specific attacks and variants of attacks to achieve the OPFOR objectives aligned to the OPFOR missions.

- Cyber OPFOR Mission 1
  - Objective: *Access*—Gain access to a system to stage an attack.
- Cyber OPFOR Mission 2
  - Objective: *Pivot*—Move laterally through the network.
- Cyber OPFOR Mission 3
  - Objective: *Deny*—Prevent communication.

- Cyber OPFOR Mission 4
  - Objective: *Deceive*—Alter data messages.
- Cyber OPFOR Mission 5
  - Objective: *Degrade*—Reduce the effectiveness of sensors and subsystems.
- Cyber OPFOR Mission 6
  - Objective: *Disrupt*—Introduce false system faults causing mission abort.
- Cyber OPFOR Mission 7
  - Objective: *Destroy*—Cause loss of data, systems, or life.
- Cyber OPFOR Mission 8
  - Objective: *Exfiltrate*—Send data to foreign nationals without detection.

The cyber OPFOR team should seek to propose attacks that support the cyber risk assessment needs of the control team and the SUA. The cyber OPFOR team may consider the capabilities of a nation-state, non-state groups encouraged or supported by a nation-state, terrorists, criminal organizations, or individuals. A challenge in developing the OPFOR mission is the complexity and length of time required to develop effects using full-spectrum methods, which may be very expensive and resource intensive. The cyber OPFOR team should propose adversary-agnostic attacks designed to test the functional performance of the cyber capabilities. Team members should first assess methods and techniques at the lowest level necessary (i.e., low-hanging fruit) to accomplish the OPFOR mission. The cyber OPFOR team may also consult the supporting intelligence information to ensure their proposed attacks accurately represent the threat for the operational mission.

OPFOR TTPs and Assumptions. The cyber OPFOR team should define TTPs the OPFOR may employ, describe assumptions bounding the allowed TTPs, including the level of the adversary and the level of covertness of the cyber OPFOR team. The team needs to know whether its actions must remain covert throughout or can become overt at some time during the exercise.

Example OPFOR TTPs (Based on the OV-1 in Figure 3-3)

* Supply chain manipulation of hardware and software.
* Exploitation of vulnerabilities in components, subcomponents, and maintenance systems (from positions in lateral systems).
* Insider can be inadvertent or deliberate.
* Social engineering.

Out of scope:
Kinetic attack on USSS-A or GMMS.

EW (e.g., jamming to create opportunities for cyber effects).

If the CTT team is under time constraints or if sufficient threat intelligence is not available, the CyWG or cyber OPFOR team lead may choose to make logical threat emulation assumptions such as "the threat actor is a highly capable adversary with nation-state resourcing, basic system knowledge, and supply chain access."

There are military advantages to remaining covert as long as possible. For example, an objective may be to exfiltrate information from the system under attack without detection. Other objectives may include causing system malfunctions or mimicking indicators of a malfunction that are indistinguishable from maintenance malfunctions. Cyberspace attacks are successful not only because of the magnitude of the effect but also because of the level of covertness achieved and maintained.

The cyber OPFOR team should outline assumptions regarding the reconnaissance information (see Section 3.2.4), weaponization efforts, and access to networks, as well as determine whether the team can combine proposed cyberspace attacks with other weapons such as missiles or EW.

Example OPFOR Assumptions

The OPFOR will attempt to stay covert when employing cyberattacks.
The OPFOR has some nation-state assistance:

* Malware via Universal Serial Bus (USB)/supply chain patch or upgrade distribution.
* Remote hacking.
* Phone/email hacking.
* Spoof capability.

The OPFOR developed code and malware to initiate an attack (cyber weapon).
The OPFOR has prior access to the platform, personnel, or GMMS.
The OPFOR has an insider at the USSS-A/GMMS base camp.

Preparation for Analysis: Define the Likelihood Assessment Methodology

Just as the control team must develop the first draft of the mission impact methodology to present during *Exercise Execution* (Step 2), the control team should also define and approve the likelihood assessment methodology. The cyber OPFOR team lead proposes the methodology for control team approval. The cyber OPFOR team will use the methodology during the team's breakout session in *Exercise Execution* (Step 2) to characterize the likelihood of developed attacks. As with mission impact, the likelihood assessment methodology would support a

consistent scoring system (typically scaled 1 to 5) that aligns to the risk matrix or risk assessment methodology (selected by the CyWG before *Exercise Preparation* (Step 1)) to use for reporting the CTT results. Typical likelihood assessments consider factors such as the cost and the success of an attack.

One approach is using a two-dimensional rubric, as depicted in Figure 3-5, to assess the technical feasibility for each cyberspace attack based on two criteria Attack Cost/Level of Effort and Attack Success Likelihood. Other databases for common cyberspace attacks (e.g., MITRE CAPEC, Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog) exist and may help to supplement or validate the likelihood assessment methodology chosen.

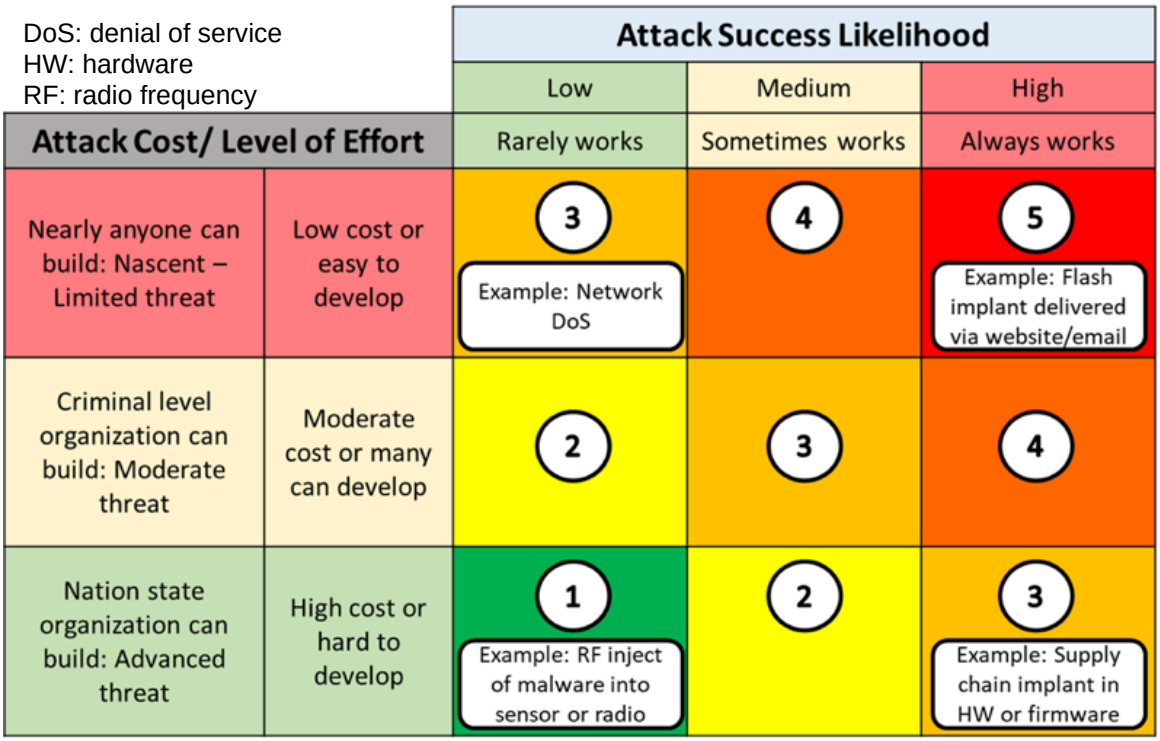


Figure 3-5. Likelihood Assessment Methodology Notional Example

The likelihood of a successful cyberspace attack may depend on certain assumptions, access method likelihoods, or conditions. When the cyber OPFOR team presents attacks during *Exercise Execution* (Step 2), the operational team may provide critical feedback about mitigations, cybersecurity controls, and operator or defender responses, which may result in a subjective upgrade or downgrade of the cyber OPFOR team's initial likelihood assessment. The cyber OPFOR team lead presents and explains the control team–approved likelihood assessment methodology during the OPFOR mission brief in *Exercise Execution* (Step 2). See *Post-Exercise*

Analysis (Step 3) (Section 3.4) for further discussion on applying the methodology and documenting the final likelihood assessment.

3.2.4 Exercise Preparation: Gather System Documentation and Conduct System Reconnaissance

Collecting reconnaissance on a system is typically the start of the cyber kill chain for staging a cyberspace attack. See Appendix A for a description of a cyber kill chain. The control team is responsible for ensuring all system information is available to both the operational and cyber OPFOR teams. The CyWG should provide the operational team lead with a system expert for each SUA in scope to support the operational team. The organization, contractors, or developers involved in the CTT gather and provide all available and relevant system documentation, guided by the cyber OPFOR team lead's requests for documentation, and develop the system overviews. Each system expert develops a system overview to present at *Execution* (Step 2). Section 3.2.5.1 describes the Data Handling Plan, including details about sharing system documentation.

Also, the control team may decide to create a reconnaissance team to conduct initial SUA cyber reconnaissance by reaching out to Service war colleges and research labs, Federally Funded Research and Development Centers, or University-Affiliated Research Centers; however, performing detailed reconnaissance will add time to Step 1. The OPFOR lead may also decide to have the cyber OPFOR team perform its own SUA reconnaissance and may or may not inform the control team in advance. The cyber OPFOR team reconnaissance may focus on specific components, the entire SUA, the developer, the supply chain, or any combination (or all). The cyber OPFOR team's reconnaissance may inform changes to the OPFOR mission or the development of specific cyberspace attacks against the system(s) in scope, or cyber OPFOR team assumptions and TTPs.

Prioritize Documentation!

Provide the cyber OPFOR team lead with the most important SUA details. Prioritize the SUA technical details associated with mission-critical functions based on the criticality analysis. The representatives for the systems and networks in scope of the operational mission should extract the high-level details to present as system briefs to the cyber OPFOR team lead.

Even if the control team pursues reconnaissance, the control team must ensure the cyber OPFOR team has access to the system briefs and full system documentation (described in this section) early enough to prepare. One best practice is to use a collaboration site with controlled access for the CTT participants to centrally locate all CTT documentation (i.e., planning and logistics, system documentation, briefs (see Section 3.2.5.2)). The system reconnaissance information could include SE specifications, diagrams, hardware and software inventories, available DoDAF

artifacts (e.g., OV-1, OV-2, OV-5, SV-1, CV-1, CV-6, StdV-1, StdV-2), architectural and interface diagrams, Capability Development Documents, TEMPs, and CONOPS guidance. The level of detail should be representative of the data the emulated adversary (i.e., the adversary the cyber OPFOR team is trying to represent) could obtain, given the level of expertise, timeline, and resources (e.g., a near-peer nation will have more resources and intelligence collection capabilities than hacktivists and small criminal organizations).

If the required documentation (design, CONOPS, etc.) is not available because of the system design's immaturity, then the control team and the CyWG must develop representative documentation as a model for the expected design or CONOPS. In many cases, the documentation is proprietary and sensitive; therefore, the CyWG should have the non-government participants sign a nondisclosure agreement (NDA) (see Section 3.2.5.1).

Table 3-1 provides a summary of minimum system documentation typically needed and briefed for a CTT. The information is also available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx).

Table 3-1. Minimum System Briefing Details

System Under Analysis Brief for Each System in Scope (As-Is and To-Be)	Details to Include in the Brief
System overview (all known or planned details)	• Mission – Describe how operators, defenders, and maintainers interact with the system during mission execution. • Functions • System diagrams (architecture, pictures, wired and wireless architectures) • Functional overview: dataflows, messages (wired and wireless) • System configuration, network diagrams • Expected or known connections and ports between components internal to the system under analysis (SUA) • Expected or known connections and ports to other components external to the SUA • Expected or known communication protocols between components • Expected or known application program interface information on SUA components

System Under Analysis Brief for Each System in Scope (As-Is and To-Be)	Details to Include in the Brief
Key dependencies (external systems, dataflows, networks, or resources that the SUA relies on to function effectively)	• External systems, networks, or resources critical to system functionality • GovCloud • External data or services • Application program interface • Third-party maintenance site or service
List of software (commercial off-the-shelf, government off-the-shelf, free open-source) and hardware, if known	Versions (operating system, applications)
Maintenance (planned or established)	• Software, firmware, hardware – Refresh cycle – Update frequency – Maintenance process • Restart and reload times • Maintenance support device details • Personnel roles in pre-mission and post-mission maintenance activities, including access to sensitive subsystems and procedures
Known vulnerabilities (not plan to remediate)	Method of discovery: scans, testing, or other analysis
System protections, if known	Controls, defensive cyber tools, cybersecurity service provider details, configurations
Physical protections, if known	Human, gates, guns, locks, etc.
Description or depiction of how the system contributes or will contribute to the operational mission	Critical functions, critical data, or mission-relevant terrain in cyberspace

The cyber OPFOR team lead, interoperability lead, and systems engineers review the gathered reconnaissance and confirm the SUA documentation contains sufficient information. The cyber OPFOR team lead may request supplemental documentation and diagrams to develop better knowledge of the SUA or may instruct the cyber OPFOR team to complete separate, open-source reconnaissance based on the operational mission and system scope.

Figure 3-6 is a flowchart summarizing the system reconnaissance and documentation process including OPFOR lead analysis activities. Figure 3-6 depicts those tasks every CTT should include (left, solid lines) and optional or recommended tasks (right, dotted lines).

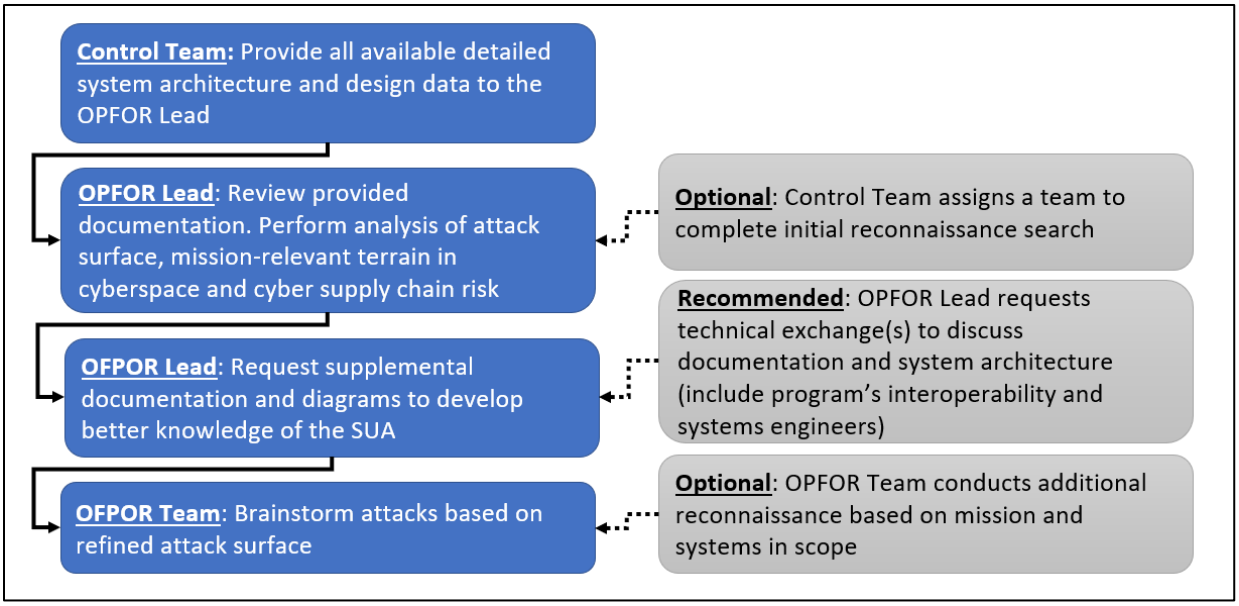


Figure 3-6. CTT System Reconnaissance and Documentation Process

A series of TEMs with selected participants is critical in helping with the *Preparation* planning between the engineers and team leads. TEMs early in the CTT process ensure distribution and analysis of relevant technical information so participants have sufficient time to read and process the details before the exercise. Examples may include the control team:

- Arranges a tour to see the installed equipment, manufacturing facilities, or testing laboratories of the SUA in the CTT. The participants' first-hand interaction provides context during the exercise.
- Holds information sessions to educate the CTT team leaders, analysis lead, data analyst, and notetakers on the objectives, deliverables, schedule, overview, and breakdown of the activities before the exercise. The information session also provides the opportunity for a dry run and beta test of the CTT instructions, tasks, and deliverables. Trainees can provide feedback on how the information will translate to the actual participants. Depending on the size and scope of the SUA(s),the control team should schedule regular meetings to allow adequate time to prepare the participants.
- Presents system (as-is and to-be) briefs in a separate session from the CTT when there are many systems in scope, such as for an FoS CTT. The presentations allow the cyber OPFOR team the opportunity to ask the engineers about in-depth technical details without immersing all participants, such as operators, in the technical specifics. Assigning technical engineers to the cyber OPFOR team can also address this need without having a separate meeting.

- Before the exercise, ensures the security lead provides instructions to the notetakers for properly marking classified materials.

The cyber OPFOR lead and team use these TEMs with the engineers, contractors, and systems developers to ensure they start the CTT with an in-depth technical grasp of the system, functions, and interfaces. Without a TEM or site visit, the *Exercise Execution* (Step 2) may result in the cyber OPFOR team being more focused on the technical networking, protocols, applications, hardware, software, and firmware rather than on the operational mission. Common questions the cyber OPFOR team may ask during a TEM, depending on the SUA maturity, include the following:

- What hardware is being used (planned) on this system?
- What operating systems are installed on (planned for) these systems, including service packs and versions?
- How does (will) the system, organization, program, etc., receive updates?
- What software is (will be) installed on each of these systems?
- What services and open ports are (will be) running on each of these systems?
- What are the key dependencies?
- Is a data feed required for cyber defense?
- What cloud services are foundational to the defense of the system?
- How are these systems normally accessed (planned to be accessed) for operations, troubleshooting, or maintenance?
- With which device does each system communicate? Through which service/port? Is the communicating device internal or external to the SUA architecture?
- Over what medium does the system communicate? Wired? Wireless? Optical?
- Is the SUA being actively monitored by a cyber defender? Is the cyber defender internal or external to the SUA architecture?
- What would be the impact on the mission if each system was brought to a degraded or failed state?
- How is trust established between system components?
- How are SUA local area networks and WANs (if relevant) configured?
- How often are these systems (will these systems be) patched?
- Do (Will) these systems reside in secured spaces?

- Do (Will) these systems have any external USB ports or digital optical disc data storage format drives?

3.2.5 Exercise Preparation: Develop Plans and Products

During *Exercise Preparation*, the control team plans and creates products necessary for the exercise. This guide recommends constructing a CTT POA&M to track all the tasks throughout the CTT and assign the personnel responsible for completing each task. An example CTT POA&M spreadsheet is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx).

3.2.5.1 Pre-Execution Plans

Nondisclosure Agreements

NDAs are the preferred tool to address the developers' or program's concerns regarding the sharing of the CTT discussions and data as well as proprietary design information. The control team should develop, or obtain from the programs or organizations involved, the necessary NDA forms before sharing proprietary system information. Ensure all non-government participants sign the agreement(s), as required, before the start of the exercise. Programs should consider requesting input from the developer's or the program's legal division. Basic NDA templates are available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx).

Rules of Engagement

The control team develops the rules of engagement (ROE) for the CTT to inform all participants of encouraged or discouraged behaviors during the exercise.

Example ROE include:

- Nondisclosure.
- Non-attribution.
- Non-retribution.
- No sidebar conversations (or OSCAR: Other side conversations are restricted).
- No interrupting others.
- Timely return from breaks.

- No pet rocks (or MOTHMAN: Move on, this has made all nap).
- Limit conversation duration (ELMO: Enough, let's move on).

If necessary, the team can also create ROE specific to the operational, cyber OPFOR, and reconnaissance teams (if used).

Data Handling Plan

The control team should obtain and review all available relevant SCGs for the SUA(s); see information on CTT classification in Section 3.1. In instances where multiple SCGs are applicable because of multiple SUAs (e.g., a platform of systems), the control team should work with the security lead to deconflict SCG guidance. The security lead must develop a plan based on the CTT classification level that clearly documents the requirements for marking, transmitting, and storing data or products produced in each CTT step. The control team must analyze the CTT data requirements and ensure all tools, the facility, and the CTT processes are at the appropriate level. The data handling plan should address the following:

- Date, location, and associated visit request information for meeting locations (e.g., *Exercise Execution*, *Post-Exercise Analysis*).
- Classification level of the event and facility (e.g., the facility is at a higher classification and the processes associated with the facility controls).
- Prohibited material.
- Guidelines for banner and portion markings.
- Classification authority and relevant details.
- Details regarding classification markings for data aggregation, as relevant.
- On-site security point of contact and expectations for the generation of classified data by participants.
- Security-reviewed plan for the storage and transmission of classified data, briefs, and reports, both digital and non-digital, designated with who is responsible for coordinating resources or collaboration tools.
- Procedure for preserving anonymity when transferring raw CTT data generated in *Exercise Execution* (e.g., written notes, audio recordings) into official reports.

The control team should set up controlled access repositories (unclassified and higher) to share system documentation, data, CTT products, and requests for information (RFIs) before the exercise to reduce the need to email documents and files. However, some CTT participants may

not have access to the SIPRNET, JWICS, or classified spaces to review and refine the documentation, despite having clearances. The control team defines the processes for sharing the information and then documents the procedures in the Data Handling Plan. Table 3-2 provides an example of the types of expected CTT data or products from each CTT step and considerations for storing and transmitting the information, if classified, throughout the CTT.

Table 3-2. Example Table for Tracking Data or Products Developed in CTTs

	Exercise Preparation	Exercise Execution	Post-Analysis Exercise Meeting #1	Post-Analysis Exercise Meeting #2	Post-Analysis Exercise Meeting #3	Reporting
Data and Products	• Data handling • Briefs • OPFOR homework	• Operational timeline • Notes • Attacks	• RFIs • Analysis table • Homework	• Analysis table • Assessment rubrics • Homework	• Analysis table • Risk matrices • Draft report	Results brief
Transmission	Compact Discs, Courier, or Shared Repository					
Storage Location	Digital or Physical					
Point of Contact	On-Site Security Lead					

Planning for the Day of the Exercise

Rooms. The control team reserves a room that accommodates all primary and backup dates required, all participants at the appropriate classification level and contains any necessary audio and visual equipment for presentation graphics. Also, make sure to reserve separate rooms for team breakout sessions (see Section 3.3.1.3) during the exercise. Appropriate spaces may be popular and booked months in advance, making multiday vacancies rare, so reserve space early.

Leadership welcome. Plan to have program leadership welcome the CTT participants, offer support, and emphasize the importance of the results. In addition, leaders have an opportunity to see how the CTT is using the resources.

Intelligence and relevant threat briefs. Arrange for an intelligence brief that presents real-world intelligence of known adversary targeting activities and capabilities. A best practice is to request the brief at the start of CTT planning to allow the intelligence organization the time required to develop the brief. The program must request support from the appropriate intelligence organization or program intelligence liaisons. Generalized intelligence briefs may not be very useful because the information will not cover future adversary cyberspace capabilities and may not be directly relevant to the SUA(s). Additionally, a relevant threat brief

that provides examples of adversary TTPs and security breaches against relevant technologies in the SUA is useful to familiarize participants.

Observers. Consider inviting the system's owners or interfacing system SMEs to the exercise. Plan space to allow stakeholder observers to attend the exercise. Limit the number of other observers and include a listen-only ROE for observers during the CTT.

Visual aids. Prepare or plan to display large, legible printouts of system interfaces, network diagrams, or other critical system diagrams for the exercise, as requested by the cyber OPFOR team lead, to help with the understanding and visualization of cyberspace attacks presented by the cyber OPFOR team.

Notetaker supplies. Plan for notetakers to either handwrite notes or use laptops at the appropriate classification level. If using MAT—the MBCRA Automation Tool discussed in Section 2.1.2—the tool's CTT module enables and enhances CTT note-taking, providing a means to capture easily read, searchable, and time-synchronized notes.

Planning for Participants

Participant invitations. The control team should distribute essential information to all participants approximately a month before the kickoff and the exercise. Usually, this information is in a calendar invite and a separate detailed email and includes read-ahead material or links to the collaboration site; maps to meeting locations (facility access, parking details, room information); local hotels; dining-out information; landing fees (for catered snacks, beverages, lunches); agenda; dress attire (e.g., military uniform of the day, business casual); instructions for submitting visit access requests; and the names, emails, and phone numbers for points of contact in case of challenges or emergencies.

Welcome packets. The control team may include items such as the agenda, participant's number (such as a name tag, an auction paddle, or some other mechanism to identify the assigned number), relevant diagrams of the SUA, an acronym list, mission details, a list of all participants and their assigned team, note-taking sheets, details for the icebreaker or social event, and a CTT participant survey to complete before the end of the event.

3.2.5.2 Pre-Execution Products

Schedule and Agenda

The control team prepares a schedule of events for the exercise. The schedule should include an agenda for the first day of the exercise (i.e., the kickoff (see Section 3.3.1)), where key personnel present a series of informational briefs to all participants.

Kickoff Briefs

The control team creates the following briefs to present at the exercise kickoff:

Administrative welcome: The control team lead or deputy provides administrative details about the building, food, and schedule, and informs participants of the notetakers' role.

CTT overview: The CTT facilitator or control team lead outlines the CTT steps and schedule for the exercise. The kickoff agenda should include time for team introductions at the start of the CTT and for the other briefs described below. The overview should also include the program objectives, explaining how the CTT fits into the overall program cyber efforts, to set the tone for the CTT.

CTT ROE: The control team lead presents the rules for the participants and teams in the CTT, intended to ensure an orderly, objective, and productive exercise (see Section 3.2.5.1).

Classification level, Data Handling Plan, NDAs: The security lead reviews the classification levels and procedures for handling and storing documents during the exercise. The lead reminds participants to precede known classified statements with an announcement of the classification level (see Section 3.2.5.1).

SUA descriptions: As mentioned in Section 3.2.4, the control team provides briefs with background information on the SUAs within the scope of the operational mission. The briefs should provide emphasis on the critical data exchanges between systems and interfaces across networks. The briefing should allow time for technical questions by the cyber OPFOR team. As noted in Section 3.2.4, the control team may decide to hold a separate meeting for the cyber OPFOR team before the kickoff to provide a deep dive into the technical details of the system, especially if the system description briefs alone would require 1 to 2 days.

At a minimum, the description should highlight the threshold "to-be" state of the future system capabilities and include all interfacing systems. Resources to consult for developing this brief could include available DoDAF artifacts (e.g., OV-1, OV-2, OV-5, SV-1 CV-1, CV-6, StdV-1, StdV-2), other descriptions that illustrate the capabilities and systems that are part of the program of record, interface control documents, SE specifications, software, and hardware. The system owner or SME could reuse an existing technical system brief, simply tailoring the content to match the objectives of the CTT.

During *Exercise Preparation*, the cyber OPFOR team lead will become more familiar with the relevant operational mission activities for the SUA and will likely identify additional desired details to include in the system description.

A best practice is to conduct the technical SUA briefs virtually with at least the cyber OPFOR team leading up to the kickoff and to share briefs with all participants to review in advance. During the kickoff, instead of briefing the SUA details again, the focus could be on clarifying questions from the cyber OPFOR team or other participants. This practice may also save time and improve OPFOR readiness.

Operational and cyber OPFOR team missions: The team leads describe their respective team missions and their assessment methodologies for mission impact and likelihood. They also present the teams' tasks for the breakout sessions and the exercise.

3.2.6 Execution Preparation: Exit Criteria

The CTT is ready for *Exercise Execution* (Step 2) when the control team meets the following conditions:

- Assigned all lead roles (e.g., OPFOR lead, security lead, analysis lead).
- Finalized systems, subsystems, or components in and out of scope.
- Evaluated the criticality analysis (missions, critical functions, and critical data) and identified gaps or errors.
- Analyzed the attack surface characterization (characterization of dataflows into and out of the system) and identified gaps or errors.
- Reviewed the threat assessment.
- Invited all participants and provided read-ahead material.
- Built welcome packets.
- Developed and approved the operational mission and scenario and the OPFOR mission.
- Developed the initial mission impact methodology.
- Developed and approved the likelihood assessment methodology.
- Completed and summarized the reconnaissance on the SUA.
- Accomplished TEMs with systems engineers, SUA cybersecurity experts, and the OPFOR.
- Developed and approved the Data Handling Plan.
- Reserved the exercise facilities and equipped them with supplies.
- Finalized all briefs.
- Obtained contact information (unclassified/classified (if possible)) for reach-back SMEs.

3.3 Step 2: Exercise Execution

This step usually takes place over a period of 3 to 5 days, which may or may not be consecutive. The major activities performed during *Exercise Execution* include:

- Conducting the exercise kickoff.
- Executing the CTT exercise.
- Collecting and reviewing the data.

Although the entire exercise nominally takes 3 to 5 days to complete, the CTT is an adaptable process that can span a longer duration (for complex scenarios or a large SUA scope). Alternatively, the control team may decide to split *Exercise Execution* into two separate events: (1) the kickoff and (2) the execution along with the data collection and review. Appendix B contains two example CTT *Exercise Execution* agendas: one for an exercise planned for 3 or more consecutive days, and one for an exercise with a separate kickoff scheduled well before the main CTT exercise. Appendix B also provides a collection of exercise support planning information containing best practices gleaned from past CTTs.

3.3.1 Exercise Execution: Kickoff

The kickoff, sometimes called a TEM, takes place over 1 to 1.5 days and sets the stage for the CTT. Because not all CTT participants are involved in the *Exercise Preparation* (Step 1), the kickoff serves as an opportunity to educate everyone on the CTT methodology and expectations.

Holding a kickoff, team breakout sessions, and TEMs in advance (2 to 4 weeks) of the main CTT exercise allows for technical clarifications and refinement of the details in the operational scenario (see Section 3.2.3.2) and OPFOR mission (see Section 3.2.3.3) and positions all teams for a more efficient CTT exercise. In addition, the control team might schedule tours of the system prototypes, example environments, support equipment, test facilities, or development laboratories for the SUA during this time. Later, at the main CTT exercise, the control team presents the updated kickoff briefs and the intelligence brief.

3.3.1.1 Pre-Exercise Meeting “Day 0”

If possible, the control team should plan to meet at the location of the CTT the day before the exercise. This preparatory meeting provides an opportunity for the team leads to address any last-minute issues such as checking clearances, discussing hot topics, and making agenda updates, as well as walking through the kickoff briefs. The control team should verify that audio and visual equipment is in working order. The control team lead or CTT facilitator can also use

this time to meet with the notetakers to provide guidance about their role and instructions on classification markings.

3.3.1.2 Kickoff Briefs

As previously described in Section 3.2.5.2, the exercise kickoff begins with a set of briefs delivered to all the participants. Typical briefs presented include the following:

- Program leadership welcome
- Administrative welcome
  - Presenter: control team lead or deputy
- CTT overview
  - Presenter: CTT facilitator or control team lead
- CTT ROE for individual participants and teams
  - Presenter: control team lead
- Classification level, Data Handling Plan, and NDAs
  - Presenters: control team lead and security lead
- System description(s)
  - Presenter: control team
- Intelligence and relevant threat brief (optional)
  - Presenter: intelligence agency or control team
- Operational and cyber OPFOR team missions
  - Includes team assessment methodologies and draft team tasks (completed in team breakout sessions)
  - Presenters: operational team lead and cyber OPFOR team lead

3.3.1.3 Team Breakout Sessions

After the kickoff briefs, the operational and cyber OPFOR teams should meet separately to complete their team tasks. The operational team details the sequence of actions to execute the operational mission (see Section 3.2.3.1), refines any details in the operational scenario as required, and supports the OPFOR by answering questions about the SUA, mission, etc. The cyber OPFOR team plans plausible cyberspace attacks to execute the cyber OPFOR mission objectives (see Section 3.2.3.3). During the breakout sessions, the operational and cyber OPFOR

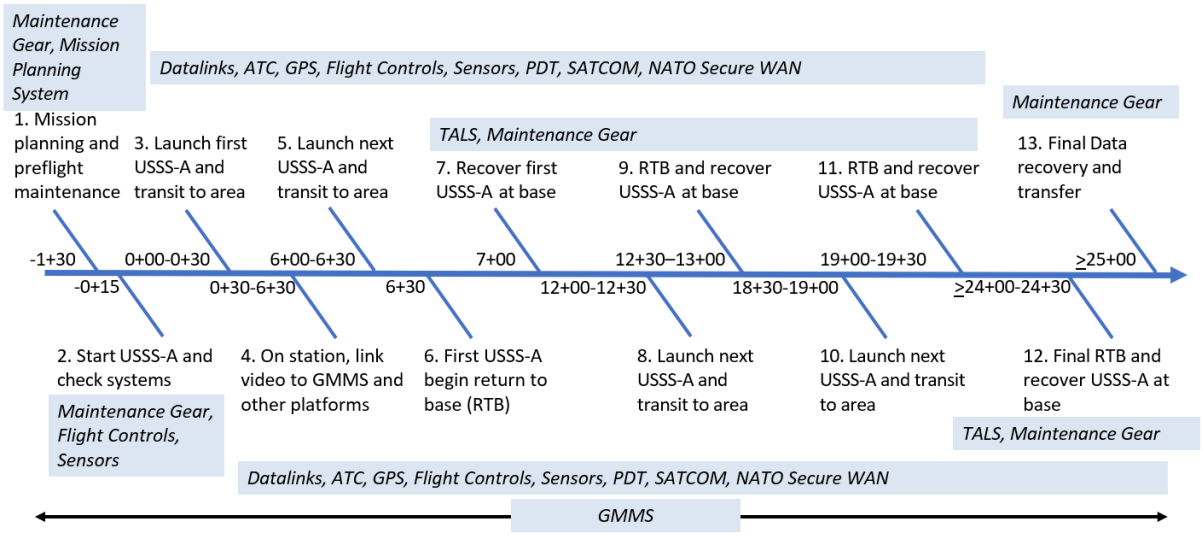
teams independently refine products they will subsequently present to the rest of the CTT participants. Conducting the kickoff and team breakout sessions before the CTT significantly enriches the teams' technical knowledge and preparation.

Operational Team Breakout Session

The operational team should review the mission and functional decomposition within the criticality analysis and correct any discrepancies. The team members will discuss the initial mission impact methodology (see Figure 3-4) and ensure they agree with or modify what "partially mission capable" or "non-mission capable" means for the SUA. The mission impact criteria should identify specific parameters that indicate mission failure and correlate with the mission and function decomposition. See the mission impact methodology information in Section 3.2.3.1 for more details. The personnel tasks and details in the operational mission support the cyber OPFOR team's development of cyberspace attacks. The cybersecurity SME who is part of the operational team should help define the level of detail sufficient for later discussions about vulnerabilities. The operational team's objective for the breakout session is to accomplish the following:

- Develop a detailed timeline of mission-essential tasks, functions, communications, or personnel actions to execute the operational mission within the context of the operational scenario timeline.
    - These critical elements will be indicative of the eventual TTPs for employing the SUA and will enable the operational team to understand SUA cyberspace effects proposed by the OPFOR.
- Update the operational team mission brief including:
    - Updating the mission impact methodology and criticality analysis.
    - Describing how all personnel would complete each task of the operational mission.
    - Explaining how the mission employs the SUA.
    - Specifying the systems, interfaces, dataflows, and protocols critical to accomplishing the operational mission.
    - Detailing the sequence of maintenance actions, as appropriate.
    - Providing a basic visualization and description of the timeline with the mission plan, critical functions, and sequence of actions (e.g., interfaces and dataflow) that occurs from pre-mission planning and maintenance to post-mission debriefs.
- Answer cyber OPFOR team questions about the mission or SUA.

Example Operational Timeline with Systems



Source: Defense Acquisition University Course CYB 5630V

Cyber OPFOR Team Breakout Session

The cyber OPFOR team's objective is to develop a list of potential exploitation pathways to execute the OPFOR mission, based on the system reconnaissance (see Section 3.2.4) for the SUA. The cyber OPFOR team reviews the SUA technical details and the operational mission (see Section 3.2.3.1) and scenario (see Section 3.2.3.2). The systems engineer or tester should provide mission-relevant input during the OPFOR cyberspace attack planning.

The cyber OPFOR team lead may provide the cyber OPFOR team with a format to develop its attacks. Example templates for OPFOR products are available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) in the Cyber Table Top Guidance folder. The format should explain the cyber OPFOR opposing mission objective, attack goals, the system attacked, the expected effects, and the assumptions made about the attack process including the initial likelihood assessment using the control team–approved likelihood assessment methodology (see Figure 3-5). The format should also give details about the attack method, including when to execute the attack in the operational mission timeline. The proposed cyberspace attacks serve as the starting points for discussion during the exercise (additional cyberspace attacks or variants may arise after discussing a proposed cyberspace attack in the exercise).

The cyber OPFOR team proposes multiple cyberspace attacks for each OPFOR mission (see Section 3.2.3.3). The cyberspace attacks should be logically plausible and based on the technical

data provided but not necessarily tested and proven to work. The cyber OPFOR team should aim to develop a set of cyberspace attacks that addresses every part of the TTPs for the operational mission. The cyber OPFOR team should not present cyberspace attacks as multiple effects occurring at once. During *Post- Exercise Analysis* (Step 3), the analysis participants document the details for each proposed cyberspace attack and mitigations (in place, planned, or proposed). During the *Reporting* phase (Step 4), the control team combines attacks to develop vignettes for the final report. The combined attacks in the vignettes will include the kill chain (see Appendix A) sequenced attacks and may include layered attacks. Layered attacks are useful to demonstrate how adversaries may combine multiple effects using a single point of presence to potentially maximize mission impact. Presenting each attack independently supports the reuse of kill-chain elements and the identification of mitigations targeting each part of the attack kill chain. This approach supports program prioritization of the actionable information.

If time permits and a computer with the appropriate classification is available for the cyber OPFOR team, the team can digitally document the proposed attacks in the analysis table (see Appendix C: Cyber Table Top Post-Exercise Analysis Resources) for later use in *Post-Exercise Analysis* (Step 3). A downloadable and tailorable template for the analysis table is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx). Regardless, the notetakers will capture the proposed cyberspace attack details and ensuing discussions.

3.3.2 Exercise Execution: CTT

The CTT exercise takes place after the kickoff and usually lasts 1 to 3 days. The operational team presents its brief, developed during the breakout session, to all the participants. The brief describes the detailed mission execution plan and the updated mission impact methodology (see Figure 3-4). Then the cyber OPFOR team presents its proposed cyberspace attacks, describing the cyber opposing mission objective (see Section 3.2.3.3), the specific system targeted, the likelihood assessment, any assumptions made, and when in the mission timeline the adversary could execute the attack. The cyber OPFOR team lead drives the CTT by introducing each new OPFOR mission as the participants collaboratively talk through the sequence for all the related cyberspace attacks, as depicted in Figure 3-7.

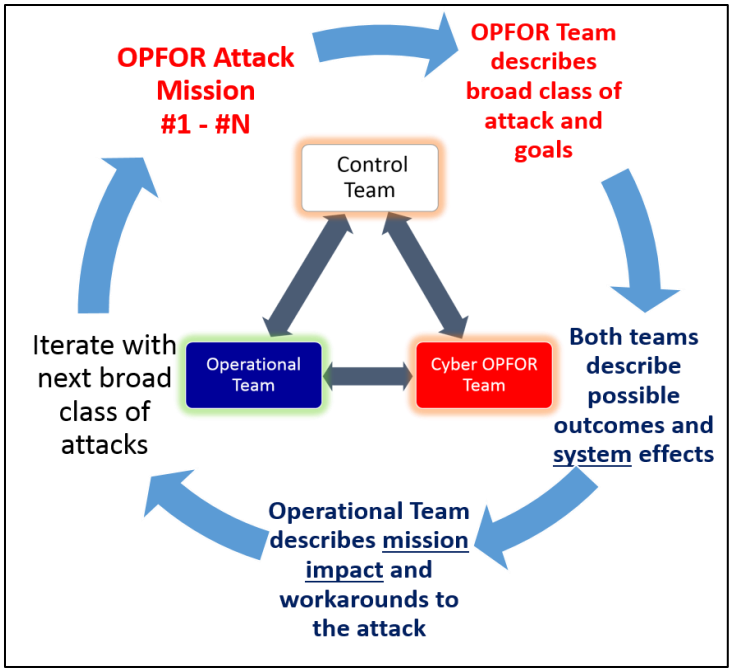


Figure 3-7. CTT Exercise Execution: Team Collaboration

The presenting cyber OPFOR team member may choose to diagram where on the operational timeline the attack will occur if the cyber OPFOR team expects a temporal attack to affect the operational mission. The cyber OPFOR team members lead a discussion on each of the developed attacks; however, they may or may not choose to display the developed attack template to the exercise participants. Displaying SUA diagrams and discussing conceptual attacks is a best practice. This guide does not recommend displaying notes and describing technical details of the attacks. Attack descriptions may not be fully refined, and technical details may distract participants unfamiliar with attack techniques from the objectives of the discussion.

The cyber OPFOR team should propose only specific attacks that look feasible after a detailed review of system documentation. The cyber OPFOR team breakout session (see Section 3.3.1.3) may need to expand to a series of team technical meetings over the weeks leading up to the CTT so the cyber OPFOR team presents feasible and relevant attacks on the SUA to the mission context.

CTTs are not meant to delve deeply into technical attack techniques because most CTT participants are usually not cyberspace technical experts and may not understand the details. The cyber OPFOR team should seek to elicit participants' responses to the conceptual attack and its intended system effect. The responses enable the cyber OPFOR team to shape and mature the attack or to branch off and evolve the attack into a variant or a completely new attack, which may prove to have more impact than the original proposed attack. The goal is to present provocative ideas to motivate and inspire participants to think more like an attacker and identify

areas of weakness that can cause mission impact. The cyber OPFOR team member should use inviting and thought-provoking phrases such as “what if…”, “have you ever seen…”, or “can you help me better understand how…”. The presenter knows the in-depth technical details for the attack technique and may have experience performing the attack against a similar SUA, but the presenter does not need to describe the details to the participants.

The cyber OPFOR team needs to understand the classification level when presenting attacks because in some cases, specific techniques against systems or tactics associated with specific nation-states will increase the classification level of the discussion. The control team should establish the expected level of detail for attacks at the start of the exercise to avoid classification level breaches.

Both the operational and cyber OPFOR teams discuss the OPFOR’s hypothesized system effects and together assess the likelihood of the OPFOR success and the mission effects of the attacks. The teams should also deliberate about critical mission areas and what opportunities those critical mission areas provide for a potential adversary. The operational team leads the discussion about the mission impact and workarounds that could prevent or mitigate the effects of the attacks presented. The teams also hold discussions about recovery times and procedures to comprehend the ability to perform the mission-critical tasks or functions. The notetakers must carefully capture all discussions about likelihood, mitigations, cybersecurity controls, and operator or defender responses because these discussions will affect the final likelihood assessments in *Post-Exercise Analysis* (Step 3). At the end of the discussion for each attack presented, the cyber OPFOR team lead should summarize for the notetakers the key data as well as any assumptions made about the attack before tackling a new attack. The participants continue to iterate over all attack methods and variants, led by the cyber OPFOR team, using this procedure.

The cyber OPFOR team’s initially proposed attack methods and plans evolve as the team learns which responses or in-place mitigations easily circumvent cyber effects, which attacks have little or no mission consequence, and which attacks have the highest impact. The operational team learns the cyber OPFOR team’s attack process, assumptions, and system-effects goals and can therefore better assess the mission impact. The control and cyber OPFOR teams should strongly encourage the operational team to identify and explain opportunities the cyber OPFOR team should consider for disrupting the operational mission. The operational and cyber OPFOR teams working together will have a better chance of assessing the likelihood of success for each attack and the possible mission effects.

The CTT is a highly interactive exercise with many conversations between the operational and cyber OPFOR teams. This interaction among engineers, operators, designers, program personnel, and cyber SMEs is the essence of a successful CTT. The responsibility of the CTT facilitator and

all three team leads is to foster a positive, non-adversarial environment and to ensure notetakers are capturing the key discussions. Fostering this environment is a critical requirement. The CTT facilitator and control team lead monitor the discussions and make sure both sides are listening to each other and that neither team is wandering away from the goal of characterizing the system (e.g., getting too far down the road or trying to "win the war"). The CTT facilitator or control team lead should prevent lengthy exchanges (e.g., see ELMO in Section 3.2.5.1) that distract from the goal of the discussion and should encourage the participants to revisit these topics at a break or during *Post-Exercise Analysis* (Step 3). The notetakers should ask clarifying questions or pause discussions during the CTT to capture the accurate information.

3.3.3 Exercise Execution: Data Collection and Review

3.3.3.1 Data Collection

Notetakers capture the main discussion throughout the CTT about the system, the cyber OPFOR team's information flow, the descriptions of the systems and equipment used in each OPFOR cyberspace attack, and the interactions among other personnel. To help facilitate follow-on analysis and note synchronization, notetakers should include periodic time stamps (e.g., every 5 or 10 minutes) in the notes.

This "write down everything" notetaker role has two main exceptions. The first is to assign one notetaker (data analyst) the role of updating the analysis table (if the cyber OPFOR team drafted the attacks in the table during the kickoff) with the discussed mission impacts, identified technical feasibility, and specified mitigations in place or planned. The second exception is to have one notetaker dedicated to the role of capturing only RFIs and other tasks participants must complete.

The notetakers' records (i.e., electronic on classified laptops or handwritten in notebooks) are the raw data of the CTT, which the lead data analyst will incorporate relevant data into the analysis table during *Post-Exercise Analysis* (Step 3).

3.3.3.2 Data Review

Daily Meetings

At the end of each CTT exercise meeting day, the control team summarizes the day's events and reviews the schedule for the day ahead with the participants. The team should consider how many attacks the participants covered and how many remain. In addition, in some cases, the control team lead may need to capture major items of interest to provide leadership with a progress report. Some RFIs are homework that require resolution before the next day of the CTT.

The control team and the notetakers also meet to assess the progress of the cyber OPFOR and operational teams. They review the attacks, address any gaps in the notes or unresolved questions, and capture requests for clarification or areas of discovery requiring follow-on information. Optionally, depending on the scope of the CTT and available time, the control team may decide to document the likelihood and impact scores using the rubrics for the day's discussed attacks. If using MAT, the CTT module facilitates this process. The control team could also use this meeting to address logistics and gaps in operational knowledge, such as the need for additional SMEs and documentation. Team leaders may need to update the CTT schedule based on the progress made by the cyber OPFOR team.

Final Day

On the final day of the CTT exercise, the control team should distribute and collect a CTT participant survey (tailor the template available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx)). The control team holds the final daily meeting to thank participants, recognize critical contributors, and provide other end-of-event announcements and acknowledgements. The control team excuses most of the participants (inviting any desired analysis participants, if desired) and meets to prepare for *Post-Exercise Analysis* (Step 3). The control team lead or CTT facilitator describes the analysis process and the time commitment. During this meeting, the control team:

- Selects the required analysis participants from the operational team (e.g., systems engineers, system operators, defenders) and the cyber OPFOR team (e.g., penetration testers). Selection should be based on demonstrated knowledge during the CTT.
- Optionally, depending on the scope of the CTT and available time, captures the likelihood and impact scores using the rubrics for the day's discussed attacks. If using MAT, the CTT module facilitates this process.
- Discusses the timeline for the analysis process and the reporting of results.
- Plans and schedules the post-*Exercise Execution* face-to-face working analysis meetings (two or more).
- Decides how to organize the data for *Post-Exercise Analysis* and whether to use or modify the analysis table template or create a different table.
- Plans how the analysis participants collaborate between meetings, including weekly conference calls, and reviews the plans for the handling of data (i.e., use of the SIPRNET, collaboration tools) documented in the Data Handling Plan (see Section 3.2.5.1). The program or data analyst consolidates the notes collected during the CTT to a shared

location or on a disk for access by the data analyst and analysis participants at the appropriate classification level.

3.3.4 Exercise Execution: Exit Criteria

The CTT is ready for *Post-Exercise Analysis* (Step 3) when the control team meets the following conditions:

- The CTT raw data (collected notes) sufficiently document the details of the operational and OPFOR missions and the technical impact on the SUA.
- The program or data analyst has consolidated the raw data into a shared location.
- The analysis participants have scheduled the *Post-Exercise Analysis* meetings and set deadlines for CTT products and reporting results.

3.4 Step 3: Post-Exercise Analysis

This step usually takes place over 30 to 60 days. The major activities performed during *Post-Exercise Analysis* include:

- Gathering data.
- Performing the initial analysis.
- Normalizing attacks.
- Finalizing risk.
- Categorizing recommendations.

The *Post-Exercise Analysis* is the most labor-intensive step in the CTT for the analysis participants and usually consists of three separate working meetings, each spanning up to 3 days, with homework assignments between each working meeting. *Post-Exercise Analysis* (Step 3) is also the most important part of the CTT because analysts synthesize the raw data into actionable information in the form of the analysis table and risk matrices the analysis participants use to create the recommendations for the program. A template for tracking key tasks during *Post-Exercise Analysis* is part of the CTT POA&M (see Section 3.2.5) and is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) in the Cyber Table Top Guidance folder. The participants could consider having a STAT SME participate in this step to “appropriately-scope” the analysis by focusing on key factors and conditions such as targeting every critical function, incorporating components associated with verifying measurable and testable cyber performance requirements, and incorporating relevant missions and mission

conditions. For more details on STAT, refer to Section 2.4 of the DoD Cyber DT&E Guidebook, Version 3.0. Contact the STAT COE for additional information via its website (https://www.afit.edu/STAT/).

3.4.1 Post-Exercise Analysis: Post-Exercise Homework

3.4.1.1 Gather Data

After the exercise concludes, the data analyst reviews and organizes the raw data (notes) generated during the CTT into the first draft of the analysis table before Working Meeting 1. The data analyst of the program may first need to transcribe or digitize the notes. During the exercise, the cyber OPFOR team or lead should have already filled in a portion (e.g., the red "OPFOR" columns) in the analysis table (see Section 3.3.1.3), in which case the data analyst should incorporate the data into the existing template. The data-gathering effort could take up to 3 weeks to complete, depending on the data analyst's schedule. Memories begin to fade the longer the analysis process takes, so this guide recommends minimizing unnecessary delays as much as possible. The control team plans the timeline on the last day of the exercise (see Section 3.3.3.2) and should account for minimizing delays. Figure 3-8 depicts the left-third of the analysis table for attacks related to access, pivot, or C2 (top of Figure 3-8) and effects (bottom of Figure 3-8). The access, pivot, and C2 methods do not have mission impact, and the analysis participants usually document and assess these major categories of attacks on a different spreadsheet tab from the effects. The first column is a unique attack identification (ID) (e.g., M1A1V1, as depicted: the "M1" represents the first OPFOR mission, the "A1" represents the first attack, and the "V1" represents the first variant of the attack). These identifiers enable shorthand for tracking and cross-referencing unique attacks.

Analysis Team	OPFOR						
Attack ID	Goal	MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Outcome
M1A1V1							
M1A1V2							
M1A2V1							

Analysis Team	OPFOR							Operational Team		
Attack ID	Goal	MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Impact	Operational Impact	Mission Impact (Rubric)	Numerical Mission Impact and Consequence
M2A1V1										
M2A2V1										
M2A2V2										

Figure 3-8. Left-Third of Analysis Tables Used in Post-Exercise Analysis Working Meeting 1

Figure 3-9 depicts the middle of the analysis table, which is the focus in Working Meeting 2 to capture the analysis participants' likelihood assessments. Both tabs containing Figure 3-8 data should contain Figure 3-9 data for documenting each attack's likelihood.

Analysis Team				
Attack Cost / Level of Effort	Attack Success Likelihood	Numerical Attack Likelihood	Analysis of Numerical Attack Likelihood Factoring in Access Method(s): New (or unchanged) value	Final Risk Assessment Coordinates

Figure 3-9. Middle Portion of Analysis Table Used in Post-Exercise Analysis Working Meeting 2

Figure 3-10 depicts the right-third of the analysis table which the analysis participants finalize during Working Meeting 3. Each analysis meeting and homework between meetings may result in additions to this portion of the analysis table. Both tabs containing Figure 3-8 data should contain Figure 3-10 data. The online template is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) in the Cyber Table Top Guidance folder and the representation in Appendix C provide detailed descriptions of each column in Figure 3-8, Figure 3-9, and Figure 3-10.

Analysis Team and System Test				
Capabilities or Mitigations In Place Today	Capabilities or Mitigations Planned for the Future	Capabilities or Mitigations Considered during CTT	Recommendations	Questions, RFIs, Further Analysis

Figure 3-10. Right-Third of the Analysis Table Finalized During Post-Exercise Analysis Working Meeting 3

Each row of the analysis table represents a unique cyberspace attack (including variants), and the columns contain the information describing the attack. When reading a row from left to right, the columns tell a comprehensive story for a specific cyberspace attack. The first column in the analysis table contains a unique identifier used to easily refer to a cyberspace attack on the risk matrix (see Section 3.4.3.2). The goal at the conclusion of the *Gather Data* activity is to have the following information filled in for all attacks: the initial unique identifier; all the red "OPFOR" columns; and, for the effects (those documented in the bottom of Figure 3-8), at least the "Operational Impact" column. The data analyst should organize the attacks logically, such as in the order presented at the CTT, with a tab for each OPFOR mission. Other cells in the analysis table may or may not have data gathered depending on CTT discussions. The control team may

or may not have resolution of the CTT-discussed RFIs. The data analyst documents open RFIs and available RFI responses in the last column of Figure 3-10 in preparation for Working Meeting 1.

Figure 3-11 and Figure 3-12 depict the two portions of the analysis table shown in Figure 3-8 with example data for access, pivot, and effect attacks, which the data analyst completes before Working Meeting 1.

Attack ID	Goal	MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Outcome
M1A1V1	Gain unauthorized access to UAV C2 interface	Initial Access: T1078.004 - Valid Accounts: Default Accounts	Exploitation of weak encryption protocols or default credentials	Adversaries exploit weak encryption or default credentials in the UAV's command-and-control (C2) interface using tools like Wi-Fi sniffers to intercept and manipulate UAV control signals.	UAV C2 interface uses default credentials or weak encryption, making it vulnerable to remote exploitation. Legacy configurations and lack of regular updates contribute to the continued use of default credentials.	Pre-mission or during mission execution	Unauthorized access to UAV C2 interface, enabling adversaries to hijack UAV control, enabling them to potentially disrupt operations or redirect the UAV.
M1A2V1	Access	Initial Access, T1566.001 - Phishing: Spear Phishing Attachment	Social engineering attack targeting UAV operators	Adversaries use spear-phishing emails or fake websites to trick UAV operators into revealing login credentials.	UAV operators lack cybersecurity training, making them susceptible to phishing attacks.	Pre-mission during operator login or mission planning	Adversaries gain unauthorized access to UAV systems, enabling manipulation of operations.
M1A3V1	Access via Malware Injection	Execution, T1059.001 - Command and Scripting Interpreter: PowerShell	Compromised maintenance laptop	Attackers compromise a maintenance laptop used for UAV diagnostics by injecting malware through phishing or USB devices. Once connected to the UAV, the malware propagates to onboard systems.	Maintenance laptops are shared among operators and lack endpoint security, making them vulnerable to compromise. Resource constraints lead to shared use of maintenance laptops, increasing exposure to malware.	Pre-mission during maintenance or diagnostics	Malware compromises UAV operations, potentially leading to loss of control or data.
M1A4V1	Pivot to Camera	Discovery, T1082 - System Information Discovery	Exploitation of onboard camera system vulnerabilities	Adversaries use onboard access to exploit vulnerabilities in the UAV's camera system, gaining access to sensitive mission data.	Onboard systems lack proper segmentation, and the camera system is not hardened against exploitation. Established access to UAV.	During mission execution	Unauthorized access to sensitive mission data, compromising operational security.
M1A5V1	Pivot to Navigation	Lateral Movement, T1570 - Lateral Tool Transfer	Exploitation of unsecured internal network protocols	Adversaries exploit unencrypted internal communication protocols to pivot from the UAV's onboard computer to its navigation system.	Internal network protocols are unencrypted, and there is no segmentation between critical systems. Malware injection successful.	During mission execution	Adversaries gain control of the UAV navigation system, leading to potential mission failure or redirection.

Figure 3-11. Example Access and Pivot Data Before Post-Exercise Analysis Meeting 1

Analysis Team	OPFOR							Operational Team		
Attack ID	Goal	MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Impact	Operational Impact	Mission Impact (Rubric)	Numerical Mission Impact and Consequence
M2A1V1	Disrupt UAV flight operations	Impact, T1565 - Stored Data Manipulation	GPS spoofing	Adversaries inject false GPS signals to mislead the UAV's navigation system, causing it to deviate from its intended path or lose navigation capability entirely.	The adversary team has previously gained a presence on the network via M1A1V1 and M1A5V1 (Lateral Movement to Navigation System).	During mission execution	UAV loses navigation capability, resulting in mission failure. The navigation system becomes unreliable, and the UAV may crash or deviate from its mission path.	Operators lose control of UAV navigation, requiring manual intervention or mission abort. Mission objectives are delayed or abandoned due to inability to reach target area.		
M2A2V1	Deny real-time ISR data delivery	Impact, T1499 - Endpoint Denial of Service	Jamming of UAV datalinks	Adversaries use radio frequency (RF) jamming to disrupt the UAV's datalinks, preventing real-time ISR data from being transmitted to the GMMS and PDT.	Proximity to the UAV's receivers	During mission execution	Real-time ISR data delivery is disrupted, preventing allied forces from receiving critical intelligence.	Operators are unable to provide ISR data to allied forces, delaying mission objectives and reducing situational awareness.		
M2A3V1	Modify ISR data	Impact, T1492 - Stored Data Manipulation	Malware modifies ISR data stored onboard the UAV	Adversaries use malware injected via a compromised maintenance laptop to alter ISR data stored onboard the UAV, corrupting the intelligence being transmitted to the GMMS and PDT.	The adversary team has previously gained access to the UAV via M1A3V1	During mission execution	ISR data stored onboard the UAV is corrupted, resulting in inaccurate or misleading intelligence being transmitted to allied forces.	Operators unknowingly transmit corrupted ISR data to allied forces, leading to poor decision-making and reduced situational awareness. Mission objectives are compromised due to reliance on inaccurate data.		
M2A4V1	Destroy UAV asset by causing it to crash or become unrecoverable.	Impact, T1485 - Data Destruction.	Malicious commands via compromised C2 interface.	Adversaries send malicious commands through a compromised C2 interface, causing the UAV to perform unsafe maneuvers or crash.	The adversary team has previously gained access to the UAV via Access Attack M1A1V1 and pivot to the UAV command system via M1A5V1 (Lateral Movement to Navigation System).	During mission execution.	UAV rendered inoperable, resulting in mission failure. The UAV crashes or becomes unrecoverable, leading to loss of the asset.	Operators lose control of UAV, requiring mission abort and asset recovery. Mission objectives are abandoned, and operational resources are diverted to recover the UAV.		

Figure 3-12. Example Effect Data Before Post-Exercise Analysis Meeting 1

3.4.2 Post-Exercise Analysis: Working Meeting 1

Working Meeting 1 is usually a 3-day meeting that takes place after the data analyst completes the *Gather Data* activity. The analysis lead or CTT facilitator reviews the purpose of the *Post-Exercise Analysis*, the expectations for the analysis meetings (all three), and the need to have analysis participants complete homework between meetings. The analysis lead also reminds the analysis participants of the cyber OPFOR mission objectives and reviews the details of the cyberspace attacks from the exercise.

3.4.2.1 Perform Initial Analysis

In Working Meeting 1, the analysis participants refamiliarize themselves with the attacks in the analysis table data to ensure the cyberspace attack data gathered so far are accurate and to identify required adjustments. The other notetakers, if in attendance, should review their own notes to identify any missing data.

The analysis participants review each cyberspace attack—that is, the data in the following columns of the analysis table: “Goal,” “Attack Method,” “Attack Description,” “Assumptions,” “When in the Mission Timeline,” “Possible System Impact” or “Possible System Outcome” (“OPFOR” columns) and “Operational Impact” and “Mission Impact (Rubric)” (“Operational Team” columns), as applicable. The analysis participants may then determine whether they need refinement or additional information (via homework). The analysis participants record the needed refinement and RFIs for the specific cyberspace attack (row) in the analysis table, either in a column at the far right (see Figure 3-10) or in the column requiring refinement.

The analysis participants should decide how to group cyberspace attacks, if they do not prefer the grouping or structure originally proposed by the analysis lead. The analysis participants may decide to group attacks by cyber OPFOR mission objectives or by the category of attack method

from the cyber kill chain (see Appendix A), that is, access, pivot, and C2. The analysis participants could also decide to group attacks based on the targeted system or operational mission phase. They may want to use separate tables or tabs for each agreed-upon grouping or to list all cyberspace attacks, sequentially by grouping, in a single tab in the analysis table. The numbering structure for the unique identifier (first column) assigned to each cyberspace attack should align with the grouping scheme. The data analyst should ensure this assignment carries forward when formulating the associated risk for the cyberspace attacks within each grouping.

The analysis participants will iterate through the data, possibly combining or splitting rows (cyberspace attacks) during the working meeting so the total number of attacks (and rows) may change in the analysis table. The participants will tailor the analysis table as needed. The analysis participants will document possible mitigations (in place, planned, or both) discussed for the SUA in the appropriate column. The analysis participants should have the original copy of the notetaker's notes along with any drawings and presentations the cyber OPFOR or operational teams produced in the CTT available for reference during each working meeting. If possible, and if the column entries are incomplete, the participants may also complete the "Mission Impact" column using the mission impact rubric (see Figure 3-4) and assign the associated "Numerical Mission Impact and Consequence" number. Usually, this task is homework for the operational team lead because the rubric may still need refinement.

Before Working Meeting 1 ends, the analysis lead should assign homework and due dates to individuals, including answering RFIs, and should refer to the Data Handling Plan (see Section 3.2.5.1) for the appropriate procedures between Working Meetings 1 and 2. Once Working Meeting 1 concludes, the analysis lead or CTT facilitator extracts and distributes the list of RFIs with due dates to the individuals responsible for providing the information needed.

3.4.2.2 Working Meeting 1 Homework

- Individuals complete assigned questions and RFIs, documented in the analysis table, and transmit the information to the data analyst by the prescribed due date.
- The data analyst addresses all editing and updating of the analysis table, including:
  - Creating new rows for any new attack or variant or combining attacks (within 1 week).
  - Publishing the updated analysis table for the other analysis participants to complete homework.
- The operational team lead consults with operational team members as needed to complete the following tasks:
  - Finalize the mission impact methodology (see Figure 3-4 and Section 3.2.3.1).

  - Enter or update the impact details in the "Operational Team" columns of the analysis table (see Figure 3-8).
  - Assign a mission impact number to the "Numerical Mission Impact and Consequence" column in the analysis table (see Figure 3-8 and Figure 3-9).
- The cyber OPFOR team lead:
  - Completes the two likelihood assessment columns ("Attack Cost/Level of Effort" and "Attack Success Likelihood") or the customized likelihood columns if tailoring the analysis table (see Figure 3-9).
  - Assigns a numerical value in the "Numerical Attack Likelihood" column (see Figure 3-9) by applying the likelihood assessment methodology (see Figure 3-5).
  - Determines subjective upgrade or downgrade factors for numerical likelihood; documents the upgrade or downgrade factors used.
  - Optional: Determines an adjustment to the likelihood value that factors in the difficulty of access method(s) and other cyber kill chain processes, as relevant and desired; documents the rationale and assigns someone to document and adjust the likelihood value in the "Analysis of Numerical Attack Likelihood Factoring in Access Method(s): New (or unchanged) value" column in the analysis table (see Figure 3-9).
- The data analyst consolidates all updates to the analysis table in preparation for Working Meeting 2.

Documenting the Final Mission Impact Assessment

The operational team lead should finalize the mission impact methodology (see Figure 3-4), developed originally during *Preparation* (Step 1) and refined during *Execution* (Step 2). The operational team is at risk of artificially inflating or deflating the impact numerical value to preconceived goals or system performance the longer the team waits to finalize the mission impact methodology. Using the mission impact methodology, the operational team lead assesses each row or attack independently. For example, if the operational mission is time dependent, then various levels of delay will result in some form of mission impact. The operational team lead will review and add necessary details to the following columns in the analysis table: "Operational Impact," "Mission Impact (Rubric)," and "Numerical Mission Impact and Consequence" (see the "Operational Team" columns in Figure 3-8) as Working Meeting 1 homework before Working Meeting 2 and use the final mission impact methodology to assign a numerical value for each attack. The "Operational Impact" column should clearly document operator responses and expected observed mission effects from the operator perspective (not the system effect). The "Mission Impact" column should use the relevant description (same exact words) that appears in the final mission impact methodology.

Documenting the Final Likelihood Assessment

The OPFOR lead will use the control team–developed and –approved version of Figure 3-5 to update, refine, or complete the two likelihood factors in the analysis table as separate columns, "Attack Cost/Level of Effort" and "Attack Success Likelihood," for each cyberspace attack (row) (see Figure 3-9). The online template is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) and the analysis table representation in Appendix C provide detailed descriptions of each column. The likelihood of a successful cyberspace attack may depend on certain assumptions, relevant access methods, or conditions. For example, the access method needed to conduct the attack may have a low likelihood as documented in a different row in the spreadsheet. The written descriptions in the "Attack Cost/Level of Effort" and "Attack Surface Likelihood" columns must provide sufficient rationale to allow a tester or cyber SME to understand the technical feasibility. In other words, the OPFOR lead should not simply enter vague terms such as "easy" or "moderate" but should instead describe the logic behind those terms to support the discussion and understanding in Working Meeting 2.

The column "Analysis of Numerical Attack Likelihood Factoring in Access Method(s): New (or unchanged) value" is optional; the analysis participants can use it to refer to specific access methods or as a method to encompass the kill chain process required to complete the attack. Additional details on mitigations, controls, and operator or defender procedures may also influence the upgrade or downgrade factors of likelihood values or the fine-tuning of the metrics that fall in between likelihood values. The cyber OPFOR team lead must document all factors considered for each attack in the appropriate columns in the analysis table and, if relevant, decide to upgrade or downgrade them as needed for the final recommended "Numerical Attack Likelihood" value. The cyber OPFOR team lead must fully document all logic associated with the selection of the "Numerical Attack Likelihood" value as Working Meeting 1 homework before Working Meeting 2.

Figure 3-13 and Figure 3-14 depict example data in the analysis table leading into *Post-Exercise Analysis* Working Meeting 2 after participants complete their homework.

Analysis Team	OPFOR										Analysis Team and System Test				
Attack ID	Goal	MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Outcome	Attack Cost / Level of Effort	Attack Success Likelihood	Numerical Likelihood	Capabilities or Mitigations In Place Today	Capabilities or Mitigations Planned for the Future	Considered Mitigations	Recommendations	Questions, RFIs, Further Analysis
M1A1V1	Gain unauthorized access to UAV C2 interface	Initial Access: T1078.004 - Valid Accounts: Default Accounts	Exploitation of weak encryption protocols or default credentials	Adversaries exploit weak encryption or default credentials in the UAV's command-and-control (C2) interface using tools like Wi-Fi sniffers to intercept and manipulate UAV control signals.	UAV C2 interface uses default credentials or weak encryption, making it vulnerable to remote exploitation. Legacy configurations and lack of regular updates contribute to the continued use of default credentials.	Pre-mission or during mission execution	Unauthorized access to UAV C2 interface, enabling adversaries to hijack UAV control, enabling them to potentially disrupt operations or redirect the UAV.	Low cost; requires basic hook like Wi-Fi sniffers and knowledge of default credentials.	High: Wireless interfaces are frequently targeted due to weak encryption and default credentials, making attack success highly likely. Weak encryption protocols and default credentials are highly susceptible to exploitation. Once the adversary executes the attack, the likelihood of successfully gaining access to the UAV C2 interface is high due to the lack of robust authentication mechanisms.	5	Basic encryption protocols and password policies are in place. Outdated encryption protocols (e.g., WPA2) are currently in use.	Strong encryption, multi-factor authentication, and regular credential updates planned.	None		What encryption protocols are currently used for UAV C2 communication? Are default credentials still in use? The UAV C2 interface currently uses outdated encryption protocols (e.g., WPA2 without additional security layers). No end-to-end encryption is implemented for command signals. Default credentials are still in use for some UAV systems due to legacy configurations and lack of regular updates.
M1A2V1	Access	Initial Access, T1566.001 - Phishing: Spear Phishing Attachment	Social engineering attack targeting UAV operators	Adversaries use spear-phishing emails or fake websites to trick UAV operators into revealing login credentials.	UAV operators lack cybersecurity training, making them susceptible to phishing attacks.	Pre-mission during operator login or mission planning	Adversaries gain unauthorized access to UAV systems, enabling manipulation of operations.	Low: requires phishing campaign and basic social engineering techniques. Phishing attacks targeting operators have been widely documented in critical infrastructure and military systems.	High: Operators are susceptible to phishing attacks due to human error and lack of training.	5	Basic email filtering and operator training are in place. Annual phishing awareness training and biannual phishing simulation exercises are conducted but lack advanced threat scenarios.		Advanced email filtering, regular operator training, and phishing simulation exercises. Include tailored phishing training and advanced simulation exercises targeting UAV-specific threats.		How often are operators trained on phishing awareness? Are phishing simulation exercises conducted regularly? Operators are trained annually on phishing awareness, but training is not tailored to specific threats targeting UAV systems. Phishing simulation exercises are conducted biannually but do not include advanced spear-phishing scenarios.
M1A3V1	Access via Malware Injection	Execution, T1059.001 - Command and Scripting Interpreter: PowerShell	Compromised maintenance laptop	Attackers compromise a maintenance laptop used for UAV diagnostics by injecting malware through phishing or USB devices. Once connected to the UAV, the malware propagates to onboard systems.	Maintenance laptops are shared among operators and lack endpoint security, making them vulnerable to compromise. Resource constraints lead to shared use of maintenance laptops, increasing exposure to malware.	Pre-mission during maintenance or diagnostics	Malware compromises UAV operations, potentially leading to loss of control or data.	Medium cost; requires phishing campaigns or physical access to maintenance laptops.	Medium: Similar methods have been used in industrial control system attacks, where compromised laptops propagate malware to connected devices. Malware injection requires persistence and physical access to the maintenance laptop or successful phishing. While feasible, the success of the attack depends on the adversary's ability to bypass endpoint security and propagate malware to the UAV.	3	Endpoint security and USB restrictions are partially implemented. Basic antivirus software is installed, but no advanced EDR systems are implemented.	Full endpoint security, USB restrictions, and malware detection systems planned.			Are maintenance laptops shared among operators? What endpoint security measures are currently in place? Maintenance laptops are shared among operators due to resource constraints, increasing the risk of compromise. Basic antivirus software is installed, but no advanced endpoint detection and response (EDR) systems are implemented.
M1A4V1	Pivot to Camera	Discovery, T1082 - System Information Discovery	Exploitation of onboard camera system vulnerabilities	Adversaries use onboard access to exploit vulnerabilities in the UAV's camera system, gaining access to sensitive mission data.	Onboard systems lack proper segmentation, and the camera system is not hardened against exploitation. Established access to UAV.	During mission execution	Unauthorized access to sensitive mission data, compromising operational security.	Medium cost; requires prior access and knowledge of camera system vulnerabilities.	Medium-High: This method has been observed in attacks targeting surveillance drones. Exploiting unencrypted internal protocols is technically feasible but requires prior access to the onboard system. The success of the attack depends on the adversary's ability to navigate the internal network and manipulate navigation data without detection.	4	Limited access controls and encryption for mission-critical data. Annual vulnerability assessments are conducted but lack advanced exploitation testing.	AES-256 encryption planned for mission-critical data, with implementation timelines to be finalized.	Encrypt mission-critical data and enhance access controls.		What encryption methods are planned for mission-critical data? Are camera system vulnerabilities regularly assessed? AES-256 encryption is planned for mission-critical data, but implementation timelines are unclear. Camera system vulnerabilities are assessed annually, but assessments do not include advanced exploitation
M1A5V1	Pivot to Navigation	Lateral Movement, T1570 - Lateral Tool Transfer	Exploitation of unsecured internal network protocols	Adversaries exploit unencrypted internal communication protocols to pivot from the UAV's onboard computer to its navigation system.	Internal network protocols are unencrypted, and there is no segmentation between critical systems. Malware injection successful.	During mission execution	Adversaries gain control of the UAV navigation system, leading to potential mission failure or redirection.	Medium cost; requires prior access and knowledge of internal protocols.	Medium-High: Similar methods have been used in industrial control system attacks, where compromised laptops propagate malware to connected devices. Accessing the UAV camera system requires prior onboard access and knowledge of system vulnerabilities. The success of the attack depends on the adversary's ability to exploit the camera system without triggering security alerts.	4	Internal protocols are unencrypted, and no segmentation exists between critical systems.		Segmentation of critical systems and encryption of internal protocols.		Are internal protocols encrypted? What segmentation exists between critical systems? Internal protocols are not encrypted, relying on legacy communication standards. No segmentation exists between critical systems, allowing lateral movement once access is gained.

Figure 3-13. Example Access and Pivot Data Before Working Meeting 2

Analysis Team	OPFOR							Operational Team			Analysis Team						Analysis Team and System Test				
Attack ID	Goal	MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Impact	Operational Impact	Mission Impact (Rubric)	Numerical Mission Impact and Consequence	Attack Cost / Level of Effort	Attack Success Likelihood	Numerical Attack Likelihood	Analysis of Numerical Attack Likelihood Factoring in Access Method(s) New (or unchanged) value	Final Risk Assessment Coordinates	Risk Matrix Ranking	Capabilities or Mitigations In Place Today	Capabilities or Mitigations Planned for the Future	Capabilities or Mitigations Considered during CTT	Recommendations	Questions, RFIs, Further Analysis
M2A1V1	Disrupt UAV flight operations	Impact, T1565 - Stored Data Manipulation	GPS spoofing	Adversaries inject false GPS signals to mislead the UAV's navigation system, causing it to deviate from its intended path or lose navigation capability entirely.	The adversary team has previously gained a presence on the network via M1A1V1 and M1A3V1 (Lateral Movement to Navigation System).	During mission execution	UAV loses navigation capability, resulting in mission failure. The navigation system becomes unreliable, and the UAV may crash or deviate from its mission path.	Operators lose control of UAV navigation, requiring manual intervention or mission abort. Mission objectives are delayed or abandoned due to inability to reach target area.	NMC. Severely impacted, total loss of functionality.	5	Low-Medium cost; requires GPS spoofing tools and knowledge of GPS vulnerabilities. Proximity to the UAV GPS receiver during operations.	High: Non military GPS highly susceptible to spooing. GPS spooling is a well-documented attack vector with high success rates when executed. UAVs rely heavily on GPS signals, and the lack of anti-spoofing measures increases the likelihood of successful disruption.	4	Access and Pivot methods are Combined likelihood of 4.	5,4	Very High	Basic GPS monitoring and anti-spoofing measures are in place. Annual GPS anti-spoofing tests are conducted but lack advanced adversary-grade scenarios.	Implementation of redundant navigation systems (e.g., INS) is planned but delayed due to budget constraints.	Use advanced GPS anti-spoofing measures and redundant navigation systems.		Are GPS anti-spoofing measures tested regularly? What redundant navigation systems are planned? GPS anti-spooling measures are tested annually, but testing does not include advanced spoofing scenarios or adversary-grade equipment. Redundant navigation systems, such as inertial navigation systems (INS), are planned but not yet implemented due to budget constraints.
M2A2V1	Deny real-time ISR data delivery	Impact, T1499 - Endpoint Denial of Service	Jamming of UAV datalink c	Adversaries use radio frequency (RF) jamming to disrupt the UAV's datalink, preventing real-time ISR data from being transmitted to the GMMS and PDT.	Proximity to the UAV's receivers	During mission execution	Real-time ISR data delayed is disrupted, preventing allied forces from receiving critical intelligence.	Operators are unable to provide ISR data to allied forces, delaying mission objectives and reducing situational awareness.	Non to Partially Mission Capable. Major Loss of Functionality	4	Medium cost; requires RF jamming equipment and knowledge of datalink frequencies.	Medium: RF jamming requires precise knowledge of datalink frequencies and sufficient power to disrupt communication. The success of the attack depends on the adversary's ability to maintain jamming over time without interference.	3	3 Likelihood remains medium due to required RF jamming equipment and adversary capabilities.	4,3	Moderate	Basic frequency monitoring is in place. Biannual anti-jamming tests are conducted but limited to low-power jamming scenarios.	Regular assessments of datalink frequencies, including adversary-grade RF interference, are planned.	Use advanced frequency monitoring and anti-jamming measures.		Are anti-jamming measures tested regularly? Are datalink frequencies regularly assessed? Anti-jamming measures are tested biannually, but testing is limited to low-power jamming scenarios. Datalink frequencies are assessed annually, but assessments do not include adversary-grade RF interference.
M2A3V1	Modify ISR data	Impact, T1492 - Stored Data Manipulation	Malware modifies ISR data stored onboard the UAV	Adversaries use malware injected via a compromised maintenance laptop to alter ISR data stored onboard the UAV, corrupting the intelligence being transmitted to the GMMS and PDT.	The adversary team has previously gained access to the UAV via M1A3V1	During mission execution	ISR data stored onboard the UAV is corrupted, resulting in inaccurate or misleading intelligence being transmitted to allied forces.	Operators unknowingly transmit corrupted ISR data to allied forces, leading to poor decision-making and reduced situational awareness. Mission objectives are compromised due to reliance on inaccurate data.	Non to Partially Mission Capable. Major Loss of Functionality	4	Medium cost; requires malware injection and knowledge of onboard data storage systems.	Medium: Modifying ISR data requires malware persistence and access to onboard data storage systems. The success of the attack depends on the adversary's ability to manipulate data without triggering integrity checks or detection mechanisms.	3	3 Likelihood remains medium due to required malware persistence and adversary capabilities, and likelihood of M1A3V1.	4,3	Moderate	Basic malware detection and data integrity checks are in place. Quarterly data integrity checks are performed but limited to basic checksum validation.	Implementation of AES-256 encrypted secure storage systems is planned but delayed due to resource constraints.	Implement advanced malware detection, data integrity monitoring, and secure storage systems.		Are data integrity checks regularly performed? What secure storage systems are planned? Data integrity checks are performed quarterly but are limited to basic checksum validation. Secure storage systems with encryption (e.g., AES-256) are planned but not yet implemented due to resource constraints.
M2A4V1	Destroy UAV asset by causing it to crash or become unrecovera ble.	Impact, T1485 - Data Destruction,	Malicious commands via compromise d C2 interface.	Adversaries send malicious commands through a compromised C2 interface, causing the UAV to perform unsafe maneuvers or crash.	The adversary team has previously gained access to the UAV via Access/ Attack M1A1V1 and pivot to the UAV command system via M1A4V1 (Lateral Movement to Navigation System).	During mission execution	UAV rendered inoperable, resulting in mission failure. The UAV crashes or becomes unrecoverable, leading to loss of the asset.	Operators lose control of UAV, requiring mission abort and asset recovery. Mission objectives are abandoned, and operational resources are diverted to recover the UAV.	NMC. Severely impacted, total loss of functionality.	5	Medium cost; requires control of C2 interface and knowledge of UAV commands.	Medium: Sending malicious commands requires control of the UAV C2 interface and knowledge of command structures. The success of the attack depends on the adversary's ability to bypass command validation and execute unsafe maneuvers.	3	3 Likelihood remains medium despite likelihood of access and pivot due to required control of C2 interface and adversary capabilities.	5,3	High	Basic command validation and anomaly detection are in place. Annual command validation tests are conducted but lack adversary-grade scenarios.	Implementation or automated return-to-base fail-safe mechanisms is planned but delayed due to technical challenges.	Implement advanced command validation and fail-safe mechanisms		Are command validation systems tested regularly? What fail-safe mechanisms are planned? Command validation systems are tested annually, but testing does not include adversary-grade scenarios. Fail-safe mechanisms, such as automated return-to-base protocols, are planned but not yet implemented due to technical challenges.

Figure 3-14. Example Data for Effects Before Working Meeting 2

3.4.3 Post-Exercise Analysis: Working Meeting 2

Working Meeting 2 is a 3-day meeting that takes place 2 to 3 weeks after Working Meeting 1. The analysis participants review the completed homework and decide to accept or modify the values for mission impact and likelihood for each cyberspace attack (rows) in the analysis table.

3.4.3.1 Normalize Attacks

During Working Meeting 2, the analysis participants reexamine, one-by-one, each row in the updated analysis table. In the process, the analysis participants review the RFIs, questions, and information gaps brought up in Working Meeting 1 and the answers to these items to resolve lingering questions. The analysis participants ensure each row in the analysis table represents an independent cyberspace attack (or significant variant) and should ensure they use consistent terminology throughout the analysis table.

Using the final mission impact methodology, the analysis participants review and possibly refine the "Operational Impact" and "Mission Impact (Rubric)" columns (the "Operational Team" columns in Figure 3-8) in the analysis table for each attack and reassess the consequences for the operational mission. Then the analysis participants confirm or adjust the value assigned in the "Numerical Mission Impact and Consequence" column (see Figure 3-8) for each cyberspace attack in the analysis table. The analysis participants may also decide to document variants in mission impacts based on modified operational assumptions.

The analysis participants also review the value assigned in the "Numerical Attack Likelihood" column (see Figure 3-9) in the analysis table for each cyberspace attack based on the cyber OPFOR team lead's inputs and the likelihood assessment methodology. The analysis participants should document any modifications to the likelihood values and the rationale behind them in the analysis table. The numerical likelihood is not an assessment of the adversary's intent to conduct the specific cyberspace attack or the probability of attack. The program may decide to incorporate actual intelligence data to improve the likelihood assessment, but ultimately, testing is the most effective way to prove or disprove any uncertainty in CTT findings.

The analysis participants should also:

- Review attack vectors and areas of emphasis not explored in the exercise to uncover any potential gaps in their analysis of the SUA.
- Document analysis gaps as recommendations for future work.
- Avoid adding additional attacks.
- Document any questions or additional RFIs in the "Questions, RFIs, and Further Analysis" column in the analysis table (see Figure 3-10).

- Identify any additional mitigations that are in place or planned in the appropriate column in the analysis table (see Figure 3-10).
- Document any testing recommendations made by the OPFOR regarding a specific attack in the "Recommendations" column in the analysis table (see Figure 3-10).

Before Working Meeting 2 wraps up, the analysis participants should assign homework and refer to the Data Handling Plan (see Section 3.2.5.1) for the appropriate procedures between Working Meetings 2 and 3. Once Working Meeting 2 concludes, the control team lead or CTT facilitator extracts and distributes the list of remaining RFIs with due dates to the individuals responsible for providing the information needed.

3.4.3.2 Working Meeting 2 Homework

- Individuals complete assigned questions and RFIs documented in the analysis table and transmit the information to the data analyst by the prescribed due date.
- The data analyst:
  - Addresses formatting inconsistencies and cleans up the analysis table (within 1 to 2 days).
  - Ensures all analysis participants have access to the updated version of the analysis table.
- Team leaders ensure program personnel and members from the operational team who did not participate in the analysis can review the analysis table to make any corrections and provide recommendations (within 1 week).
- The control team lead and CTT program personnel develop the initial set of recommendations documented in the analysis table (see Figure 3-10).
  - NOTE: It is critical to develop this list of recommendations for the SUA to create the actionable information before *Reporting* (Step 4).
- The data analyst or analysis lead:
  - Builds the initial risk matrices (described below) using the values from the analysis table and the program risk reporting methodology, based on the grouping of attacks.
  - Extracts key data from the analysis table to build simple tables listing attacks for the results briefs.
- The cyber OPFOR team lead coordinates with the control team lead to identify specific sets of attacks to build attack vignettes for the results briefs.

- The control team lead and CTT facilitator draft the unclassified portions of the technical brief (see Section 3.5.2) and executive brief (see Section 3.5.3).

Risk Matrix

The data analyst plots each cyberspace attack grouping on a separate risk matrix using the unique identifier in the first column in the analysis table (see Figure 3-8). Figure 3-15 is an example of a risk matrix, adapted from NIST SP 800-30 by adding colors, depicting example effects.

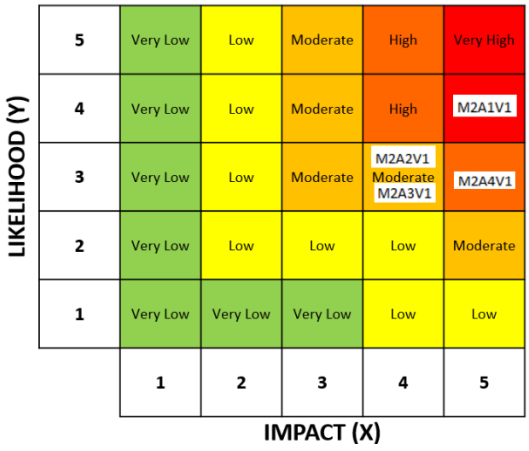


Figure 3-15. Example Data Plotted on Risk Matrix Based on NIST SP 800-30

The numerical mission impact values and numerical likelihood values from the columns in the analysis table are the x-coordinates and y-coordinates, respectively, of the risk matrix (Figure 3-15) (see the "Numerical Mission Impact and Consequence" column in Figure 3-8 and the "Analysis of Numerical Attack Likelihood Factoring in Access Method(s): New (or unchanged) value" column in Figure 3-9). Appendix C contains more information about using the risk matrix.

The risk matrix is a common tool used to evaluate cyber risks; the program can apply other available methods, such as the Common Vulnerability Scoring System (CVSS), as desired (see the Forum of Incident Response and Security Teams (FIRST) CVSS Website at https://www.first.org/cvss/).

3.4.4 Post-Exercise Analysis: Working Meeting 3

Working Meeting 3 is a 3-day meeting that takes place 2 to 3 weeks after Working Meeting 2. At the conclusion of this meeting, the analysis participants complete the analysis table, representing the actionable information including recommendations (see Figure 3-10); risk matrices; a draft technical brief; and a draft executive brief.

3.4.4.1 Finalize Risk

The analysis participants conduct a final review of the changes to the analysis table and review the set of risk matrices.

The analysis participants then discuss and finalize the coordinates in the risk matrix associated with each attack grouping. The final risk matrices serve as a visualization of the CTT results, and the control team will use them in the technical brief.

3.4.4.2 Categorize Recommendations

After the *Finalize Risk* activity, the analysis participants review the assigned homework and discuss the capabilities of the system(s) for averting or mitigating the risk associated with each cyberspace attack in the analysis table (see Figure 3-10). Some attacks may not have any entries in the mitigation columns (in place, planned, or considered). In the absence of documented (in place, planned, or considered) mitigations, the analysis participants may provide recommendations for further analysis in the "Recommendations" column.

Next, for each cyberspace attack, the analysis participants review the pertinent homework and discuss the recommendations for the program (actions) based on the associated risk and any current, planned, or recommended mitigations for the SUA. These recommendations usually are one of the following four categories:

- **Test**: Test the system to determine the level of risk associated with specific attacks or vignettes.
- **Accept or Hold**: Accept or hold the risk, which may be low, unknown, or unmitigable.
- **Mitigate**: Identify and implement a specific mitigation technique.
- **Further Analyze**: Investigate further to determine whether testing, mitigating, or accepting is appropriate.

Example Recommended Actions (Based on the OV-1 in Figure 3-3)

Test to determine whether malware can be injected via a compromised maintenance laptop to alter ISR data stored onboard the UAV, corrupting the intelligence being transmitted to the GMMS and PDT.

Accept that spear phishing emails or fake websites could trick UAV operators into revealing login credentials.

Mitigate by implementing mitigations: Deploy GPS anti-spoofing measures and redundant navigation systems.

Further analyze system architecture to determine whether the adversary can pivot from the UAV's onboard computer to its navigation system.

- After implementing planned segmentation of critical systems and encryption of internal protocols, determine whether pivot from the UAV's onboard computer to its navigation system is still possible.

The analysis participants should try to identify obvious tests that a test team could easily conduct in a laboratory setting. If there are many variants to a cyberspace attack, consider evaluating the worst-case scenario.

The analysis table should include as much detail in each row and column as possible to explain each attack and the details that resulted in the risk values and the recommendations. After the analysis participants finalize the actionable information (from the analysis table and risk matrices) for the SUA, they should work to finalize the draft technical brief (see Section 3.5.2) to report the results of the CTT. The analysis table is the source document for addressing specific questions about the CTT recommendations and findings.

The analysis participants may also need to finalize the draft executive brief (see Section 3.5.3) depending on the briefing schedule. The executive brief is often a subset of the technical brief.

3.4.5 Post-Exercise Analysis: Exit Criteria

The CTT is ready for *Reporting*, Step 4, when the control team meets the following conditions:

- Organized and refined the CTT notes with SMEs.
- Completed the analysis table attack likelihood and mission impact details.
- Created and refined the risk matrices with SMEs.
- Developed actionable recommendations for the SUA.

- Scheduled the technical and executive briefs.
- Obtained program concurrence with the findings and recommendations.

3.5 Step 4: Reporting

This step varies in duration. The major activities performed during *Reporting* include:

- Prioritizing the recommendations.
- Completing the development of the technical brief.
- Developing the executive brief.

3.5.1 Reporting: Prioritize Recommendations

For the SUA, the control team lead and key program personnel must determine the priority of the cybersecurity risks and recommendations identified during *Post-Exercise Analysis* (Step 3) and highlight them in the technical and executive briefs. The areas to highlight may include addressing the vulnerabilities with high mission impact, leadership areas of concern, and strategic issues with quick or easy tactical resolutions. Aligning the recommendations to the program's testing and engineering schedule may prove useful. If any missions or critical functions were not the focus of the current CTT or the focus during a previous CTT with the current system configuration and operational employment intentions, then the CyWG will need to schedule additional CTT(s) to assess the other systems, missions, critical functions, and/or interfaces not explored during the most recent CTT iteration. To maximize effectiveness, the CyWG should schedule these events in relatively close succession to achieve an accurate and system-wide understanding of potential cyber risks to the system and to identify risk remediations and mitigations as soon as possible.

In the reports, the control team lead should emphasize both the adversary's potential opportunities to disrupt the operational mission and the system's realistic operational resilience. The control team lead is the individual responsible for conducting the briefs and should be familiar with all information captured in the analysis table. The control team lead is responsible for delivering all CTT notes and the final analysis table containing all CTT findings and recommendations to the CyWG. The CTT notes and final analysis table capture the detailed findings and recommendations not included in the technical and executive briefs described in the following sections.

3.5.2 Reporting: Complete the Technical Brief

The technical brief describes the entire CTT effort of preparation, research, execution, and analysis, from Step 1 through Step 3, and contains the following information:

- Objectives, assumptions, and benefits.
- Key leadership and participating and supporting organizations.
- Operational mission and scenario overview:
  - Key diagrams and information.
- OPFOR mission overview:
  - Intelligence, known and unknown.
- Summary of results:
  - Risk matrix with the total number of attacks in each cell.
  - Mission impact and likelihood assessment methodologies:
    - Upgrade or downgrade factors, if used.
- Detailed results:
  - Access methods overview and assessment.
  - High-level summary of all attacks.
  - Risk matrices.
  - Attack scenarios or vignettes (one per risk matrix, typically).
- Recommendations and next steps.
- Optional: Collated data and select excerpts from the CTT participant survey.

The control team can gather all the unclassified information from the kickoff briefs to use in the detailed technical brief. The detailed results (usually classified findings) include the OPFOR cyberspace attack vignettes selected by the control team or analysis participants and developed by the cyber OPFOR team lead. Each vignette should provide a complete story of how the cyberspace attack played out, from the attack assumptions and description, through the effects to the operational mission. The vignettes are an opportunity to layer multiple attacks in parallel or in sequential nature to explain how an adversary could create a mission-impacting attack. If possible, identify the most vulnerable components of the system or the subsystems contributing to each cyberspace attack, or provide a summary of this information. Also, consider including any findings that changed for a system or subsystem from a previous CTT or other MBCRA methodology. Reference the data from the analysis table and present extracts of relevant

information in a simple table along with the risk matrices. A template for the technical brief is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx).

3.5.3 Reporting: Develop the Executive Brief

The executive brief provides a high-level overview of the CTT steps and presents the recommendations and key actionable information about the SUA. The executive brief highlights the following information:

- Value and benefits of the CTT.
- Summary of attacks and recommendations.
- Impacts on FoS, as relevant, and plans to inform other programs.
- Next steps (e.g., testing to validate findings, implementing mitigations).
- Optional: Collated data and select excerpts from the CTT participant survey.

The control team lead can extract information from the technical brief, but the language to describe the cyberspace attack scenarios should be understandable to the warfighter. The executive brief provides a visual depiction summarizing the operational mission (to give context, see Section 3.2.3.1) and the cyber OPFOR mission objectives (see Section 3.2.3.3), highlighting the recommendations. When presenting the executive brief, the program should take ownership of the results, but it is helpful to have operational and technical leads in attendance to reinforce the information and recommendations.

3.5.4 Reporting: Exit Criteria

When the control team meets the following conditions, the CTT is complete:

- Delivered all CTT notes and the completed analysis table with all findings and recommendations to the CyWG.
- Presented the technical brief to CTT participants and other interested stakeholders.
- Presented the executive brief to leadership.

3.6 Wrapping Up a CTT

The CTT is not a typical wargame with moves and countermoves but is a tool designed to increase decision-maker and warfighter understanding of the cyber warfare domain in a mission

context and to help T&E programs better allocate their engineering and testing resources. After the CTT, the CyWG should focus on validating the risks using T&E; implementing the recommendations into the early design or into engineering changes; ensuring the CyWG is continuously monitoring the identified risks; and planning for the next MBCRA as part of ongoing cyber T&E planning activities. The CyWG plays a critical role in maintaining CTT continuity by leveraging outputs from completed CTTs to inform future CTTs. By systematically incorporating lessons learned and actionable insights, the CyWG enhances the quality and efficiency of each subsequent CTT. This iterative approach strengthens the overall cybersecurity posture, ultimately contributing to the development of a more secure and resilient system.

Appendix A: Cyber Table Top Exercise Preparation Resources

CTT Examples

Although the need to gain an initial understanding of a system or to characterize the attack surface is certainly present in early development, the need to understand the architecture and system exposures can arise multiple times across the system's life cycle because of system upgrades, system modifications, different environments, and emerging or evolving threat capabilities. The following list provides several examples where a CTT would be valuable:

- CTTs provide a means of communication among the engineering, testing, and program management personnel who are trying to understand the risk to the system under development from the cyber warfare domain. The timing of this CTT may be very early in the program planning to enable a common understanding of the cybersecurity challenges the program will have to address. An early CTT may inform the allocation of resources to disciplines within the program office dealing with the many aspects of cybersecurity. It will also inform the selection and tailoring of controls and the application of control overlays during the DoD RMF process.
- Systems beginning their test planning and test data management process could leverage CTTs to determine what constitutes adequate developmental testing before operational testing (e.g., supporting the "Attack Surface Characterization" phase in the six-phase cybersecurity T&E process).
- CTTs could serve as a tool during development and continuous monitoring to determine whether the program has overlooked emergent cyber vulnerabilities in the SUA (especially in the support and maintenance subsystems). For example, portable USB flash drives emerged in early DoD CTTs as a cyber threat not previously considered, prompting the need to identify and implement appropriate mitigations.
- Cyber test teams should use CTTs to generate threat vignettes for all phases of threat-based cyber testing and to put potential risks into an operational context. In this way, CTTs could help determine the test environment requirements and inform the authorizing officials' decisions about the risk to the network.
- CyWGs can use a smaller-scale CTT, possibly a 1-day "mini" CTT, to perform quick turnaround risk assessments on vulnerability assessment findings to evaluate mission risks. Mini CTTs are useful for smaller stand-alone systems that do not require large participation and multiple days.

CTT Roles and Team Responsibilities

Team Roles and Responsibilities

Control team: Leads the entire CTT effort and provides logistical support from *Exercise Preparation* (Step 1) through *Reporting* (Step 4). Reminder: The control team includes the operational team lead and deputy and the cyber OPFOR team lead and deputy. The control team should use the checklist in Appendix D: Cyber Table Top Checklistsand the CTT POA&M to accomplish the following:

- Recruit participants; set goals, objectives, and deliverables; and manage all CTT logistics (e.g., SCG, NDAs, facility reservations, meeting information, supplies, computers, Data Handling Plan, food and beverage plan, social event(s), presentations, documentation sharing via a collaboration site, and welcome packets).
- Adjudicate issues; ensure the CTT participants hear all minority views; support notetakers; and capture recommendations.
- Lead *Post-Exercise Analysis*.
- Report actionable results.

Operational team: Is most engaged during the CTT *Exercise Execution* (Step 2). The operational team should use the checklist in Appendix D: Cyber Table Top Checklists to accomplish the following:

- Develop the notional plan to execute operational mission orders or achieve the operational objective within the future timeline and scenario.
- Present the notional timeline, actions, and procedures of the multiday mission—planning through post-mission tasks including maintenance.
- Assess the impact on mission accomplishment of successful attacks.
- Provide required expertise for *Post-Exercise Analysis* (Step 3).

The operational team should include expertise such as military and civilian testers; individuals with operational or functional experience relevant to the mission or systems; system operators or users; organizations involved with the system development; personnel with weapons and tactics experience relevant to the mission; system maintainers; engineers familiar with the differences between the current “as-is” and “to-be” system; subsystem SMEs; anti-tamper SMEs; system security engineers; program protection SMEs; safety SMEs; logistics and sustainment SMEs; CSSPs and network defenders; and the program cybersecurity SME.

Cyber OPFOR team: Is most engaged during the *Exercise Execution* (Step 2). The cyber OPFOR team lead may engage with team members in advance to perform reconnaissance, plan cyberspace attacks, and assign missions to cyber OPFOR team members. The cyber OPFOR team should use the checklist in Appendix D: Cyber Table Top Checklists to accomplish the following:

- Review all available SUA technical documentation and available or collected reconnaissance during the planning phase.
- Review the operational mission sequence.
- Develop a list of potential exploitation pathways based on the reconnaissance for each SUA.
- Perform most attack planning and development before CTT kickoff and execution.
- Present the general OPFOR mission approach and attacks.
- Develop and lead the discussion of cyberspace attacks to execute the cyber OPFOR mission objectives.
- Provide required expertise for *Post-Exercise Analysis* (Step 3).

The cyber OPFOR team is composed of offensive cyberspace operators (contractor, government, academia); authorized cyber team penetration testers and OTA representatives (e.g., DoD Cyber Red Team); defensive and offensive cybersecurity SMEs; cyber developmental testers; cyber range personnel; interoperability engineers; EW testers; CSSPs or network defense personnel for the system; and systems engineer or tester (provides operational perspective).

Individual Roles and Responsibilities

Not all CTTs require all roles; one person can perform two or more roles, and some individuals can support multiple teams.

Control team lead: Has overall authority and responsibility for the exercise; may function as the analysis lead; is the expert on the SUA; identifies the appropriate program and operational and user contacts to participate in *Exercise Execution* (Step 2); and is responsible for prioritizing recommendations and developing the executive brief in *Reporting* (Step 4).

CTT facilitator: Supports the control team lead; keeps the control team on track, which is particularly helpful during the program's first CTT; adjudicates questions and issues that arise; and is the expert on the CTT process, bringing experience and contacts from other CTTs. The CTT facilitator should train notetakers and focus on successful data collection during the exercise. Best practices when managing notetakers:

- Assign notetakers to support each team as soon as possible—early involvement ensures better SUA and objective comprehension.
- Use the notetaker training available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website in the Cyber Table Top Guidance folder (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) to customize training for the assigned notetakers.
- Ensure the schedule permits time for notetakers to ask questions.
- Emphasize the importance of detailed and focused note-taking (narrow the scope).
- Give notetakers a computer, if possible.

Operational team lead: Is responsible for planning the team's operational mission and ensuring the team deliverables are within CTT time constraints; serves on both the operational and control teams; has general experience and knowledge across the scope of the mission and scenario; and is a strong leader who fosters discussion without dominating (or allowing others to dominate) the conversation.

Cyber OPFOR team lead: Is the most important role in CTT *Exercise Execution*, besides the notetakers, and is responsible for planning the cyber OPFOR mission objectives (in Step 1); serves on both the cyber OPFOR and control teams; is an expert in cyber offensive or defensive operations (or both), cybersecurity vulnerability assessments, and cyber warfare operations; has a strong personality and is communicative; leads *Exercise Execution* (Step 2); fills in the results table and risk matrices during *Post-Exercise Analysis* (Step 3); and creates cyberspace attack vignettes in *Reporting* (Step 4). This appendix includes more details about the role of the cyber OPFOR team lead in the CTT process.

Analysis lead: Directs the *Post-Exercise Analysis* (Step 3) and is responsible for generating actionable information and CTT results; is organized, analytical, and a cybersecurity SME; is part of the control team and may be on the OPFOR; and must develop knowledge of the SUA, typical missions, and cybersecurity concepts (developed before or during CTT efforts).

Data analyst: Functions as a notetaker during the CTT; supports the analysis lead for *Post-Exercise Analysis* (Step 3) by organizing all raw notes and maintaining configuration management for the analysis data during and between analysis meetings; is organized and analytical; has at least a general level of cybersecurity knowledge; is capable of developing knowledge of the SUA and the missions; is part of the control team; and optimally supports the OPFOR.

Notetaker: Records all relevant discussions—who said what—and diagrams attacks, as required, during *Exercise Execution* (Step 2); is ideally assigned to focus on one team during the breakout sessions after kickoff; is detail oriented, a good listener, and organized; has good short-term memory; ideally has general CTT experience; and needs some familiarity with the SUA, typical missions, or cybersecurity to effectively follow the discussions and understand the right data to capture. As explained in Section 3.2.1.1, the notetakers have a "superpower" during the exercise to stop the conversation whenever necessary and request clarification to ensure accurate data collection. Detailed note-taking helps with information recall between CTT *Execution* (Step 2), *Post-Exercise Analysis* (Step 3), and *Reporting* (Step 4).

Notetaker best practices include the following:

- Understand the operational event:
  - Ensure the understanding of information exchanges and paths used for communication.
  - Clarify the links between hardware and software.
  - Formulate potential vulnerabilities based on the information provided.
  - Focus on one point at a time (the CTT execution is controlled chaos).
- Illustrate thoughts:
  - Create illustrations to accompany notes.
  - Pictorialize all notes and annotate them when possible.
  - Identify communication paths, information flow, and type (voice, wired, wireless, etc.).
  - Consider all phases of the mission (planning, reconnaissance, maintenance, execution, etc.).
- Gather key information:
  - Precisely define the attack, systems, equipment, applications, and impact.
  - Verify the mission consequence and probability of each attack.
  - Map the attack tree and corresponding mitigation efforts.
- Reiterate and confirm the information:
  - Aggregate the information and compare notes with other notetakers.
  - Create a separate list of questions based on the discussion.
  - Be sure to speak up and note points of confusion for clarification.

- Consult with other notetakers to answer follow-on questions.

Operational and cyber OPFOR deputy team leads (optional): Support team leads as desired. Having empowered backup coverage for key roles is vital when participants have conflicts.

Security lead: Is responsible for classification derivations of all CTT data; is an expert on the program classification guide; has knowledge of the PPP; coordinates the appropriate classified facilities for the exercise, data analysis, and other classified meetings; develops and publishes the data handling or management plan for the *Exercise Execution* (Step 2) and *Post-Exercise Analysis* (Step 3); manages the visit requests for participants; manages NDAs (if applicable); and provides input regarding classification and data handling for the CTT kickoff briefs.

Intelligence lead: Supports the collection of intelligence information from the program or the intelligence organization supporting the program; develops and coordinates intelligence briefs for the CTT including intelligence relevant to the CTT mission, such as targets of interest or enemy activities, and intelligence on known cyber TTPs related to the program data, SUA, interfaces, etc.

Importance of the Cyber OPFOR Team Lead Role

The cyber OPFOR team lead, or OPFOR lead, is involved in all four steps of the CTT (driving the *Exercise Execution* (Step 2) and *Post-Exercise Analysis* (Step 3)) and is critical to the success of the assessment. Successful OPFOR leads not only possess broad offensive and defensive cyberspace operations knowledge but also have strong leadership skills and the ability to communicate clearly. OPFOR leads bring their passion and commitment to the CTT by educating participants and improving the awareness of cyber threats to DoD missions. By fostering creative thought, inspiring provocative ideas, and cultivating a non-adversarial collaborative environment for learning, the OPFOR leads motivate the cyber OPFOR team to research and defend plausible attacks, and they encourage all CTT participants to identify the greatest areas of concern with respect to the mission the system supports. Because this role is so critically important, this section reiterates the duties of the OPFOR lead throughout the CTT.

During *Preparation* (Step 1), the OPFOR lead participates in planning meetings; works with the CTT control team to plan the event; and communicates relevant information to the rest of the cyber OPFOR team members. OPFOR leads seek the requisite technical documentation and information by asking questions about the system, mission, maintenance, etc., until they have sufficient information to develop the set of cyber opposing mission objectives. Technical deep dives and lab or site visits are a best practice for the OPFOR. The OPFOR lead requests and attends those fact-finding events. During planning, the OPFOR lead helps to filter out superfluous information from critical data and distill the key information into the kickoff briefs.

The OPFOR lead also provides expert input on the program's selected likelihood assessment methodology.

During *Exercise Execution* (Step 2), the OPFOR lead attends the kickoff event (preferably held well before the rest of the event); presents the OPFOR mission brief; and asks questions during other briefs to (1) improve understanding among all participants and (2) encourage the cyber OPFOR team members to ask questions they may have. The OPFOR lead coordinates the attack brainstorming activities of the cyber OPFOR team, whether they occur between the kickoff event and the exercise or during the cyber OPFOR team breakout sessions. During brainstorming, the OPFOR lead reminds the team they should be developing a wide range of representative attacks across the range of effects (deny, degrade, disrupt, destroy, deceive, or exfiltrate) and the attacks should be plausible, initially using the likelihood assessment methodology to understand the technical feasibility of the developed attacks. The OPFOR lead must structure the attack presentations by the cyber OPFOR team members to ensure a consistent approach and flow. The OPFOR lead guides the attack presentations, evolving the attacks as warranted by the discussion during the event. The OPFOR lead also:

- Decides the order in which to present the attacks.
- Decides the appropriate level of detail for the audience.
- Encourages the operational team to engage and interact during the presentation.
- Understands and explains (if necessary) possible countermeasures and workarounds.
- Explains likelihood using the likelihood assessment methodology.
- Adjusts the attacks as needed to identify mission-impacting events.

The OPFOR lead should aspire to get through as many attacks as possible while eliciting discussions on feasibility, plausibility, and likelihood to educate all participants. On average, each attack takes up to 20 minutes to describe and debate.

During *Post-Exercise Analysis* (Step 3), the OPFOR lead attends all analysis meetings; assigns and completes homework; reviews the analysis table; develops and refines the attack description details, level of effort, and attack success likelihood; and offers suggestions for mitigation and testing.

Finally, during *Reporting* (Step 4), the OPFOR lead helps the control team finalize the results as a brief, a report, or both, by developing and describing attack vignettes. OPFOR leads attend all out-briefings as desired by the program and are available to present the attack vignettes and analysis process if needed.

Responsible, Accountable, Consulted, and Informed Matrix

Figure A-1 depicts an example of a CTT "Responsible, Accountable, Consulted, and Informed" (RACI) matrix. The tailorable Excel version is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) in the Cyber Table Top Guidance folder.

Responsible (R): The person or people who do the work to complete the task.

Accountable (A): The person who is ultimately answerable for the completion of the task and has the authority to approve or reject the work.

Consulted (C): The person or people who provide input or expertise before the task is completed.

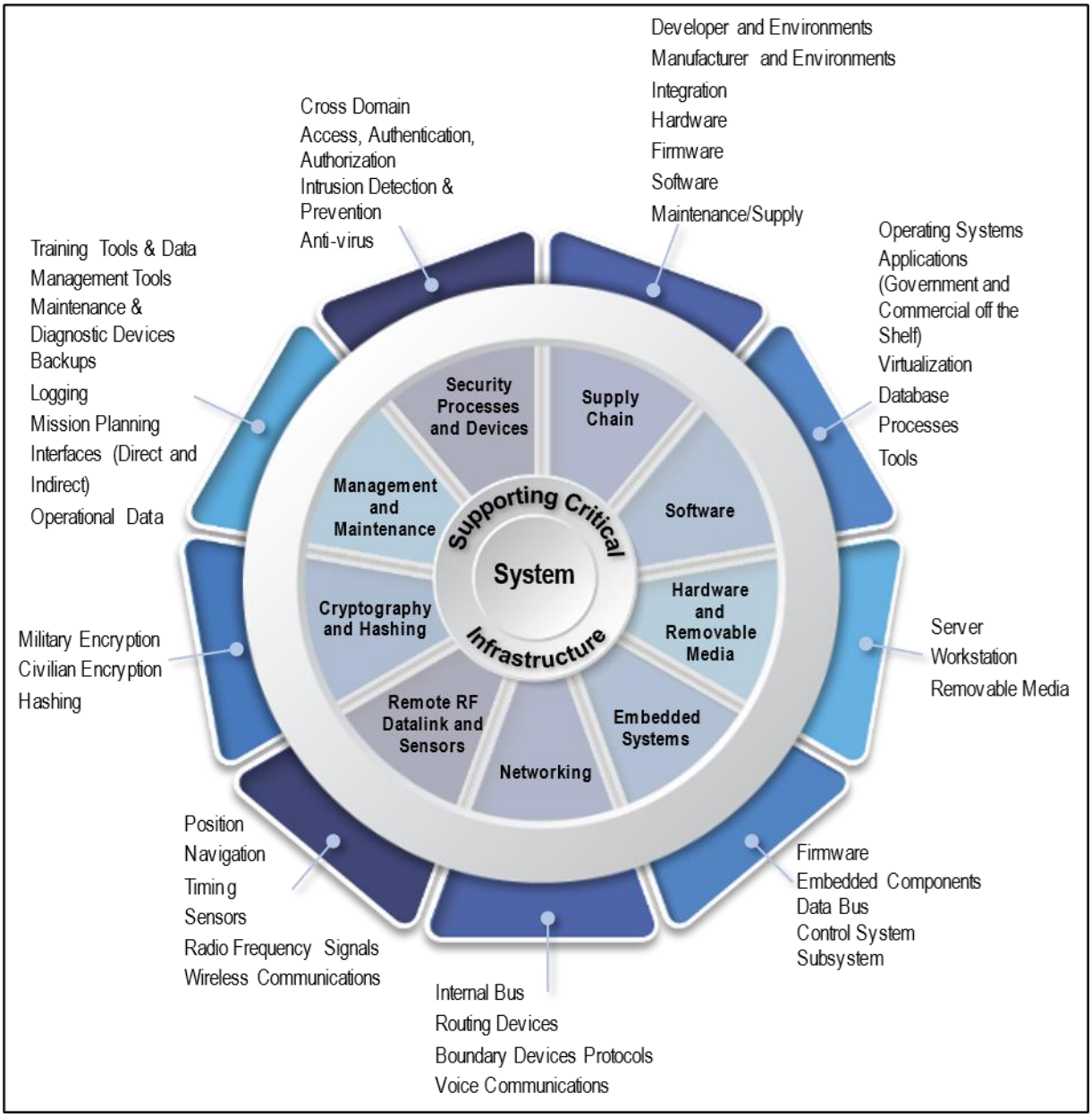
Informed (I): The person or people who are kept informed of the progress or completion of the task, but are not actively involved in its execution.

CTT ACTIVITIES →	EXERCISE PREPARATION	Select Personnel, Event Logistics & Planning	Gather System Documentation and Collect System Reconnaissance	Develop Operational Mission & Scenario	Develop OPFOR Mission & Perform Reconnaissance	Define Initial Mission Impact Methodology	Define Likelihood Assessment Methodology	Develop Data Handling Plan	Develop Kickoff Brief	EXERCISE EXECUTION	Present Potential Attack Vectors	Collect & Review Data	POST EXERCISE ANALYSIS	Perform Likelihood and Impact Assessment	Develop Cybersecurity Risk Matrix	Identify Mitigations	Develop Recommendations	Develop Vignettes	REPORTING	Develop Technical Brief	DevelopExecutive Brief
STAKEHOLDERS																					
Program Manager or Equivalent	PREP	A	A	A	A	A	A	A	A	EX	A	A	POST	A	A	A	A	A	RPT	A	A
Chief Developmental Tester or System Engineering Lead		C	C	C	C	I	I	I	C		C	C		C	C	I	C	C		C	C
Approving Official or representative		I	C	I	I	I	I	I	I		I	I		I	I	I	I	I		I	I
CONTROL TEAM																					
Control Team Lead	PREP	A-R	A-R	A	A	A-R	A-R	A-R	A-R	EXECUTE	A	A	POST ANALYSIS	A	A	A	A-R	A	REPORT	A-R	A-R
CTT Facilitator		C	C	C	C	C	C	C	R		C	C		C	C	C	C	C		C	C
Operational Team Lead		C	A-R	A-R	C	R	C	C	R		C	A-C		C-R	R	R	C	R		C-R	C
OPFOR Team Lead		C	C-R	C	A-R	C	R	C	R		R	A-C		C-R	R	R	C	R		C-R	C
Note Takers		I	I	I	I	I	I	C	I		I	R		C	C	C	I	C		I	I
Deputy Team Leads (if applicable)		A-R-C	A-R-C	A-R-C	A-R-C	A-R-C	A-R-C	A-C	A-R		A-C-R	A-C		A-C-R	A-R	A-R	A-R-C	A-R		A-R-C	A-C
Security Lead		A-R-C	C	I	I	I	I	R	C		I	C		C	I	-	-	C		C	C
Intelligence Lead		C	I	C	C	C	C	C	R		C	C		C	C	C	I	C		C	C
Data Analyst		I	I	I	I	I	I	C	I		I	R		I	R	C	C	I		I	I
Analysis Lead		I	I	I	I	I	I	I	I		I	I		R	R	R	R	R		C-R	C
OPERATIONAL TEAM																					
Operational Team Lead	PREP	C	A-R	A-R	C	R	C	C	R	EXECUTE	C	A-C	POST ANALYSIS	C-R	R	R	C	R	REPORT	C-R	C
System Operators		I	C	C	C	C	C	I	C		C	I		I-C	I	C	I	I		I	I
Operational SME		I	C	C	C	C	C	I	C		C	I		I-C	I	R	I	I		I	I
System Maintainer and Logistics		I	C	C	C	C	C	I	C		C	I		I-C	I	R	I	I		I	I
CSSP		I	C	C	C	C	C	I	C		C	I		I-C	I	C	I	I		I	I
Anti Tamper		I	R	C	C	C	I	I	C		C	I		I-C	I	R	I	I		I	I
Information Systems Security Engineer		I	R	C	C	C	C	I	C		C	I		I-C	I	R	I	I		I	I
Information Systems Security Manager		I	R	C	C	C	C	I	C		C	I		I-C	I	R	I	I		I	I
Lead Software Engineer/Analyst		I	C	C	C	C	I	I	C		C	I		I-C	I	R	I	I		I	I
System Developers		I	R	C	C	C	C	I	C		C	I		I-C	I	R	I	I		I	I
Security Champion (DevSecOps)		I	C	C	C	C	I	I	C		C	I		I-C	I	C	I	I		I	I
Safety SMEs		I	C	C	C	C	I	I	C		C	I		I-C	I	R	I	I		I	I
Logistics and sustainment SMEs		I	C	C	C	C	I	I	C		C	I		I-C	I	R	I	I		I	I
M&S SME		I	C	C	C	C	I	C	C		C	I		I-C	I	C	I	I		I	I
CYBER OPPOSING FORCE (OPFOR) TEAM																					
OPFOR Team Lead	PREP	C	C-R	C	A-R	C	R	C	R	EXECUTE	R	A-C	POST ANALYSIS	C-R	R	R	C	R	REPORT	C-R	C
DoD Cyber Red Team		I	I	C	C	C	C	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Certified Ethical Hackers		I	I	C	C	C	C	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Defensive and Offensive cybersecurity SMEs		I	I	C	C	C	C	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Cyber Test Range		I	I	C	C	C	C	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Electronic Warfare testers		I	I	C	C	C	I	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Interoperability engineers		I	I	C	C	C	I	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Lead D&TE Organization		I	I	C	C	C	I	I	C		C	I		I-C	I-C	I	I	I-C		I	I
Operational Test Agency or Operational Test Organization		I	I	C	C	C	I	I	C		C	I		I-C	I-C	I	I	I-C		I	I
Cyber DT&E and OTA/OTO Technical Experts		I	I	C	C	C	I	I	C		C	I		I-C	I-C	C	I	I-C		I	I
Software Assurance Testing SME		I	I	C	C	C	I	I	C		C	I		I-C	I-C	C	I	I-C		I	I
STAT and Design of Experiments SME		I	I	C	C	C	I	I	C		C	I		I-C	I-C	C	I	I-C		I	I

Figure A-1. Example CTT RACI Matrix

Attack Surface

Characterizing the attack surface helps programs analyze how an adversary can execute a cyber kill chain against a system. One tool to assist with attack surface analysis is the "wheel of access" depicted in Figure A-2.



Source: DoD Cyber DT&E Guidebook, Version 3.0

Figure A-2. Wheel of Access

The wheel depicts some of the more common access paths that may exist for a system. Figure A-2 is one example and not an authoritative representation of all possible access points. An attack surface can be anywhere in the hierarchy of the system or from opportunities in the SE process, including supply chains and developmental environments. OPFOR teams can use this access representation to generate ideas and vignettes for explaining how an attacker might gain access to the system.

Adversary Tactics

A resource for cyber OPFOR teams and during analysis is the MITRE ATT&CK database. (https://attack.mitre.org/) "MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."

Cyber Kill Chain

Cyber attackers, such as an advanced persistent cyber threat (e.g., nation sponsored), perform a chain of actions to conduct offensive operations against systems and networks. Several variants of the process exist, but they involve activities such as those in the cyber kill chain depicted in Figure A-3 and described below.

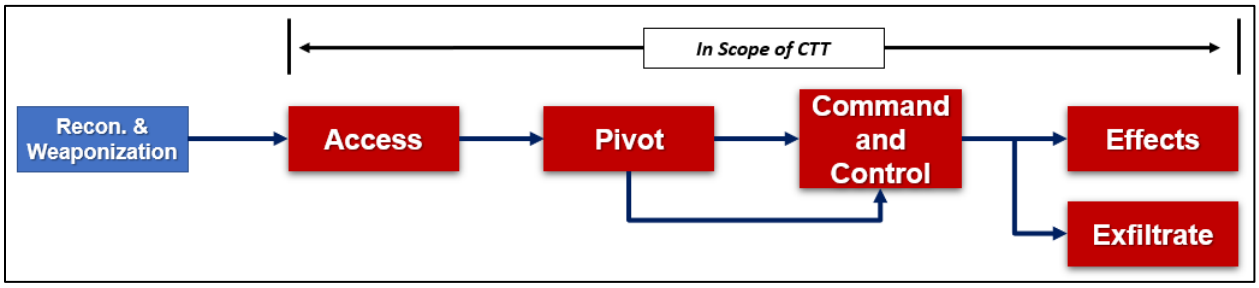


Figure A-3. Cyber Kill Chain

Reconnaissance and Weaponization. Attackers gather information before the actual attack. This action helps them devise possible ways to exploit vulnerabilities in the system software and architecture and use social engineering to initiate an attack. Most information they garner is publicly available on the Internet. The attacker uses an exploit and creates a malicious payload to send to the victim. Attackers will likely try this out in their own laboratory or cybersecurity range before unleashing it on the victim.

Access. The attacker sends the malicious payload to the victim by one or many intrusion methods, or the attacker remotely gains access to the system via various attack vectors. See Figure A-2 for examples of points of access to a system.

Pivot. The attacker moves cyber weapons or remote presence between computing systems and interfacing computer systems in or connected to the targeted platform, ultimately establishing a presence for a cyber weapon or remote access on the targeted platform.

Command and Control. The attacker establishes bidirectional communication with a cyber weapon operating within the targeted platform. The attacker creates a C2 channel to continue to

operate the internal assets remotely. This action is relatively generic and relevant throughout the attack, not only during malware installation.

Effects. The attacker performs the actions to achieve the attacker's actual goals on the victim's system. The actions taken can involve an elaborate active attack process that takes months and thousands of small actions to achieve. The mission effect may be one or a combination of denial, disruption, deception, degradation, or destruction of data or systems. Typically, these attacks are on the availability and integrity of data and systems with the goal of compromising the platform's mission.

Exfiltrate. The attacker is using presence or a cyber weapon to conduct confidentiality attacks against the platform. Exfiltration is another type of mission effect that often has secondary and/or tertiary effects on the targeted system or other systems (not necessarily in scope). The exfiltrated data enables an adversary to execute kinetic or non-kinetic attacks. These attacks often continue until they are detected, or until DoD updates or replaces the platform.

Appendix B: Cyber Table Top Exercise Execution Resources

Notional CTT Exercise Execution Agendas

Option 1: Kickoff held the same week as the CTT

- Day 1 events (participants):
  - Welcome aboard, administrative, security, safety briefs (combined teams).
  - CTT program leadership speaker – setting the stage (combined teams).
  - CTT purpose and objectives brief (combined teams).
  - System description brief (combined teams).
  - Intelligence brief (combined teams).
  - Operational mission and scenario brief (combined teams).
  - OPFOR mission brief (combined teams).
  - Team breakout sessions.
  - Day 1 summary (control team).
- Day 2 events (participants):
  - Teams continue separate breakout sessions, as needed.
  - Operational team task brief – operational timeline developed in team breakout session (combined teams).
  - OPFOR cyber opposing mission objective #1 (combined teams).
    - More attacks may be completed on this day depending on the schedule.
  - Discussions and clarifications (combined teams).
  - Day 2 summary (control team).
- Day 3 events (participants).
  - OPFOR cyber opposing mission objective #2–N (combined teams).
    - Pick up where the event left off on Day 2.
  - Discussions and clarifications (combined teams).
  - Lessons learned (combined teams).
  - *Post-Exercise Analysis* planning meeting (control team).

Option 2: Kickoff held 3 or more weeks before the CTT

- Kickoff events (participants):
  - Welcome aboard, administrative, security, safety briefs (combined teams).
  - Kickoff speaker – setting the stage (combined teams).
  - CTT purpose and objectives brief (combined teams).
  - System description brief (combined teams).
  - Operational mission and scenario brief (combined teams).
  - OPFOR mission brief (combined teams).
  - Technical and mission scope questions (combined teams).
  - Day 1 summary (control team).
- Kickoff Day 2 (participants):
  - Team breakout sessions – the day after kickoff or at some point before the *Exercise Execution* (participants).
    - Operational team:
      - Operational mission and scenario refinement (operational team).
      - Operational mission execution planning session (operational team).
      - Operational mission impact development or refinement (operational team).
    - Cyber OPFOR team:
      - Technical deep dive with system SMEs.
      - Reconnaissance or open-source analysis brief (OPFOR).
      - Vulnerability, general attack planning session (OPFOR).
- CTT *Execution* Day 1 events (participants). The Day 1 briefs can be abbreviated from kickoff, highlighting the updates made after kickoff, because they should be a review for nearly everyone, and the full briefs should be available on the CTT collaboration site. Optional: Instruct participants to read the briefs as prework before the CTT.
  - Welcome aboard, administrative, security, safety briefs (combined teams).
  - CTT program leadership speaker – setting the stage (combined teams).
  - CTT purpose and objectives brief (combined teams).
  - System description brief (combined teams).
  - Intelligence brief (combined teams).

  - Operational mission and scenario brief (combined teams).
  - OPFOR mission brief (combined teams).
  - OPFOR cyber opposing mission objective #1 (combined teams).
  - Discussions and clarifications (combined teams).
  - Day 1 summary (control team).
- CTT Day 2–X events (participants):
  - OPFOR cyber opposing mission objectives #2–N (combined teams).
  - Discussions and clarifications (combined teams).
  - Summary (control team).
- CTT last day events (participants):
  - Conclude OPFOR cyber opposing mission objectives (combined teams).
  - Discussions and clarifications.
  - Lessons learned (combined teams).
  - *Post-Exercise Analysis* planning meeting (control team) – enter supporting information.

Exercise Support Planning

Kickoff or Exercise Supplies

The control team should create welcome packets for all CTT participants, and print copies of the kickoff briefs for reference during the exercise.

- Welcome packet: agenda; name or number tag; list of participants; SUAs diagram; acronym list; note sheet; CTT participant survey

Other useful resources and supplies to have available:

- Dry-erase markers
- Permanent markers
- Correction fluid bottles
- Whiteboards
- Pens

- Self-stick easel pads
- 11x17 laminated diagrams
- Rubber bands for large brainstorming sheets
- Name or number tags for participants – reusable or stickers
- Large envelopes
- NOFORN stamps with ink (as required)
- SECRET stamps with ink (as required)
- CUI stamps with ink (as required)
- Cover sheets for Secret documents
- Composition notebooks (college ruled) or notetaker binders with formatted note-taking pages
- Secret laptops (minimum 2)
- 4x6 index cards (labeled by number) for observers to submit questions and lessons learned

Room Configuration

The control team reserves rooms at the appropriate classification level that can accommodate all participants and observers (it is better to overestimate the size of space necessary). One or two smaller rooms may be needed for the team breakout sessions in addition to the main room holding the exercise. The team rooms should have flip charts, maps (as needed), sticky notes or self-stick easely pads, and markers to aid with the discussion and brainstorming assignments.

Consider the organizational layout of the main *Exercise Execution* room; circular or oval seating facilitates discussion and helps notetakers see everyone. Notetakers should be distributed throughout the room to capture both main issues and sidebar discussions in their area. The room should contain audio and visual equipment for presentation graphics at the proper classification level. Display architectural drawings (laminated, if possible) in the main *Exercise Execution* room, showing connections and system interdependences.

Consider seating participants by team membership. Having teams sit together facilitates note-taking, enables team members to confer with each other, and builds team camaraderie.

Consider the comfort and well-being of the participants by ensuring beverages, snacks, and facilities are readily available. Cyber OPFOR teams thrive on caffeine!

Support During the Exercise

The control team ensures each participant has a number and provides number badges or name or number tents to identify who is speaking when the notetakers are recording the conversations during the CTT. It is easier for the notetakers to hear and write a number than a name. Ask participants to state their assigned number when speaking to help notetakers more easily capture who is speaking.

Throughout the CTT—before starting, taking breaks, and restarting the activities—all participants should be reminded of the classification level by the security lead or the control team lead. Also, ask participants to caveat known classified statements with an announcement of the classification level.

Appendix C: Cyber Table Top Post-Exercise Analysis Resources

Analysis Table Column Descriptions

The analysis table, broken up into three parts for readability in Figure 3-8, Figure 3-9, and Figure 3-10, is an Excel spreadsheet used to document all the details for each proposed attack as a unique row. A downloadable and tailorable template is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) in the Cyber Table Top Guidance folder. The template provides descriptions for each column, which are also provided in Figure C-1, Figure C-2, Figure C-3, and Figure C-4. Figure C-1 includes a description for or "Possible System Outcome" (for attacks focused on access, C2, and pivots) or "Possible System Impact" (for attacks causing an effect). For access, pivot, or C2 attacks, the possible outcome is described. For attacks expected to cause a system effect or mission impact, the possible system impact is described. See Figure 3-8 for the two different versions of the OPFOR sections.

Column	Description
Attack ID	OPFOR Mission number, attack number, and variant number *e.g.* M1A01V2
Goal	Goal of the attack with respect to the OPFOR mission; Gain access, cause an effect, steal data *e.g.* delay operational mission
MITRE ATT&CK Tactic, Technique, T-Code (Optional)	Enables submitting a sanitized version of each attack to the Ontology for Attacks in Cyber Risk Assessments and identifying D3FEND techniques to prevent or mitigate - see DoD CTT Guide for more information. Select the applicable MITRE ATT&CK Tactic, Technique, and T Code ID (T####) from https://attack.mitre.org/versions/v11 NOTE: OACRA is currently based on v11.3 of MITRE ATT&CK.
Attack Method	The broad class of attack the adversary will employ to execute the OPFOR mission; there may be multiple attack types capable of executing the mission. *e.g.* SQL injection
Attack Description	The technical description of the attack; may generate variants because they can have very different mission impacts, consequences, costs, etc. E.g. delete entries for customer database
Assumptions	Assumptions about the attack process and systems under attack; e.g. the adversary team has previously gained a presence on the network
When in the Mission Timeline	Specific event, circumstances, or specific times in the operational scenario when the attack is executed; and explanation why that matters, if relevant
Possible System Outcome or Possible System Impact	Description of possible outcomes to the systems under attack or the description of the impact on the system if the effect occurs. Don't break out into separate variants unless relevant. *e.g.,* Customer entries are deleted from the databases and data is unavailable until restored from backup.

Figure C-1. Column Descriptions in the OPFOR Analysis Table Section

Column	Description
Operational Impact	Description of the operational mission effort. *e.g.,* operators can't pull up customer records in support of mission execution and have to bring systems down for unplanned maintenance for 3 hours.
Mission Impact (Rubric)	Description of the high level consequences to the overall operational mission state: Full Mission Capable Partial Mission Capable Not Mission Capable
Numerical Mission Impact and Consequence	Using an operational mission rubric to assess mission impact, assign a numerical value for *Operational Impact* and *Mission Impact (Rubric)* columns

Figure C-2. Column Descriptions in the Operational Mission Analysis Table Section

Column	Description
Attack Cost / Level of Effort	An estimation of how difficult the attack is to execute; this is a combination of the technical complexity, the availability of system information (or the system) to an adversary prior to the attack; Assumptions should be excluded from consideration e.g. if network access is assumed the difficulty of that should be excluded and factored in later as desired. e.g., Easy to develop; similar attack demonstrated in public domain; extension of attack demonstrated in public domain; difficult to develop; timing the attack is difficult Easy, Moderate, Difficult
Attack Success Likelihood	The likelihood the attack will be successful when executed and have the stated attack result (due to technical complexity, etc.) and NOT an estimate of the likelihood that a real-world adversary would use this attack
Numerical Attack Likelihood	Using the OPFOR Rubric, taking into account the *Attack Cost / Level of Effort* and the *Attack Success Likelihood* of the attack succeeding, a numerical value will be assigned for likelihood. (Value: 1-5)
Analysis of Numerical Attack Likelihood Factoring in Access Method(s): New (or unchanged) value	Used to subjectively downgrade or upgrade the attack when considering access methods. If the attack required some type of access to a specific network, this column will factor the difficulty of gaining that access with the attack level of effort and likelihood of success. This may result in the likelihood value in column N increasing or decreasing.
Final Risk Assessment Coordinates	Represented as coordinates, *e.g.,* (3,5) X-Axis: Numerical Mission Impact and Consequence Y-Axis: Analysis of Numerical Likelihood Factoring in Access Method(s)

Figure C-3. Column Descriptions in the Likelihood and Final Risk Analysis Table Section

Column	Description
Capabilities or Mitigations In Place Today	Description of how specific cybersecurity controls or other mechanisms the system under analysis has in place today that would mitigate the attack.
Capabilities or Mitigations Planned for the Future	Description of how specific cybersecurity controls or other mechanisms the system under analysis had planned for the future that would mitigate the attack.
Capabilities or Mitigations Considered during CTT	Description of general cybersecurity controls or other mechanisms that could be implemented into the system under analysis and would mitigate the attack.
Recommendations	Follow-on recommendations the program conducting the CTT should consider for each attack. Should be some high level categorization with amplifying data *e.g.,* Accept Risk, Investigate Further, Test, etc.
Questions, RFIs, Further Analysis	Any unanswered questions or requests for more information that are needed to inform CTT analysis; Questions that need to be investigated after the CTT is over.

Figure C-4. Column Descriptions in the Mitigations, Recommendations, Questions, and RFI Analysis Table Section

Using the Risk Matrix

The risk matrix is the primary visualization tool for a CTT. The program can use alternate methodologies for analyzing and presenting results. This guide recommends using the NIST SP 800-30 risk matrix (see Figure 3-15) to ensure risk assessments are consistent with the DoD RMF.

Cybersecurity risk, as with other risks, consists of likelihood on the vertical, or y, axis of the matrix, and impact or consequence on the horizontal, or x, axis. For cybersecurity risk, the likelihood component is more complex than simply a probability that the event will occur as is common for traditional risk matrices.

The likelihood factor is a function of the threat and the vulnerability factors, Likelihood = *f(threat, vulnerability)*, resulting in the risk being a function of factors for both likelihood and impact: Risk = *f(threat, vulnerability, impact)*. Without a threat or a vulnerability, the risk would be 0. Threat, vulnerability, and impact have their own factors to consider when assessing the likelihood for cybersecurity:

threat = *f(attacker, motive, target, access, capabilities, level of effort)*

vulnerability = *f(findable, penetrable, corruptible, concealable, irreversible)*

impact = *f(system susceptibility, duration, mission criticality)*

Reducing cybersecurity risk then involves affecting the subfactors within the three main factors: threat, vulnerability, and impact. Increasing a threat's requisite level of effort, reducing the threat's access, or reducing findable vulnerabilities would cause the likelihood factor to be lower. Reducing impact may focus on lowering system susceptibility or the duration of impact.

"As stated in Section 3.4.3.1, for a CTT, likelihood is generally not an assessment of the adversary's intent to conduct the specific attack or the probability the system will be susceptible to the attack. Therefore, the analysis participants typically do not assess the threat portion of likelihood during analysis; however, if the program has dedicated intelligence support, the intelligence experts should participate in the analysis and should factor the threat assessment into likelihood. The program can request intelligence experts provide more insight into adversary targeting or use the CTT findings to investigate targeting if unknown. The intelligence assessment may result in an increase or decrease to the likelihood value.

The analysis table provides a column to uniquely track and identify each of the attacks presented and analyzed during the CTT using a numbering technique. This technique includes the OPFOR mission number (M#), the attack number within that mission (A#), and the variant number for that specific attack (V#). The combination of the three letters and numbers serves as the unique identifier. For example, M2A1V2 indicates OPFOR mission 2, attack 1 within that mission, and variant 2 of that attack. The presence of "V2" in the identification implies there is at least one other variant of attack 1 within mission 2 (i.e., M2A1V1).

Figure C-5 depicts four attacks, and no variants for mission 2 plotted onto the risk matrix.

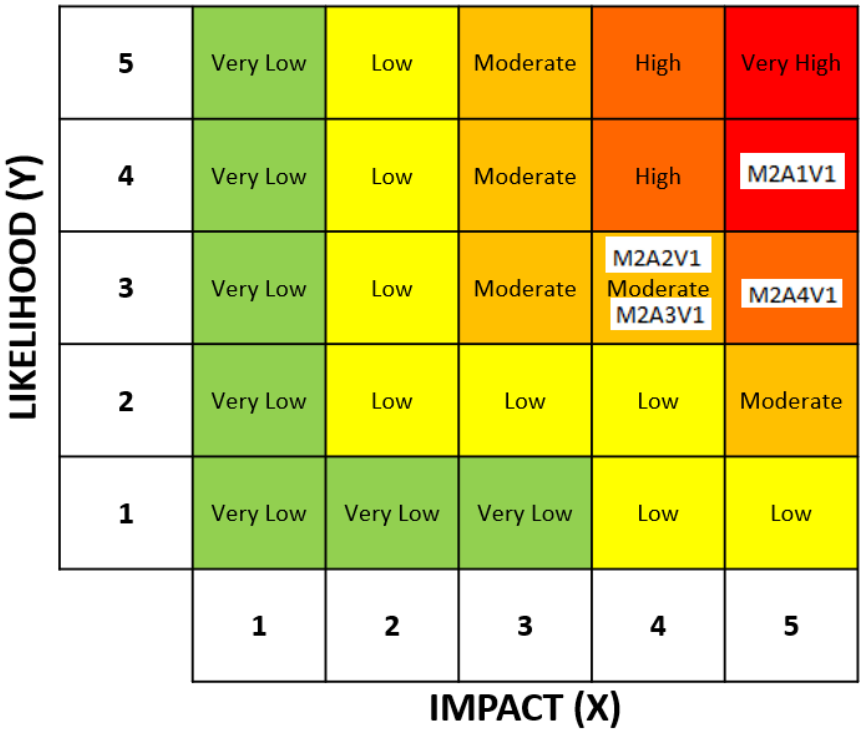


Figure C-5. Notional Risk Matrix Depicting Four Attacks

Reading the risk on the matrix for M2A1V1:

- Successful execution of variant 1 of attack 1 for OPFOR mission 2 would leave the system non-mission capable.
- This attack is likely to work based on the assumptions that the adversary previously gained a presence on the network.

Because the likelihood factor can be subjective and depends heavily on the OPFOR subject matter expertise and incomplete intelligence assessments, the program should plan cyber testing for the areas of greatest concern to more accurately assess the probability.

Submitting Sanitized Attacks to OACRA

As discussed in Section 2.1.3, the control team can contribute to the OACRA instances on the SIPRNET by sanitizing the results. The OACRA template (Excel file) is available in the OSDRE-DoD-Cyber-Table-Tops Team CTT-Guidance-Documents channel and on the CTT Intelink Website (https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx) in the Cyber Table Top Guidance folder. The template provides tips for sanitizing the attacks.

Figure C-6 depicts the example effects shown in Figure 3-14 sanitized in the OACRA template.

OPFOR - REMOVE PROGRAM SPECIFIC IDENTIFYING CONTENT										OPFOR/Engineers (If none are relevant, submit new Target)		Analysis Team
Goal	MITRE ATT&CK Domain	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Attack Description	Attack Vector Superclass	Attack Vector Class	Assumptions	Attack Timing	Possible Outcome or Possible System Impact	Cyber Target Superclass	Cyber Target Class	Common Mitigations
Disrupt	Enterprise_Domain	Impact_Enterprise	Stored Data Manipulation (T1565.001)	Adversaries inject false GPS signals to mislead the navigation system.	System_Artifact	Navigation System	The adversary team has previously gained a presence on the network.	Mission Execution/Mission Task	Loss of navigation capability. The navigation system becomes unreliable.	Information_Artifact	Position Data	Aadvanced GPS anti-spoofing measures and redundant navigation systems.
Deny	Enterprise_Domain	Impact_Enterprise	Endpoint Denial of Service (T1499)	Adversaries use radio frequency (RF) jamming to disrupt datalinks.	Communication_Entity	Radio Receiver	Proximity to the receivers.	Mission Execution/Mission Task	Data delivery is disrupted.	Cyber_Communication	Radio Frequency Signal	Advanced frequency monitoring and anti-jamming measures.
Degrade	Enterprise_Domain	Impact_Enterprise	Stored Data Manipulation (T1565.001)	Adversaries use malware injected via a compromised maintenance laptop to alter data.	Information_Artifact	Maintenance Laptop	The adversary team has previously gained access to the system.	Mission Execution/Mission Task	Stored data is corrupted.	Information_Artifact	Data	Advanced malware detection, data integrity monitoring, and secure storage systems.
Destroy	Enterprise_Domain	Impact_Enterprise	Data Destruction (T1485)	Adversaries send malicious commands through a compromised C2 interface.	System_Artifact	Command and Control System	The adversary team has previously gained access.	Mission Execution/Mission Task	System rendered inoperable, leading to loss of the asset.	Cyber_Communication	Cyber Messaging	Advanced command validation and fail-safe mechanisms

Figure C-6. OACRA Template with Sanitized Attacks

Appendix D: Cyber Table Top Checklists

Control Team

Step 1: Exercise Preparation

- □ Confirm funding is available and allocated to perform the entire exercise, from planning through reporting.
- □ Develop and publish to participants a CTT POA&M that includes the required delivery of products such as SUA technical data; submission of visit requests; dates for the kickoff, TEMs, and CTT *Execution*; quick-look reports (if used); and the final report or brief.
- □ Schedule control team planning meetings.
- □ Recruit the exercise participants:
  - □ Operational team.
  - □ Cyber OPFOR team.
- □ Designate leaders for the operational and cyber OPFOR teams.
- □ Reserve the facilities and obtain the proper equipment and supplies for the exercise.
- □ Request intelligence and threat briefs.
- □ Obtain and review the criticality analysis.
- □ Obtain and review the threat assessment.
- □ Obtain and review the attack surface characterization.
- □ Identify the scope of the assessment (e.g., critical functions, targeted data of the SUA, cyber boundary, trusted vs. assumed-compromised interfaces or data).
- □ Approve the operational team's mission (e.g., ISR, combat search and rescue) and background operational scenario.
- □ Approve the cyber OPFOR team's mission and cyber opposing mission objectives that include or exclude classes of threat vectors (e.g., supply chain, insider threat, social media exploitation).
- □ Develop and approve the initial mission impact methodology.
- □ Develop and approve the likelihood assessment methodology.
- □ Set up controlled access repositories at the appropriate classification level to store and share CTT information.
- □ Obtain SUA reconnaissance information.
- □ Develop the Data Handling Plan for storage and dissemination of classified material throughout the CTT.

- □ Develop ROE for the CTT and teams.
- □ Develop the exercise schedule and kickoff agenda.
- □ Develop the exercise kickoff briefs.
- □ Train and educate the team leads, data analyst, and notetakers.
- □ Distribute participant information: read-ahead material or collaboration site, travel information, instructions for submitting visit access requests, parking map, driving directions to the facility, attire, facility and room location, food options, clearance level restrictions, etc.
- □ Bring supplies to the exercise, including notebooks or laptops for notetakers.

Step 2: Exercise Execution

- □ Keep each team within the bounds that have been set by their respective missions, ROE, and scenarios.
- □ Adjudicate any questions or issues that arise.
- □ Ensure discussions do not sidetrack participants or bog them down on one point ensuring the exercise continues to flow (use ELMO and MOTHMAN).
- □ Ensure operational and cyber OPFOR teams are completing data products in the time allotted for each day of the exercise.
- □ Ensure notetakers capture the discussion and RFIs from participants.
- □ Secure all exercise materials (e.g., notes, drawings, and other data products) following the Data Handling Plan.
- □ Recruit *Post-Exercise Analysis* participants from the CTT teams.
- □ Create the timeline for *Post-Exercise Analysis* meetings.
- □ Collect lessons learned and feedback from participants.

Step 3: Post-Exercise Analysis

- □ Disseminate data products to analysis participants.
- □ Refine and organize data in the analysis table.
- □ Track the completion of homework and RFIs.
- □ Draft results briefs (executive and technical).

Step 4: Reporting

- □ Produce the technical brief detailing the results of the CTT to SE and test personnel.
- □ Produce the executive brief to the program office.

- □ Analyze surveys and provide feedback from the exercise to help improve the CTT process.

Operational Team

Step 1: Exercise Preparation

- □ Review all read-ahead material or other preparation as requested by the control team.
- □ Define the operational mission and draft the scenario; determine the plausibility and completeness of the mission orders and the background scenario.
- □ Provide input to the initial mission impact methodology.
- □ Review documentation detailing the functions, interactions, communication requirements, procedures, and systems used during:
  - □ Mission preparation.
  - □ Mission execution.
  - □ Maintenance activities.

Step 2: Exercise Execution

- □ Develop the overall operational mission plan to execute in response to the mission orders provided by the control team.
- □ Refine a brief that outlining operator functions, interactions, communications, systems, and procedures for:
  - □ Mission planning.
  - □ Mission execution.
  - □ Pre-mission and post-mission maintenance, both scheduled and unscheduled.
- □ Refine or update the mission impact methodology.

Step 3: Post-Exercise Analysis

- □ Complete Working Meetings 1 and 2 homework.
- □ Participate in the risk assessment analysis.
- □ Review deliverables for accuracy and completeness.

Step 4: Reporting

- □ Review the draft executive and technical briefs.
- □ Support the out-brief of technical results.
- □ Provide feedback from the exercise to help improve the CTT process.

Cyber OPFOR Team

Step 1: Exercise Preparation

- □ Review the materials provided by the control team.
- □ Review all system reconnaissance information before the exercise.
- □ Define the OPFOR mission.
- □ Develop a list of cyber opposing mission objectives and classes of attacks based on the reconnaissance review.
- □ Provide input to the likelihood assessment methodology.
- □ Conduct TEMs (either after the separate kickoff or before *Exercise Execution*).

Step 2: Exercise Execution

- □ Develop a list of potential attack surface pathways in the team breakout session after the kickoff.
- □ Present potential threat vectors and attack methods applicable to each cyber opposing mission objective.
- □ Assess the likelihood of proposed attacks.

Step 3: Post-Exercise Analysis

- □ Complete Working Meetings 1 and 2 homework.
- □ Participate in the post-exercise risk assessment analysis.
- □ Review deliverables for accuracy and completeness.

Step 4: Reporting

- □ Review the draft executive and technical briefs.
- □ Support the out-brief of technical results.
- □ Provide feedback from the exercise to help improve the CTT.

Appendix E: Common Cyber Table Top Challenges and Mitigations

Table E-1 provides CTT challenges and mitigations. The most effective approach to mitigating these challenges is to use an experienced CTT facilitator who can guide the teams.

Table E-1. CTT Common Challenges and Mitigations

Challenge	Potential Mitigation
Buy-in from senior leadership	• Provide initial engagement using the CTT 101 brief to set expectations and clarify the purpose. • Utilize other organizations that have completed CTTs to serve as advisors.
Unrealistic expectations regarding the goals and timeframe	• Provide initial engagement using the CTT 101 brief to set expectations and clarify the purpose. • Use a realistic staffing estimate and CTT average timelines. – The scope of systems can result in longer or shorter timelines.
Scoping of the mission by the operational team lead	• Use the system or mission concept of operations (CONOPS), concept of employment, OV-1 (if none created, develop one during the control team meetings), and Operational Mode Summary/ Mission Profiles. • Use templates and seek advice from other CTT facilitators.
Team composition	• Ensure the program provides engineers, testers, an information security team, and possibly other functional areas (logistics, contracting) depending on CTT objectives. • Consider each aspect of the CTT: – The systems in scope help select the right engineers and desired industry support and other contractors. – The mission, operations, and interfaces help determine the operators, defenders, maintainers, and other stakeholders. – The technology, protocols, and architecture help determine the needed cyber expertise. • Aim for diversity, not quantity.
Participant motivation	• Provide food and beverages. • Include scheduled breaks. • Incorporate humor and icebreakers. • Host social events. • Encourage leaders to attend and welcome everyone. • Thank people each day.
Administrative hurdles	• Use the CTT Plan of Action and Milestones (POA&M).
Lack of security guidance and requirements	• Discuss security early in *Preparation* and do not proceed until the program decides to write guidance or selects the guidance to follow. • For requirements, ask the program to baseline assumptions that are realistic or plausible.

Challenge	Potential Mitigation
Lack of a concept of operations (CONOPS)	• Use the available documentation for some DoD systems explaining how DoD will use the system: – Concept of employment, a functional requirements document, Operational Mode Summary/Mission Profiles, or other documentation. – Joint Mission Essential Task Lists. – DoD Architecture Framework Operational Viewpoints (e.g., OV-1, OV-2, OV-5).
Geographic obstacles (distance, time zones) that inhibit communication	• Use video teleconferencing (VTCs) and collaborative sites (i.e., SharePoint). – Careful planning and regular communication are essential. – CTT execution is not effective via VTC or conference call.
Lack of proper understanding of CTT team roles before the exercise begins	• Meet with each key lead to clarify their role, answer questions, and provide assistance. • Emphasize the CTT team roles during the CTT 101 brief.
Complaints about the lack of realism	• Have experienced personnel thoroughly review the operational team's mission during *Preparation* to ensure that the mission is realistic. • Insist on realistic and known attacker techniques—those known through experience or documented in intelligence or open source. • As a CTT facilitator, keep up-to-date with current events and work to learn attacker techniques. • Ensure that the cyber opposing force (OPFOR) team presents summary attacks based on realistic capabilities and is prepared to explain the specifics.
Inadequate facilities	• Use the CTT POA&M for planning. • Visit and inspect the facilities well in advance with the control team lead.
Minority opinion dominating discussions	• Use “MOTHMAN” (Move on, this has made all nap) as a rule of engagement (ROE). • Be careful not to offend speakers. • Place the topic in the “parking lot” (whiteboard/notetaker) and follow up with the individual separately.
Ineffective communication (the conversation gets too technical or goes off on tangents, or discussions take longer than planned)	• Use a “parking lot” (whiteboard/notetaker) to capture the conversation. • Use “ELMO” (Enough, let’s move on) as an ROE. • Be careful not to offend speakers.
Data sufficiency gaps (knowing whether the notetakers obtained sufficient data)	• Conduct end-of-day reviews of the attacks and notes. • Use a separate notetaker to capture only requests for information (RFIs). • Ask the operational team and program office (at the end of an attack) if they need more details.

Challenge	Potential Mitigation
Lack of a Data Handling Plan for execution products	• "Ensure that the Data Handling Plan is built during *Exercise Preparation*. • Plan data handling early and track it in the CTT POA&M.
Key resources missing on the day of the CTT exercise	• Plan for backups in the CTT POA&M and beg, borrow, or steal from the hosting facility as needed.
Lack of a plan for *Post-Exercise Analysis*	• To avoid a delay in the analysis: – Discuss the plan for *Post-Exercise Analysis* before CTT *Execution*. – Finalize the plan on the last day of the exercise in a control team meeting. • Use leadership briefs to drive the schedule. – If there are no leadership briefs scheduled yet, or the CTT objectives are not driving a completion date, then plan three 3-day analysis meetings—one per month.
Recognition of the appropriate level of detail required for the mission definition and system technical documentation	• Use the OPFOR lead's inputs to drive the desired details. • As the CTT facilitator, become familiar with the system(s) and missions to guide the effort. • Hold technical deep dives and conduct a practice run on the briefs to gauge the depth of the details.
Pertinent examples beyond the classification level of the CTT	• Anticipate this challenge by ensuring that program security is involved and participants understand the security classification guidance. • Document the need for higher-level breakout rooms and necessary data handling in the Data Handling Plan if there is any chance a higher classification could occur. • Have a plan for what-if.
Dismissive behavior by the operational team	• Engage program office leadership to address indications of an adversarial climate or defensiveness. • Pursue one-on-one communication if the issue is with a single individual. • If the dismissive attitude is toward the plausibility of attacks, either the CTT facilitator or a member of the OPFOR must be prepared to back up the details with real-world parallels (classified or not). – Utilize real-world intelligence briefs and include intelligence representatives.
Derailed discussions by participants	• Use "ELMO" (Enough, let's move on) to stop the discussion. • Document the off-topic idea in the "parking lot" (whiteboard/ notetaker). • Address the issue one-on-one (with program support, if necessary).
Insistence on design invulnerability by systems engineers	• Engage program office leadership to address indications of an adversarial climate or defensiveness. • Encourage the OPFOR member to present the attack by saying, "What would happen if…," rather than, "This attack is destroying…".

Challenge	Potential Mitigation
	• Promote a less adversarial demeanor and educational approach for the OPFOR.
"Pet rocks" or axes to grind	• Use a "parking lot" (whiteboard/notetaker) to capture conversations that are off topic or "pet rocks." • Reiterate the purpose and objectives of the CTT. • Use "MOTHMAN" (Move on, this has made all nap) as an ROE. • Be careful not to offend speakers.
Subject matter expert (SME) non-participation or limited availability	• Obtain firm commitments from all SMEs during the *Preparation* stage. – If commitments are wishy-washy, then plan a backup. • If the SME simply cannot be available for the entire CTT, plan to present attacks relevant to the SME only when the SME is present.
Program reluctance to share discovered vulnerabilities	• As the CTT facilitator, work to sanitize and share the data, removing the linkage to the program (program-agnostic information). • Arrange to have the receiver sign a nondisclosure or similar agreement. • Recommend program leaders meet with the leaders for the organization who can benefit from the details. • Request military component leadership (program, T&E organization) determine the details to share or not. – In the end, the program makes the determination for what and how to share, not the CTT facilitator.
Lack of participant clarity on what data is important for analysis	• As the CTT facilitator, present a clear CTT overview and define specific objectives for the desired discussions and data.
Management of classified materials between meetings and locations	• Ensure that the program staff writes, reviews, and shares a Data Handling Plan with the control team, notetakers, and the hosting facility. • Ensure program security is involved.
Lack of awareness of the best analysis participants by the control team	• Because the control team selects the analysis participants, supplement this effort only when specific expertise becomes apparent during CTT *Execution*, such as a critical engineer (demonstrated extensive knowledge) or a strong operational expert. • If an OPFOR member is the SME on high-impacting attacks, request the OPFOR member participate in the analysis. – The program's budget for external participants may result in those SMEs being "on call" instead of at the meetings.
The control team lead's inexperience with translating the exercise findings into high-level briefs	• Ensure the control team lead uses the templates. • Emphasize the leadership interest items and have the control team lead seek leadership guidance from the program office. • As the CTT facilitator, build the core results and let the control team lead work from that framework.

Challenge	Potential Mitigation
Overreporting (technical staff and SMEs report too many details; the standard reporting format is overly complicated)	• For system documentation, use the OPFOR lead to drive the desired level of detail. • For the OPFOR attacks, remind the lead to have technical staff and SMEs keep the brief simple and high level. • Document the technical attack details in *Post-Exercise Analysis*.
Non-attendance of the control and operational team leads at analysis meetings	• Do not hold analysis meetings without the control and operational team leads. • Plan the meetings in advance to accommodate their schedules. • Reschedule the meetings when conflicts arise.
Insufficient time for homework between analysis meetings	• To address this indication of poor schedule planning, either: – Reschedule the analysis meetings to allow time to complete homework. – Expand the number of days for the analysis meetings to support completing homework before or allow time just after the main analysis meeting.
No resolution of requests for information (RFIs) by the third working meeting	• Depending on the criticality of the unanswered RFIs, the analysis lead should request assistance from the control team lead or the organization to resolve essential RFIs. • Push for responses on needed information early in the *Post-Exercise Analysis*
Cyber OPFOR team with low interest or poor preparation	• Carefully consider the selection of cyber OPFOR team members. • Work with the program to ensure adequate funding for qualified expertise. • Schedule frequent OPFOR check-ins: – Helps detect the issue sooner. – Provides more time to implement a plan B, such as having the control team propose the attack concepts.

Glossary

This glossary includes definitions of some terms that teams may use or reference when conducting a CTT. Provided sources for the terms and definitions include both authoritative government sources and open-source literature. When the definition does not include a source, the definition is specific for use in this guide.

access. The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (National Initiative for Cybersecurity Careers and Studies (NICCS) Glossary)

advanced persistent threat. An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period; adapts to defenders' efforts to resist it; and is determined to maintain the level of interaction needed to execute its objectives. (NIST CSRC Glossary)

attack surface. The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from that system, component, or environment. (NIST CSRC Glossary)

attack vector. A method of conducting a cyberspace attack; how an attacker gains unauthorized access; a path or means by which an attacker gains access to a system to deliver a payload or malicious outcome. Attack vectors enable an attacker to exploit system vulnerabilities, including the human element. Also called *threat vector*.

cyber risk. The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat would exploit a particular vulnerability, with associated consequences.

cyber survivability. The cybersecurity and cyber resiliency abilities of warfighter systems to prevent, mitigate, recover from, and adapt to adverse cyber-incidents that could impact mission related functions. (Cyber Survivability Implementation Guide, Version 4)

cyber warfare. Actions, typically by a nation-state or non-state actor to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks. (NICCS Glossary)

cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (National Security Presidential Directive-54)

cyberspace attack. Actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires. (Joint Publication (JP) 3-12)

defensive cyberspace operations. Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity. Also called DCO. (JP 3-12)

enabling operations. The first stage of a cyberspace attack where the threat gains information about the targeted systems and users.

exploit. A technique or program designed to break into a system by taking advantage of an accessible vulnerability in the attack surface.

exploitation. The act of infiltrating target systems to extract and gather intelligence data.

family of systems (FoS). A series of systems that share the same basic core system characteristics, e.g., a main battle tank (MBT). (DAU Glossary)

insider threat. The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. (NIST CSRC Glossary)

kill chain. A sequence of activities that produces warfighting effects within a mission area in the battlespace. (JP 3-09)

level of effort. The amount of work an attacker must invest to successfully achieve the goals of a cyberspace attack. A function of ability, motivation, and desired impact.

likelihood of occurrence. A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. (NIST SP 800-30)

mission-relevant terrain in cyberspace. All devices, internal links, external links, operating systems, services, applications, ports, protocols, hardware, software on servers, and other technical aspects of a system required for the function of a critical asset; may exist external to the DoD cyberspace. (Forthcoming DoDM 5000.UY)

offensive cyberspace operations. Missions intended to project power in and through cyberspace. Also called OCO. (JP 3-12)

operational resilience. The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions. (DoDI 8500.01)

payload. A term that describes the component of an attack, once a vulnerability has been exploited, that causes an impact on the system. For example, if a software agent, such as a virus, has entered a given IT system, it can be programmed to reproduce and retransmit itself, or destroy or alter files in the system. Payloads can have multiple programmable capabilities and can be remotely updated.

red team. Personnel who challenge planning assumptions from an adversary's perspective. (JP 5-0)

risk. A measure of the extent to which an entity is threatened by a potential circumstance or event and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (NIST SP 800-53)

risk assessment. The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the DoD RMF process. (NIST CSRC Glossary)

supply chain attack. Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate IT hardware, software, operating systems, peripherals (IT products) or services at any point during the life cycle. (NIST CSRC Glossary)

supply chain management. A cross-functional approach to procuring, producing, and delivering products and services to customers. Military supply chain management is the discipline that integrates acquisition, supply, maintenance, and transportation functions with the physical, financial, information, and communications networks in a results-oriented approach to satisfy joint force materiel requirements. (DAU Glossary)

supply chain risk. The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system. (CNSSI 4009)

supply chain risk management. A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). (DAU Glossary)

system of systems (SoS). A set of unique systems that perform a common mission by combining the synergistic effect of multiple systems, e.g. a howitzer, a fire control computer, and a counter battery radar. (DAU Glossary)

threat. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS. (NIST CSRC Glossary)

threat vector. See *attack vector*.

Acronyms

ATC	air traffic control
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AWACS	Airborne Warning and Control System
C2	command and control
CAPEC	Common Attack Pattern Enumeration and Classification
CNSSI	Committee on National Security Systems Instruction
COE	center of excellence
CONOPS	concept of operations
CSRC	Computer Security Resource Center
CSSP	cybersecurity service provider
CTT	Cyber Table Top
CUI	controlled unclassified information
CV	Capability Viewpoint
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CyWG	cyber working group
D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
DAU	Defense Acquisition University
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDI	DoD instruction
DoDM	DoD manual
DoS	denial of service
DT	developmental test
DT&E	developmental test and evaluation
EDR	endpoint detection and response
EW	electromagnetic warfare

FIRST	Forum of Incident Response and Security Teams
FoS	family of systems
GMMS	ground mission management system
GPS	Global Positioning System
HW	hardware
IC	intelligence community
IDA	Institute for Defense Analyses
INS	inertial navigation system
ISR	intelligence, surveillance, and reconnaissance
ISSE	information systems security engineer
ISSM	information systems security manager
IT	information technology
JP	Joint Publication
JWICS	Joint Worldwide Intelligence Communications System
M&S	modeling and simulation
MAT	MBCRA Automation Tool
MBCRA	mission based cyber risk assessment
MBSE	model-based systems engineering
NATO	North Atlantic Treaty Organization
NDA	nondisclosure agreement
NICCS	National Initiative for Cybersecurity Careers and Studies
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OACRA	Ontology for Attacks in Cyber Risk Assessments
OPFOR	opposing force
OT	operational test
OT&E	operational test and evaluation
OTA	operational test agency
OTO	operational test organization

OV	Operational Viewpoint
PDT	portable database terminal
POA&M	Plan of Action and Milestones
PPP	Program Protection Plan
RACI	responsible, accountable, consulted, and informed
RF	radio frequency
RFI	request for information
RMF	Risk Management Framework
ROE	rules of engagement
RTB	return to base
RTC	Redstone Test Center
SATCOM	satellite communications
SCG	security classification guide
SE	systems engineering
SIPRNET	Secret Internet Protocol Router Network
SME	subject matter expert
SoS	system of systems
SP	special publication
STAT	scientific test and analysis techniques
StdV	Standards Viewpoint
SUA	system under analysis
T&E	test and evaluation
TALS	tactical aircraft landing system
TEM	technical exchange meeting
TEMP	Test and Evaluation Master Plan
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UON	urgent operational need
USB	Universal Serial Bus

USSS-A	Unmanned Soldier Support System–Airborne
VTC	video teleconference
WAN	wide-area network

References

Ambroso, M. A., and R. T. Hutton. “Comparative Review of DoD Mission-Based Cyber Risk Assessment Methodologies.” IDA Paper P-8736. Institute for Defense Analyses, December 2017.

Committee on National Security Systems Instruction 4009, “Committee on National Security Systems (CNSS) Glossary,” March 2, 2022.

de Naray, R. Kuzio, and K. Galvin. “Comparative Review of DoD MBCRAs: 2020 Updates and New Methodologies,” IDA Document P-14309. Institute for Defense Analyses, September 2020.

Department of Defense Cyber Developmental Test and Evaluation Guidebook. Version 3.0. Office of the Under Secretary of Defense for Research and Engineering, June 2025.

DoD Directive 5000.71, “Rapid Fulfillment of Combatant Commander Urgent Operational Needs and Other Quick Action Requirements,” October 18, 2022.

DoD Directive 5205.07, “Special Access Program Policy,” September 12, 2024.

DoD Instruction 5000.02, “Operation of the Adaptive Acquisition Framework,” January 23, 2020, as amended.

DoD Instruction 5000.73, “Cost Analysis Guidance and Procedures,” October 24, 2024.

DoD Instruction 5000.74, “Defense Acquisition of Services,” January 10, 2020, as amended.

DoD Instruction 5000.75, “Business Systems Requirements and Acquisition,” February 2, 2017, as amended.

DoD Instruction 5000.80, “Operation of the Middle Tier of Acquisition,” December 30, 2019, as amended.

DoD Instruction 5000.81, “Urgent Capability Acquisition,” December 31, 2019.

DoD Instruction 5000.82, “Requirements for the Acquisition of Digital Capabilities,” June 1, 2023.

DoD Instruction 5000.83, “Technology and Program Protection to Maintain Technological Advantage,” July 20, 2020, as amended.

DoD Instruction 5000.84, “Analysis of Alternatives,” August 4, 2020.

DoD Instruction 5000.85, “Major Capability Acquisition,” August 6, 2020, as amended.

DoD Instruction 5000.86, “Acquisition Intelligence,” September 11, 2020.

DoD Instruction 5000.87, “Operation of the Software Acquisition Pathway,” October 2, 2020.

DoD Instruction 5000.88, “Engineering of Defense Systems,” November 18, 2020.

DoD Instruction 5000.89, “Test and Evaluation,” November 19, 2020.

DoD Instruction 5000.90, “Cybersecurity for Acquisition Decision Authorities and Program Managers,” December 31, 2020.

DoD Instruction 5000.91, "Product Support Management for the Adaptive Acquisition Framework," November 4, 2021.

DoD Instruction 5000.95, "Human Systems Integration in Defense Acquisition," April 1, 2022.

DoD Instruction 5000.97, "Digital Engineering," December 21, 2023.

DoD Instruction 5000.98, "Operational Test and Evaluation and Live Fire Test and Evaluation," December 9, 2024.

DoD Instruction 5010.44, "Intellectual Property (IP) Acquisition and Licensing," October 16, 2019.

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended.

DoD Manual 5000.UY, "Cyber Developmental Test and Evaluation," Forthcoming.

National Institute of Standards and Technology Special Publication 800-30, "Guide for Conducting Risk Assessments," Revision 1, September 2012.

National Institute of Standards and Technology, Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, September 2020.

Summary of the 2023 Cyber Strategy of the Department of Defense, 2023.

Websites

Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CTT Intelink.
https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx

DAU Acquisition Policies.
https://aaf.dau.edu/aaf/policies/

DAU CTT Course.
https://www.dau.edu/courses/cyb-5630v

DAU Glossary.
https://www.dau.edu/glossary

DoD Issuances.
https://www.esd.whs.mil/DD/DoD-Issuances/

FIRST CVSS.
https://www.first.org/cvss/

Joint Engineering and Test Enterprise Portal.
https://jetep.dso.mil/

MITRE ATT&CK.
https://attack.mitre.org/

MITRE ATT&CK version 11.3.
https://attack.mitre.org/versions/v11

MITRE CAPEC.
https://capec.mitre.org/

MITRE CVE.
https://www.cve.org/

MITRE CWE.
https://cwe.mitre.org/

MITRE D3FEND.
https://d3fend.mitre.org/

NICCS Glossary.
https://niccs.cisa.gov/resources/glossary

NIST CSRC Glossary.
https://csrc.nist.gov/glossary

NIST NVD.
https://nvd.nist.gov/

STAT COE.
https://www.afit.edu/STAT/

Summary of the 2023 Cyber Strategy of the Department of Defense, 2023.
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf

Department of Defense Cyber Table Top Guide

Office of the Director, Developmental Test, Evaluation, and Assessments
Office of the Under Secretary of War for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301-3030
osd.r-e.comm@mail.mil
https://www.cto.mil/dtea/cyber