TC 3-12.2.90

MISSION THREAD DEFENSE

FEBRUARY 2024

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

Training Circular
No. 3-12.2.90

Headquarters
Department of the Army
Washington, DC, 05 February 2024

MISSION THREAD DEFENSE

Contents

Page

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Figures

Preface

TC 3-12.2.90 provides a methodology for units to apply systems thinking to mission assurance, focusing specifically on cyberspace and cyber dependencies. This publication serves as an aid for units to understand system functions as a part of mission analysis to support planning and the Army design methodology.

The target audience for this publication are the staffs of units requesting, directing, planning, or conducting defensive cyberspace operations. It will also aid all those responsible for cybersecurity or assuring missions with significant cyberspace components or dependencies.

Commanders, staffs, and subordinates must ensure that their decisions and actions comply with applicable United States, international, and in some cases host-nation laws and regulations. Commanders at all levels must ensure that their Soldiers operate in accordance with the law of war and the rules of engagement (see FM 6-27). They also adhere to the Army Ethic as described in ADP 6-22.

TC 3-12.2.90 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. This publication is not the proponent for any Army terms. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

This publication applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent for this publication is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Branch, United States Army Cyber Center of Excellence. The technical review authority is the Cyber Protection Brigade, United States Army Cyber Command. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Cyber Center of Excellence and Fort Eisenhower, ATTN: ATZH-OPD (TC 3-12.2.90), 419 B Street, Fort Eisenhower, GA 30905-5735, or e-mail to usarmy.eisenhower.cyber-coe.mbx.gord-fe-doctrine@mail.mil.

This page intentionally left blank.

Introduction

This publication introduces mission threads as a useful concept for planning the protection and defense of missions or capabilities. A mission thread generally includes all activities required to execute a specific mission or task. Aligning thoughts and actions along an end-to-end set of activities (or mission thread) enables commanders, planners, analysts, and operators to better synchronize and focus their efforts to achieve a desired end state. Analysis of mission threads also allows units to identify and assess risk to critical functions. The results inform decisions to accept, reduce, avoid, or elevate the risk. Units may choose short-, medium-, and long-term actions to reduce the likelihood of a critical function failure and reduce its operational impact. Operational context—time, threat disposition, and organizational and geographic boundaries drive risk-informed actions and their intensity.

Mission thread analysis is particularly useful for planning protection measures in cyberspace. The pervasiveness of embedded computers means that many of the functions upon which the military depends utilize cyberspace. As with all professional endeavors, continuous learning and experiential growth are essential components of success. Mission thread analysis is no different as an analyst may be required to reengineer portions of a mission thread; assess and improve its defensive posture; and actively hunt to defeat adversaries on the network. This publication is meant to inform the reader of mission thread analysis and serves as a launching point for continued study and experiential growth within this segment of the Defensive Cyber Force mission. Cyberspace expertise is an essential component of mission thread analysis and may play a role in actions reducing the risk to the function.

This publication provides a general overview of the systems perspective and systems thinking based on joint and Army doctrine and introduces a process to systematically analyze critical functions. Analytic methods and how derived information informs protection measures are also covered. It is important to note that while some aspects of mission thread analysis and associated planning are unique, these functions are meant to nest within, rather than replace existing Army processes, such as the military decision-making process. This publication contains four chapters and two appendixes:

- **Chapter 1** introduces the concepts of systems thinking and mission threads and explains how mission thread analysis supports mission analysis and protection planning.
- **Chapter 2** explains the process for analyzing mission threads.
- **Chapter 3** provides additional detail on mission thread analysis.
- **Chapter 4** discusses the context for defending mission threads, how the results of mission thread analysis drive operations, and the roles and responsibilities for mission thread defense.
- **Appendix A** provides an example of how a cyber protection team could defend a mission thread.
- **Appendix B** provides an example checklist for an initial survey of a mission thread.

This page intentionally left blank.

Chapter 1

Applying a Systems Perspective

The interactions among cyberspace, the electromagnetic spectrum, and the physical environment create opportunities and vulnerabilities that may not be readily apparent. Targets that are otherwise secure in one domain may be directly or indirectly vulnerable through system interactions with, and dependencies on, other domains. This chapter introduces a method to use a system perspective during mission analysis to identify these interactions and dependencies and inform protection planning.

SYSTEMS

1-1. A *system* is a functionally, physically and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole (JP 3-0). Militaries rely on systems to sustain and conduct operations. They include weapon systems, such as the Bradley fighting vehicle, conceptual systems such as the military decision-making process, and composite systems, such as a unit's system for delivering indirect fires. The latter is built from other systems, such as radios, call-for-fire procedures, and artillery assets, and may be referred to as a system of systems. Changes or effects on one element can influence other elements and the output or results of the system. For example, the failure of a drivetrain immobilizes a vehicle or chemical impurities alter the effectiveness of propellant and the resultant ammunition produced by a manufacturing line.

1-2. Systems thinking, or systems perspective, is an analytic method to generate understanding of the greater function or output of multiple components involved in performing a function or mission. Systems thinking involves analyzing the components of a function along with their associated activities and interdependent outputs. Understanding complex functions from a systems perspective provides the commander with information regarding the overall purpose and interdependencies of a system and aids in the prioritization of defense of mission-critical components. Throughout the analytic process, planners consider the operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) to understand how or why a system functions and to identify potential threat avenues of approach into the defended mission.

1-3. As with intelligence preparation of the operational environment, employing a systems perspective is a staff function that will generally not be successful if performed in isolation. By understanding system components and examining problem sources or causes across a system, individuals and staffs are better able to develop and implement holistic solutions. Refer to FM 5-0 and ATP 5-0.1 for more information on systems thinking.

1-4. Because cyberspace is a constructed domain, composed of many interacting systems, systems thinking is particularly relevant for cyberspace operations and understanding the interaction of cyberspace and the electromagnetic spectrum with the physical domains of air, space, maritime, and land. The concept of mission threads facilitates system thinking oriented on a specific task or function. Joint mission threads are operationally driven, technically supported descriptions of the end-to-end set of activities required to execute a mission or mission task (CJCSI 3500.02C).

1-5. From a defensive perspective, the mission thread might be the steps needed to execute a critical function for the theater or organization such as the rapid deployment of forces into an area of responsibility. Alternatively, an offensive perspective may seek to deny the enemy's ability to conduct a function, such as suppressing the enemy's ability to conduct air defense. In both instances, units apply systems thinking to understand the processes, components, dependencies, and interactions from both a technical and organizational perspective. This understanding requires tracing the function through the nodes and linkages of the associated system to identify the mission thread. Analysis of the mission thread may reveal vulnerabilities and limitations of elements of the system or of the entire system. These insights can support offensive targeting and exploitation or protection planning and operational mitigation measures.

Note. For this publication, the term mission thread has the same definition as joint mission thread, but without an implied joint context.

1-6. Within the context of mission threads, the terms capability, function, task, and mission provide slightly different ways of expressing what the mission thread accomplishes. While these terms have subtle differences, any of them can be used as the starting point for identifying a mission thread:

- **Functions** focus on the outcomes of a system, what it does or can do.
- **Capabilities** are functions with associated conditions or performance metrics.
- **Tasks** are the actions, or steps to achieve the function.
- **Missions** are tasks with associated purposes.

1-7. Mission threads describe the entire process to perform a function and includes components and systems internal to the system. It encompasses the nodes, linkages, and other elements associated with a specific function of the system. Mission threads are inherently multidomain and may traverse network boundaries and network owners. In most instances the mission thread will extend beyond a single system. The thread may require actions performed by other systems, organizations, and personnel. Effectively protecting or targeting mission threads requires analysis beyond a specific portion of cyberspace, geographic area, or organizational responsibility.

Tasks, Functions, Capabilities, and Mission Threads

A tank has is able to engage targets at 4 kilometers. The function is destroying targets; the task is the act of doing so. The associated mission thread describes the round, the components of the tank, the crew, and all steps and conditions necessary to acquire and destroy the target.

1-8. Analysis of mission threads contributes to assuring a system's capabilities and functionality by identifying vulnerabilities and limitations. The description of a mission thread—including the level of detail and which elements are identified—will vary based on the scope, emphasis, threat, and other elements of the operational context. In the context of protection planning, the definition and description of the mission thread should be based on observation and analysis. This analysis typically starts as part of mission analysis and is refined and updated throughout the rest of the operations process. The analysis may also be used to inform acquisitions, risk assessments, and contingency plans. To analyze mission threads units must—

- **Define**—identify the task or function that must be accomplished and the process or activities through which it is accomplished.
- **Describe**—understand the how the system operates by analyzing the characteristics of components, their external dependencies, and their interactions with other components of the mission thread.
- **Assess**—determine the value as a target; identify the limitations and vulnerabilities of the system, how and where failures could occur, and what the impact is on the mission thread.
- **Refine**—refine the analysis to the appropriate level of detail and based on new understanding.

1-9. The mission thread analysis process reveals how impacts on different elements affect the overall function. For defensive cyberspace operations, identifying and analyzing vulnerabilities during planning contributes to the development of short-, medium-, and long-term mitigation measures. Because of the ubiquity of computers and the physical layer of cyberspace, these mitigation measures may apply outside of cyberspace or to functions and elements that might not be otherwise associated with cyberspace. For instance, a mission may require a redundant power source (generator) to ensure continuous operation. In this case, the generator control system may create an additional attack vector a malicious cyber actor can exploit. Mission thread analysis enables analysts to dissect the components of the larger system, revealing this type of interdependency and its associated vulnerabilities for follow-on mitigation measures. Ultimately, mission thread analysis results in risk assessments and decisions. Commanders can avoid, mitigate, or accept the risk. Their actions may include changing how the capability is employed, mitigating the risk throughout the mission thread, reengineering portions of the mission thread, or preparing to operate with diminished capabilities. Commanders may employ a mixture of these actions varied by time, geography, intensity, and triggering events as part of a holistic protection plan.

WHEN TO USE MISSION THREAD ANALYSIS

1-10. When applied to functions critical to friendly forces, mission thread analysis allows organizations to reduce operational risk. It can inform operational use of the function and drive protection actions such as survivability measures, security operations, and defensive operations. These actions may be simultaneous, sequenced over time, or planned as on-order missions. They may also range from short- to long-term actions and involve a variety of different stakeholders and warfighting functions.

1-11. Often no single organization can perform mission thread analysis organically due to cross-organizational processes and dependencies as well as the need for deep technical expertise that may only reside in select organizations, such as depot-level maintenance. Additionally, the analysis may identify external and non-DOD dependencies that require coordination with and support from interagency partners and the private sector. If organizational hierarchies prevent unity of command, the relevant organizations must coordinate and achieve unity of effort for effective analysis.

1-12. Mission thread analysis works best as part of a larger mission assurance or protection planning effort. It can assist defensive cyber forces who have been assigned a broad mission to focus and prioritize their efforts. As part of the mission thread analysis, analysts identify the mission-relevant terrain in cyberspace and analyze its potential impacts to the mission. Mission relevant terrain in cyberspace includes all devices, internal and external links, operating systems, services, applications, ports, protocols, hardware, and software on servers, required to enable the function of a critical asset or the completion of a mission. Some mission-relevant terrain in cyberspace may exist outside the DOD network.

PLANS FOR MAJOR OPERATIONS

1-13. Units responsible for planning major operations, contingencies, and other plans with long time horizons, may apply the concept of mission threads to analyze the critical functions and tasks that support those missions. This analysis informs operational risk assessment and may required adjusting plans. The unit may take actions to reduce the risk at the short-, medium-, or long-term, or plan contingency actions for the future based on the potential risk.

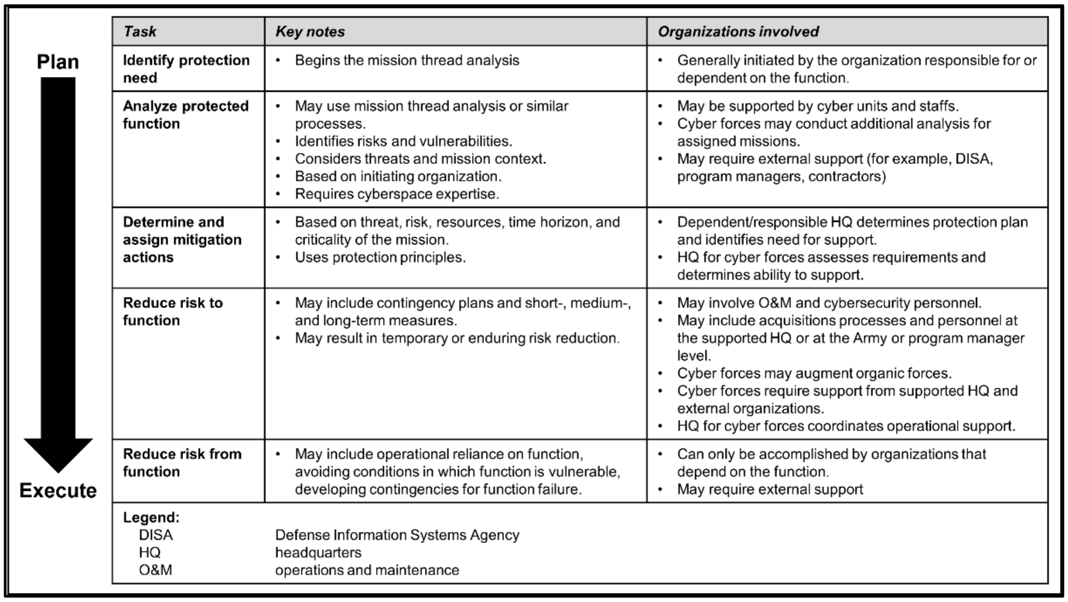
BROAD MISSION ASSURANCE OR PROTECTION MANDATE

1-14. Units with a broad mission assurance or protection mandate may analyze mission threads as part of their risk assessment or planning process. A mandate may be implicit or explicit and may include organizations with geographic or functional responsibilities, such as garrisons and cybersecurity service providers. Through their planning processes they must identify their critical functions or tasks. Mission thread analysis assists in identifying and assessing risks to operations. Units must prioritize identified risks and decide the appropriate actions to take. This may include accepting traditional risk management decisions of reducing the risk, avoiding the risk, or elevating the risk to a higher echelon for decision. Follow-on actions may also include tasks to further understand the risk, such as confirming or denying details and assumptions about the mission thread, testing execution, and simulating failure conditions.

CYBERSPACE DEFENSE MISSIONS

1-15. Cyber forces may be tasked to conduct cyberspace defense or support the continued operation of a mission thread. Their assignment is based on the protection priorities of echelons above corps and may include countering current and future threats. This assignment may be captured in a campaign or contingency plan. They may also be assigned to defend other Army activities in support of strategic priorities. The mission may explicitly identify the defended function based on the task or purpose, or the mission may require staff analysis to identify the implied functions based on a broader task and purpose.

1-16. Understanding the function requires support from the users and owners of the function. The identification and analysis of these functions focuses the defense by assessing risk and informing mitigations. Mission analysis by higher headquarters is essential to ensure that mission parameters are sufficient for the function and accomplishable by the assigned force. Because cyberspace mission threads often cross network boundaries, shortfall in mission analysis may result in the misallocation of forces, insufficient authorities, and ultimately mission failure. Figure 1-1 outlines the major tasks, key notes, and organizations involved in applying the mission thread concepts to protection.


Plan
Execute

Task	*Key notes*	*Organizations involved*
Identify protection need	• Begins the mission thread analysis	• Generally initiated by the organization responsible for or dependent on the function.
Analyze protected function	• May use mission thread analysis or similar processes. • Identifies risks and vulnerabilities. • Considers threats and mission context. • Based on initiating organization. • Requires cyberspace expertise.	• May be supported by cyber units and staffs. • Cyber forces may conduct additional analysis for assigned missions. • May require external support (for example, DISA, program managers, contractors)
Determine and assign mitigation actions	• Based on threat, risk, resources, time horizon, and criticality of the mission. • Uses protection principles.	• Dependent/responsible HQ determines protection plan and identifies need for support. • HQ for cyber forces assesses requirements and determines ability to support.
Reduce risk to function	• May include contingency plans and short-, medium-, and long-term measures. • May result in temporary or enduring risk reduction.	• May involve O&M and cybersecurity personnel. • May include acquisitions processes and personnel at the supported HQ or at the Army or program manager level. • Cyber forces may augment organic forces. • Cyber forces require support from supported HQ and external organizations. • HQ for cyber forces coordinates operational support.
Reduce risk from function	• May include operational reliance on function, avoiding conditions in which function is vulnerable, developing contingencies for function failure.	• Can only be accomplished by organizations that depend on the function. • May require external support

Legend:

DISA	Defense Information Systems Agency
HQ	headquarters
O&M	operations and maintenance

Figure 1-1. Tasks to apply mission thread concepts

Chapter 2
Analysis Methodology

Given a function, units analyze mission threads to identify anticipated, indirect, or non-obvious approaches through which a critical task, function, or capability might be affected. This analysis is inherently cross-functional and requires collaboration across the staff and with external organizations. When used for a function critical to friendly forces, the outputs of this process drive protection and defensive planning and shape employment considerations for the system and function.

MISSION THREAD ANALYSIS

2-1. Mission thread analysis may be used for both offensive and defensive planning. It is applicable when the following conditions exist:

- There is a function, capability, or tasks to be affected or protected.
- The relevant system to accomplish the function uses cyberspace or the electromagnetic spectrum.
- Direct methods to affect the target do not exist or are challenging to the attacker.

2-2. The tasks for mission thread analysis are—

- Define the mission thread—what and how.
- Describe the functioning and implementation—how and why.
- Assess the target value—what if and so what.
- Refine—what else.

2-3. The outputs of mission thread analysis may include—

- Effects chains.
- Short-, medium-, and long-term approaches.
- Actions targeting any or all components of the mission thread.
- Actions involving physical attacks on supporting components.
- Methods relying on a combination of actions.
- Actions or effects outside the defined physical or organizational boundaries.

2-4. Identification of critical or key interactions, dependencies, subtasks, and components can assist in focusing efforts. However, units must be disciplined in their analysis to avoid fixation, pursuing ‘rabbit holes,’ or never-ending analysis, as analyzing of all possible elements of a system may be an insurmountable task. Systems are often composed of other systems and analysis can be performed to increasing layers of detail. The scope of the analysis—its breadth and depth—is guided by mission requirements and understanding of the operational environment. Units should analyze threads progressively, looking at the breadth of one layer before pursuing additional analysis. Subsequent iterations of analysis may consider a broader scope for the mission thread or look at an additional layer of depth for one or more aspects of the thread.

2-5. The following concepts are useful when discussing the elements of systems and mission threads. When analyzing systems that are composed of other systems, these terms may be prefixed with ‘sub-’ to disambiguate references to lower-level systems from the overall system.

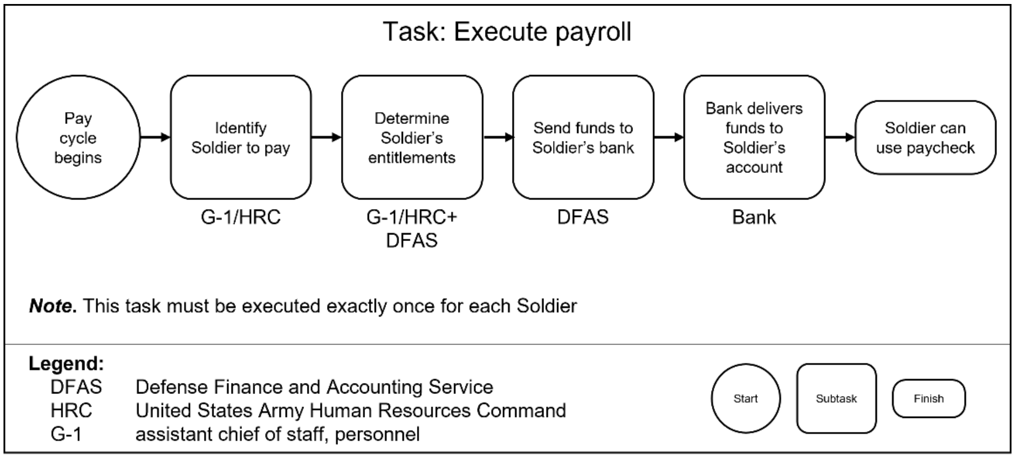
- **Process**—the sequence of a set of activities to accomplish a task. A process consists of a series of actions or steps and the transitions between them to go from a starting state or condition to an end-state. These steps involve one or more components and have additional dependencies.
- **Components**—elements of the system that perform action steps or are used by action steps. These may be systems or distinct portions of systems.

- **Dependencies**—external requirements of the system or process. Dependencies are outside the process and may act asynchronous to the process or system. They include conditions or characteristics of the state under which the process or individual steps operate. They are often expressed as 'given x' or 'assuming y.'
- **Interactions**—the informational or physical exchanges between components. Interactions can be viewed as inputs and outputs of system components.

DEFINE THE MISSION THREAD

2-6. Mission thread analysis starts with the identification of an initial task, function, or capability. During the define step, the staff refines the task, function, or capability being assessed and identifies the process or activities through which it is accomplished. The staff must both identify what constitutes successful functioning and what advantage a threat might seek. For example, if a threat has access to Blue Force Tracker, the system may still function properly, but the threat can now see the location of all friendly forces.

2-7. Defining the thread includes enumerating the subtasks or actions taken, the related components—personnel, equipment, or subsystems—and the inputs and outputs of each subtask. Critical to this step is understanding the accomplishment of the overall task or function to focus subsequent analysis. The results of this step should facilitate creating a high-level process or functional diagram. Figure 2-1 provides an example process diagram with appropriate additional information for the Department of the Army-level task 'execute payroll.'



Note. This task must be executed exactly once for each Soldier

Legend:

DFAS	Defense Finance and Accounting Service
HRC	United States Army Human Resources Command
G-1	assistant chief of staff, personnel

Figure 2-1. Example process diagram

2-8. When defining the mission thread, the unit establishes the conceptual logic of how the function is accomplished. The definition of the thread should identify the major elements and explain, in a non-technical manner, how the major subtasks combine to perform the function.

2-9. The example in figure 2-1 provides a high-level depiction of the mission thread. The process begins with the pay cycle and ends with the Soldier being able to use his or her paycheck. Each of the intermediate steps or subtasks is labeled with the actors involved. The example also includes assumptions about the starting state and characteristics of success. However, the description is relatively conceptual without in-depth detail, the assumptions use the terms 'all information' or 'appropriate system;' the actors are large and generic organizations; and the subtasks do not provide specific details.

2-10. During the define step, it is useful to ask what and how. Analysts should identify what happens before and after this step and how the pieces work together to accomplish the task. The following questions are useful when defining the mission thread:

- What is the task or function that is being accomplished?

- What constitutes successful or acceptable accomplishment?
- What is the trigger or starting condition for the task?
- What steps or subtasks occur, and in what order?
- Who or what completes each subtask?
- What is being accomplished in the subtasks?
- What is the input and output for the subtask?
- Are there critical assumptions or resource requirements for the subtask?

2-11. Techniques for identifying the subtasks and processes include conducting interviews and reviewing policies, procedures, and battle drills. It may require scoping to specific scenarios or vignettes and performing tabletop exercises or walking through the process.

DESCRIBE THE FUNCTIONING AND IMPLEMENTATION

2-12. Staffs build upon their understanding of the mission thread by describing each of the identified elements. This includes identifying the specific actors, task, purpose, performance criteria, and objects used during subtasks. The staffs describe the interaction between components, capturing where information flows between components and requirements such as those for timing, synchronization, or format. Throughout this step, the staff identifies any additional dependencies on external and shared resources or assumptions about the state of the system, such as available electrical power or satellite connectivity.

Common Dependencies Relating to Cyberspace

-
- Electricity.
- Positioning, navigation, and timing.
- Environmental controls and sensing (for example, heating, ventilation, and air conditioning).
- Networking and communications—Internet Protocol addresses, routing tables, and physical media (electromagnetic spectrum and wired).
- Authentication, public key infrastructure, and communications security.
- Industrial control systems and supervisory control and data acquisition.
- Update process.

2-13. The describe step adds detail to the general concept and context defined previously. For instance, the step ‘determine Soldier’s entitlements’ from figure 2-1 would expand to include the databases, interchange protocols, and procedures involved in making that determination. Successive iterations of the analysis process add increasing detail to the description of the mission thread and its elements. The level of detail for each iteration varies based on the mission requirements and the analysis up to that point. The description and subsequent refinement may use perspectives such as the cyberspace layers—physical, logical, and cyber-persona, the dimensions of the operational environment—physical, human, and information, and information technology models, such as the open systems interconnection model.

2-14. The mission-relevant terrain in cyberspace relating to a specific mission thread is a subset of the total components and external dependencies of that mission thread. The mission-relevant terrain in cyberspace for a given mission thread may include any element of cyberspace, including physical devices, software, data, or specific frequency bands of the electromagnetic spectrum.

Conceptual step: ‘system A updates system B’

-
- Different architectural approaches or design patterns:
- System A publishes updates to system B.
- System B requesting updates of system A.
- Different time aspects—
- Updates are synchronous based on time.
- Updates are asynchronous based on an event.
- Differences due to abstraction—
- System A is really three separate update servers that leverage load balancing.
- The system administrator runs a script that tells system B to get updates from system A.
- The update process is bi-directional because it uses transmission control protocol and transmission layer security, which require handshakes.
- Updates come from system A but are cached for the network on system C (or vice versa).
- The update is based on a uniform resource locator which first requires a Domain Name System query.
- Differences due to change—
- System B gets updates based on a uniform resource locator. The associated Internet Protocol address for system A has changed.
- System B used to get updated by system A, but a firewall rule prevents it, the software license expired, or the software has reached its end-of-life.
- System A was replaced with system D, but the documentation was not updated.

2-15. Analysts must focus on describing the thread accurately for the current depth of analysis. Describing the thread with excessive detail wastes effort, hinders understanding of the overall thread, and risks fixation or overlooking key insights. Analysts must be aware that different abstractions, changes in the network environment, and other factors cause differences between the description and reality.

ASSESS THE TARGET VALUE

2-16. Staffs use their understanding of the key elements and functioning of mission threads to determine what failures could occur, how they could occur, and what their impact would be. This understanding goes beyond cybersecurity compliance and vulnerability scanning. Instead, it considers how threats may use their capabilities to affect the defended function. This assessment occurs through multiple lenses, considering both the cyberspace domain and the physical domains. The perspective in which an element is critical may differ from the domain in which it is vulnerable or in which the ultimate effect manifests. For example, a retransmission site is critical for its function in cyberspace but is vulnerable to physical attack.

2-17. Each element of the thread—the components, dependencies, subtasks, and interactions—could impact the overall function or task. The staff identifies the most significant risks, building effects chains to understand the impact. These chains can be expressed as a series of propositions ‘if x then y’ that might build linearly or have a tree-like structure as multiple impacts converge or as an impact on one element cascades to many other elements.

2-18. Elements to consider during this assessment include—

- Starting state and ending state.
- Subtasks.
- Components.
- Dependencies and assumptions.
- Interactions between subtasks and components.

2-19. Questions analysts should ask during assessment of limitations and vulnerabilities include—

- What are the requirements of the element?
- What are the timing, accuracy, or other performance standards?
- What are the different ways the element could fail?
- How could failure be induced?
- What happens if this fails? What are the impacts along the thread?
- How do we know if it has failed?
- Are there redundancies, contingencies, or other mitigations?

2-20. Staffs combine their understanding of the vulnerabilities with their understanding of the threats. They must consider threat capabilities and the actions the threat would have to take to exploit the vulnerabilities and affect the function. Based on the planning context, staffs may generate threat courses of action relating to the critical function or specific vulnerabilities. These courses of action can inform assessments of the risk and may be used when determining measures to mitigate the risk.

Common Threat Considerations for Cyberspace

Items to consider:

- Routers, load balances, firewalls, virtual private network concentrators, and other network infrastructure.
- Accounts, accesses, and privileges.
- Applications, and services.
-
- Questions to ask:
-
- What account access or privileges are required for an action?
- What are the possible attack vectors?
- Which systems and personas have elevated access or privileges?
- How can a computer be physically and logically accessed and with what personas?
- What logical and physical mitigations prevent or detect rogue devices, software, and accounts?
- What software applications are running on the system and in the network?
- How is the software updated, patched, and otherwise managed?
- What tools exist on the system or in the network that could be exploited by a threat?
- How could the threat pivot through the system or the network?
- What shared systems and services exist?
- Are programs sharing a virtual machine, hypervisor, kernel, or physical machine?
- Where could the threat hide? Network infrastructure? Network interface cards?
- Where are monitoring blind spots?
- What monitoring occurs on routers, load balancers, industrial control systems, supervisory control and data acquisition systems, and weapon systems?

2-21. Staffs use structured analytic techniques (refer to ATP 2-33.4), such as brainstorming, what-if analysis, and red-teaming to perform this assessment. Tools such as the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) matrix provide a standardized approach to assess the value of different components in each domain and throughout the process or the phase of the operation. Refer to FM 3-60 for more details on the CARVER matrix.

REFINE THE ANALYSIS

2-22. This process is iterative. Staffs continue to refine their analysis to account for a changing operational environment, increase understanding, and support requirements for increased levels of detail. The level of detail is often driven by protection requirements and initial assessments of elements and their potential value as targets for adversaries. This refinement includes—

- Correcting or adjusting existing analysis based on new understanding.
- Analyzing a component or subtask in greater depth and detail.
- Broadening the scope to analyze dependencies.
- Accounting for existing redundancies or mitigations in the system or process.

- Updating the analysis for changes in the operational environment, disposition of forces, or system being analyzed.

2-23. The goal of refinement should be to provide the analysis necessary to meet operational requirements. Refinement must be prioritized based on areas that will be most productive.

OUTPUTS AND RESULTS

2-24. From the assessment and any subsequent refinement, units identify direct and indirect effects that—individually or through cumulative and cascading effects—impact the overall function. Refer to JP 3-60 for more information on direct, indirect, cumulative, and cascading effects. These effects represent vulnerabilities and limitations of the system. Based on identified vulnerabilities and limitations, the protection plan may include mitigation actions at the short-, medium-, and long-term time horizon. For example, after identifying that weather can cause power disruptions and affect the cranes used for railhead operations, the commander may require daily weather reports, purchase backup generators, or initiate acquisition of gasoline-powered cranes. Other actions to address vulnerabilities may include—

- Adding redundancies in equipment or processes.
- Adding information requirements to detect the start of a cascading effect.
- Mitigating the vulnerability.
- Mitigating the effects of the vulnerability.
- Changing methods or considerations for employing the system or function.
- Building in contingencies for the failure of the function.

2-25. For risks involving cyberspace and of sufficient priority, actions may include requesting cyber forces and assigning them cyberspace defense missions or missions that enable future survivability and defense. These missions generally involve mission-relevant terrain in cyberspace related to the defended mission thread. If there is insufficient risk or priority, units may still use the results of their analysis to understand their mission-relevant terrain in cyberspace and inform future decisions.

2-26. Based on their analysis of a mission thread, units may identify vulnerabilities outside their authority or scope. For instance, the organization might not have control over their software supply chain. In these instances, the organization implements controls within their scope to mitigate the risk and may coordinate with other organizations for more comprehensive mitigation measures. Significant external risk that cannot be effectively mitigated at the current level may warrant elevating the risk to a higher commander for decision.

This page intentionally left blank.

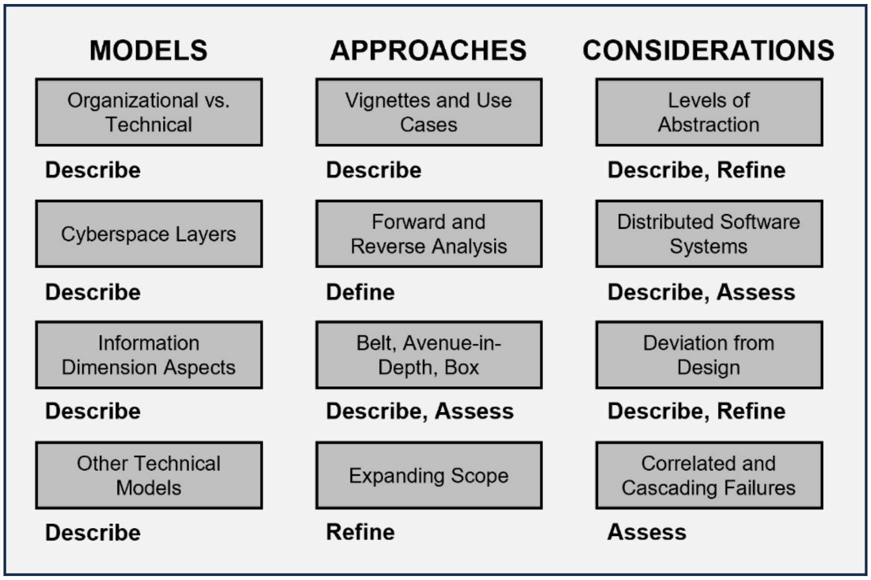
Chapter 3

Analysis Perspectives, Models, Approaches, and Considerations

This chapter describes several tools to assist in mission thread analysis. They primarily focus on methods that assist in the describe and assess steps.

TOOLS

3-1. Figure 3-1 depicts various analysis tools, along with the analysis step in which they are primarily used. The analysis methods discussed in ATP 2-33.4 and TM 5-698-4 can also be adapted to mission thread analysis.



MODELS	APPROACHES	CONSIDERATIONS
Organizational vs. Technical **Describe**	Vignettes and Use Cases **Describe**	Levels of Abstraction **Describe, Refine**
Cyberspace Layers **Describe**	Forward and Reverse Analysis **Define**	Distributed Software Systems **Describe, Assess**
Information Dimension Aspects **Describe**	Belt, Avenue-in-Depth, Box **Describe, Assess**	Deviation from Design **Describe, Refine**
Other Technical Models **Describe**	Expanding Scope **Refine**	Correlated and Cascading Failures **Assess**

Figure 3-1. Tools for mission thread analysis

PERSPECTIVES AND MODELS

ORGANIZATIONAL CONTEXT AND TECHNICAL DETAILS

3-2. Understanding the mission thread requires understanding not just the conceptual process but also the technical implementation of that process in physical systems or components and the organizational context in which it is executed.

- Technical details—the system responsible for processing data during one step is running Ubuntu 18.04.1 on a 32-bit advanced reduced instruction set computer machine (ARM) system.
- Organizational context—the user accounts are created by system admin in the network enterprise center who works 0900–1700 on Tuesday and Thursdays.

CYBERSPACE LAYER MODEL

3-3. The cyberspace layer model describes cyberspace in terms of three interrelated layers: physical network, logical network, and cyber-persona. Capturing the mission thread's elements and interactions within each layer can assist in arriving at a complete analysis of the thread in cyberspace. For example, expanding the analysis of an element with key properties for the logical network may identify its physical network location and that it is vulnerable to physical threats.

INFORMATION DIMENSION

3-4. The *information dimension* represents the content and data that individuals, groups, and information systems communicate and exchange, as well as the analytics and technical processes used to exchange information within an operational environment (FM 3-0). The information dimension's significant characteristics can be further evaluated in relation to the physical and human dimensions of the operational environment. Many of the interactions between elements of a mission thread occur within the information dimension. Analyzing these interactions through each aspect may provide additional insights.

OTHER TECHNICAL MODELS

3-5. Relevant technical models may be useful for describing technical aspects of the mission thread such as communication protocols or information exchanges. For example, the 7-layer open systems interconnection model may be useful for may be useful for capturing the details of an Internet-based information exchange between two devices. Similarly, it might be useful to apply the concepts of encapsulation to capture the multiple layers of encoding schemes and modulation techniques for a custom communication protocol between two military devices. These other models should be chosen because they fit the situation and should not be forced into every part of the analysis.

APPROACHES

3-6. There are a variety of approaches defensive cyber forces can use to analyze a mission thread. Some common approaches include—

- Vignettes and use cases.
- Forward and reverse analysis.
- Cursory assessments.
- Belt, avenue-in-depth, and box.
- Expanding scope.

VIGNETTES AND USE CASES

3-7. There may be a variety of methods through which some functions can be accomplished. For instance, engagement with indirect fires can be accomplished with different types of mortars and artillery which effects the headquarters through which the request must go through. In these cases, it is often useful to define a set of vignettes or uses cases that more specifically define the operational context for the function. The staff then analyzes each function. These cases may address all possible scenarios or may focus on the scenarios that are most important. In the previous example, the staff may create two scenarios. One that involves Soldiers calling for fire from assets organic to their brigade combat team and another involving preplanned targets for external assets.

FORWARD AND REVERSE ANALYSIS

3-8. While processes generally proceed from a starting step to an ending step, analysts may find it useful to consider the steps of the mission thread in a different sequence. Rather than building progressively from the starting step, they might begin with the end state and identify the preceding steps until reaching the beginning. They might also combine methods by working out from a branching point or working inward from two points. The variation is of particular use when defining the thread but may also be useful to describe or assess it.

CURSORY ASSESSMENTS

3-9. Cursory or hasty assessments provide a technique for analysts to focus their efforts on those areas most likely to be significant during both describe and define steps. For instance, units may spend less time on a system known to be out of scope, redundant, or secure. Alternatively, they may focus on single points of failure and exposed elements. This decision may use an abbreviated applicate of formula methods such as CARVER or be more informal based on mission analysis, experiences, or other considerations. Cursory assessments introduce the potential to overlook key insights based on analyst bias. If time permits after completing the analysis, units may revalidate cursory assessments with more deliberate assessments.

BELT, AVENUE-IN-DEPTH, AND BOX

3-10. Units may the use the course of action analysis methods of belt, avenue-in-depth, and box to guide analysis. Geographic boundaries might not be the most effective for all mission threads, and units might consider boundaries based on organizations, networks, or aspects of the process diagram generated from the define step. Units must pay particular attention when selecting boundaries to ensure critical vulnerabilities do not occur at or between the boundaries. Refer to ATP 5-0.2-1 for more information about course of action analysis methods.

EXPANDING SCOPE

3-11. After completing each iteration of analyzing the thread, staffs may determine that they need to further refine their understanding before they can fully assess the vulnerabilities and how to protect the mission. They generally have two options to expand the scope of analysis to improve understanding: develop more detail on critical elements of the system or bring key dependencies of the system into the scope of analysis. The choice to do either is contextually dependent. The choice is influenced by the availability of relevant documentation and subject matter experts as well as the element or dependency's importance for mission success. In either case, the additional analysis should focus on answering ambiguities or information gaps identified during previous iterations.

CONSIDERATIONS

3-12. Considerations for analysts include—

- Levels of abstraction.
- Distributed software systems.
- Deviation between design, implementation, and functioning.
- Correlated and cascading failures and impact propagation.

LEVELS OF ABSTRACTION

3-13. Different levels of abstraction may be appropriate for the virtual, logical, and physical layers. Abstractions are useful for avoiding fixation during the analysis process, but they can also hide important details of how the system functions. For example, it may be useful to identify a web service as a single entity at all three layers of cyberspace early in the analysis process. However, expanding the scope of analysis may identify that the service consists of a load balancer and web server. This is an important detail as there are attacks that exploit this specific setup (for example, request smuggling). This new level of detail may be sufficient for the logical layer, even if the physical layer is further broken down to identify multiple physical devices for the load balancer and web server.

DISTRIBUTED SOFTWARE SYSTEMS

3-14. Distributed software systems, such as a sharded database or cluster of compute resources, need special consideration during a systems analysis process. Conceptually, they act as a single system. However, this conceptual view hides significant complexity that can have consequences under abnormal conditions. Analysts must identify and understand the failover protocols, consensus protocols, and capacity management algorithms that the system uses. This informs whether manual intervention may be needed to reset after a sequence of failures. While these sequences are unlikely under normal conditions, many distributed systems assume network and component failures are random – or at least not actively malicious. In an adversarial setting, this assumption may be invalid and represent an otherwise unapparent vulnerability. Additionally, these protocols and underlying algorithms must choose between consistency of data in the system or availability of the system to service requests. Understanding the system's specific trade-off point and how a threat may be able to trigger failures may help identify vulnerabilities.

DEVIATION BETWEEN DESIGN, IMPLEMENTATION, AND FUNCTIONING

3-15. While engineering documents, network diagrams, and configuration documents are useful in describing the mission thread, analysts must keep in mind their limitations. Analysts must extract the level of detail appropriate for the analysis process rather than matching the analysis specificity to the provided data. For instance, including media access control addresses while still working at the conceptual layer may suggest a physical implementation that is incorrect. This often occurs when the documentation is out of date or incomplete such as when it does not include all media access control addresses for the system. Observation and logging of system operations, to include stimulating processes or portions of it, can be used to confirm, deny, and expand upon assumptions.

CORRELATED AND CASCADING FAILURES AND IMPACT PROPAGATION

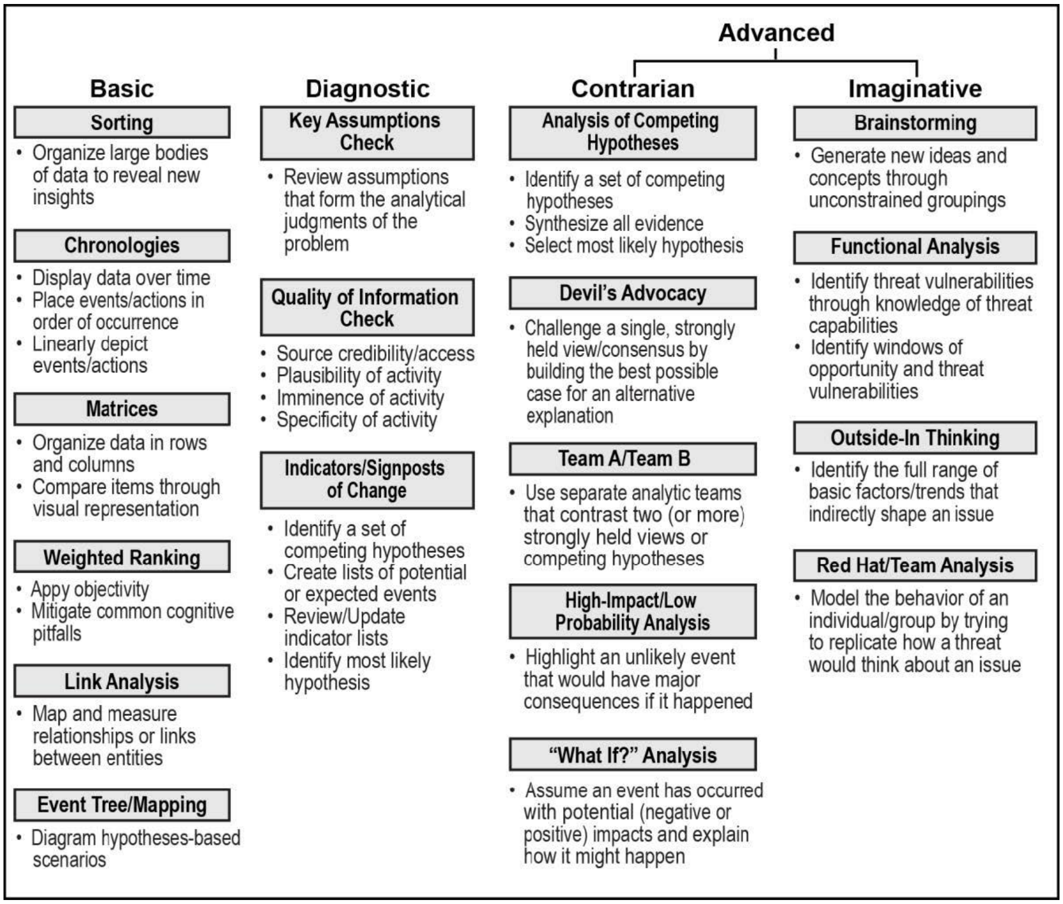
3-16. The concepts of correlated and cascading failures can be useful for determining how the failure of an element propagates upward to impact the mission thread. Many models for component failure assume that each failure of independent of other ones. However, this assumption is often wrong. A failure may indicate similar failures are likely (correlated failures) or cause—either directly or indirectly—additional failures (cascading failures).

3-17. An example of a correlated failure is hard disk failures. The lifespans of disks vary significantly even within a single product line. However, the lifespan of disks from the same manufacturing batch have much less variability. If all the disks in a system came from the same batch, there is a high risk of numerous hard drive failures following the first instance of a drive failing. As a result, what would otherwise be a minor failure in one component becomes several failures across the system with a much larger impact.

3-18. Cascading failures are similar in that they affect likelihood of other failures, but they cause, rather than simply indicate, the subsequent failures. Load balancing frequently exhibits this behavior. When one of the resources behind a load balancer fails, the current load is redistributed across the remaining resources. If the first resource failed because it was overused, this redistribution is likely to cause another resource to become overused and fail. The process repeats and turns a single failure of a redundant resource into a failure of the entire resource which is much more likely to impact the overall system.

ADDITIONAL ANALYSIS METHODS

3-19. Figure 3-2 on page 15 provides a summary of additional analysis methods that may be useful during mission thread analysis. Refer to ATP 2-33.4 for further information about how and when to use these structured analytic techniques.



Advanced

Basic

Sorting
- Organize large bodies of data to reveal new insights

Chronologies
- Display data over time
- Place events/actions in order of occurrence
- Linearly depict events/actions

Matrices
- Organize data in rows and columns
- Compare items through visual representation

Weighted Ranking
- Appy objectivity
- Mitigate common cognitive pitfalls

Link Analysis
- Map and measure relationships or links between entities

Event Tree/Mapping
- Diagram hypotheses-based scenarios

Diagnostic

Key Assumptions Check
- Review assumptions that form the analytical judgments of the problem

Quality of Information Check
- Source credibility/access
- Plausibility of activity
- Imminence of activity
- Specificity of activity

Indicators/Signposts of Change
- Identify a set of competing hypotheses
- Create lists of potential or expected events
- Review/Update indicator lists
- Identify most likely hypothesis

Contrarian

Analysis of Competing Hypotheses
- Identify a set of competing hypotheses
- Synthesize all evidence
- Select most likely hypothesis

Devil's Advocacy
- Challenge a single, strongly held view/consensus by building the best possible case for an alternative explanation

Team A/Team B
- Use separate analytic teams that contrast two (or more) strongly held views or competing hypotheses

High-Impact/Low Probability Analysis
- Highlight an unlikely event that would have major consequences if it happened

"What If?" Analysis
- Assume an event has occurred with potential (negative or positive) impacts and explain how it might happen

Imaginative

Brainstorming
- Generate new ideas and concepts through unconstrained groupings

Functional Analysis
- Identify threat vulnerabilities through knowledge of threat capabilities
- Identify windows of opportunity and threat vulnerabilities

Outside-In Thinking
- Identify the full range of basic factors/trends that indirectly shape an issue

Red Hat/Team Analysis
- Model the behavior of an individual/group by trying to replicate how a threat would think about an issue

Figure 3-2. Structured analytic techniques

This page intentionally left blank.

Chapter 4

Application for Cyber Forces

This chapter discusses the context for defending mission threads, how the results of mission thread analysis drive operations, and the roles and responsibilities of defensive cyber forces for mission thread defense.

OVERVIEW

4-1. Mission thread analysis is particularly relevant to cyberspace; the pervasiveness of embedded computers means that many functions use cyberspace. Cyberspace expertise is an essential component of mission thread analysis and may play a role in actions to reduce risk to the function. These actions may target results in the long-, medium-, or short-term for either increased overall protection as well as increased protection at specific times, in specific places, or against specific threats. These actions involve cybersecurity and cyberspace defense tasks and may include reengineering aspects of the mission thread, assessing or improving defensive posture, or on-call or time-limited operations to actively hunt for and defend against threat activity.

ANALYSIS ACTIVITIES

4-2. While mission thread analysis and mitigation actions are a staff function, this chapter focuses on their application by the cyber protection team (CPT) and similar defensive cyber forces. CPTs specialize in performing a variety of cyberspace defense actions. Cyberspace defense is actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures (JP 3-12). Through mission analysis, planning, and cyberspace defense actions, CPTs set the conditions for, and conduct, operations to preserve critical functions in support of Army and combatant commander priorities. The primary activities of CPTs and other defensive cyber forces are—

- Assessing defensibility in cyberspace.
- Conducting a cyberspace defense.
- Assisting in planning and mission thread analysis.
- Conducting reconnaissance and analysis to support planning.
- Supporting survivability of the mission thread.
- Advising rearchitecting of the mission thread, if necessary.

4-3. Figure 4-1 on page 18 shows how analysis activities nest in the context of supporting a larger protection mission. As part of protection planning, the supported organization decides on actions to take and controls to implement. These controls may include tasks for cyber forces to augment a supported organization, which must also be prioritized by commanders with operational control of those forces. The execution of these actions may be immediate, spread over time, or executed on order as part of contingency plans. While the figure shows the tasks in the context of a larger protection mission, they and the concept of mission threads are broadly applicable to defensive cyberspace operations. Forces may complete these tasks as independent operations, in combination as part of a larger operation, or as a series of operations. The complexity and specific scope of the mission determine degree of autonomy and integration required with external staffs and organizations.

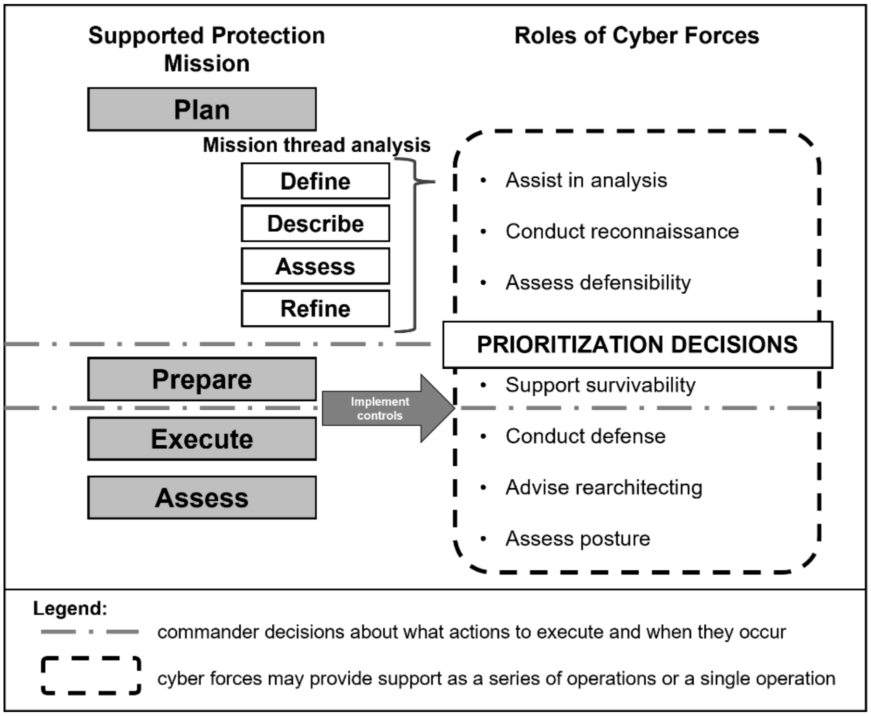


Figure 4-1. Analytic tasks within a protection mission

TASKS FOR CYBER FORCES

ASSESS DEFENSIBILITY IN CYBERSPACE

4-4. Cyber forces may be required to assess threats to, and the defensive posture of, a specific system, process, or other element of a mission thread. As part of this task, the cyber forces may refine the feasibility of potential threat courses of action identified during mission thread analysis. As part of this assessment, the cyber force anticipates how a threat would attack the system. They generally focus on determining whether the system's current configuration counters the identified threat capabilities or actions.

4-5. The actions for this type of mission will depend on the balancing the risk individual actions pose to current operations with the risk that incomplete or inaccurate information poses to future operations. For systems that are currently mission critical, this assessment may consist only of reviewing of documents, logs, and configuration files. As the criticality of future operations increases relative to current operations, cyber forces may take more intrusive actions. These actions range from emplacing additional sensors and actively pulling information off devices to conducting simulated attacks to validate proper functioning of defensive measures. Cyber forces may conduct this task at the end of an operation to validate improvements to the defensive posture.

CONDUCT A CYBERSPACE DEFENSE

4-6. Cyber forces may be tasked to defend critical systems from threats in cyberspace. These missions are generally bounded in time based on priorities by phase of an operation or another external context. When the cyber force conducts a defense, they are augmenting the defensive posture of the local and regional operators of the system and must ensure they apply the protection principles for their plan. When cyber forces employ their assets, they should be layered across the network with existing assets that provide similar capabilities and should only provide explicit redundancy for the most critical assets. Cyberspace defense missions—like defenses in general—must account for a transition back to steady-state operations. During these transitions, cyber forces must record any new information learned about the network and vulnerabilities for future reference by both the local operators, regional operators, and cyber forces conducting a later defense.

ASSIST IN PLANNING AND MISSION THREAD ANALYSIS

4-7. Cyber forces, including headquarters and staff elements, may assist organizations responsible for or dependent on a function with analyzing the cyberspace component of the associated mission thread. The supported organization must guide the analysis based on their priorities and understanding of operational context relating to the use of that function. Cyber forces provide technical expertise to the analysis process. This typically includes describing and assessing cyberspace elements of the mission thread. When refining understanding, cyber forces may define how cyberspace subtasks operate within the overall thread. This analysis may either be an independent task or the first step of a larger mission.

CONDUCT RECONNAISSANCE AND ANALYSIS IN SUPPORT OF PLANNING

4-8. As part of mission thread analysis, cyber forces may be required to conduct network reconnaissance to better understand the cyberspace aspects of the mission thread. This may include broad requirements to understand the function or specific requirements to validate assumptions or test functionality. Reconnaissance helps analysts identify and understand the deviations in descriptions based on the level of abstraction and between design and implementation (see chapters 2 and 3).

SUPPORT SURVIVABILITY OF THE MISSION THREAD

4-9. As part of preparation for, or in lieu of, an active defense, cyber forces may help local and regional operators harden and reengineer the system. These measures improve the enduring protection of the system and enable more effective augmentation for active defense. Cyber forces provide threat- and security-focused expertise to system operators. Based on the operators' understanding of the mission and system as-implemented, defensive cyber forces can develop a plan to deny or degrade the threat's ability to create effects. This may include more restrictive cybersecurity measures or tailored measures to disrupt specific steps of a potential kill chain.

ADVISE REARCHITECTING OF THE THREAD

4-10. Often the best way to improve the security of a mission thread is to rearchitect portions of its design to reduce its exposure in cyberspace. This approach is generally infeasible in the short- or medium-term because these changes are highly invasive and change the requirements of both the analyzed system and possibly adjacent systems with which it interacts. Rearchitecting a mission thread involves collaboration among operators, acquisition personnel, organizations that rely on the system's function, and subject matter experts in cybersecurity and system details. Defensive cyber forces can advise this process by identifying unnecessary exposure in cyberspace that could be avoided with a different design, for example, removing a centralized point of failure within the network or using formally verified software for critical components of the system.

CONSIDERATIONS FOR PLANNING AND EXECUTION

4-11. Units plan and prioritize protection efforts based on the results of mission thread analysis, the protection principles, and the operational context. While the commander responsible for a mission thread bears primary responsibility for its protection, other organizations support the effort based on their capabilities and priorities. The headquarters with operational control of cyber forces contributes to protecting the thread based on the relative priority of the thread and availability of protection assets. The acquisition system supports protecting the thread through refinement of future requirements and the purchase and delivery of materiel. All relevant organizations must communicate to ensure the protection plan remains accurate and sufficient as priorities and the operational environment change.

PROTECTION PRINCIPLES

4-12. Staffs and defensive cyber forces—such as a CPT—use the results of mission thread analysis and the protection framework to develop the defensive plan. While the mission owner has primary responsibility for the protection plan, every element supporting or augmenting the plan must understand these principles and integrate them into their portion of the plan. The principles of protection dictate that protection must be—

- Comprehensive.
- Integrated.
- Layered.
- Redundant.
- Enduring.

Comprehensive

4-13. The mission owner's plan should account for the full range of capabilities available from complementary assets like CPTs to rearchitect the system and update its acquisition requirements. Some of these assets may only be available for a short duration (for example, CPTs) while others may have long lead times before becoming effective—such as updating requirements. The plan should not fixate on a single capability but should use all allocated protection assets to preserve the thread's functionality.

Integrated

4-14. Every protection plan must be integrated into the larger context of the mission thread. The plan must not impose restrictions on the thread's functionality or conflict with how an adjacent organization or mission uses the thread. Additionally, the protection measures emplaced by different units should not interfere with each other. For example, a CPT operating on the network must coordinate with the local cybersecurity service provider and local network defenders to ensure that efforts to harden firewall rules or routing rules do not interfere with the CPT's sensor overlay.

Layered

4-15. Protection plans must employ a layered approach to defense. This layered approach consists of—

- Perimeter defense.
- Proactive monitoring.
- Security training.

4-16. It is important to remember the protection plan cannot solely consider the cyberspace domain. It must also account for vulnerabilities in the air, land, maritime, and space domains and the electromagnetic spectrum. It must account for protecting critical assets from both physical security and survivability perspectives. While the physical aspects of this are beyond the scope of this discussion, layered can also apply to the deliberate sequencing of measures across network or other boundaries. As an example, sensors emplaced to detect unauthorized or unexpected connections should not just exist at the exterior gateway. CPTs can identify additional sensor points throughout the network which would provide additional detection opportunities and reduce the likelihood that a threat can bypass the sensors.

Redundant

4-17. Critical vulnerabilities must be covered by multiple, distinct protection capabilities. This principle differs from layering in that it focuses on failure modes rather than depth of coverage. In cyberspace, the plan must account for systematic failure modes that affect multiple capabilities. A technical countermeasure employed by the threat may bypass all instances of a layered capability. A physical device failure may take down all capabilities sharing a span port while the network continues to function as normal. Redundant protection measures such as utilizing a firewall to block external connections, a network sensor further inside the network to alert and trigger response actions, and finally host logging and monitoring on the host itself.

4-18. These separate capabilities reduce the likelihood of a threat possessing an unknown capability that bypasses or neutralizes all protection assets and achieve an effect. CPTs must ensure that they balance operational efficiency with the principle of redundancy as sharing infrastructure may be expedient at the cost of robustness.

Enduring

4-19. The protection plan must be a continuous activity. While it may call for complementary capabilities or shifting organic assets to reinforce for periods of increased risk, it must be sustainable and continue to sufficiently mitigate risk. From a cyber perspective, this will often be the most restrictive principle for developing an effective protection plan. The analytical and technical capabilities of a CPT can temporarily contribute to a system's defensibility, but defenders must still mitigate risk to an acceptable level when those capabilities depart. Similarly, organic capabilities may be able to reinforce the security of a critical subsystem by moving sensors or increasing logging and monitoring activity, but this may not be sustainable if it requires increased manpower for analysis or forgoes longer-term maintenance or hardening efforts. CPTs can assist in establishing enduring capabilities for the mission owner by providing sensor coverage while the mission owner acquires additional capabilities and by assisting in the initial tuning of advanced analytics to the defended network.

PROTECTION MEASURES

4-20. When developing the protection plan, staffs apply a variety of layered protection measures across the system and sequence them in implementation. These measures provide different cost-benefit trade-offs based on speed of implementation, maintenance costs, and overall reduction to the mission's risk. For cyberspace measures, there are two broad categories to consider:

- Temporary measures that are time bound.
- Enduring measures that provide continual protection.

4-21. While some enduring measures can be implemented quickly, they often require longer time for initial implementation than temporary measures of similar protection value.

Temporary Measures

4-22. The protection plan may include temporary measures to mitigate additional risk for a limited time or against specific threats. These measures are only used for a limited time because they impose costs while they are active. Implementing additional controls or turning off non-critical functions of a system are some of the simplest protection measures and, but they often impact operational efficiency to some degree. Reinforcing existing control measures, such as monitoring or switching to allow-lists on a firewall, is another measure, but this often requires a corresponding increase in manpower. Finally, on-order missions from external organizations to reinforce the organic protection plan are generally temporary measures. This is because additional assets used to augment the defense may shift to other mission priorities based on phases of an operation or changes in the operational environment. Temporary protection measures may include—

- Turning off less critical features or capabilities.
- Additional restrictive control measures on system and data access.
- Enabling intrusion detection and intrusion prevention systems with high false positive rates.
- Frequently resetting or reimaging systems to known-good configurations.
- Hunt operations (refer to TC 3-12.2.98).

Enduring Measures

4-23. The protection plan should also include enduring measures that continue to mitigate system risks indefinitely. These measures often involve adding redundant capabilities, reengineering portions of the system to reduce vulnerabilities, or introducing new cybersecurity capabilities. The cost and time horizon of these measures vary substantially based on the scope of the changes from short-term measures (such as tightening the firewall rules of a network) to long-term solutions such as rearchitecting the system's requirements to inform the next acquisition cycle. Enduring measures include developing new cyberspace capabilities through the acquisition process or by DOD cyberspace capability developers. These capabilities may enable other enduring or temporary measures. Enduring protection measures may include—

- Adding additional intrusion detection and prevention capabilities to the system.
- Developing cyber capabilities which enable more effective or efficient protection measures.
- Hardening elements of the system to reduce their vulnerability.
- Adding redundant or contingency capabilities to reduce the criticality of elements.
- Coordinating with acquisition personnel and other organizations to rearchitect the thread so that it is more defensible.

TIME HORIZONS

4-24. Units may take actions with short-, medium-, and long-term time horizons. Short-term actions can be taken quickly but often have temporary or limited effects. Long-term actions often take more time, cost more, and require external coordination, but will deliver significant and enduring benefits. Units may use short-term actions as gap solutions based on a period of increased risk or while waiting for longer-term, enduring actions. There is not a clear distinction between time horizons, and it vary based on the resources and planning horizons of the organization.

INTENSITY, DURATION, AND TRANSITIONS

4-25. Increasing security in the short term often requires additional capacity, reduced efficiency for the affected users, or both. For instance, changing a firewall to block all but essential connections may make the network more secure at the cost of blocking connections and webpages that might useful but not essential. Similarly, adding security controls or more extensively monitoring security traffic may require a higher cost for people and equipment. Commanders balance the benefit of increased security with the cost and may use boundaries—such as geographic, network, or organizational—time, or conditions to focus the control to the time and place of highest risks. This may include 'be prepared to' missions and contingency plans.

4-26. Through the request and tasking processes, cyber forces can provide increased expertise and capacity for a finite duration. Supported organizations and supporting cyber forces coordinate to maximize the impact of these operations. This coordination includes deliberate plans to transition any knowledge or capabilities for enduring use and identifying those capabilities which cannot be sustained indefinitely.

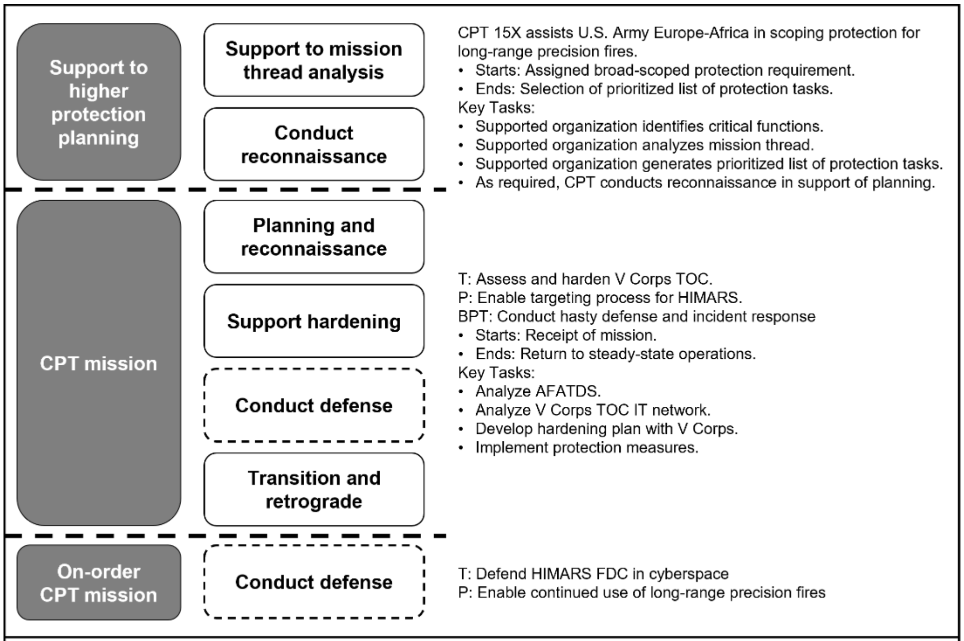
Appendix A

Cyber Protection Team Mission Perspective

This appendix outlines an example sequence of activities or missions for a cyber protection team supporting the defense of a mission thread. While the activities and timeline are based on historical missions, the specifics of such an effort are driven by the supported organization and will vary based on the mission thread and larger operational context.

MISSION ASSIGNMENT

A-1. USAREUR-AF is concerned about the risk to long-range precision fires and requests support to identify and protect the cyberspace aspects. ARCYBER assigns CPT 15X to support USAREUR-AF. Figure A-1 depicts the operational tasks CPT 15X conducts to support initial planning then conduct a well-scoped defensive operation.


Support to higher protection planning
Support to mission thread analysis
Conduct reconnaissance
CPT mission
Planning and reconnaissance
Support hardening
Conduct defense
Transition and retrograde
On-order CPT mission
Conduct defense

CPT 15X assists U.S. Army Europe-Africa in scoping protection for long-range precision fires.
- Starts: Assigned broad-scoped protection requirement.
- Ends: Selection of prioritized list of protection tasks.

Key Tasks:
- Supported organization identifies critical functions.
- Supported organization analyzes mission thread.
- Supported organization generates prioritized list of protection tasks.
- As required, CPT conducts reconnaissance in support of planning.

T: Assess and harden V Corps TOC.
P: Enable targeting process for HIMARS.
BPT: Conduct hasty defense and incident response
- Starts: Receipt of mission.
- Ends: Return to steady-state operations.

Key Tasks:
- Analyze AFATDS.
- Analyze V Corps TOC IT network.
- Develop hardening plan with V Corps.
- Implement protection measures.

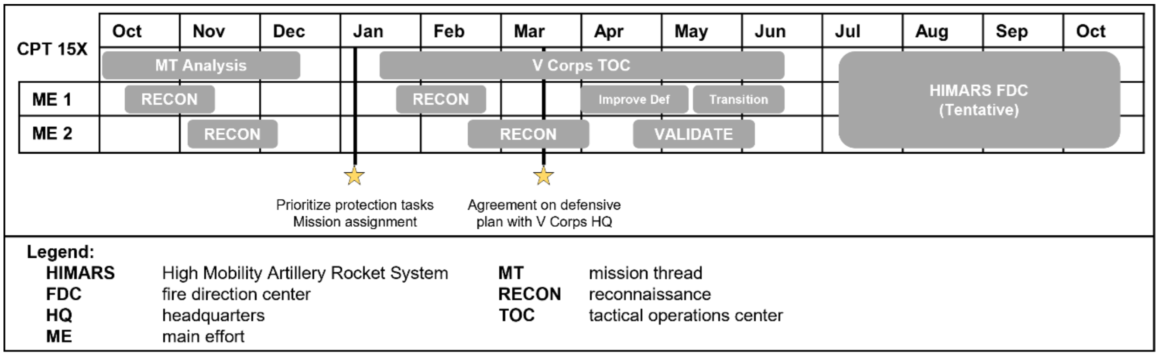
T: Defend HIMARS FDC in cyberspace
P: Enable continued use of long-range precision fires

Legend:

AFATDS	Advanced Field Artillery Tactical Data System	IT	information technology
BPT	be prepared to	P	priority
CPT	cyber protection team	T	task
FDC	fire direction center	TOC	tactical operations center
HIMARS	High-Mobility Artillery Rocket System		

Figure A-1. Example cyber protection team operational tasks

A-2. Figure A-2 on page 26 depicts the cyber protection brigade’s operational tasks sequenced over time by mission element.



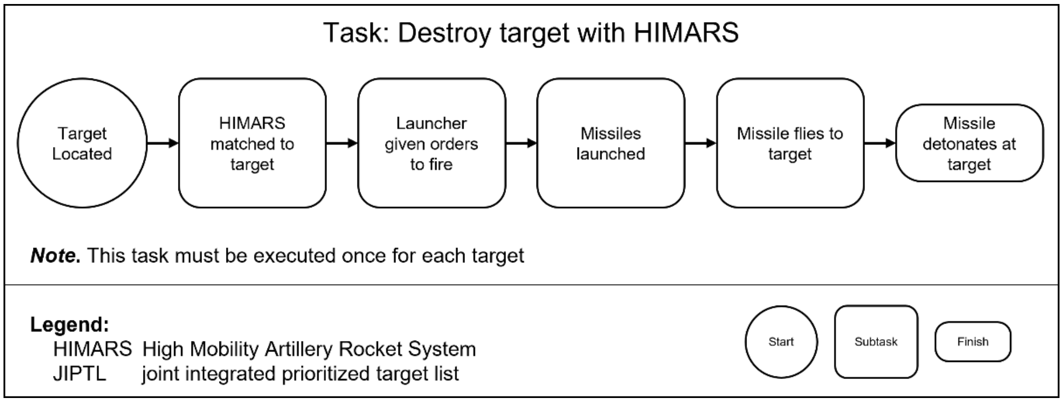
Legend:

HIMARS	High Mobility Artillery Rocket System	MT	mission thread
FDC	fire direction center	RECON	reconnaissance
HQ	headquarters	TOC	tactical operations center
ME	main effort		

Figure A-2. Notional cyber protection team operations timeline

SUPPORT TO HIGHER PROTECTION PLANNING

A-3. In the example in figure A-3, CPT 15X works with the USAREUR-AF fires cell and an identified field artillery brigade to define a mission thread. They decide to focus on the High Mobility Artillery Rocket System and generate an initial depiction of the mission thread. To describe the mission thread in more detail, the CPT conducts reconnaissance of the V Corps tactical operations center, the fire direction center, and the High Mobility Artillery Rocket System. The team's reconnaissance includes reviewing system and network design documents and collecting and analyzing traffic from select portions of the network.



Note. This task must be executed once for each target

Legend:

HIMARS	High Mobility Artillery Rocket System
JIPTL	joint integrated prioritized target list

Figure A-3. Example mission thread for destroying a target with High Mobility Artillery Rocket System

A-4. From the analysis, USAREUR-AF prioritizes the following cyber-related protection tasks:

- Assess and improve the defensive posture of the V Corps tactical operations center.
- Assess and improve the defensive posture of fire direction centers.
- Coordinate with the program manager to assess and harden the High Mobility Artillery Rocket System.

A-5. The team identifies the following out-of-scope dependencies:

- Dependency on Global Positioning System for High Mobility Artillery Rocket System guidance.
- Dependency on the joint process for connecting sensor to shooter.
- Dependency on the joint integrated prioritized target list.

ASSIGNED CYBER PROTECTION TEAM MISSION

A-6. CPT 15X is tasked to improve the cyberspace defenses of the V Corps tactical operations center to enable the targeting process for the High Mobility Artillery Rocket System. They begin by coordinating with the V Corps staff to plan a reconnaissance of the network on which their Advanced Field Artillery Tactical Data System and other supporting elements are located. They then conduct the reconnaissance and identify opportunities to harden the existing configuration as well as specific vulnerabilities in cyberspace that a threat could target, such as single points of failure in the network along the critical path of ordering the High Mobility Artillery Rocket System to launch. The CPT then works with the G-3 and G-6 to harden the relevant systems of record and supporting information technology infrastructure. As part of this process, the team performs a deliberate transition of any new protection measures to V Corps' control before retrograding.

ON-ORDER CYBER PROTECTION TEAM MISSION

A-7. Based on the results of the mission thread analysis process, other protection measures and the Army's operational priorities, ARCYBER may also task CPT 15X to be prepared to conduct a deliberate defense of the High Mobility Artillery Rocket System fire direction control system in support of USEUCOM's operation plans.

This page intentionally left blank.

Appendix B
Leader's Reconnaissance Checklist

This appendix provides an example checklist for conducting a leader's reconnaissance as part of mission thread analysis.

PRE-PLANNING AND COORDINATION

NAME OPERATION AND PUBLISH MISSION WARNING ORDER TO DEFENSIVE CYBER FORCES

- Establish SharePoint or other knowledge management site for mission repository.
- Establish IKE cyber tasking order and battlespace for defensive cyber forces at echelon.
- Notify stakeholders and inform of intent for mission thread defense—
- Mission owner leadership.
- Local network enterprise center leadership.
- Cybersecurity service provider leadership.
- Establish mission working group battle rhythm for cross-organizational coordination prior to leader's reconnaissance.

BUILD MISSION CONTEXT

- Understand mission owner task critical assets and determine relevance to mission thread.
- Review network documentation from the mission or network owner.
- Request counterintelligence estimate from the G-2 or S-2.
- Request circuit

DECONFLICT OTHER MISSIONS AND ASSETS

- Check with Headquarters, Department of the Army to determine other missions or assets that may be in-progress along the mission thread, including—
  - Defense Threat Reduction Agency.
  - Joint mission assurance assessment teams.
  - Threat Systems Modeling Office.
- Assess whether joint or other Service defensive cyberspace operations missions will affect mission owner networks.
  - Ongoing or scheduled red team assessments.
  - Ongoing or scheduled cyber readiness inspection activity missions.
  - Ongoing or scheduled network modernization activities.
  - Ongoing or scheduled adjacent unit defensive cyberspace operations (Joint Force Headquarters-Department of Defense Information Network or other Service defensive cyber forces).

VERIFY AND COORDINATE ACCESS

- Confirm visitor access requests and clearance transfer.
- Confirm specialty or non-standard access requirements.
- Determine personal protective equipment requirements.

> ***Note.*** Most industrial facilities require specialized safety training or the use of personal protective equipment while in the facility. Examples include arc-flash training, hard hats, hearing protection, eye protection, and safety shoes.

FINAL COORDINATION AND AGENDA DEVELOPMENT

- Send mission owners an enterprise and industrial control system questionnaire.
- Verify knowledge management portal and IKE repository are established for information sharing.
- Set leader's reconnaissance agenda with mission owner points of contact and align non-local stakeholders, including the higher headquarters and local cybersecurity service providers.

EXECUTION

This checklist represents a common 3-day mission thread defense leader's reconnaissance agenda. Leaders should adjust their agenda to the scope and timeline of the assigned mission.

DAY 1: UNDERSTANDING MISSION AND MISSION DATA

Defensive Cyber Force In-Brief to Mission Owner

End State: Mission Owner understands defensive cyber force capabilities and mission owner responsibilities in mission thread defense.

Mission Owner Overview—Overview of Tenants, Mission, and Footprint

End State: Defensive cyber forces can understand what mission owner does or provides, including functions and capabilities.

Physical Tour of Mission Site—Tour Mission Tread Areas, Including Task Critical Assets, if Applicable

End State: Defensive cyber forces understand the physical scope and expanse of the organization's cyber and physical footprints.

Data Lifecycle Discussion with Data Owners—How Employees Interact With Data of Interest

End State: Defensive cyber forces understand how employees interact with networks and data. This is usually a discussion in the mission owners actual work footprint (data laboratory, research area, production area, business operation area, or other area) with end users and the local network defenders.

> ***Note.*** During this step, defensive cyber forces should develop a sense of the scope and information technology footprint of the supported command. This affords defensive cyber forces a chance to talk to non-information technology personnel to better understand their interaction with networks and data, as well as cyber hygiene, such as authentication types, use of removable or optical media, and data security measures.

Data Flow Chart for the Organization Discussion

> ***Note.*** During this step, the mission owner defines a typical day in the life of sensitive data.

End State: Identify all stakeholders, information technology staff, and local defenders. Understand data dependencies supporting them mission function or capability—

- What data over which the mission owner does not have visibility the mission relies on.

- Whether task-critical assets depend on data.
- Where data over which the mission owner does not have control is produced, analyzed, processed, and stored. Possible locations include cloud systems, enterprise applications, a joint data system, cleared defense contractors, out-stations or satellite offices, federally funded research and development centers, or university-affiliated research centers.
- Continuity of operations sites.

DAY 2: UNDERSTANDING KEY TERRAIN IN CYBERSPACE AND DATA OVERLAY

Local Network Owner Discussion.

> ***Note.*** During this step, defensive cyber forces gain understanding of the role of local network owners and management of their mission networks—unclassified, classified, closed, or restricted, or unique mission networks. The cybersecurity service provider leadership should take part in this discussion.

End State: Defensive cyber forces understand the network footprint (with diagrams).

- Number of users by enclave.
- Geographic dispersion.
- External circuits and supporting agencies (cybersecurity service provider, network enterprise center, and the Defense Information Systems Agency).
- Whether local site visibility of the network and endpoints is adequate.
- Recent assessment results and trends.

Other Mission Networks and Cybersecurity Service Provider Discussion

> ***Note.*** During this step, defensive cyber forces gain an understanding of other mission networks that support the mission thread. Examples include Defense Research and Engineering Network and Secure Defense Research and Engineering Network.

End State: Defensive cyber forces understand—

- The current network footprint and security posture (with diagrams).
- The number of users by site.
- peering points to other networks.
- Ongoing modernization efforts.
- Whether local administrators have visibility over the network and endpoints.

Facility-Related Control Systems With Installation Management or Garrison Public Works

End State: Understand how facility related control systems communicate and on which network.

- Whether the site uses networks for heating, ventilation, and air conditioning; fire and intrusion alarms; or security badging.
- Who has visibility over this network traffic and how it is managed.

Industrial Control Systems Supporting the Mission, if Applicable Based on Mission

End State: Defensive cyber forces understand mission owner industrial control systems and how their network infrastructure and endpoints are managed and secured.

Non-Standard Tenants and Cleared Defense Contractor Discussion

End State: Defensive cyber forces understand other network tenants on Army-owned infrastructure.

- Whether cleared defense contractors support their own clients on the installation.
- Whether the cleared defense contractor has an office on post that runs its own network, or their network uses Army infrastructure.

DAY 3: TECHNICAL DEEP DIVE AND FOCUSED BREAKOUTS

> ***Note*****.** The defensive cyber force reconnaissance team can break out to address goals in parallel, based on their expertise.

Requests for Information and Breakout Discussions—Schedule Meetings to Dive Deeper into Areas of Concern

End State: Review defensive cyber force and mission owner objectives.

- Provide final requests for information for mission owner points of contact to answer.
- Revisit topics for clarity and any other day 1 or day 2 topic areas not addressed or well-understood.

Follow-Up Technical Exchange with Local Network Administrators (Network and System Technical Leads)

End State: Defensive cyber forces conduct an in-person, over the conference table review of current network architecture, sensor overlay, and endpoint visibility between defensive cyber force analysts and mission or site technical leads.

Leader's Reconnaissance Stakeholder Out-Brief

End State: Defensive cyber forces provide the mission owner and site leadership an out-brief that highlights the priority of protecting mission data, outlines actions and timeline for future engagement and mission milestones, and any major areas of concern based on the leader's reconnaissance.

> ***Note*****.** Time available will drive day 3 fact-finding priorities. In more well-scoped missions, this day may not be required or might be a half day with afternoon travel. In undefined missions, the day 3 agenda may be developed as information from day 1 and day 2 events bring to light formerly unknown data equities, networks, and concerns that require further understanding.

POST-RECONNAISSANCE ACTIVITIES

DEVELOP TRIP REPORT

- Discuss site and mission owner points of contact and areas of responsibility. An organizational chart with points of contact is useful in preparing the trip report.
- Discuss leader's reconnaissance findings in accordance with the agenda and address areas of concern and areas for further analysis.
- List leader's reconnaissance attendees in case further requests for information emerge or the mission is delayed or cancelled.
- List and identify any collected network documentation or artifacts and where defensive cyber forces will store them.
- Highlight who received the leader's reconnaissance out brief and any other senior stakeholders.

Collect Requests for Information that Require Defensive Cyber Force Support

Note. Some mission thread defense missions require support or additional information from other service providers. The defensive cyber force element should send requests for information to Headquarters, Department of the Army, the Defense Information Systems Agency, the Cyber National Mission Force, or other Service cyber forces, as necessary.

- Submit requests for information to appropriate commands and ensure dissemination of all answered requests for information.
- Authorize direct liaison appropriately to progress cross-cutting information between staffs.
- Refine battle rhythm to continue to progress mission planning and coordination across units.

Develop Defensive Cyber Force Mission Thread Decision Brief

- Geographic mission owner, site, and data overview.
- Logical mission owner, site, and data overview.
- Identified potential gaps and data limitations preventing defensive cyber force maneuver and technical reconnaissance.
- Begin drafting an operational approach.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ARCYBER	United States Army Cyber Command
ARM	advanced reduced instruction set computer machine
ATP	Army techniques publication
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CPT	cyber protection team
DA	Department of the Army
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
JP	joint publication
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
S-2	battalion or brigade intelligence staff officer
TC	training circular
TM	technical manual
USEUCOM	United States European Command
USAREUR-AF	United States Army Europe-Africa

SECTION II – TERMS

cyberspace defense

Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures. (JP 3-12)

information dimension

The content and data that individuals, groups, and information systems communicate and exchange, as well as the analytics and technical processes used to exchange information within an operational environment. (FM 3-0)

system

A functionally, physically and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole. (JP 3-0)

This page intentionally left blank.

References

All URLs accessed 1 June 2023.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. September 2023.

FM 1-02.1. *Operational Terms*. 9 March 2021.

FM 1-02.2. *Military Symbols*. 18 May 2022.

RELATED PUBLICATIONS

CHAIRMAN OF THE JOINT CHIEFS OF STAFF PUBLICATIONS

Chairman of the Joint Chiefs of Staff issuances are available online: https://www.jcs.mil/library/.

CJCSI 3500.02C. *Universal Joint Task List Program*. 19 December 2022.

JOINT PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/doctrine.

JP 3-0. *Joint Campaigns and Operations*. 18 June 2022.

JP 3-12. *Joint Cyberspace Operations*. 19 December 2022.

JP 3-60. *Joint Targeting*. 28 September 2018.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 6-22. *Army Leadership and the Profession*, 31 July 2019.

ATP 2-33.4. *Intelligence Analysis*. 10 January 2020.

FM 3-60. *Army Targeting*. 11 August 2023.

ATP 5-0.1. *Army Design Methodology*. 1 July 2015.

ATP 5-0.2-1. *Staff Reference Guide Volume 1*. 7 December 2020.

FM 3-0. *Operations*. 1 October 2022.

FM 5-0. *Planning and Orders Production*. 16 May 2022.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.

TM 5-698-4. *Failure Modes, Effects and Criticality Analysis (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*. 29 September 2006.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, Department of the Army Forms are available on the Army Publishing Directorate Website: https://armypubs.army.mil.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

RECOMMENDED READINGS

FM 3-12. *Cyberspace Operations and Electromagnetic Warfare*. 24 August 2021.

Index

Entries are by paragraph number.

This page intentionally left blank.

TC 3-12.2.90
05 February 2024

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2403101

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.