The Department of Defense Cyber Table Top Guide

Version 2.0

16 September 2021

Department of Defense Cyber Table Top Guide

Director of Defense Research and Engineering (Advanced Capabilities)
Deputy Director for Engineering
Deputy Assistant Secretary of Defense Developmental Test, Evaluation, and Assessments
3030 Defense Pentagon
3C160
Washington, DC 20301-3030
E-mail: osd.pentagon.ousd-re.mbx.communications@mail.mil
Website: https://ac.cto.mil/engineering/

Cleared for open publication: 16 September 2021, Department of Defense Office of Prepublication and Security Review

REVISION HISTORY

DATE	VERSION	REMARKS
2 July 2018	1	Initial Draft
16 September 2021	2	Changed “Guidebook” to “Guide” in title and throughout Updated cybersecurity policy (Section 2.1-2.2, pg.2-5) Expanded discussion on cyber intelligence support (Section 2.3.1, pg. 6) Improved analysis table–figures, descriptions and examples (Section 3.3, pg. 36, 39, 43 & Appendix D, pg. D-1 – D-3) Revised likelihood assessment methodology (Section 3.1.2.3.1, pg. 21) Added scientific test and analysis techniques such as design of experiments (DOE) (Section 3.0, pg. 9) Revision of the Analysis Lead role (Section 3.1.1.1.4, pg. 11 & 3.3.1.1, pg. 37) Revision of the Data Handling Plan (Section 3.1.4.1.3, pg. 26) Revision of the Documenting Final Mission Impact Assessment (Section 3.3.2.2.1, pg. 38-39) Updated references (Appendix A, pg. A-1) Modified wheel of access–figure and discussion (Appendix B, pg. B-7)

Executive Summary

The Department of Defense (DoD) recognizes cyberspace as a warfighting domain and expects cyberspace attacks to be part of future wars. All DoD systems operate in an increasingly complex, networked environment. System engineers and testers must design, verify, and validate cybersecurity, cyber survivability, and operational resilience requirements for all 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 cybersecurity, cyber survivability, and operational resilience. The Test and Evaluation (T&E) 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 vulnerable systems in the field. This guide describes methods for early identification and categorization of cyber risks, as well as identification of associated critical mission and system functions.

The Cyber Table Top (CTT) is a focused, intellectually intensive exercise that explores the effects of cyber offensive operations on the capability of US systems to carry out their missions. It is a wargame-like exercise that centers on two teams with opposing missions: the military forces charged with executing an operational mission and the cyber mission forces attempting to oppose those military forces.

The CTT provides System Engineers, Program Managers, Information System Security Managers, Information System 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 developers, and Program Manager's engineering and test teams with opportunities for risk reduction throughout the life cycle of the acquisition program and reduces the likelihood of discovering cyber vulnerabilities during Operational Test.

Contents

Executive Summary ii
1 Introduction 1
1.1 Purpose 1
1.2 Organization 1
1.3 Audience 1
2 Background 2
2.1 DoD Cyber Strategy, Objectives, and Policy 2
2.1.1 Mission-Based Cyber Risk Assessments 2
2.2 CTTs Across the Acquisition Life Cycle 4
2.3 CTT Purpose and Benefits 5
2.3.1 Intelligence Support 6
2.3.2 Risk reporting 6
3 CTT Process 7
3.0 Before Starting a CTT 7
3.1 Step 1 – Exercise Preparation 9
3.1.1 Exercise Preparation – Teams 9
3.1.2 Exercise Preparation – Team Missions 14
3.1.3 Exercise Preparation – System Documentation and System Reconnaissance 22
3.1.4 Exercise Preparation – Plans and Products 25
3.1.5 Execution Preparation - Exit Criteria 28
3.2 Step 2 – Exercise Execution 28
3.2.1 Exercise Execution – Kickoff 29
3.2.2 Exercise Execution – CTT 32
3.2.3 Exercise Execution – Data Collection and Review 34
3.2.4 Exercise Execution - Exit Criteria 35
3.3 Step 3 – Post-Exercise Analysis 35
3.3.1 Post-Exercise Analysis – Post-Exercise Homework 35
3.3.2 Post-Exercise Analysis – Working Meeting 1 37
3.3.3 Post-Exercise Analysis – Working Meeting 2 40
3.3.4 Post-Exercise Analysis – Working Meeting 3 42
3.3.5 Post-Exercise Analysis - Exit Criteria 44
3.4 Step 4 – Reporting 44

3.4.1 Reporting – Prioritize Recommendations 44
3.4.2 Reporting – Technical Brief 45
3.4.3 Reporting – Executive Brief 45
3.4.4 Reporting - Exit Criteria 46
3.5 Wrapping up a CTT 46
Acronym List 48
Glossary 49
Appendix A: References A-1
Appendix B: CTT Exercise Preparation Resources B-1
Appendix C: CTT Exercise Execution Resources C-1
Appendix D: CTT Post-Exercise Analysis Resources D-1
Appendix E: CTT Checklist E-1

List of Figures

Figure 1. Functional Polices 3
Figure 2. Adaptive Acquisition Framework and Corresponding Pathway Policy 3
Figure 3. Cyber T&E Activities 4
Figure 4. CTT Steps 7
Figure 5. CTT Collaboration Diagram 10
Figure 6. Example OV-1 Graphic Displaying the Sub-Systems Under Analysis in the CTT 15
Figure 7. Mission Impact Methodology Notional Example 16
Figure 8. Likelihood Assessment Methodology Notional Example 21
Figure 9. CTT System Reconnaissance and Documentation Process 24
Figure 10. CTT Exercise Execution – Team Collaboration 32
Figure 11. Portions of Analysis Tables Used in Post-Exercise Analysis Working Meeting 1 36
Figure 12. Portion of Analysis Table Used in Post-Exercise Analysis Working Meeting 2 39
Figure 13. Risk Matrix based on NIST SP 800-30 Rev 1 (Reference (g)) 42
Figure 14. Portion of Analysis Table Used in Pre-Exercise Analysis Working Meeting 3 43
Figure 15. Cyber Kill Chain B-6
Figure 16. Wheel of Access B-7
Figure 17. Column Descriptions in the OPFOR Analysis Table Section D-1
Figure 18. Column Descriptions in the Operational Mission Analysis Table Section D-2
Figure 19. Column Descriptions in the Likelihood and Final Risk Analysis Table Section D-2
Figure 20. Column Descriptions in the Mitigations, Recommendations, Questions, and RFI Analysis Table Section D-3
Figure 21. Notional Risk Matrix Depicting Three Attacks D-4

1 Introduction

1.1 Purpose

Department of Defense (DoD) systems increasingly depend upon complex, interconnected, information technology (IT) 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 the DoD and its warfighters. The Cyber Table Top (CTT) process is a best practice and includes an intellectual wargame-like exercise followed by analysis. The exercise and analysis in the CTT facilitates identification and comprehension of risks from potential cyber vulnerabilities. The purpose of this guide is to provide an overview of the CTT process, guidance on performing a CTT, and instructions for generating actionable information on potential cyber threats for the Program Manager. Programs or organizations may tailor this process and the templates to meet individual organization or program needs.

1.2 Organization

This guide contains three chapters, including this overview chapter. Chapter 2 provides background information. Chapter 3 explains the four steps in the CTT process. Following Chapter 3 are an acronym list, glossary, and the appendices:

- Appendix A: References
- Appendix B: CTT Exercise Preparation Resources
- Appendix C: CTT Exercise Execution Resources
- Appendix D: CTT Post-Exercise Analysis Resources
- Appendix E: CTT Checklist

Dynamic and tailorable electronic resources are available online, at the CTT Intelink Website: https://intelshare.intelink.gov/sites/resp/CTT/SitePages/Home.aspx

1.3 Audience

The intended audience for this guide includes Program Managers, Program Test Leads, Lead System Engineers, Information System Security Engineers (ISSEs), Information System Security Mangers (ISSMs), Chief Developmental Testers, Lead Developmental Test and Evaluation (DT&E) Organizations (LDTOs), Operational Test Agencies (OTAs), other Operational Test and Evaluation (OT&E) organizations, system developers/contractors, analysts performing the cyber analysis, planning, or testing for DoD acquisition programs and 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 apertures. Adversaries could design attacks to cause mission effects via disruption, denial-of-service, data corruption, data exfiltration, and data or system destruction, in a coordinated fashion with kinetic and electronic warfare attacks.

2.1 DoD Cyber Strategy, Objectives, and Policy

The DoD requires a cyber strategy that addresses rapidly evolving threats. The 2018 DoD Cyber Strategy Summary (Reference (a)) outlines the objectives for DoD cyberspace missions, which includes defending DoD networks, securing DoD data, and strengthening the resilience of systems against malicious cyber activity. The "invest[ment] in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations" is further emphasized in the Summary of the 2018 National Defense Strategy (Reference (b)). Department of Defense Instruction (DoDI) 8500.01 "Cybersecurity" (Reference (c)) defines "Operational Resilience" 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; it measures progress, identifies problems, and characterizes cyber survivability, resilience, 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

The DoDI 5000.89, "Test and Evaluation," requires acquisition programs conduct Mission-Based Cyber Risk Assessments (MBCRAs) (Reference (d)). At the time of publication of this guide, the DoD is updating the DoD Cybersecurity Test and Evaluation Guide to the DoD Cyber Test and Evaluation Companion Guide v3.0 (Reference (e)). That Guide will describe the use of MBCRAs throughout the system development life cycle. The updated DoD Cyber T&E Companion Guide, v3.0, will support DoD Adaptive Acquisition Framework (AAF), Figure 2, Reference (f)) and functional policies (i.e. DoDI 5000.89) (Figure 1), which mandate that acquisition programs evaluate cybersecurity, cyber survivability, and operational resilience in the conduct of risk management activities. DoD policy and guidance requires cyber risks be assessed at technical reviews so that system cyber threats be understood and used to determine operational impacts. Risk assessment methodologies should be consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Guide for Conducting Risk Assessments" (Reference (g)). Since NIST SP 800-30 is adaptable by design, it provides a framework for numerous MBCRA methodologies in use throughout DoD.

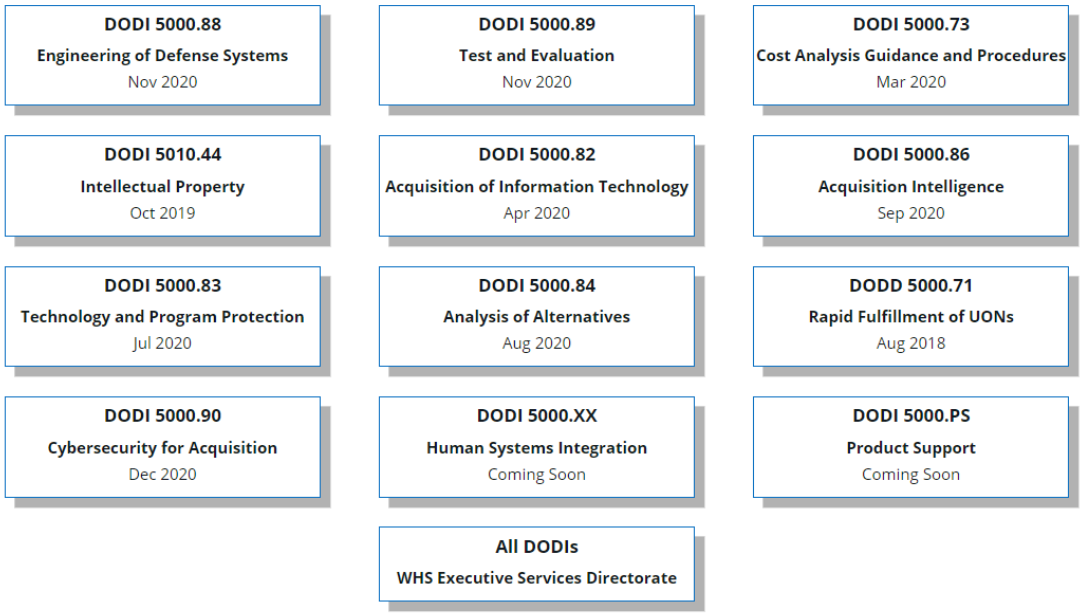


Figure 1. Functional Polices

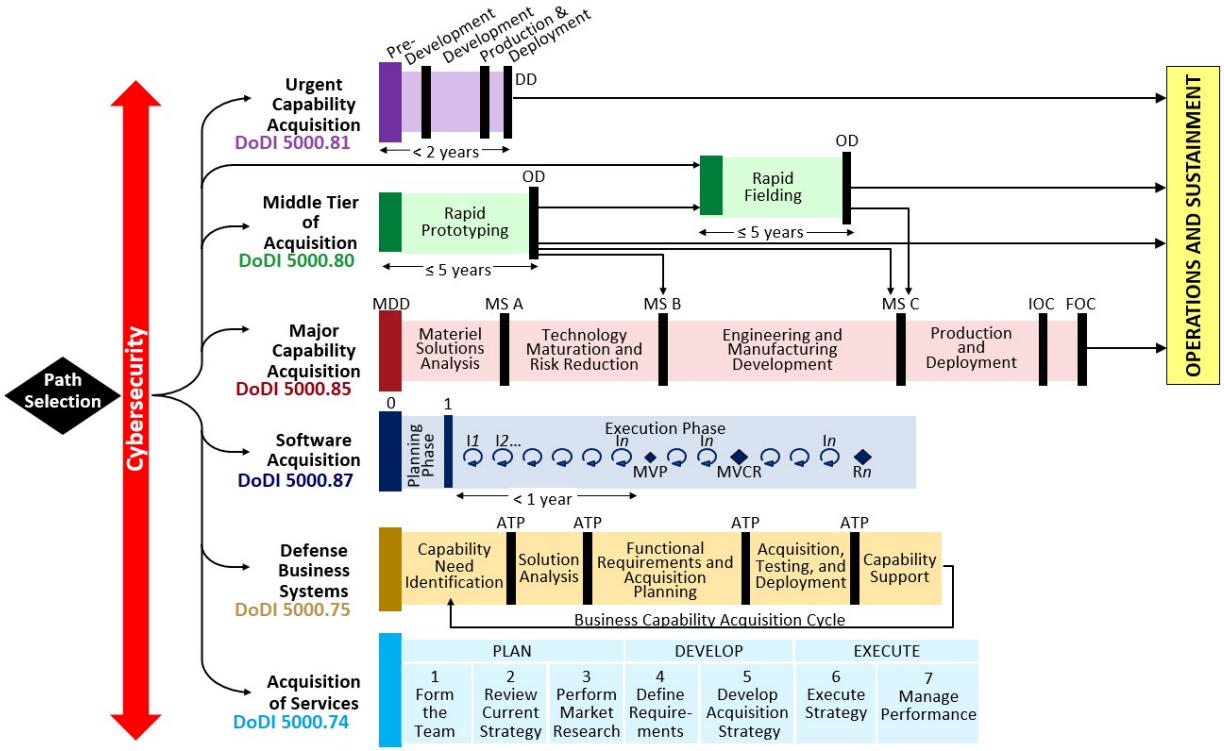


Figure 2. Adaptive Acquisition Framework and Corresponding Pathway Policy

Programs should select the MBCRA methodology that is most aligned to their program needs (e.g., information, resources, and schedule). The 2017 Institute for Defense Analysis (IDA) Paper P-8736, "Comparative Review of DoD Mission-Based Cyber Risk Assessments" (Reference (h)), reviews many MBCRA methodologies and provides a decision diagram to help programs

select an MBCRA methodology. IDA Paper P-14309 is the 2020 update to the initial MBCRA review that specifies inactive or replaced methodologies and describes several new methodologies (Reference (i)). Some of the Service methodologies are limited distribution, and as a result, the IDA papers are not publicly released, but are available on the CTT Intelink Website (§1.2). The updated DoD Cyber T&E Companion Guide, (Reference (e)), will include a releasable summary version of the IDA reports and the decision diagram.

The CTT is one of the MBCRA methodologies consistent with NIST SP 800-30 (Reference (g)). CTTs are useful for early characterization of cyber vulnerabilities and associated mission impacts, and are easily adapted as DoD updates policy. DoD has refined the CTT methodology by incorporating lessons learned from the CTTs conducted.

2.2 CTTs Across the Acquisition Life Cycle

The update (currently under development) to the DoD Cyber T&E Companion Guide (Reference (e)) describes five iterative activities for cyber T&E (Figure 3) performed for developing or updating a cyber T&E strategy and for conducting cyber T&E events. This updated cyber T&E adaptive process will support the varying cadences of the five AAF pathways: Urgent Capability Acquisition, Middle Tier of Acquisition, Major Capability Acquisition, Software Acquisition, and Defense Business Systems (Figure 1). The sixth pathway, Acquisition of Services, is not subject to T&E, but may still use a CTT to inform the cyber risks to the acquired service, if the service is digital (such as a web application). Unlike many MBCRA methodologies, a program can use CTTs at any time in a system's life cycle. Programs should update or conduct CTTs during the Conduct iteration before the planned test events during that iteration (Figure 3). The CTT does not require high fidelity in system designs. As an example, for Major Capability Acquisitions (Reference (d)), CTTs can be a tool to understand the cybersecurity, cyber survivability, and operational resilience requirements prior to Milestone A; expanded to support the characterization of the attack surface prior to Milestone B; used to scope cooperative vulnerability identification and adversarial cyber developmental test events by the developer and the government prior to Milestone C; used to inform Operational Test and Evaluation, and used to inform continuous monitoring after Milestone C.

Figure 3. Cyber T&E Activities

CTTs can supplement risk assessment reporting for the Risk Management Framework (RMF) (Reference (j)) in support of obtaining an Authorization to Operate. The results allow Program

Managers, ISSMs, ISSEs, engineers, and testers to assess the risk of cyber threats to a system. Through an understanding of mission-based cyber risk, decision makers can then prioritize what to test (and why), what risks will be accepted or mitigated, and what requires further investigation in the engineering process.

2.3 CTT Purpose and Benefits

The purpose of the CTT process is to provide Program Managers, ISSMs, ISSEs, system 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 program leadership determines what actions are required 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.

Available intelligence can play an important role in the CTT, but often the intelligence information may be limited. Although it is difficult to determine enemy intentions, the CTT can include a focus on an enemy's potential capabilities. The CTT helps prioritize the most exploitable attack surfaces and identify the attack methods that, if successful, could be the most harmful to the mission. There is a subtle but important distinction to note about the CTT: **the goal is to identify the systems and capabilities the cyber opposition forces could target that would have a major impact on the success of an operational mission, not what an adversary is actually targeting.**

The activities in the four successive steps of the CTT build on one another to generate:

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

Chapter 3 provides more details about the activities and products in each step and provides estimates for how long each step may take. CTTs do not produce an exhaustive and comprehensive list of everything an attacker could possibly do to the system. The CTT should generate a representative set of attacks, exploiting potential vulnerabilities based on the information available.

The CTT process offers multiple benefits:

- Socializes the concept of cyberspace as a warfare domain with program leadership.
- Bridges the gap between the IT and functional mission viewpoints through a disciplined approach to co-educate.
- Looks beyond a single system to the cyber vulnerabilities of system of systems (SoS) and family of systems (FoS) within the disciplined context of a specific mission thread.
- Aids in identifying vulnerable components and interfaces that can help focus supply chain risk management efforts.
- Defines the possible first steps 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.
- Identifies areas for improved operator, defender, and maintainer training.
- Identifies and characterizes potential mission risk from cyber effects.
- Aids in assessing contributing effects and impacts of supporting platforms, systems, and stakeholders in a mission context.

2.3.1 Intelligence Support

Cyber threat intelligence can inform each stage of the system engineering process. By understanding known adversary capabilities or intentions as well as what gaps lie within the intelligence community and what can potentially be exploited in the system, the program begins a feedback loop to iteratively either request key information from the intelligence community or to share CTT results with the intelligence community. The intelligence community can then look specifically at the areas explored in the CTT to inform the program in the future. With the increased intelligence knowledge of cyber threats, the program can reduce risk and advise system engineering and developmental testing of emerging systems. The CTT also facilitates the program's partnership with the intelligence community to inform 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 the 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 the intelligence analyst early in discussions about the system in the CTT process provides an opportunity for them 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:

- Technology – hardware, software, manufacturer, version
- Architecture – sub-systems, data flow, interfaces, functionality
- Mission – system purpose, intent, area of responsibility, operational dependencies, intended environments

2.3.2 Risk reporting

Prior to executing a CTT, the program must select or determine a risk methodology to guide the final reporting. Traditionally, the program reports risk using a five by five matrix, as described in NIST SP 800-30 (Reference (g)). The analysis associated with producing the matrices may involve varying levels of rigor that includes analysis of threats, vulnerabilities, and impact. The streamlined CTT process focuses on understanding the technical risks and associated mission impacts more than on the threat intent. However, since the process is tailorable, the program may also decide to integrate validated threat information. Ultimately, participants need to understand the analysis approach prior to starting a CTT. By "beginning with the end in mind," the program 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.

3 CTT Process

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

The four steps in a CTT are:

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

CTTs require a small team of personnel committed to performing all four steps and a larger group of participants (from the program and other organizations) that are involved mainly in Exercise Execution. Throughout this chapter, "Exercise" will refer to all Step 2 activities.

Figure 4 illustrates the four CTT steps along with their major activities and average number of calendar days to complete (based on past CTTs). Smaller programs will likely have shorter timelines. See Appendix B for several examples for how programs can use CTTs. The critical step for generating the 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 the data needed during Post Exercise Analysis produces a successful outcome for the program when presenting the results during Reporting (Step 4). The DoD intends for the CTT process to be adaptable and fit the needs of many different users.

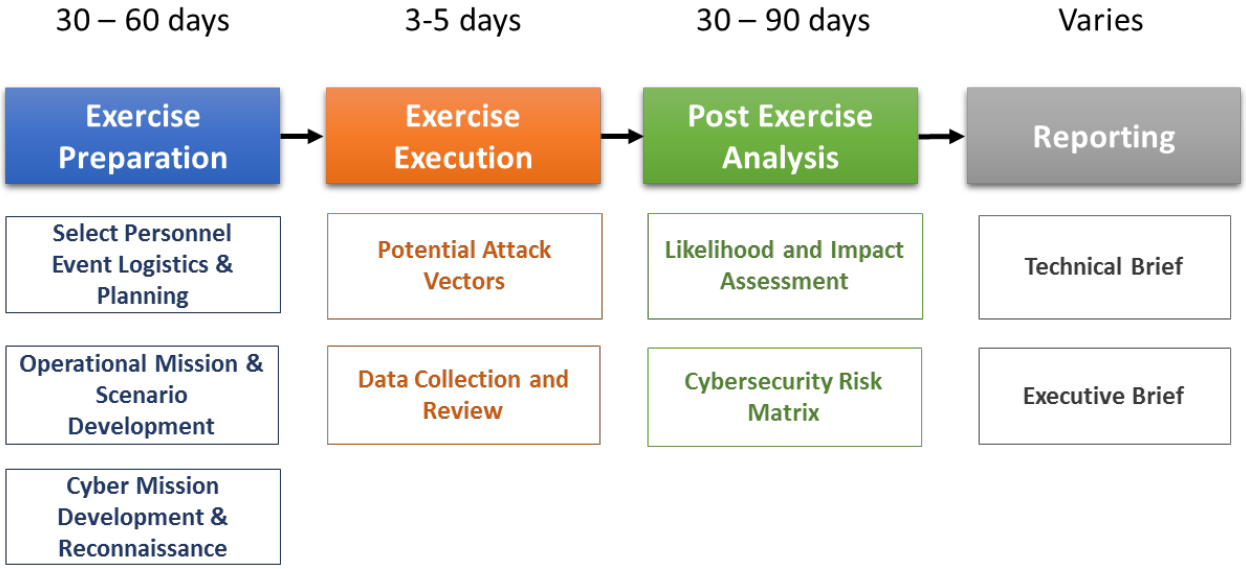


Figure 4. CTT Steps

3.0 Before Starting a CTT

The program's cyber working group or the program's lead for system security engineering will initiate the planning for a MBCRA. If a CTT is selected as the MBCRA methodology, then one of the program representatives will advocate for the CTT to program leadership to begin the

process. In order to conduct an effective CTT, the CTT advocate should ensure the program meets several conditions prior to beginning Step 1:

Obtained buy-in from program leadership. To earn leadership buy-in, the CTT advocate 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 leadership across the program's functional areas. Program leadership buy-in ensures resourcing (time, personnel) for the CTT is available.

Program Office approval, Program Office ownership of the process, and Program Office understanding of resource expectations. The program leads the CTT, provides information and documentation about the systems in scope, and determines the CTT schedule, manpower, and funding constraints. A successful CTT integrates both contractor or developer and government participation. Programs do not always plan for funding CTTs or include the necessary contractor support in their industry contracts, which can become an issue when acquiring essential information. See Appendix B, as well as the DoD Cyber T&E Companion Guide v3.0 (Reference (e)) for notional contract language for supporting CTTs.

Recruited an experienced CTT Facilitator. An experienced CTT Facilitator (see §3.1.1.1.2) has taken part in previous CTTs. The CTT Facilitator is prepared to guide the program leadership and CTT participants through the process by explaining the expectations of the Exercise and ensuring completion of the activities and products in each step.

Defined Operational Mission. The program will select a mission from the known missions the system supports, or from system provided functions. The mission selected depends on critical components of interest in the system under analysis. The possibilities range from an isolated mission for a single system to multiple missions executed in coordination with other platforms. (See §3.1.2.1.2).

Defined the intended subset of systems and interfaces that comprise the system under analysis 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 a FoS executing a common mission? Selection of the system under analysis determines factors such as duration, resources, and expertise of the participants in the CTT.

Determined the classification level of the CTT. The classification level constrains the cyber threat intelligence that can be shared, examined, and discussed in the CTT, and should be set based on the objectives for the CTT and the Program's Security Classification Guide (SCG). The classification level may also exclude some participants. For mature programs, the SCG, developed as part of the Program Protection Plan (PPP), describes the level of classification, distribution statement, ability to release the findings to foreign partners, and how to address cyber vulnerabilities discussed in the CTT and eventually documented in the report. Early in a program's life cycle, before finalizing the SCG, an agreement with the program for the CTT data and analysis results is necessary with respect to classification level, distribution statement, and to whom to release the information. Holding a CTT at the SECRET level, even if the program system engineering and testing documents are Controlled Unclassified

Information (CUI) or unclassified, protects the potential cyber vulnerabilities while their sensitivity is uncertain. The program should also consider the classification of the aggregation of potential vulnerabilities. The CTT Intelink Website (§1.2) has overarching SCGs available, that delineate generally how to handle cyber vulnerabilities, to provide guidance to programs that do not have a SCG.

Agreed upon and well-defined objectives (deliverables, timeline) for the CTT. The program 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.

Application of scientific test and analysis techniques (STAT). Including techniques such as design of experiments (DOE) can aid in structuring the CTT, analyzing its results and assessing risk (see https://www.afit.edu/STAT/). Recruiting subject matter experts (SME) early in the planning of the CTT can ensure the activities and products are designed with STAT best practices.

3.1 Step 1 – Exercise Preparation

Typically, a program takes between 30-60 days for this step. The major activities performed during Exercise Preparation are:

- Select the Team members
- Define the Team missions and enabling scenarios with systems in scope
- Prepare Initial Mission Impact Assessment Methodology
- Define Likelihood Assessment Methodology
- Collect the system documentation, or initiate open source reconnaissance for documentation
- Define and develop the plans and products

3.1.1 Exercise Preparation – Teams

Personnel participating in a CTT are part of one of these Teams as illustrated in Figure 5.

- Control Team
- Operational Team
- Cyber Opposing Force (OPFOR) Team

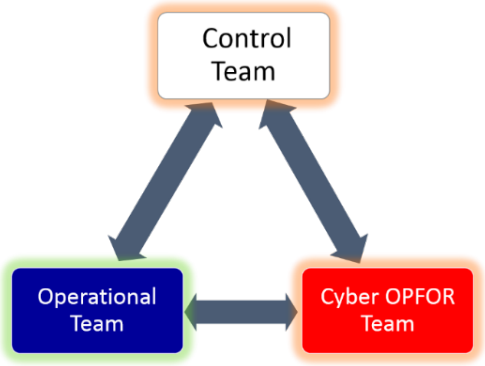


Figure 5. CTT Collaboration Diagram

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

The sub-sections below describe the roles in the CTT and the optimal personnel to consider for each Team. See Appendix B for a quick reference guide on the CTT Team Roles and Responsibilities. All participants must have the proper level of security clearance decided on by the Control Team.

3.1.1.1 *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. Assemble the Control Team early in Exercise Preparation, since they are 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 comprised of the Control Team Lead, CTT Facilitator (recommended for the program's first CTT), **Operational Team Lead** (see §3.1.1.2.1), **OPFOR Team Lead** (see §3.1.1.3.1), and Note Takers.

Other Control Team roles include Deputy Team Leads, Security Lead, Intel Lead, Data Analyst, and Analysis Lead. Keep the number of personnel to the minimum required and Control Team members can serve multiple roles, as desired.

3.1.1.1.1 Control Team Lead

The Control Team Lead has the overall authority and responsibility for the CTT. The Control Team Lead also represents the program and typically has a leadership role in the program sponsoring the CTT.

The Control Team Lead needs to have broad knowledge of the system and insight into the program's schedule and operational mission as well as the authority to ensure personnel from the program support the CTT.

3.1.1.1.2 CTT Facilitator

For a program's first CTT, a CTT Facilitator is helpful in supporting the Control Team Lead. 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 towards satisfying the program's objectives. 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.

3.1.1.1.3 Note Takers

The Note Takers record all relevant discussions during the Exercise, including who said what[1]. This guide recommends that the CTT use at least four Note Takers. This guide also recommends having the Note Takers attend the first Post Exercise Analysis (Step 3) meeting.

3.1.1.1.4 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). This guide recommends an analytic, detail oriented, and organized individual that understands cyberspace attacks for this role.

Analysis Lead: directs the 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, and ensuring the products are within the CTT's scope and time constraints. The Analysis Lead serves on both the Control Team and either the OPFOR or Operational Team.

Control Team Deputy Lead: handles management, logistics, and administrative tasks throughout the CTT.

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

Intel Lead: supports the collection/coordination of intelligence information on known nation

[1] The Control Team may choose to assign all CTT participants an identification number they can call out when speaking during the Exercise to aid the Note Takers.

state offensive cyberspace capabilities and known cyber tactics against the system under analysis.

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:

- Chief developmental tester
- Lead test engineer
- System lead engineer
- System security engineer
- Other engineers familiar with 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 and/or with the system(s) under analysis
- OTAs
- Cybersecurity SMEs
- Prime contractor representatives/systems developers
- STAT/DOE SMEs

3.1.1.2 *Operational Team*

The Operational Team consists of the planned users, defenders, and maintainers of the system responsible for executing their mission (including cyber defensive operations, and system maintenance). This team also includes the engineers and developers that will describe the technical design features and system capabilities for the OPFOR Team. The Operational Team develops the Operational Mission (§3.1.2.1), the System Documentation (§3.1.3) and system(s) overview brief(s) (§3.1.4.2) for the CTT. To plan a realistic and effective Operational Mission, the Team should have knowledge in the following areas:

- The system design, interfaces, and communication paths or data flows in support of the Operational Mission
- The current and planned tactics, techniques, and procedures (TTPs) for the operators and the system under analysis used to accomplish the intended mission
- The current "as is" system capabilities and future "to be" system capabilities, if applicable
- The pre-mission planning, post-mission debrief, and maintenance activities and systems, as applicable
- The current system acquisition and test planning

Identify the Operational Team members during Exercise Preparation. The Operational Team Lead may decide to have these members collect material and develop briefings. The size of the Operational Team will depend upon the system(s), network(s), sensor(s), etc. in scope for the CTT.

3.1.1.2.1 Operational Team Lead

The Operational Team Lead, designated by the Control Team Lead, supports all four steps and is responsible for planning the Operational Mission (§3.1.2.1), System Documentation (§3.1.3) and ensuring the Operational Team deliverables are within the CTT time constraints. The Operational Team Lead serves on both the Operational and Control Teams. The Operational

Team Lead should have operational knowledge and experience relevant to the systems and missions in the CTT.

3.1.1.2.2 Operational Team Members

The scope of the systems involved in the CTT should drive the selection of CTT personnel for the Operational Team. Personnel to consider for the Operational Team (by the Operational Team Lead) include, but are not limited to, the following:

- Military and civilian personnel with required operational or functional experience from DT and OT organizations, reserve organizations, or from the operational user and test communities
- System operators or end users
- Personnel with weapons and tactics experience relevant to the mission
- Organizations involved with the system development
- Maintainers (e.g., intermediate, organizational, and depot level)
- Engineers familiar with the differences between the current "as is" and "to be" state of system(s) of interest (hardware, software, and support equipment)
- Subsystem SMEs (e.g., radar, networks, satellite communication)
- Anti-Tamper SMEs
- System Security Engineers and Program Protection SMEs
- Safety SMEs
- Logistics and sustainment SMEs
- Cybersecurity service providers (CSSPs) or network defense personnel for the system under analysis
- Cybersecurity SME, ISSM

The program cybersecurity SME can ensure the Operational Mission (§3.1.2.1) execution details and Operational Team products (such as the system brief and architecture documentation) are sufficient for subsequent discussions in Exercise Preparation with the OPFOR Team. Participants in the above list can include personnel from industry (e.g., prime contractors or subcontractors).

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

3.1.1.3 *OPFOR Team*

The OPFOR Team develops attacks to achieve the OPFOR Mission (§3.1.2.3) for the Exercise. The OPFOR Team does not have to be large to be effective. A diverse OPFOR Team with broad offensive and defensive cyber testing or cyber operational warfare backgrounds provides the opportunity for proposing a variety of potential attacks. The OPFOR Team should be familiar with publicly known software weaknesses: common attack patterns (Common Attack Pattern Enumeration and Classification (CAPEC), (Reference (k)), information-security vulnerabilities (common vulnerabilities and Exposures, (Reference (l)), common weakness enumerations, (Reference (m)), and the National Vulnerabilities Database (NVD), (Reference (n)).

The OPFOR Team Lead may choose to coordinate with the OPFOR Team members during Exercise Preparation to perform open source reconnaissance (§3.1.3), mission planning, and

attack surface analysis activities. The recommended size of the OPFOR Team is 4-8, but the size may depend upon the availability of people with the desired cybersecurity expertise and the technologies in scope.

3.1.1.3.1 OPFOR Team Lead

The OPFOR Team Lead, designated by the Control Team Lead, supports all four steps and is responsible for planning the OPFOR Mission (§3.1.2.3) and the cyberspace attacks that drive the Exercise. **The 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 program**. Appendix B describes the importance of the OPFOR Team Lead in the CTT and his/her responsibilities throughout all four steps in detail. The OPFOR Team Lead must have a background in defensive and offensive cyber and have participated in previous CTTs. The OPFOR Team Lead also needs to be an effective communicator who can explain cyberspace attacks from the perspective of an operational user. The 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 OPFOR Team Lead serves on both the OPFOR and Control Teams.

3.1.1.3.2 OPFOR Team Members

Personnel to consider for the OPFOR Team include the following:

- Authorized cyber team penetration testers and Operational Test Agency Representatives (e.g. National Security Agency (NSA)-certified Red Team)
- Certified ethical hackers (contractors or government personnel), (personnel with other offensive certifications are equally desirable)
- Defensive and offensive cybersecurity SMEs
- Cyber developmental testers/analysts (those aligned to test for the program and others)
- Cyber range (DoD, national or commercial) personnel
- Electronic Warfare testers
- Interoperability engineers
- CSSPs or network defense personnel for the system under analysis
- System engineers or testers

The use of personnel from academia (such as professors or graduate students at military service postgraduate schools or war colleges, service academies, or research universities) with relevant offensive and defensive cyber certifications could be considered and may have the added benefit of familiarity with DoD systems.

A member of the program's or developer's systems engineering or DT team should also be part of the OPFOR Team to assist OPFOR Team members with understanding the systems and subsystems under development that will carry out the Operational Mission (§3.1.2.1) and to help the Operational Team members during the Exercise when the OPFOR Team is explaining cyberspace attacks.

3.1.2 Exercise Preparation – Team Missions

The Operational and OPFOR Team Leads define and document their respective Missions for

the CTT and then the Control Team reviews and approves. Develop the Operational Mission before the OPFOR Mission, because the OPFOR Team Mission will target the Operational Team Mission.

3.1.2.1 *Operational Mission*

The Operational Mission is a specific mission featuring the system under analysis. Most systems support multiple different missions and functions. Missions may range from an isolated mission with just one single system (e.g., transporting equipment and personnel between locations), to missions that are 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, command and control).

Program artifacts, such as the requirements documents, engineering plans, PPP, Test Evaluation Master Plan (TEMP)/Test Strategy, or Department of Defense Architecture Framework (DoDAF) views (e.g., the Operational View - 1 (OV-1) is the "High-Level Operational Concept Graphic"), if available, support Mission development. These documents holistically provide a description of the subset of systems and interfaces for the various missions the system under analysis supports. See System Reconnaissance (§3.1.3) for more information about system documentation. Figure 6 is an example OV-1, which depicts the systems and networks that comprise the system under analysis.

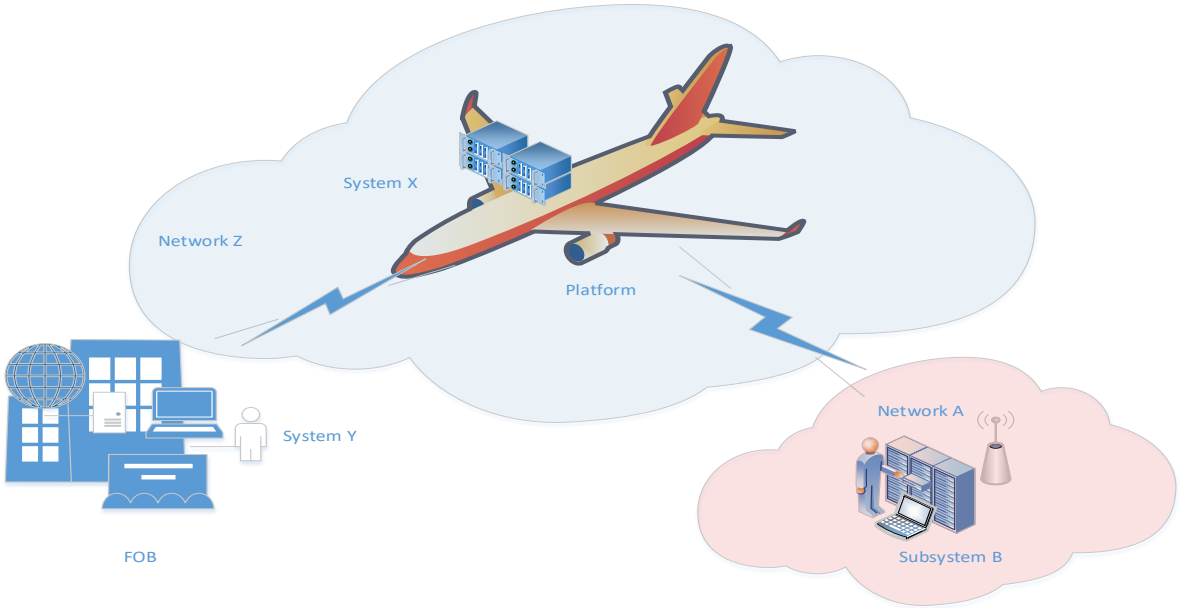


Figure 6. Example OV-1 Graphic Displaying the Sub-Systems Under Analysis in the CTT

The range of Operational Missions can be:

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

EXAMPLE OPERATIONAL MISSION

Platform Z will support a 2-day training mission using System X

The Team develops the Operational Mission early in Exercise Preparation since the OPFOR Mission is dependent on the mission specified for the system under analysis. 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 OPFOR Teams due to expertise needed and stakeholder interest.

3.1.2.1.1 Preparation for Analysis – Prepare the Initial Mission Impact Methodology

In preparation for guiding the discussions of mission impact during Exercise Execution (Step 2), the Control Team should develop an initial Mission Impact Methodology. The Operational Team will further refine the methodology during the team's breakout in Exercise 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 program prior to Preparation) to use for reporting 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 7 is an example Mission Impact Methodology. The columns depicted may not apply to all CTTs, and there is no requirement to have a specific number of columns, nor to complete criteria for every row for impacts 1-5. Operational Teams should determine the appropriate columns and the corresponding criteria for what constitutes at least Fully Mission Capable, Partially Mission Capable, and Non-Mission Capable according to the system under analysis and associated mission and scenario.

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

Figure 7. Mission Impact Methodology Notional Example

The Mission Impact Methodology enables consistency when assessing the overall CTT Operational Mission or Mission Essential Functions. The Control Team will attempt to represent which is most appropriate based on the program's objectives in the initial draft 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). Adjustment of the Mission Impact Methodology is performed during Execution (Step 2) and the methodology is finalized in Post Exercise Analysis (Step 3) (§3.3.2.2.1).

3.1.2.1.2 Selecting Systems in Scope for the Operational Mission

The choice of the subsystems included in the system under analysis limits potential cyberspace attacks to select interfaces, subsystems, FoS, or SoS under consideration in the CTT. Although the program should decide the scope of the system under analysis prior to starting a CTT, the program may identify additional systems during the Operational Mission development to include or exclude. Exploring interfaces beyond the program's authorization boundary and span of control may not be feasible. The Control Team must consult the system SMEs to ensure correct interpretation of all of the system information when narrowing down the critical components of interest in the system under analysis. Some interfaces and subsystems not included in the scope of the first CTT may require additional CTTs to address them. The Team must thoroughly explain assumptions regarding interfacing systems outside of the program's authorization boundaries.

EXAMPLE SYSTEMS IN SCOPE AND ASSUMPTIONS

System X, Subsystem Y, and Network Z are in the scope of the CTT, but Network A and Subsystem B are not in the scope.

3.1.2.2 *Operational Scenario*

The Operational Scenario acts as the backdrop for the CTT 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.

Not all programs 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 resource or financial management support, planning a mission, maintaining a critical system, and so on, 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 conflict breaks out and how threats may have effects in such a circumstance. Alternatively, related systems under analysis (non-warfighting and warfighting

systems) or routine operations can form the basis of a relevant scenario for a CTT.

3.1.2.2.1 Factors to Consider for the Operational Scenario

Area of Operations: The Scenario can be set in a real (e.g., in the U.S., outside the U.S.) or fictitious geographic area. A fictitious location avoids any political sensitivities of warfare planning that involves potential adversaries, but may require extensive preparation in developing the fictitious area compared to using an actual location.

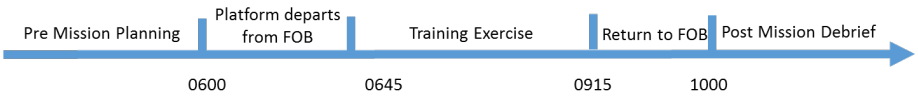
Real geographic areas make it easier to identify actual distances, choke points, facility sites such as airfields and bases, current task force organizations, the location of the potential enemy forces and specific intelligence information. However, using too specific of an area could result in a set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

EXAMPLE SCENARIO AREA OF OPERATION

The Platform will depart from forward operating base A each day and proceed to the designated training range airspace. The training mission will begin when the platform has reached 30,000 feet in altitude in the training range. The training mission will end when the platform departs the training range, successfully returns to forward operating base A and the crew performs post mission debrief.

Schedule/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



The Platform will depart from forward operating base A each day at 0600 and should arrive at the training range by 0645.

Duration: Execution across hours, days, or months may lead to the discovery of other cybersecurity vulnerabilities or opportunities for cyberspace attacks not previously identified. Possibilities include executing one task over a short timeframe, executing multiple tasks that could take place over more than one crew cycle, tasks during watch standing (day/night), or tasks when systems are undergoing maintenance.

EXAMPLE OPERATIONAL SCENARIO DURATION

The training exercise will last approximately 2-3 hours each day and the crew will spend 45 minutes in transit to and from the training range.

Weather: The Scenario can include varying weather conditions such as rain, sleet, fog, chemical attacks, and airborne pollutants. A detailed weather overlay could be included as part of the preparation of the battlefield for mission planning. This could help the Operational and OPFOR Teams discuss the potentially magnifying effects different weather conditions could have on successful cyberspace attacks.

EXAMPLE OPERATIONAL SCENARIO WEATHER

The scenario assumes cold temperatures and clear skies.

Operational Assumptions: State any assumptions that bound the scenario and the discussions about the system(s). These may include the level of readiness of the systems (such as level of maintenance and personnel training), political climate, the importance of the mission, and if a state of war exists. The scenario may begin with an order from a higher authority down to the unit represented by the Operational Team.

EXAMPLE OPERATIONAL SCENARIO ASSUMPTIONS

The scenario assumes a peacetime training mission, fully functioning operational equipment to support the mission, trained and experienced operators, and explicit trust between the operator and Platform Z.

3.1.2.3 *OPFOR Mission*

The OPFOR Team Lead defines the OPFOR Mission as an overarching objective to prevent the success of the Operational Mission.

EXAMPLE OPFOR MISSION

Employ offensive cyber operations in combination with electronic warfare operations to prevent success of Platform Z's training mission.

The OPFOR Team Lead defines a series of specific cyberspace attack missions across a typical cyberspace attack kill chain that are intended to deny, disrupt, or degrade the Operational Mission (§3.1.2.1) for the system under analysis, directly or indirectly (e.g., through deception or destruction), or various other objectives as defined by the OPFOR Team Lead. See Appendix B for a description of an attack kill chain. See System Reconnaissance (§3.1.3) for more details

about the documentation provided for the system under analysis.

The objective of each cyberspace attack mission usually focuses on a class of attack methods and their effects. Below are examples of tailorable Cyber OPFOR Mission Objectives. Tailoring may be to the specific system under analysis, the Operational Mission, or the objectives for the CTT. Later in the CTT, the OPFOR Team will develop specific attacks and variants of attacks to achieve the OPFOR's 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 OPFOR Team may consider emulating 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. Team members should first assess methods and techniques at the lowest level necessary (i.e. low-hanging fruit) to accomplish the OPFOR Mission. The 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 Team should define TTPs the OPFOR may employ, describe assumptions that bound the allowed TTPs, and include the level of the adversary and the level of covertness of the OPFOR Team. The OPFOR Team needs to know whether their actions must remain covert throughout, or can become overt at some time during the Exercise.

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 examples are to cause system malfunctions or mimic indicators of a malfunction that are indistinguishable from maintenance malfunctions. Successful cyberspace attacks are not only

EXAMPLE OPFOR TTPs

Supply chain manipulation of hardware and software
Exploitation of vulnerabilities in components, sub-components, and maintenance systems (from positions in lateral systems)
Unwitting insider exploitation via social engineering
Complicit insider exploitation via low level support staff
Electronic warfare (e.g. jamming to create opportunities for cyber effects)

because of the magnitude of the effect, but also because of the level of covertness achieved and maintained.

The Team should outline assumptions regarding the reconnaissance information (§3.1.3), weaponization efforts, and access to networks, as well as determine whether the cyberspace attacks can be used in conjunction with other weapons such as missiles or electronic warfare.

EXAMPLE OPFOR ASSUMPTIONS

The OPFOR will attempt to stay covert when employing cyberattacks.
The OPFOR has the capabilities and resources of a nation state actor.
The OPFOR has a presence on Network A. Network A is a potential OPFOR attack vector.

3.1.2.3.1 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 the Likelihood Assessment Methodology. The OPFOR Team will use the methodology during the Team's breakout 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 (typically scaled 1 to 5) that aligns to the risk matrix or risk assessment methodology (selected by the program prior to Exercise Preparation (Step 1)) to use for reporting the CTT results. Typical likelihood assessments consider factors such as the (1) cost and (2) success of an attack. One common approach is using a three-dimensional rubric

		Attack Success Likelihood		
		Low	Medium	High
Attack Cost/ Level of Effort		Rarely works	Sometimes works	Always works
Nearly anyone can build: Nascent – Limited threat	Low cost or easy to develop	3 Example: Network DoS	4	5 Example: Flash implant delivered via website/email
Criminal level organization can build: Moderate threat	Moderate cost or many can develop	2	3	4
Nation state organization can build: Advanced threat	High cost or hard to develop	1 Example: RF inject of malware into sensor or radio	2	3 Example: Supply chain implant in HW or firmware

Figure 8. Likelihood Assessment Methodology Notional Example

depicted in Figure 8 to assess the technical feasibility for each cyberspace attack using the criteria "level of effort of the attack" (row, Attack Cost/Level of Effort) and "likelihood of the attack successfully working if it were developed and launched" (column, Attack Success Likelihood). Several databases for common cyberspace attacks (e.g. CAPEC, Reference (k)) exist and may help to supplement or validate the chosen Likelihood Assessment Methodology.

The likelihood of a successful cyberspace attack may depend on certain assumptions, accesses, or conditions. When the 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 OPFOR Team's initial likelihood assessment. The OPFOR Team Lead presents and explains the Control Team defined Likelihood Assessment Methodology during the OPFOR Mission brief in Exercise Execution (Step 2). See Post Exercise Analysis (Step 3) (§3.3.2.2.2) for further discussion on the application of the Methodology.

3.1.3 Exercise Preparation – System Documentation and System Reconnaissance

A program can perform a CTT at any point in the system development life cycle. If the system design is still immature, then comprehensive system documentation may not be available. In this case, the program may need to define some assumptions or provide surrogate designs to use during the CTT. The Control Team is responsible for gathering the system information and providing it to both the Operational and OPFOR Teams. The program should provide the Operational Team Lead with a system expert for each system in scope. That system expert develops a system overview to present at Execution (Step 2). Collecting reconnaissance on a system is the first step in any attack kill chain for staging a cyberspace attack. See Appendix B for a description of an attack kill chain. The Control Team may decide to create a Reconnaissance Team to conduct initial, open-source system cyber reconnaissance by reaching out to service war colleges and research labs, Federally Funded Research and Development Centers, or University Affiliated Research Centers; however, this will add time to Step 1. Alternatively, the Program, contractors, or developers involved in the CTT can gather and provide the relevant system documentation, guided by the OPFOR Team Lead's requests for documentation, and develop the system overviews. See the Data Handling Plan (§3.1.4.1.3) for details about sharing system documentation.

If the Team pursues reconnaissance, the system briefs are still required and full system documentation (see §3.1.3) should still be provided to the OPFOR. A 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 §3.1.4.2.2). The system reconnaissance information could include system engineering specifications, diagrams, hardware and software inventories, DoDAF artifacts, architectural and interface diagrams, Capability Development Documents, TEMPs, and Concepts of Operations (CONOPS) guidance. The level of detail should be representative of the data that might be obtained given the level of expertise, timeline, and resources of the adversary that the OPFOR Team is emulating (e.g., a near-peer nation will have more resources and intelligence collection capabilities than hacktivists and small criminal organizations).

If necessary documentation (e.g., design, CONOPS, etc.) is not available due to the system design's immaturity, then the Control Team and the program must develop representative documentation as a model for the expected design or CONOPS. In many cases the documentation is proprietary and sensitive, therefore the Program should have the participants sign a non-disclosure agreement (NDA) (§3.1.4.1.1).

Do not bombard the OPFOR Team Lead with too much system detail. The program or representatives for the systems and networks in scope of the Operational Mission must extract the high-level details to present as system briefs to the OPFOR Team Lead. Below, and on the CTT Intelink Website (§1.2), is a summary of minimum system documentation typically needed for a CTT:

For each system, the brief may include:

- System overview
    - Mission
    - Functions
    - System Diagrams (architecture, pictures)
    - Functional overview - data flows/messages
    - System configuration/network diagrams
    - Connections to other components (internal, external)
- List of software (commercial off-the-shelf/government off-the-shelf) and hardware
    - Versions (OS, applications)
- Maintenance
    - Software, firmware, hardware
        - Refresh cycle
        - Update frequency
        - Maintenance process
    - Restart and reload times
- Known vulnerabilities (not being remediated)
- System protections
- Physical protections
- Describe or depict how system contributes to operational mission

The OPFOR Team Lead and/or program's interoperability and systems engineers review the reconnaissance gathered and confirm there is sufficient information on the system under analysis provided in the documentation. The OPFOR Team Lead may request supplemental documentation and diagrams to develop better knowledge of the system under analysis or instruct the OPFOR Team to complete separate, open source reconnaissance based on the Operational Mission and System Scope.

Figure 9 is a flow chart summarizing the system reconnaissance and documentation process. Depicted are those tasks that should always be conducted (left, solid lines) and optional tasks (right, dotted lines) in the CTT.

The OPFOR Lead may also ask the Team members to perform open source reconnaissance on components of the system, the system, and/or the developer/supply chain. This may inform the OPFOR Mission, developing specific cyberspace attacks against the system(s) in scope, or

OPFOR Team assumptions and TTPs.

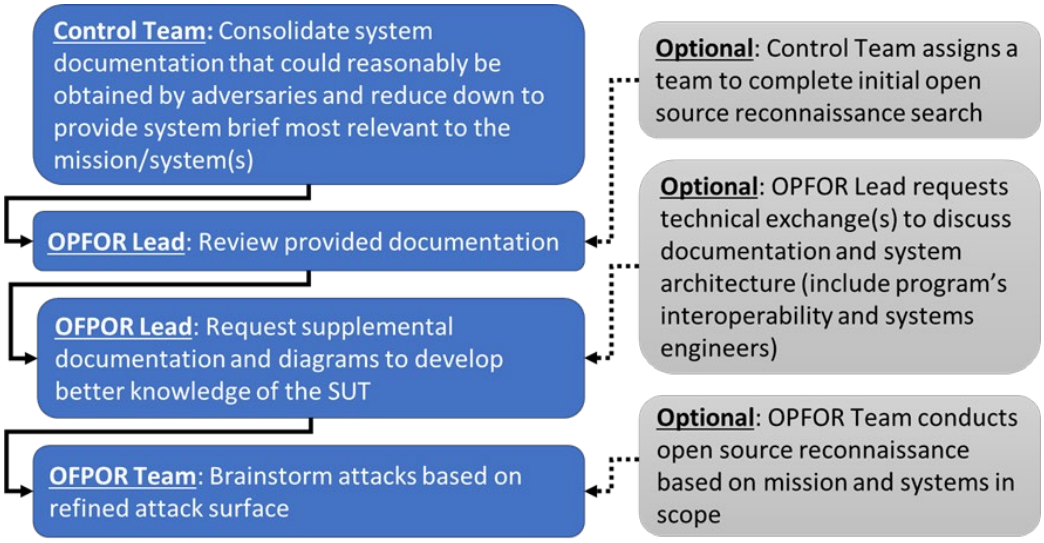


Figure 9. CTT System Reconnaissance and Documentation Process

3.1.3.1 *Technical Exchange Meetings and Site Visits*

A series of technical exchange meetings (TEMs) with select participants are critical in helping with the preparation planning between the program engineers and Team Leads. This ensures distribution of technical information early in the CTT and participants have sufficient time to read and process it before the Exercise. Examples include the following:

1. If possible, arrange a tour of the equipment/laboratories of the system under analysis in the CTT. The participants' first-hand interaction provides context during the Exercise.
2. Hold information sessions to educate the Team Leadership, Analysis Lead, Data Analyst, and Note Takers on the objectives, deliverables, schedule, overview, and breakdown of the activities prior to the Exercise. This 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 system(s) under analysis, schedule regular meetings to allow adequate time to prepare the participants.
3. It is advisable to present system(s) under analysis (as-is/to-be) briefs a separate session from the CTT when there are a large number of systems in scope, such as for a FoS CTT. This allows the OPFOR Team the opportunity to ask about in-depth technical details of the engineers without immersing all participants, such as operators, in the technical specifics. Assigning technical engineers to the OPFOR can also address this need without having a separate meeting.
4. Prior to the Exercise, the Security Lead may provide instructions to the Note Takers for properly marking classified materials.

The OPFOR Lead and Team use these TEMs with the engineers, contractors, and system 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 CTT Execution (Step 2) may result in the OPFOR being more focused on technical networking, protocols, applications, hardware, software, and firmware rather than on the operational mission. Common questions the

OPFOR may ask during a TEM are:

- What hardware is being used on this system?
- What operating systems are installed on these systems? This includes service packs and versions.
- What software is installed on each of these systems?
- What services and/or open ports are running on each of these systems?
- How are these systems normally accessed for operations, troubleshooting, or maintenance?
- With which devices does each system communicate? How do they communicate?
- What would be the impact of the mission if each system was brought to a degraded or failed state?
- How often are these systems patched?
- Do these systems reside in secured spaces?
- Do these systems have any external USB ports or CD/DVD drives?

3.1.4 Exercise Preparation – Plans and Products

During Exercise Preparation, the Control Team plans and creates products necessary for the Exercise. This guide recommends constructing a Plan of Action and Milestones (POAM) to track all the tasks throughout the CTT and assign personnel responsible for completing each task. An example POAM spreadsheet is available on the CTT Intelink Website (§1.2).

3.1.4.1 *Pre-Execution Plans*

3.1.4.1.1 Non-Disclosure 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 prior to sharing proprietary system information. Ensure all participants sign the agreement(s), as required, prior to the start of the Exercise. Programs are encouraged to have the developer or the program's legal division provide input. Basic NDA templates are available on the CTT Intelink Website (§1.2).

3.1.4.1.2 Rules of Engagement

The Control Team develops the Rules of Engagement (ROE) for the CTT to inform all participants of what behaviors are encouraged or discouraged during the Exercise.

Example ROEs include:

- Non-disclosure
- Non-attribution
- Non-retribution
- No side bar conversations
- No interrupting
- ELMO: Enough, Let's Move On

If necessary, the Team can also create ROEs specific to the Operational, OPFOR, and Reconnaissance Teams (if used).

3.1.4.1.3 Data Handling Plan

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 step of the CTT. 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 prohibited material
- Guidelines for banner and portion markings
- Classification authority and relevant details
- On site security point of contact (POC) and expectations for the generation ofclassified data by participants
- Security-reviewed plan for storage and transmission of classified data, briefs, and reports, both digital and non-digital, designated with who is responsible for coordinating resources and/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 Secret Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System, or classified spaces to review and refine the documentation, despite having clearances. The Control Team defines the processes for sharing the information and documents the processes in the Data Handling Plan. Table 1 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 1. Example Table for Tracking Data or Products Produced in CTT

	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	CDs, Courier, or Shared repository					
Storage Location	Digital or Physical					
Contact POC	On site Security Lead					

3.1.4.1.4 Planning the Day of the Exercise

Rooms: Reserve a room that accommodates all participants at the appropriate classification level and contains any necessary audio/visual equipment for presentation graphics. Also, make sure to reserve separate rooms for Team Breakout Sessions (§3.2.1.3) during the Exercise.

Leadership Welcome: Plan to have program leadership welcome the CTT participants, offer support, and emphasize the importance of the results. In addition, leadership has 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. The program must request this support from the appropriate intelligence organization or program intelligence liaisons. Additionally, a relevant threat brief that provides examples of adversary TTPs and security breaches 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.

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 OPFOR Team Lead, to help with understanding and visualization of cyberspace attacks presented by the OPFOR Team.

Note Taker Supplies: Plan for Note Takers to either handwrite notes or use laptops at the appropriate classification level.

3.1.4.2 *Pre-Execution Products*

3.1.4.2.1 Schedule and Agenda

The Control Team prepares a schedule of events for the Exercise. This includes an agenda for the first day of the Exercise (the Kickoff (§3.2.1)), where key personnel present a series of informational briefs to all participants.

3.1.4.2.2 Kickoff Briefs

The Control Team creates the following briefs that they will present at the Exercise Kickoff:

Administrative Welcome: Administrative details including the building, food, and schedule. Also informs participants of the Note Takers' role.

CTT Overview: 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 time 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: Presents the rules for the participants and Teams in the CTT that are designed to endure an orderly, objective, and productive exercise (§3.1.4.1.2).

Classification Level, Data Handling Plan, NDAs: The Security Lead reviews the classification levels and procedures for handling/storing documents during the Exercise. Participants should be reminded to precede known classified statements with an announcement of the classification level (§3.1.4.1.3).

System Description: As mentioned in §3.1.3, a brief is required with background information on the system(s) under analysis or the system(s) within the scope of the Operational Mission. Place emphasis on critical data exchanges between systems and interfaces across networks. The briefing should allow time for technical questions by the OPFOR Team. As noted in §3.1.3.1, a separate meeting may be planned in advance of the Kickoff to deep dive into the technical details of the system, especially if the System Description Briefs alone would require 1-2 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 DoDAF artifacts, other descriptions that illustrate the capabilities/systems that are part of the program of record, interface control documents, system engineering 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 OPFOR Team Lead will become more familiar with the relevant Operational Mission activities for the system under analysis and will likely identify additional desired details to include in the System Description.

Operational and OPFOR Team Missions: The Team Leads describe their respective Team Missions, assessment methodologies for mission impact and likelihood, and present the Teams' tasks for the breakouts and Exercise.

3.1.5 Execution Preparation - Exit Criteria

The CTT is ready for Exercise Execution (Step 2) when the Control Team meets the following conditions:

- All lead roles assigned (e.g., OPFOR Lead, Security Lead, Analysis Lead)
- All participants are invited and provided read-ahead material
- Operational Mission and Scenario and OPFOR Mission developed and approved
- Initial Mission Impact Methodology developed
- Likelihood Assessment Methodology developed and approved
- Reconnaissance on system under analysis completed and summarized
- Data Handling Plan developed and approved
- Exercise facilities reserved and equipped with supplies
- All briefs are finalized

3.2 Step 2 – Exercise Execution

This step usually takes place over a period of 3-5 days. The major activities performed during Exercise Execution are:

- Kickoff of the Exercise
- Execute the CTT Exercise
- Collect the Data and Review

The entire Exercise nominally takes 3 days to complete, but it is an adaptable process that can span several days (for complex scenarios) or be split into two separate events (e.g., if limited by the availability of key participants). Appendix C contains two example CTT Exercise

Execution Agendas, one for an Exercise planned for three or more consecutive days, and one for an Exercise with a separate Kickoff scheduled well in advance of the main CTT Exercise. Appendix C also provides a collection of exercise support planning information containing best practices gleaned from past CTTs.

3.2.1 Exercise Execution – Kickoff

The Kickoff takes place over 1-1.5 days and sets the stage for the CTT. Since 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 in advance (2-4 weeks) of the main CTT Exercise allows for technical clarifications and refinement of the details in the Operational Scenario (§3.1.2.2) and OPFOR Mission (§3.1.2.3). In addition, the Control Team might schedule tours of the system prototypes, example environments, support equipment, test facilities, or development laboratories for the system under analysis during this time. Later, at the main CTT Exercise, the Control Team presents the updated Kickoff briefs and the intelligence brief.

3.2.1.1 *Pre-Exercise Meeting "Day 0"*

If possible, arrange for the Control Team to meet at the location of the CTT a day prior to the Exercise. This 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 test out audio/visual equipment to make sure it is in working order. The Control Team Lead and/or CTT Facilitator can also use this time to meet with the Note Takers to provide guidance about their role and instructions on classification markings.

3.2.1.2 *Kickoff Briefs*

As previously described in §3.1.4.2.2, the Exercise Kickoff begins with a set of briefs delivered to all the participants. The typical briefs presented are:

- Program Leadership Welcome
- Administrative Welcome
  - Presenter: Control Team Lead/Deputy
- CTT Overview
  - Presenter: CTT Facilitator/Control Team Lead
- CTT ROE – 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/Control Team
- Operational and OPFOR Team Missions
  - Includes team assessment methodologies and draft Team tasks (to be completed in Team Breakout Sessions)
  - Presenters: Operational Team Lead and OPFOR Team Lead

3.2.1.3 *Team Breakout Sessions*

After the Kickoff Briefs, the Operational and OPFOR Teams meet separately to complete their Team tasks. The Operational Team details the sequence of actions to execute the Operational Mission (§3.1.2.1) and the OPFOR Team plans plausible cyberspace attacks to execute the Cyber OPFOR Mission Objectives (§3.1.2.3). During the breakout sessions, the Operational and OPFOR Teams independently refine products they will subsequently present to the rest of the CTT participants.

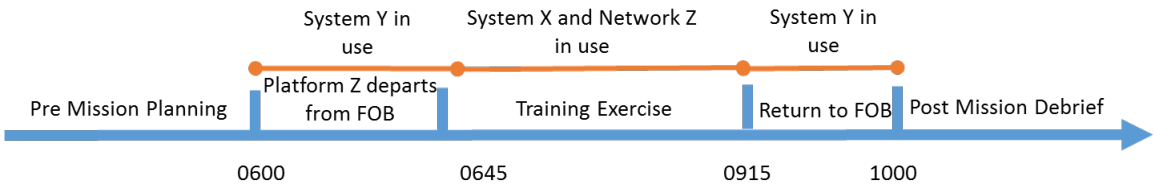
3.2.1.3.1 Operational Team Breakout

The Operational Team's objective for the breakout session is to develop the sequence of mission essential tasks, functions, communications, or 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 system under analysis. Ideally, the Operational Team specifies the systems, interfaces, data flows, and protocols critical to accomplishing the Operational Mission. The Operational Team will also develop the sequence of maintenance actions.

The Operational Team should discuss the initial Mission Impact Methodology (Figure 7) and ensure they agree with or modify what "partially mission-capable" or "not mission-capable" means for the system under analysis. The mission impact criteria should identify specific parameters that indicate mission failure. See Mission Impact Methodology §3.1.2.1.1 for more details. The explanation of the planned Operational Mission supports the OPFOR Team's development of cyberspace attacks. The cybersecurity SME that is part of the Operational Team should help define the level of detail sufficient for later discussions about vulnerabilities.

The Operational Team develops a brief that provides updates to the Mission Impact Methodology and documents how all operators would complete each step of the Operational Mission. This brief should also describe how the mission employs the system under analysis. The Team also provides a basic visualization and description of the mission plan, including the sequence of actions (e.g., interfaces and data flow) that occurs between pre-mission planning and maintenance to post-mission debriefs.

EXAMPLE OPERATIONAL TIMELINE



with associated sequence of actions that take place during each segment of time

3.2.1.3.2 OPFOR Team Breakout

The OPFOR Team's objective is to develop a list of potential exploitation pathways to execute the OPFOR Mission, based on the System Reconnaissance (§3.1.3) for the system under analysis.

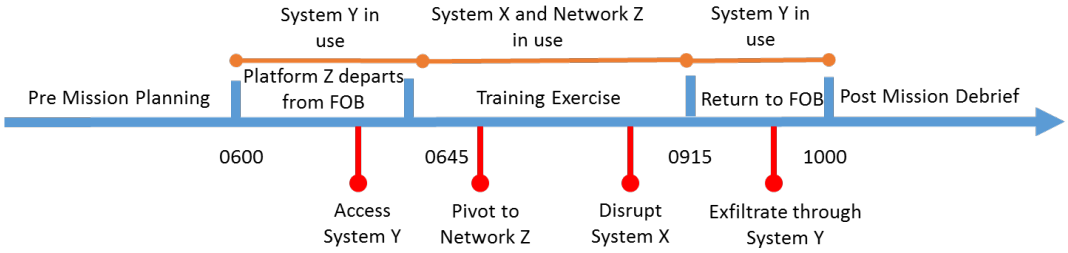
The OPFOR Team reviews the high-level network diagrams and the Operational Mission (§3.1.2.1) and Scenario (§3.1.2.2). The system engineer/tester should provide mission-relevant input during the OPFOR cyberspace attack planning.

The OPFOR Team Lead may provide the OPFOR Team with a format to develop their attacks. Example templates for OPFOR products are available on the CTT Intelink Website (§1.2). 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 to include the initial likelihood assessment using the Control Team-approved Likelihood Assessment Methodology (Figure 8). 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 will be used 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 OPFOR Team proposes multiple cyberspace attacks for each OPFOR Mission (§3.1.2.3). The cyberspace attacks should be logically plausible and based on the technical data provided, but not necessarily tested and proven to work. The OPFOR Team should aim to determine a set of cyberspace attacks that address every part of the TTPs for the Operational Mission. The 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 (Appendix B) 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 result in potentially a greater mission impact. Presenting each attack independently supports reuse of kill chain elements and identifying 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 OPFOR Team, the Team can digitally document the proposed attacks in the Analysis Table (Appendix D), for use later in Post-Exercise Analysis (Step 3). A downloadable and tailorable template for the Analysis Table is on the CTT Intelink Website (§1.2). Regardless, the Note Takers will capture the presented proposed cyberspace attack details and ensuing discussions.

EXAMPLE OPERATIONAL TIMELINE with OPFOR Attacks



3.2.2 Exercise Execution – CTT

The CTT Exercise takes place after the Kickoff and usually lasts 1-3 days. The Operational Team presents their brief, developed during the breakout session, to all the participants. It describes the detailed mission execution plan and an update of the Mission Impact Methodology (Figure 7). Then the OPFOR Team presents their proposed cyberspace attacks, describing the Cyber Opposing Mission Objective (§3.1.2.3), the specific system targeted, likelihood assessment, any assumptions made, and when the attack could be executed. The OPFOR Team Lead drives the CTT by introducing each new OPFOR Mission as the participants work together collaboratively talking through the sequence for all the related cyberspace attacks (Figure 10).

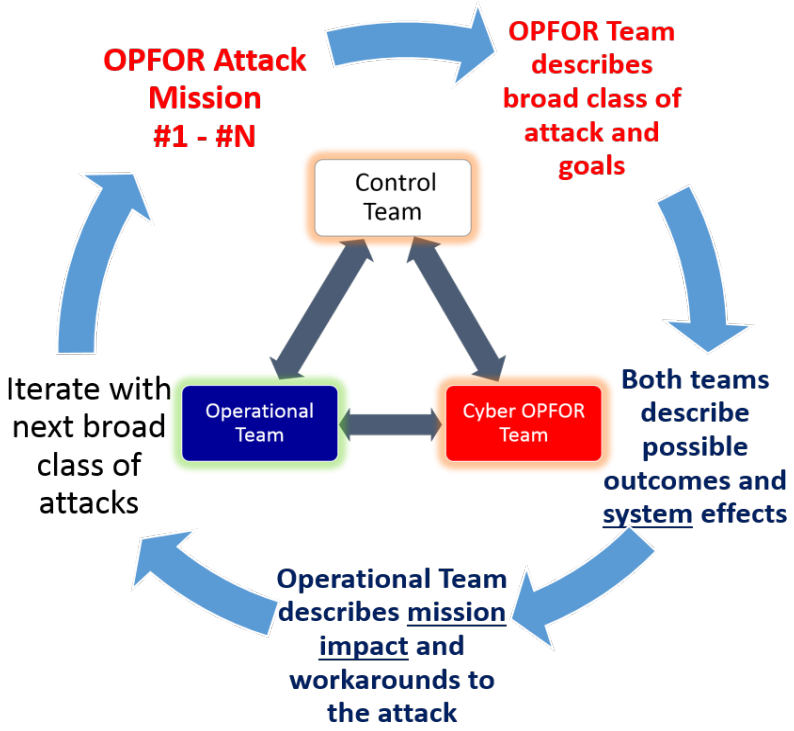


Figure 10. CTT Exercise Execution – Team Collaboration

The presenting OPFOR Team member may choose to diagram where on the Operational Timeline the attack will occur if the OPFOR Team expects a temporal attack to impact the Operational Mission. The 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. A best practice is not to display the attacks. This will allow the participants' responses 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 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 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 OPFOR Teams discuss the possible hypothesized system effects and together assess the likelihood of the OPFOR success and 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 Note Takes must carefully capture all discussions about likelihood, mitigations, cybersecurity controls, operator, or defender responses, as these discussions will impact the final likelihood assessments in Post-Exercise Analysis (Step 3). At the end of the discussion for each attack presented, the OPFOR Team Lead should summarize the key data as well as any assumptions made about the attack for the Note Takers, prior to tackling a new attack. The participants continue to iterate over all attack methods and variants, led by the OPFOR Team, using this procedure.

The OPFOR Team's initially proposed attack methods and plans evolve as they learn what 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 OPFOR Team's attack process, assumptions, and system-effects goals, and can therefore better assess the mission impact. **The Control and OPFOR Teams should strongly encourage the Operational Team to identify and explain opportunities the OPFOR Team should consider for disrupting the Operational Mission.** The Operational and 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 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 Note Takers are capturing the key discussions. This 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 table lengthy exchanges (e.g. ELMO, §3.1.4.1.2) that distract from the goal of the discussion and encourage the participants to revisit them at a break or during Post-Exercise Analysis (Step 3). Note Takers also are empowered to ask clarifying questions or pause discussions during the CTT to capture the accurate information.

3.2.3 Exercise Execution – Data Collection and Review

3.2.3.1 *Data Collection*

Note Takers capture the main discussion throughout the CTT about the system, the OPFOR Team's information flow, descriptions of the systems and equipment used in each OPFOR cyberspace attack, and the interactions among other personnel.

There are two main exceptions to this "write down everything" Note Taker role. The first is to assign one Note Taker (the Data Analyst) the role of updating the Analysis Table (if the 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 Note Taker dedicated to the role of only capturing RFIs and other tasks that participants must complete.

The Note Takers' records (i.e., electronic on classified laptops or handwritten in notebooks) are the raw data of the CTT and will be incorporated into the Analysis Table during Post-Exercise Analysis (Step 3).

3.2.3.2 *Review*

3.2.3.2.1 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 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 prior to the next day of the CTT.

The Control Team and the Note Takers also meet to assess the progress of the 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. The Control Team meeting could also use this meeting to address logistics and gaps in operational knowledge, such as the need for additional SMEs and documentation. Team Leadership may need to update the CTT schedule based on the progress made by the OPFOR Team.

3.2.3.2.2 Final Day

On the final day of the CTT Exercise, the Control Team meets to prepare for Post-Exercise Analysis (Step 3). The Control Team Lead and/or the CTT Facilitator describes the analysis process and the time commitment. During this meeting, the Control Team:

- Selects the analysis participants, potentially from the Operational and OPFOR Teams.
- Discusses the timeline for the analysis process and reporting of the 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 SIPRNet, collaboration tools) documented in the Data Handling Plan (§3.1.4.1.3). The program or Data Analyst consolidates the notes collected during the CTT to a shared location or put on a disk and made available to the Data Analyst and the analysis participants at the appropriate classification level.

3.2.4 Exercise Execution - Exit Criteria

The CTT is ready for Post-Exercise Analysis (Step 3) when the Control Team meets the following conditions:

- CTT raw data (collected notes) sufficiently documents the details of the Operational and OPFOR Missions and the technical impact on the system under analysis
- The program or Data Analyst consolidates the raw data in a shared location
- The analysis participants schedule the Post-Exercise Analysis Meetings and set deadlines for CTT products and reporting results

3.3 Step 3 – Post-Exercise Analysis

This step usually takes place over 30-90 days. The major activities performed during Post-Exercise Analysis are:

- Gather Data
- Initial Analysis
- Normalize Attacks
- Finalize Risk
- Categorize 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 three days, with homework assignments between each Working Meeting. Step 3 is also the most important part of the CTT because analysts synthesize the raw data into actionable information in the form or the Analysis Table and Risk Matrices (see Figure 11 - Figure 14) which 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 POAM (§3.1.4) and available on the CTT Intelink Website (§1.2). The participants should consider having a SME expert in STAT/DOE participate in this Step to "right-scope" the analysis by focusing on key factors and conditions.

3.3.1 Post-Exercise Analysis – Post-Exercise Homework

3.3.1.1 *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 program may first need to transcribe or digitize the notes. During the Exercise, the OPFOR Team/Lead should have already filled in a portion (e.g. red "OPFOR" columns) in the Analysis Table (§3.2.1.3.2), in which case the Data Analyst should incorporate

the data into the existing template. The data gathering effort could take up to three weeks to complete, depending upon the Data Analyst's schedule. Memories begin to fade the longer the analysis process takes so it this guide recommends minimizing unnecessary delays as much as possible. The Control Team plans the timeline on the last day of the Exercise (§3.2.3.2.2) and should account for minimizing delays. Figure 11 below depicts the left third of the Analysis Table for Attacks related to Access, Pivot, or Command and Control (top of Figure 11) and Effects (bottom of Figure 11), Figure 12, the middle third, and Figure 14, the right third. [2] The online template on the CTT Intelink Website (§1.2) and the representation in Appendix D provide detailed descriptions of each column.

Analysis Team	OPFOR					
Attack ID	Goal	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible Outcome
M1A1V1						
M1A2V1						

Analysis Team	OPFOR						Operational Team		
Attack ID	Goal	Attack Method	Attack Description	Assumptions	When in the Mission Timeline	Possible System Impact	Operational Impact	Mission Impact (Rubric)	Numerical Mission Impact and Consequence
M2A1V1									
M2A1V2									

Figure 11. Portions of Analysis Tables Used in Post-Exercise Analysis Working Meeting 1

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 that is used to easily refer to a cyberspace attack on the Risk Matrix (§3.3.3.2.1). The goal at the conclusion of the Gather Data activity is to have the initial unique identifier, all the Red OPFOR columns, and, for the Effects (those documented in the bottom of Figure 11), at least the Operational Impact Column, filled in for all attacks. The Data Analyst should organize the attacks logically, such as in 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 upon what was discussed during the CTT. There may be resolved or still outstanding RFIs – all of which the Data Analyst documents in the last column of Figure 14 in preparation for Working Meeting 1. Appendix D provides a description for each

[2] Access, Pivot, and Command and Control attacks are presented separately to support identifying mitigations along the attack path leading to an effect. These types of attacks have no mission impacts. Therefor these attacks are not represented using a risk matrix. Only Likelihood assessments apply to Access, Pivot, and Command and Control attacks.

column in Figure 11, Figure 12, and Figure 14.

3.3.2 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 the 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.

3.3.2.1 *Initial Analysis*

In Working Meeting 1, the analysis participants re-familiarize themselves with the attacks in the Analysis Table data to ensure the cyberspace attack data gathered so far are accurate and identify required adjustments. The other Note Takers, if in attendance, should review their own notes to identify any missing data.

The analysis participants review each cyberspace attack, i.e., Goal, Attack Method, Description, Assumptions, and When in the Mission Timeline; the Possible System Impact or Possible System Outcome (OPFOR columns); 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 (Figure 14) or in the column requiring refinement.

The analysis participants should decide how to group cyberspace attacks, if the grouping or structure first proposed by the Analysis Lead is not preferred. The analysis participants may decide to group attacks by Cyber OPFOR Mission Objectives or by category of attack method from the Cyber Kill Chain (Appendix B), i.e., access, pivot, and command and control. 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/tabs for each agreed-upon grouping, or 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 every 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 Team 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 and/or planned) discussed for the system under analysis in the appropriate column. The Team should have the original copy of the Note Taker's notes along with any drawings and presentations the OPFOR or Operational Teams produced in the CTT available for reference during each Working Meeting. If possible and not already complete, the participants may also complete the Mission Impact using the Mission Impact rubric (Figure

7) and assign the associated Numerical Mission Impact and Consequence. Usually, this task is homework for the Operational Team Lead because the rubric may still need refining.

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 (§3.1.4.1.3) 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.

3.3.2.2 *Working Meeting 1 Homework*

- Individuals complete assigned questions and RFIs documented in the Analysis Table and transmit by the prescribed due date to the Data Analyst
- Data Analyst addresses all editing and updating of the Analysis Table, including:
    - Create new rows for any new attack or variant, or combines attacks (within one week)
    - Publish the updated Analysis Table for the other analysis participants to complete homework
- Operational Team Lead consults with Operational Team members as needed to:
    - Finalize Mission Impact Methodology (Figure 7, §3.1.2.1.1)
    - Enter or update impact details in the (Operational Team columns, Figure 11) of the Analysis Table
    - Assign mission impact number to the Numerical Mission Impact and Consequence column in the Analysis Table (Figure 11)
- 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 (Figure 12)
    - Assigns a numerical value in the Numerical Attack Likelihood column applying the likelihood assessment methodology (Figure 8)
    - Determines subjective upgrade or downgrade factors for numerical likelihood and documents the upgrade/downgrade factors used
    - Optional steps: Determines an adjustment to the likelihood value that factors in the difficulty of access method(s) and other cyber kill chain steps, as relevant and desired; Documents the rationale and assigns someone to document and adjust the likelihood value in the Analysis Table in the column Analysis of Numerical Likelihood Factoring in Access Method: New (or unchanged) value (Figure 12)
- Data Analyst consolidates all updates to the Analysis Table in preparation for Working Meeting 2

3.3.2.2.1 Documenting Final Mission Impact Assessment

The Operational Team Lead should finalize the Mission Impact Methodology, Figure 7, developed initially developed 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 they wait to finalize the Mission Impact Methodology. Using the Mission Impact Methodology, the Operational Team Lead

assesses each row/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 in the Operational Impact; Mission Impact (Rubric) and Numerical Mission Impact and Consequence columns (Operational Team columns, Figure 11) in the Analysis Table as Working Meeting 1 Homework prior to 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.

3.3.2.2.2 Documenting Final Likelihood Assessment

The OPFOR Lead will use the Control Team developed and approved version of Figure 8 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) (Figure 12). The online template on the CTT Intelink Website (§1.2) and the Analysis Table representation in Appendix D provide detailed descriptions of each column. The likelihood of a successful cyberspace attack may depend on certain assumptions, accesses, 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 Attack Cost/Level of Effort and Attack Surface Likelihood must be detailed and complete to allow a tester or cyber SME to understand the technical feasibility described. In other words, the OPFOR Lead should not simply enter vague terms such as "easy" or "moderate," but instead describe the logic behind those terms to support discussion and understanding in Working Meeting 2.

The column *Analysis of Numerical Likelihood Factoring in Access Methods* is optional and the analysis participants can use it to refer back to specific access methods or as a method to encompass the kill chain steps required to complete the attack. Additional details on mitigations, controls, and operator or defender procedures may also influence the upgrade/downgrade factors of likelihood values or fine-tuning of the metrics that fall in between likelihood values. The 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 as needed for the final recommended Numerical Attack Likelihood value. The OPFOR Team Lead must fully document all logic associated with the selection of the Numerical Attack Likelihood value as Working Meeting 1 Homework prior to Working Meeting 2.

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 12. Portion of Analysis Table Used in Post-Exercise Analysis Working Meeting 2

3.3.3 Post-Exercise Analysis – Working Meeting 2

Working Meeting 2 is a 3-day meeting that occurs 2-3 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 per cyberspace attack (rows) in the Analysis Table.

3.3.3.1 *Normalize Attacks*

During Working Meeting 2, the analysis participants re-examine, 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 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) (Operational Team columns, Figure 11) 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 column and Numerical Mission Impact and Consequence (Figure 11) for every cyberspace attack in the Analysis Table. The analysis participants may also decide to document variants in mission impacts based on modified Operational Assumptions. For example, an aircraft carrier that is actively under a kinetic attack is fully mission capable if it can launch aircraft while the launching system is under a cyberspace attack. However, that same aircraft carrier may be non-mission capable during peacetime operations if the same cyberspace attack is launched.

The analysis participants also review the value assigned in the Numerical Attack Likelihood column (Figure 12) in the Analysis Table for every cyberspace attack based on the OPFOR Team Lead's inputs and the Likelihood Assessment Methodology. The analysis participants should document any modifications and the rationale behind the modifications to the likelihood values in the Analysis Table. The numerical likelihood is not an assessment of the adversary's intent to conduct the specific cyberspace attack, nor 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 system under analysis
- Document any questions or additional RFIs in the Questions, RFIs, and Further Analysis column in the Analysis Table (Figure 14)
- Identify any additional mitigations that are in place or planned that should be updated in the appropriate column of the table
- Document any testing recommendations made by the OPFOR regarding a specific attack in the Recommendations column (Figure 14)

Before Working Meeting 2 wraps up, the analysis participants should assign homework and refer to the Data Handling Plan (§3.1.4.1.3) for the appropriate procedures between Working Meetings 2 and 3. Once Working Meeting 2 concludes the Control Team Lead or the CTT Facilitator extracts and distributes the list of remaining RFIs with due dates to the individuals responsible for providing the information needed.

3.3.3.2 *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 due date prescribed
- Data Analyst
    - Addresses formatting inconsistencies and cleans up the Analysis Table (within 1-2 days)
    - Ensures all analysis participants have access to the updated version
- Team Leadership ensures program personnel and members from the Operational Team but not participating in analysis are given the Analysis Table to make any corrections and to provide recommendations (within 1 week)
- Control Team Lead and CTT program personnel:
    - Develop initial set of recommendations documented in the Analysis Table (Figure 14)
        - NOTE: It is critical to develop this list of recommendations for the system under analysis in order to create the actionable information. If this step is not performed as homework, it must be performed prior to Reporting (Step 4)
- Data Analyst or Analysis Lead:
    - Builds initial Risk Matrices (Figure 13, §3.3.3.2.1) using values from the Analysis Table, the program risk reporting methodology, and based on the grouping of attacks
    - Extracts key data from the Analysis Table to build simple tables listing attacks for the final results briefs
- OPFOR Team Lead identifies specific sets of attacks to build attack vignettes for the final results briefs
- Control Team Lead and CTT Facilitator draft the unclassified portions of the Technical (§3.4.2) and Executive (§3.4.3) Briefs

3.3.3.2.1 Risk Matrix

The Data Analyst plots each cyberspace attack grouping on a separate Risk Matrix using the first column with a unique identifier in the Analysis Table (Figure 11). Figure 13 is an example of a Risk Matrix, adapted from the NIST Guide for Conducting Risk Assessments SP 800-30 Rev. 1 (Reference (g)).

The Numerical Mission Impact values are the x-coordinates and the Numerical Likelihood values, from the columns in the Analysis Table (Figure 11, Figure 12, respectively), are the y-coordinates of the Risk Matrix (Figure 13). Appendix D 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 (Reference (o)), as

desired.

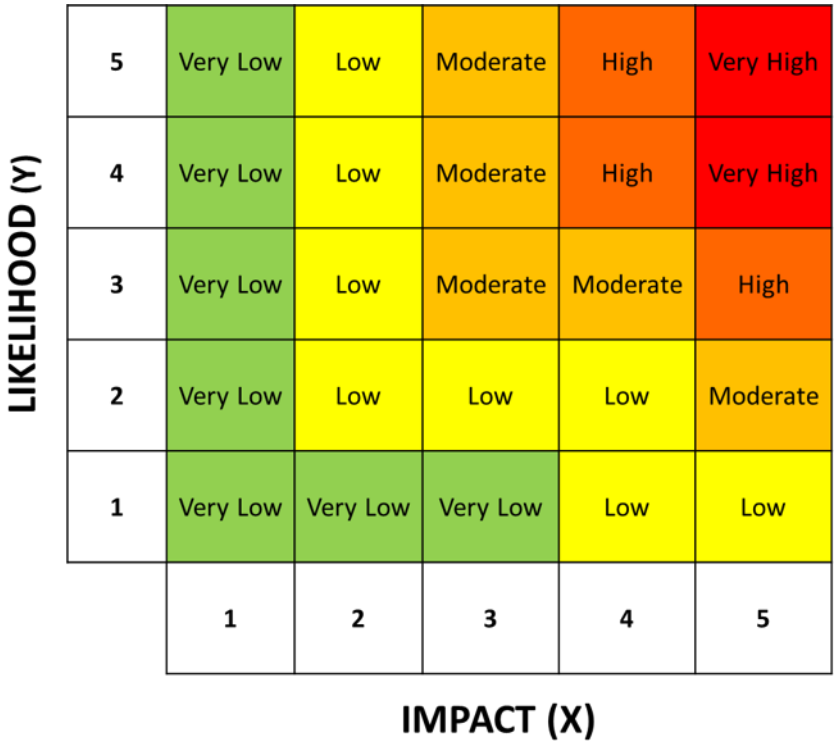


Figure 13. Risk Matrix based on NIST SP 800-30 Rev 1 (Reference (g))

3.3.4 Post-Exercise Analysis – Working Meeting 3

Working Meeting 3 is a 3-day meeting that occurs 2-3 weeks after Working Meeting 2. At the conclusion of this meeting the Analysis Table, representing the actionable information including recommendations; Risk Matrices; a draft technical results brief; and a draft executive level brief are all completed.

3.3.4.1 *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 results brief.

3.3.4.2 *Categorize Recommendations*

After the Finalize Risk activity, the analysis participants review the assigned homework and

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 14. Portion of Analysis Table Used in Pre-Exercise Analysis Working Meeting 3

discuss the capabilities of the system(s) for averting or mitigating the risk associated with each cyberspace attack in the Analysis Table (Figure 14). Figure 14 depicts the right third of the Analysis Table. The online template on the CTT Intelink Website (§1.2) and the representation in Appendix D provide detailed descriptions of each column. Some attacks may not have any entries in the Mitigations columns. No documented mitigations might result in specific recommendations to address mitigating the attack 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 system under analysis. These recommendations usually are one of the following four categories:

1. **Test** - The system requires testing to determine level of risk associated with specific attacks or vignettes.
2. **Accept or Hold** - The risk may be low, unknown, or unable to be mitigated.
3. **Mitigate** - Identify and enact specific mitigation technique.
4. **Further Analysis** - Investigate further to determine if testing, mitigating, or accepting is appropriate.

EXAMPLE RECOMMENDED ACTIONS

Test - to determine if access to system Y can be established during pre-mission planning.

Accept - that data may be exfiltrated through System Y because there is no mission essential information at risk.

Mitigate – by implementing design change in system architecture of component Q.

Further analyze - system architecture to determine if the adversary can pivot to Network Z from System Y.

- After implementing planned mitigation B, analyze system architecture and interface controls to determine if the adversary can still pivot to System Y from Network Z.
- Engage with Network Z cyber defenders to understand TTPs for detection.

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 system under analysis, they should work to finalize the draft Technical Brief (§3.4.2) 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 (§3.4.3) depending upon the briefing schedule. The Executive Brief is often a subset of the Technical Brief.

3.3.5 Post-Exercise Analysis - Exit Criteria

The CTT is ready for Reporting, Step 4, when the Control Team meets the following conditions:

- Organize and refine CTT notes with SMEs
- Complete the Analysis Table attack likelihood and mission impact details
- Create and refine Risk Matrices with SMEs
- Develop actionable recommendations for system under analysis
- Scheduled briefs
- Program concurrence with the findings and recommendations

3.4 Step 4 – Reporting

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

- Prioritize the Recommendations
- Complete the Technical Brief
- Develop the Executive Brief

3.4.1 Reporting – Prioritize Recommendations

For the system under analysis, 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 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. The program will also want to consider whether the system needs additional CTTs due to other systems, missions, or interfaces not explored. The Control Team Lead should emphasize in the reports both the adversary's potential opportunities to disrupt the Operational Mission, as well as 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 should practice giving the brief to the analysis participants, if possible, prior to the actual briefing to become more effective at presenting the results.

3.4.2 Reporting – 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, benefits
- Key leadership and participating/supporting organizations
- Operational Mission and Scenario Overview
    - Key diagrams and information
- OPFOR Mission Overview
    - Intelligence, known and unknown
- Summary of Results
    - Risk Matrix with total number of attacks in each cell
    - Mission Impact and Likelihood Assessment Methodologies
        - Upgrade/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

The Control Team can pull information from the Kickoff Briefs to use in the detailed Technical Brief. This information is often not classified. The Detailed Results (usually classified findings) include the OPFOR cyberspace attack vignettes selected by the Control Team and/or analysis participants and developed by the 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. This is 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 MBCRA. 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 on the CTT Intelink Website (§1.2).

3.4.3 Reporting – Executive Brief

The Executive Brief provides a high-level overview of the CTT steps and presents the recommendations and key actionable information about the system under analysis. 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

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, §3.1.2.1) and the Cyber OPFOR Mission Objectives (§3.1.2.3), 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.

3.4.4 Reporting - Exit Criteria

- Technical Brief presented to CTT participants and other interested stakeholders
- Executive Brief presented to leadership

3.5 Wrapping up a CTT

The CTT is not a typical wargame with moves and counter-moves, but is a tool designed to increase both the leadership's and the warfighter's 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 Team reports the CTT results in Step 4, the Control Team Lead or CTT Facilitator should gather feedback from the program about their thoughts on the CTT and ask them to complete the anonymous DoD CTT Survey using the "Program-POST-Reporting-Survey-Info" file available on the CTT Intelink Website (§1.2). The answers to the survey help DoD assess the value of and help improve the CTT process.

Programs can use CTT Exercises throughout the acquisition process to design and field more cyber resilient systems and plan efficient and effective cyber T&E strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

Acronym List

AAF	Adaptive Acquisition Framework
CAPEC	Common Attack Pattern Enumeration and Classification
CONOPS	Concepts of Operations
CSSP	Cybersecurity Service Provider
CTT	Cyber Table Top
CUI	Controlled Unclassified Information
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDI	Department of Defense Instruction
DOE	Design of Experiment
DT	Developmental Test
DT&E	Developmental Test and Evaluation
FoS	Family of System
IDA	Institute for Defense Analysis
ISSE	Information System Security Engineer
ISSM	Information System Security Manger
IT	Information Technology
MBCRA	Mission-Based Cyber Risk Assessment
NDA	Non-Disclosure Agreements
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerabilities Database
OPFOR	Cyber Opposing Force
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTRR	Operational Test Readiness Review
OV-1	Operational View - 1
POAM	Plan of Action and Milestones
POC	Point of Contact
PPP	Program Protection Plan
RFI	Request for Information
RMF	Risk Management Framework
ROE	Rules of Engagement
SCG	Security Classification Guide
SIPRNet	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SoS	System of Systems
STAT	Scientific Test and Analysis Techniques
T&E	Test and Evaluation
TEMP	Test Evaluation Master Plan
TTP	Tactics, Techniques, and Procedure

Glossary

The following glossary includes definitions of some terms that teams may use or reference when conducting a CTT. Sources for terms and definitions include both authoritative government sources and open source literature.

A		
	Access	Ability and means to communicate with or interact with a system, use system resources to handle information, gain knowledge of the information the system contains, or control system components/functions. (Reference (p)).
	Advanced Persistent Threat	An attacker with substantial means, organization, and motivation to carry out a sustained assault against a specific target. They are advanced because they are capable of conducting anonymous, stealthy, and extremely sophisticated attacks, tailored to a specific target. They are persistent in that they are difficult to detect, deter, prevent, and remove.
	Attack Surface	All of the different points where an attacker could get into a system, and where they could get data out. The system's exposureto reachable and exploitable vulnerabilities; i.e., any connection, data exchange, service, removable media, etc., that could exposethe system to potential threat access.
	Attack Vector	Method of conducting a cyberspace attack; how attacker gains unauthorized access; path or means by which an attacker gainsaccess to a system to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element. Also called *Threat Vector*.
B		
C		
	Cyber	A prefix used to describe a person, thing, or idea as part of the computer or information age.
	Cyber Risk	Potential for an unwanted/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 Warfare	Actions, typically politically motivated, by a nation-state or non-state actor, to penetrate another nation's computers or networks for the purposes of causing damage or disruption.
	Cyberspace Attack	Cyberspace actions that create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. ((Reference (p)).
	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. (Reference (p)).
	Cyber Survivability	The ability of warfighter systems, and system defenders, to prevent, mitigate, recover from and adapt to adverse cyber-events that could

		impact mission related functions, by applying a risk-managed approach to achieve and maintain an operationally relevant risk posture, throughout its lifecycle. (Proposed, Joint Staff, J6)
D		
	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. (Reference (s)).
E		
	Enabling Operations	The first stage of a cyberspace attack where the threat gains information about the targeted systems and users.
	Exploit	Technique/program designed to break into a system by taking advantage of an accessible vulnerability in the attack surface.
	Exploitation	Act of infiltrating target systems to extract and gather intelligence data.
F		
	Family of Systems	A set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects (Reference (q)).
G		
H		
I		
	Insider Threat	The threat that an insider will use her/his 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. (Reference (p)).
J		
K		
	Kill Chain	A sequence of activities that produce warfighting effects, within a mission area, in the battlespace.
L		
	Level of Effort	Amount of work an attacker must invest to successfully achieve the goals of a cyberspace attack. 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. (Reference (p))
M		
N		
O		
	Offensive Cyberspace Operations	Missions intended to project power in and through cyberspace. Also called OCO. (Reference (s))
	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. (Reference (c))
P		

	Payload	Term that describes the component of an attack, once a vulnerability has been exploited, that causes am impact to 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/alter files in the system. Payloads can have multiple programmable capabilities and can be remotely updated.
R		
	Red Team	An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (Reference (s)).
	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (Reference (p)).
	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 RMF (Reference (j)).
S		
	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 information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. (Reference (p)).
	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.
	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 a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.
	Supply Chain Risk Management	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, supplied product and its subcomponents, or supply chain (initial production, packaging, handling, storage, transport, mission operation, and disposal).

	System of Systems	A set or arrangement of systems resulting from the integration of independent and useful systems into a larger system that delivers unique capabilities. (Reference (q)).
T		
	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 denial of service. (Reference (p)).
	Threat Vector	See *Attack Vector*.
U		
V		
W		
X		
Y		
Z		

Appendix A: References

a) Department of Defense, *The 2018 DoD Cyber Strategy*, September 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

b) Department of Defense, *Summary of the 2018 National Defense Strategy of the UnitedStates of America*. https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

c) Department of Defense Instruction 8500.01, "Cybersecurity", March 14, 2018. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

d) Department of Defense Instruction DoDI 5000.89, "Test and Evaluation", November 19,2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF?ve r=Plc85E0-NVNide91K3XQLA%3D%3D

e) Department of Defense, *Cyber Test and Evaluation Companion Guide*, Version 3.0, (UNDER DEVELOPMENT)

f) Department of Defense Instruction 5000.02, "Operation of the Adaptive AcquisitionFramework", January 23, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf

g) National Institute of Standards and Technology, *Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments*, September 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

h) Ambroso, Michael and Rhiannon Hutton, *Comparative Review of DoD Mission-Based Cyber Risk Assessments*, Alexandria, VA: Institute for Defense Analyses, P-8736, February 2018.

i) de Naray, Rachel K. and Keith Galvin, *Comparative Review of DoD MBCRAs: 2020 Updates and New Methodologies*, Alexandria, VA: Institute for Defense Analyses, P-14309, September 2020.

j) Department of Defense Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology", March 12, 2014. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

k) MITRE, "Common Attack Pattern Enumeration and Classification (CAPEC)", https://capec.mitre.org

l) MITRE, "Common Vulnerabilities and Exposures (CVE)", https://cve.mitre.org/

m) MITRE, “Common Weakness Enumerations (CWE)”, https://cwe.mitre.org/

n) National Institute of Standards and Technology, “National Vulnerability Database (NVD)”, https://nvd.nist.gov/

o) FIRST “Common Vulnerability Scoring System (CVSS)”, https://www.first.org/cvss

p) Committee on National Security Systems, “Committee on National Security Systems(CNSS) Glossary”, CNSSI No. 4009, April 6, 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

q) Defense Acquisition University, “Glossary of Defense Acquisition Acronyms and Terms”, https://www.dau.edu/glossary/Pages/Glossary.aspx

r) MITRE, “Adversarial Tactics, Techniques and Common Knowledge”, https://attack.mitre.org/wiki/Main_Page

s) Chairman of the Joint Chiefs of Staff, “DOD Dictionary of Military and Associated Terms”, January 2021. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Appendix B: CTT Exercise Preparation Resources

CTT Examples

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

- 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 that will have to be addressed in the program. This may inform the allocation of resources to disciplines within the Program Office dealing with the many aspects of cybersecurity. It will also inform the tailoring of control selection and control overlays during step 2 of the RMF process.
- Systems beginning their test planning and test data management process could leverage CTTs to determine what constitutes adequate developmental testing prior to operational testing (e.g., supporting the "Attack Surface Characterization" Phase in the six-phase cybersecurity test and evaluation process).
- CTTs could serve as a tool during development and continuous monitoring to determine whether emergent cyber vulnerabilities have been overlooked in the system under analysis (especially in the support and maintenance subsystems). E.g., Portable Universal Serial Bus (USB) flash drives became an emergent cyber threat not previously considered and to inform mitigations.
- CTTs could be used to generate threat vignettes for adversarial, threat-based testing after known vulnerabilities from cooperative vulnerability identification events have been addressed. In this way, they could help determine the environment needed for threat-based testing and inform Authorizing Officials decisions about the risk to the network.
- A smaller-scale, "mini" CTT, could be used to perform quick turn-around risk assessments on vulnerability assessment findings to evaluate mission risks, which often can be accomplished in 1 day or less. 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).

- Step 1 - Recruits participants and sets goals, objectives and deliverables
- Step 2 - Adjudicates issues, ensures minority views are heard, and captures recommendations
- Step 3 - Leads Post-Exercise Analysis
- Step 4 - Reports actionable results

Operational Team: Most engaged during the CTT Exercise Execution (Step 2)

- Develops notional plan to execute operational mission orders and/or achieve operational objective within the future timeline and scenario
- Presents the notional timeline, actions and procedures of the multi-day mission: Planning through post-mission tasks including maintenance
- Assesses the impact to mission accomplishment of successful attacks
- May be needed for post-CTT analysis

Comprised of 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"; subsystem SMEs; Anti-Tamper SMEs, System Security Engineers and Program Protection SMEs; safety SMEs; logistics and sustainment SMEs; CSSPs and network defenders, program cybersecurity SME.

Cyber Opposing Force (OPFOR): Most engaged during the Exercise Execution (Step 2); OPFOR Team Lead *may* engage with Team members in advance to perform reconnaissance, plan/assign missions.

- Review System Reconnaissance information
- Review the Operational Mission sequence
- Develop a list of potential exploitation pathways based on reconnaissance for each system
- Present the general OPFOR Mission approach and attacks
- Develop and lead discussion of cyberspace attacks to execute the Cyber Opposing Mission Objectives
- Participate in Post-Exercise Analysis (Step 3), as required

Comprised of certified ethical hackers (contractor, government, academia); authorized cyber team penetration testers and Operational Test Agency Representatives (e.g. NSA-certified Red Team); defensive and offensive cybersecurity SMEs; cyber developmental testers; cyber range personnel; interoperability engineers; electronic warfare testers, CSSPs or network defense personnel for the system, system engineer or tester (provides operational perspective).

Individual Roles and Responsibilities

Control Team Lead: has overall authority and responsibility for the exercise; typically, the Analysis Lead; expert on system/program under analysis; identifies the appropriate program and operational/user contacts to participate in Exercise Execution (Step 2); responsible for prioritizing recommendations and the executive brief in Reporting (Step 4).

CTT Facilitator: supports Control Team Lead, keeps Control Team on track, particularly helpful during program's first CTT, adjudicates questions and issues that arise; expert on the CTT process bringing experience and contacts from other CTTs.

Operational Team Lead: responsible for planning the Team's Operational Mission and ensures the Team deliverables are within the CTT time constraints; serves on both Operational and Control Teams; general experience/knowledge across the scope of the Mission and Scenario; strong leader, fosters discussion without (or allowing others) dominating the conversation.

OPFOR Team Lead: **most important role in the CTT** and responsible for planning the Cyber OPFOR Mission Objectives (in Step 1); serves on both OPFOR and Control Teams, expert in cyber offensive and/or defensive operations, cybersecurity vulnerability assessments, cyber warfare operations; strong personality, communicative. Drives Exercise Execution (Step 2), fills in the results table, risk matrices during Post-Exercise Analysis (Step 3), and creates cyberspace attack vignettes in Reporting (Step 4). For more details about the role of the OPFOR Team Lead in the CTT process, see the following section.

Analysis Lead: directs the Post-Exercise Analysis (Step 3) and responsible for the developing the actionable information results from the CTT. Organized, analytical, cybersecurity SME; part of the Control Team.

Data Analyst: note taker 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. Organized, analytical, at least a general level of cybersecurity knowledge.

Note Takers: records all relevant discussions, who said what, and diagrams attacks, as required, during Exercise Execution (Step 2). Detail oriented, good listener, organized, good short-term memory, helpful to have general CTT experience and knowledge with the system under analysis, typical missions, or cybersecurity.

Operational and OPFOR Deputy Team Leads: supports Team Leads as desired.

Security Lead: responsible for classification derivations of all CTT data; expert on program classification guide, knowledge of Program Protection Plan; coordinates appropriate classified facilities for the Exercise, data analysis, and other classified meetings; develops and publishes the data handling/management plan for the Exercise (Step 2) and Post-Exercise Analysis (Step 3); manages the visit requests for participants; manages Non-disclosure agreements (if applicable); provides input regarding classification and data handling for the CTT Kickoff briefs.

Intel Lead: supports the collection of intelligence information; From the program or intelligence organization supporting the program; develops/coordinates intelligence briefs for the CTT to include relevant intelligence to the CTT mission such as targets of interest or enemy activities, and intelligence related to known cyber tactics, techniques and procedures to the program data, system under analysis, interfaces, etc.

Importance of OPFOR Team Lead Role

The 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 strong leadership skills, and the ability to communicate clearly. They bring passion and commitment for educating and improving awareness of cyber threats to DoD missions to the CTT. By fostering creative thought, inspiring provocative ideas, and cultivating a non-adversarial collaborative environment for learning, they motivate the OPFOR Team to research and defend plausible attacks and all CTT participants to identify 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 OPFOR Team members. The OPFOR Lead seeks the requisite technical documentation and information, asking questions about the system, mission, maintenance, etc. until they have sufficient information[3] to develop the set of Cyber Opposing Mission Objectives. Technical deep dives or lab/site visits may be required, and if so, the OPFOR Lead requests and attends those fact-finding events. If during the course of planning superfluous information is provided, the OPFOR Lead helps to filter out the 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 in advance of the rest of the event), presents the OPFOR Mission brief, and asks questions during other briefs to (1) improve understanding amongst all participants and (2) encourage the OPFOR Team members to ask questions they may have. The OPFOR Lead coordinates the attack brainstorming activities of the OPFOR Team, whether between the Kickoff event and the Exercise, or during OPFOR Team Breakouts. During brainstorming, the OPFOR Lead reminds the Team that they should be developing a wide range of representative attacks, across the range

[3] High-level system under test interface and network diagrams, including key external networks and categories of information obtained from the internet, Non-classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet).

of effects (deny/degrade/disrupt/destroy/deceive/exfiltrate), and that the attacks should be plausible, using the Likelihood Assessment Methodology initially to understand technical feasibility of the developed attacks. The OPFOR Lead must structure the attack presentations by the OPFOR Team members to ensure a consistent approach and flow. The OPFOR Lead guides attack presentations, evolving attacks as warranted by discussion during the event. He/she also:

- decides the order in which to present 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 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 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 brief and/or report by developing and describing attack vignettes. They attend all out briefings as desired by the program, and are available to present the attack vignettes and analysis process if needed.

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 follow a sequence similar to the cyber kill chain steps depicted and described here:

Figure 15. Cyber Kill Chain

Step 1: Reconnaissance and Weaponization. Attackers gather information before the actual attack. This helps them devise possible ways to exploit vulnerabilities in the system software and architecture as well as how to socially engineer. 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. The attacker will likely try this out in his own laboratory or cyber security range before unleashing it on the victim.

Step 2: 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 14 for examples of points of access to a system.

Step 3: 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.

Step 4: Command and Control. The attacker establishes bidirectional communication with a cyber weapon operating within the targeted platform. The attacker creates a command and control channel in order to continue to operate the internal assets remotely. This step is relatively generic and relevant throughout the attack, not only when malware is installed. Also called C2.

Step 5: Effects. The attacker performs the steps to achieve the attacker's actual goals on the victim's system. This can be an elaborate active attack process that takes months, and thousands of small steps, in order 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 availability and integrity of data and systems with the goal of compromising the platform's mission.

Step 6: Exfiltrate. Using presence or a cyber weapon to conduct confidentiality attacks against the platform. This is another type of mission effect and can continue until detected, if detected, or until the platform is replaced.

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" (Figure 16). The wheel depicts some of the more common access paths that may exist for a system. Figure 16 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 systems engineering process, including supply chains and developmental environments. OPFOR Teams can use this access representation to generate ideas for the kill chain steps and to produce vignettes for explaining how an attacker might gain access to the system.

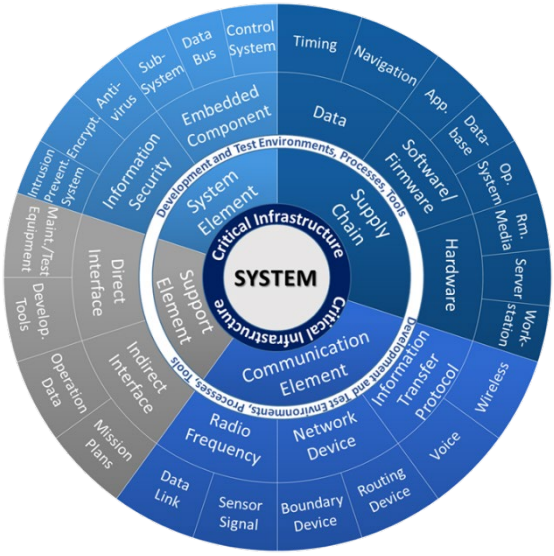


Figure 16. Wheel of Access

Adversary Tactics

A resource for OPFOR Teams and during analysis is MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) database, (Reference (r)). This site is "a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's life cycle and the platforms they are known to target. ATT&CK™ is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected."

Appendix C: CTT Exercise Execution Resources

Notional CTT Exercise Execution Agendas

Option 1: Kickoff held the same week as the CTT

- Day 1 Events (Participants)
  - Welcome Aboard/Admin/Security/Safety Briefs (Combined Teams)
  - CTT Program Leadership Speaker – Setting the Stage (Combined Teams)
  - Cyber Table Top Purpose/Objectives Brief (Combined Teams)
  - System Description (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 (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 you 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 in advance of the CTT

- Kickoff Events (Participants)
  - Welcome Aboard/Admin/Security/Safety Briefs (Combined Teams)
  - Kickoff Speaker – Setting the Stage (Combined Teams)
  - Cyber Table Top Purpose/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 prior to the 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)
    - 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)
  - Welcome Aboard/Admin/Security/Safety Briefs (Combined Teams)
  - CTT Program Leadership Speaker – Setting the Stage (Combined Teams)
  - Cyber Table Top Purpose/Objectives Brief (Combined Teams)
  - System Description Brief (Combined Teams)
  - Intelligence Brief (Combined Teams attend)
  - Operational Mission and Scenario Brief (Combined Teams)
  - OPFOR Mission Brief (Combined Teams)
  - OPFOR Cyber Opposing Mission Objectives #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)

Exercise Support Planning

Kickoff/Exercise Supplies

Create Welcome Packets for all CTT participants and print copies of the Kickoff briefs for referencing during the Exercise.

- **Welcome Packet:** Agenda • Name/number tag • List of Participants • Systems Under Analysis Diagram • Acronym List • Note sheet • Survey

Other useful resources and supplies to have available:

• Black/Red/Blue Dry Erase Markers • Black/Red/Blue Magic Markers/Sharpies • White Out Bottles • White Boards • Black/Blue Pens • Easel Board-size Sticky Note Pads • 11x17 laminated Diagrams • Rubber bands for large brainstorming sheets • Name/number Tags for Participants- reusable or stickers • Large envelopes	• NOFORN stamps w/ink (as required) • SECRET stamps w/ink (as required) • FOUO stamps w/ink (as required) • Cover sheets for secret documents • Composition notebooks (college ruled) or note taker 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

Reserve rooms at the appropriate classification level that can accommodate all participants and observers (better to overestimate the size of space necessary). One or two smaller rooms may be needed for the Team Breakouts in addition to the main room holding the Exercise. The Team rooms should have flip charts, maps (as needed), sticky papers, and markers to aid with the discussion and brain storming assignments.

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

Consider the comfort and well-being of the participants by ensuring beverages, snacks, and facilities are readily available.

During the Exercise

Assign each participant a number and make number badges or name/number tents to identify who is speaking when the Note Takers are recording the conversations during the CTT. Ask participants to state their assigned number when speaking to help Note Takers more easily capture who is speaking.

At the CTT, prior to starting, taking breaks and re-starting 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 D: CTT Post-Exercise Analysis Resources

Analysis Table Column Descriptions

The Analysis Table, broken up for readability in Figure 11, Figure 12, and Figure 14 into three parts, is an excel spreadsheet used to document all of the details with each proposed attack as a unique row in the spreadsheet. A downloadable and tailorable template is on the CTT Intelink Website (§1.2). The template provides descriptions for each column, which are also provided below in Figures Figure 17-Figure 20. Figure 17 presents two similar columns depending upon if the attack is focused on access, pivot, command and control, or causing an effect. For access, pivot, or command and control 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 11 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
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 Outcome	Description of expected outcome of access, pivot, ot command and control (C2) efforts; may include description of expected privileges gained, new system accessed (post pivot), or description of ability to perform a trigger or other C2.
Possible System Impact	Description of possible outcomes to the systems under attack and 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 17. 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 18. Column Descriptions in the Operational Mission Analysis Table Section

Column	Description
Attack Cost / Level of Effort	A 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 if 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 19. 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 20. 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. Alternate methodologies for analyzing and presenting results can be used. The CTT uses the National Institute for Standard (NIST) Special Publication 800-30, Revision 1 (Reference (g)) risk matrix (Figure 13 to ensure consistency in risk assessments with the Risk Management Framework (Reference (j)).

Cybersecurity risk, as with other risks, consists of likelihood on the vertical, or y, axis of the matrix, and impact/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 assessed for traditional risk matrices.

The likelihood factor consists of the threat and the vulnerability, Likelihood = f(threat, vulnerability), resulting in the risk equation being: 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 sub-factors within the three main factors. Increasing a threat's requisite level of effort, reducing the threat's access would cause the likelihood factor to be lower, as would reducing finable vulnerabilities. Reducing impact may focus on lowering system susceptibility or the duration of impact.

As previously stated, for a CTT, likelihood is generally not an assessment of the adversary's intent to conduct the specific attack, nor the probability the system will be exposed to the attack. Therefore, the analysis participants typically do not assess the threat portion of likelihood during analysis, but if the program has dedicated intelligence support, the intelligence support should participate in the analysis and factor the threat assessment into likelihood. Intelligence experts can be asked to 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 for the CTT using a numbering technique. The numbering 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 serve as the unique identifier. For example, M2A1V2 indicates OPFOR mission 2, attack #1 within that mission, and variant #2 of that attack. This implies there is at least one other variant of attack 1 within mission 2 (M2A1V2).

below depicts three notional variants of mission 2, attack 1 plotted onto the risk matrix.

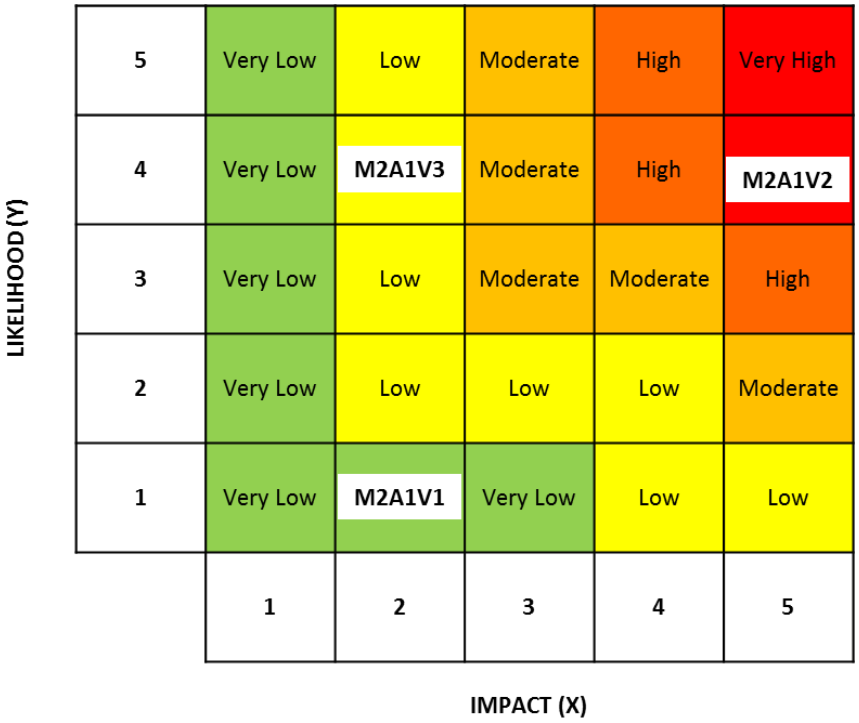


Figure 21. Notional Risk Matrix Depicting Three Attacks

Reading the risk on the matrix for M2A1V2:

- Successful execution of the second variant of attack 1 for OPFOR mission 2 would leave system non-mission capable.
- This attack is highly likely to work based on the assumptions that the adversary
    - Gains access and the required privileges on the network to execute the attack
    - Launches a successful effect against system under test

Since the likelihood factor can be subjective and depends heavily on the OPFOR subject matter expertise and incomplete intelligence assessments, cyber testing should be planned for the

areas of greatest concern to assess the probability more accurately.

Appendix E: CTT Checklist

Control Team

Step 1: Exercise Preparation:

- □ Recruit the Exercise participants:
  - □ Operational Team
  - □ OPFOR Team
- □ Designate Leaders for Operational and OPFOR Teams
- □ Approve Operational Team's Mission (e.g., Intelligence, Surveillance, and Reconnaissance, Combat Search and Rescue) and background Operational Scenario
- □ Approve OPFOR Team's Mission and Cyber Opposing Mission Objectives that include/exclude of classes of threat vectors (e.g., supply chain, insider threat, social media exploitation)
- □ Develop and approve initial Mission Impact Methodology
- □ Develop and approve Likelihood Assessment Methodology
- □ Set up controlled access repositories at the appropriate classification level to store and share CTT information
- □ Obtain system under analysis Reconnaissance information
- □ Develop the Data Handling Plan for stowage and dissemination of classified material throughout CTT
- □ Develop ROE for the CTT and Teams
- □ Develop Exercise Schedule and Kickoff Agenda
- □ Develop Exercise Kickoff Briefs
- □ Train and Educate Team Leads, Data Analyst, and Note Takers
- □ Reserve the facilities, obtain proper equipment and supplies for Exercise
- □ Bring supplies to the Exercise, including notebooks or laptops for Note Takers

Step 2: Exercise Execution

- □ Keep each Team within the bounds that have been set by their perspective missions, ROE, and scenarios
- □ Adjudicate any questions or issues that arise
- □ Ensure participants are not sidetracked or bogged down on one point such that the exercise continues to flow
- □ Ensure Operational and OPFOR Teams are completing data products in the time allotted for each day of the Exercise.
- □ Ensure Note Takers capture the discussion and requests for information (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 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 Analysis Table
- □ Track homework and requests for information completion
- □ Draft results briefs (Executive and Technical)

Step 4: Reporting

- □ Produce Technical Brief detailing the results of the CTT to System Engineering and Test Personnel
- □ Produce Executive Brief to Program Office

Operational Team

Step 1: Exercise Preparation

- □ Review all read ahead material or other preparation as requested by the Control Team
- □ Define 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 that will help step through the functions, interactions, communication requirements, procedures and systems used during:
    - □ Mission preparation
    - □ Mission execution
    - □ Maintenance activities

Step 2: Exercise Execution

- □ Develop overall Operational Mission plan to execute in response to the mission orders provide by the Control Team
- □ Refine a brief that documents how operators would step through the functions, interactions, communications, systems, and procedures for:
    - □ Mission Planning
    - □ Mission Execution
    - □ Pre-mission and post-mission maintenance both scheduled and unscheduled
- □ Refine/update Mission Impact Methodology

Step 3: Post-Exercise Analysis

- □ Complete Working Meeting 1and 2 Homework
- □ Participate in risk assessment analysis
- □ Review deliverables for accuracy and completeness

Step 4: Reporting

- □ Review draft Executive and Technical Briefs
- □ Support outbrief of technical results
- □ Provide feedback from Exercise to help improve CTT process

OPFOR Team

Step 1: Exercise Preparation:

- □ Review materials provided by the Control Team
- □ Review all system reconnaissance information prior to the Exercise
- □ Define OPFOR Mission
- □ Develop a list Cyber Opposing Mission Objectives, classes of attacks based on the reconnaissance review
- □ Provide input to the Likelihood Assessment Methodology

Step 2: Exercise Execution

- □ Develop a list of potential attack surface pathways
- □ Present potential threat vectors and attack methods applicable to each Cyber Opposing Mission Objective
- □ Assess likelihood of proposed attacks

Step 3: Post Exercise-Analysis

- □ Complete Working Meeting 1and 2 Homework
- □ Participate in Post-Exercise risk assessment analysis
- □ Review deliverables for accuracy and completeness

Step 4: Reporting

- □ Review draft Executive and Technical Briefs
- □ Support outbrief of technical results
- □ Provide feedback from Exercise to help improve CTT process