TC 3-12-2-98

HUNT OPERATIONS

FEBRUARY 2024

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

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil) and the Central Army Registry Site (https://atiam.train.army.mil/catalog/dashboard).

Training Circular
No. 3-12-2-98

Headquarters
Department of the Army
Washington, DC, 02 February 2024

Hunt Operations

Contents

Page

Preface ..... **iii**
Acknowledgements ..... **v**
CHAPTER 1 ..... **1**
IMPORTANCE OF HUNT OPERATIONS **1**
Defensive Cyber Forces and Cavalry 1
Role of Defensive Cyber Forces in Hunt Operations 1
Defensive Cyber Force Employment in Army Operations 4
Organizations 7
CHAPTER 2 ..... **11**
HUNT METHODOLOGY **11**
Components of Hunt 11
Hunt Tasks 23
CHAPTER 3 ..... **25**
THREAT **25**
Understanding Cyberspace Actors 25
Enemies, Adversaries, and Neutral Parties 25
Potential Threat Groups 26
Threat Characteristics 29
CHAPTER 4 ..... **35**
SHAPE, ENGAGE, AND CONSOLIDATE GAINS **35**
Understanding the Operational Environment 35
Shaping the Environment 35
Consolidating Gains 36
CHAPTER 5 ..... **37**
COMMAND AND CONTROL **37**
Command and Control for Hunt Operations 37
The Exercise of Command and Control 39
The Operations Process 39

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

Integrating Processes and Continuing Activities 51
CHAPTER 6 57
HUNT 57
Fundamentals, Methods, and Management 57
Hunt Techniques 58
Hunt Methods 60
Hunt Management 63
Hunt Assets and Systems 64
Forms of Hunt 65
General Hunt Planning and Execution Considerations 67
Hunt Handover 70
CHAPTER 7 73
SECURITY 73
Security Operations 73
Counterreconnaissance 76
Types of Security Operation 76
CHAPTER 8 85
SUSTAINMENT 85
Logistics 85
Hunt Sustainment 85
Source Notes 87
Glossary 89
References 93
Index 95

Figures

Figure 1-1. Defensive cyber force hunt planning cell 7
Figure 2-1. The components of proactive hunt (V diagram) 11
Figure 2-2. Information context for hunting 13
Figure 2-3. Iterative hunting process 17
Figure 2-4. Sample spot report-cyber 21
Figure 2-5. Sample cyber incident story board 22
Figure 3-1. Sophistication of potential threat groups 27
Figure 3-2. Pyramid of Pain for malicious cyber actor indicators 30
Figure 3-3. Sample defensive cyber force intelligence assessment 31
Figure 5-1. Simple network abstraction 41
Figure 5-2. Information requirements 43
Figure 5-3. Development of hunt guidance 44
Figure 6-1. Hunt operations framework 60
Figure 6-2. Hunt tempo 69
Figure 6-3. Example hunt guidance with engagement, disengagement, displacement, and bypass criteria 70

Preface

TC 3-12.2.98 provides tactics, techniques, and procedures by which defensive cyber forces conduct hunt operations as part of defensive cyberspace operations.

The tactics, techniques, and procedures contained in this publication are intended to be used as a guide and are not prescriptive. This publication outlines the framework in which defensive cyber forces conduct hunt operations to identify and defend against malicious activity in the DOD network. To properly apply the tactics, techniques, and procedures in this publication, readers should also be familiar with FM 3-12.

The principal audience for this publication is cyber professionals in the United States Army Cyber Protection Brigade who conduct defensive cyberspace operations and the commanders and staffs of units who request and receive defensive cyberspace operations support from the cyber protection brigade.

Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates 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 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 3-12.2.98 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. The mention of commercial products in this regulation does not imply endorsement by either the DOD or the United States Army.

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 Gordon, ATTN: ATZH-OPD (TC 3-12.2.98), 419 B Street, Fort Gordon, GA 30905-5735, or e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@army.mil.

This page intentionally left blank.

Acknowledgements

The copyright owners listed here have granted permission to reproduce material from their works.

The Source Notes lists other sources of quotations and photographs.

MITRE ATT&CK® Matrix, MITRE Corporation. https://attack.mitre.org/.

The Pyramid of Pain. SANS Institute, David Bianco. 2013. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

TTP-Based Hunting, MITRE and Roman Daszczyszak et al., March 2019. https://www.mitre.org/news-insights/publication/ttp-based-hunting.

This page intentionally left blank.

Chapter 1
Importance of Hunt Operations

"The cyber protection brigade at Fort Gordon, Georgia, is our defensive response force, our Cyber Cavalry"

Lt. Gen. Paul Nakasone, March 30, 2017.

DEFENSIVE CYBER FORCES AND CAVALRY

1-1. USCYBERCOM's approach to defensive cyberspace operations hunt is rooted in classical reconnaissance and security operations. During hunt operations, defensive cyber forces will engage in reconnaissance- and security-related tasks common to traditional cavalry forces.

1-2. Defensive cyber forces primarily defend the DOD network—the Department of Defense information network (DODIN). The *Department of Defense information network* is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone (JP 6-0).

1-3. Hunt operations enable supported commanders to conduct offensive operations to seize, retain, and exploit the initiative to gain and maintain a position of relative advantage in continuous competition in cyberspace. Hunt operations enable offensive and defensive cyberspace operations, DODIN operations, and influence operations. Defensive cyber forces conduct hunt operations to develop the situation and to identify, create, and preserve options to seize, retain, and exploit the initiative.

1-4. Effective hunt operations confirm or deny the commander and staff's initial understanding and visualization of the tactical and operational situation and further develop the intelligence picture to allow the commander to describe, direct, lead, and assess operations and make effective decisions.

1-5. Hunt operations provide a continual flow of information that helps commanders cope with uncertainty, gain and maintain threat contact under favorable conditions, identify opportunities, prevent surprise, and make timely decisions. Hunt operations create advantageous conditions for future offensive operations that seize, retain, and exploit the initiative.

ROLE OF DEFENSIVE CYBER FORCES IN HUNT OPERATIONS

1-6. Hunt is a tactical mission task undertaken in friendly controlled or contested cyberspace to identify and characterize threat presence and activity on the network. A hunt operation is analogous to reconnaissance and security tasks.

1-7. Hunt operations allow commanders to visualize the operational environment, understand the situation, and make decisions. An *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Hunt operations answer commanders' critical information requirements, mitigate risk, and identify threat weaknesses.

1-8. Defensive cyber force organizations employ appropriate combinations of mission elements and analytic support cells using a range of analytic techniques at echelon to both fight for information and develop the situation through stealthy tactics and observation based upon the mission variables of mission, enemy, terrain, troops and support available, time available, civil considerations, and informational considerations—METT-TC (I). Examples of the information for which the defensive cyber force fights include—

- Malware and other indicators of compromised security posture.
- Threat activities in the defended network.
- Threat targeted key terrain.
- Point of origin of an attack within the network.
- Attribution of a given attack.

- Mitigation points and actions.

HISTORICAL ROLES OF CAVALRY

1-9. Armies have used cavalry forces to capitalize upon their significant advantage in mobility that made them well suited for long-range reconnaissance and security operations. Cavalry forces' ability to fight also made them well suited for creating and providing options for the commander, shaping subsequent fights, and enabling timely decisions to seize, retain, and exploit the initiative. Reconnaissance and security gave commanders the ability to concentrate forces at decisive points while protecting against surprise. Cavalry continued to play key roles such as—

- Conducting reconnaissance operations to detect enemy weaknesses and strengths.
- Conducting security to provide early warning and maneuver space.
- Covering retreats.
- Countering enemy cavalry.
- Countering enemy infantry attacks.
- Administering the decisive blow through isolation and pursuit.

THE MODERN CAVALRY-LIKE ROLE OF THE DEFENSIVE CYBER FORCE

1-10. The three fundamental missions of the defensive cyber force are hunt operations, mission thread defense, and incident response. This training circular discusses the core functions and tactics of hunt operations. Hunt operations set conditions for successful follow-on operations by the defensive cyber force or the unit for which they are conducting hunt operations.

ENABLING COMMAND AND CONTROL

1-11. The cyber mission force conducts continuous hunt operations mainly through their organic defensive cyber force organizations. Cyber mission forces must counter adaptive and determined threats and consolidate tactical gains. Effective hunt operations improve situational understanding and help commanders to—

- Understand the technical and tactical dynamics within an area of support.
- Visualize operations in the context of mission variables of METT-TC (I).
- Achieve situational understanding.
- Develop the situation through action in close contact with enemy.
- Execute operations with higher degrees of flexibility, adaptability, synchronization, and integration.
- Identify or create options to seize, retain, and exploit the initiative.

PROVIDE ACCURATE AND TIMELY INFORMATION TO SUPPORT THE OPERATIONS PROCESS AND INTELLIGENCE COLLECTION CYCLE

1-12. Most defensive cyberspace operations begin at a position of intelligence and information disadvantage. Typically, information about the friendly network terrain and situation is incomplete. Serialized intelligence products are often unavailable or are lacking in detail, depth and context. The defensive cyber force must self-generate accurate and timely hunt information on the enemy and network terrain. To understand, visualize, describe, direct, lead and assess combat operations, the cyber mission force relies on information collection assets, including—

- Intelligence from national intelligence sources, military intelligence units, electromagnetic warfare, and cyberspace operations platforms. These assets assist in developing and adjusting the plan during the operations process.
- Surveillance information from across the cyber operations force's operational forces in Joint Force Headquarters-DODIN, the Defense Information Systems Agency, and the Service entities responsible for installing, operating, securing, and maintaining the network.
- Hunt—The commander's best means of rapidly closing information gaps, visualizing their operational environment, and understanding their situation.

1-13. Commanders require timely and accurate information during the execution of operations. Operations in cyberspace are no different. Timely information on the impacts from within and through cyberspace directly affect commanders at every echelon from tactical to strategic operations and sustainment. The

primary source of timely and relevant information in cyberspace is the hunt elements of the defensive cyber force.

1-14. Defensive cyber force units—

- Hunt threats and mitigate the threat's ability to conduct cyberspace deception in friendly networks.
- Provide the most reliable means of assessing defensibility of friendly networks.
- Operate actively, not passively. Defensive cyber forces find the threat, further develop the situation, and force the threat to reveal more information, including intentions and fighting ability.
- Disseminate relevant information to commanders immediately.
- Develop recommendations for supported commanders to seize, retain, and exploit the initiative.

1-15. By performing hunt, defensive cyber forces provide commanders combat information needed to seize opportunity or reduce risk at the right place and time. Defensive cyber forces can often inform the commander of strengths and weaknesses that are not readily evident when observing traditional warfighting domains. When properly employed, they can inform the commander on the threat's composition, disposition, strengths, and weaknesses. Defensive cyber forces can also locate the decisive point in cyberspace. Uniquely, the decisive point in cyberspace may be something otherwise deemed as innocuous.

Note. Combat information is reported to commanders and staffs to aid in situational understanding and decision making, rather than processing and analysis to turn it into tactical intelligence. In this context, combat information is not restricted to combat operations; it applies across the competition continuum. Refer to FM 3-0 for more information about the competition continuum—competition, crisis, and armed conflict.

OPERATE AS COMBINED ARMS DEFENSIVE CYBER FORCE AND SIGNAL TEAMS

1-16. Defensive cyber force organizations are part of a broader combined arms teams that, when paired with traditional signal and cybersecurity assets, form close support relationships that utilize appropriate combinations of signal, cybersecurity and defensive cyber force operations to accomplish their mission. Various organizations, from tactical signal support to DODIN-wide cybersecurity assets, are equipped, organized, and trained to identify enemy actions and defend the unified network. While conducting secure and defend tasks, they may identify opportunities for hunt operations. Defensive cyber force units, conversely, must move continually and at times rapidly to positions of tactical advantage to observe, hunt, and enable counterattack. Defensive cyber force units require organized, integrated, and synchronized support from all signal and cybersecurity assets to ensure effective hunt operations.

1-17. Defensive cyber forces satisfy commanders' critical information requirements by employing all available combat power. The enemy continually seeks to protect or conceal vital cyber access and key tools and assets. Defensive cyber force units fight for information within their capabilities to develop the situation rapidly and accurately report the specific details of the enemy and the tactical situation. The close support between signal and cybersecurity assets and defensive cyber force allows hunt efforts to develop the situation to maximize information collection and assist the commander in visualizing and understanding the area of operations.

1-18. These operations are the simultaneous or synchronized employment of signal and cybersecurity assets and defensive cyber force to seize, retain, and exploit the initiative. Effective close support operations are built upon relationships, mutual trust, and a common understanding of the operational environment and the mission. They require detailed planning, coordination, and synchronized employment of forces to achieve the commander's objectives and ensure freedom of movement and action.

PROVIDE REACTION TIME

1-19. Army commanders use a supporting defensive cyber force to develop tactical and operational depth and to create sufficient reaction time and maneuver space. Defensive cyber force organizations conduct stealthy hunt operations to detect and observe enemy developments in depth across the supported commander's critical networks, data, applications, and weapons. The defensive cyber force develops the situation by fighting for information to buy the time required for an effective response to enemy actions in cyberspace. Hunt operations develop the situation to prevent Army commanders from fighting at a

disadvantage. Effective hunt operations provide space to maneuver, creating flexibility for the commander to respond to unanticipated enemy actions or developments. Hunt operations provide time for the commander to assess the situation, determine a course of action, issue orders, make continuous assessments, issue additional fragmentary orders, and maneuver.

PRESERVE COMBAT POWER AND ACHIEVE ECONOMY OF FORCE

1-20. To develop the situation, defensive cyber forces locate enemy forces, identify key network terrain, and interact with the organic signal and cybersecurity forces. As they do so, defensive cyber forces provide reaction time and maneuver space to allow commanders to preserve critical warfighting networks. Defensive cyber forces provide security for commanders' network-enabled assets that protect and preserve combat power and force generation.

1-21. In the offense, effective defensive cyber force operations seek to deny the threat a means to disrupt or degrade force deployment and maneuver. In defensive tasks, an effective defensive cyber force operation provides early warning, counters enemy cyber reconnaissance efforts, and identifies enemy cyber elements to enable counterattack by offensive cyber forces of the cyber national mission force. As a result, defensive cyber force organizations, by their role, apply the joint operations principle of economy of force—expend minimum-essential combat power on secondary efforts to allocate the maximum possible combat power on primary efforts. The capabilities of the defensive cyber force are made more robust by the flexible response enabled by virtually projecting cyber forces from the central hubs of cyberspace operations tied to the global cryptologic sites. Refer to JP 3-0 for more information about the principles of joint operations.

FIGHT FOR INFORMATION

1-22. The information friendly commanders seek is generally of equal importance to the enemy, who will attempt to protect that information. Defensive cyber forces seek to preserve freedom of maneuver and overcome enemy efforts to disguise critical information. Defensive cyber forces fight for information within their capabilities to develop the situation rapidly. They accurately report the details of the situation for actions inside the friendly network or beyond it at the discretion of the supported commander, in coordination with the designated cyber commander.

DEFENSIVE CYBER FORCE EMPLOYMENT IN ARMY OPERATIONS

1-23. Army commanders and staffs, supported by their cyberspace electromagnetic activities sections, determine the cyber hunt requirements for the operation. A cyber hunt may be initiated based on three primary cues:

- Through receipt of exquisite intelligence indicting a compromise. Intelligence about a threat actor, that threat's tactics, techniques, and procedures, and its actions in a particular network drive hunters to quickly identify the threat and develop a plan to counter it.
- Based on what a commander considers key terrain in cyberspace, commander's critical information requirements, or what intelligence indicates is a set of networks a threat is likely to target. For example, a threat may be interested in critical infrastructure and key resources in the continental United States, which may cause a commander to systematically hunt on all critical infrastructure and key resources in the United States to confirm or deny adversary presence and harden the networks to prevent future intrusions.
- If an unexplained anomaly is detected and the supported commander requests a hunt to confirm or deny presence of threat activity.

1-24. The commander issues hunt planning guidance early to ensure that hunt tasks (see paragraph 2-49) can precede the mission and identify options to seize, retain, and exploit the initiative. Hunt operations often begin before completion of course of action analysis step of the military decision-making process so the defensive cyber force unit can inform the planning effort.

1-25. Defensive cyber forces conduct hunt tasks in contact with enemy forces and supporting signal and cybersecurity forces. This allows commanders to accomplish their core missions. Defensive cyber forces enable supported commanders' ability to take appropriate actions at the decisive moment to seize the initiative or consolidate gains while preparing for the next mission.

1-26. For hunt operations to be most effective, they must be nested with the global authorities derived from Commander, USCYBERCOM. Defensive cyber forces function optimally when they are held as part of the overall cyber mission force. Army commanders should consider the type of defensive cyberspace operations support they need early in the planning process using their organic cyberspace electromagnetic activities sections and their reachback to subject matter experts at ARCYBER. Commanders and staffs should develop cyberspace information requirements throughout the operations process and continuously assess, add, or delete requirements during planning and execution.

1-27. Defensive cyber force commanders and staffs conduct operations consistent with the fundamentals of hunt. They assist in identifying gaps or weaknesses as well as opportunities to exploit and improve the situational understanding. Hunt operations answer priority intelligence requirements and enable the commander to make decisions and direct forces to achieve mission success. Hunt operations enable successful offense, defense, and stability tasks. Commanders and staffs identify information gaps during the military decision-making process and continuously assess, adapt, add, and remove information requirements throughout the operation. Staffs identify specified, implied, and essential tasks to achieve mission success during mission analysis, reviewing available assets and identifying resource and information shortfalls.

1-28. During mission analysis, staffs identify critical facts and assumptions that aid in the development of the commander's critical information requirements. Commander's critical information requirements consist of priority intelligence requirements and friendly force information requirements, which enable timely decision making. A *priority intelligence requirement* is the intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support (JP 2-0). Priority intelligence requirements identify information about the enemy, terrain, weather, and civil considerations that the commander considers most important and have impact upon future decisions. A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).

1-29. Based on identified information requirements, staffs assign tasks to prioritize, manage, and develop information collection leading to future decisions. As staffs identify information necessary for successful execution, the staff recommends and assigns appropriate tasks for defensive cyber force units to conduct hunt and provide answers that allow the commander to make decisions and capitalize on opportunities.

General Employment of Defensive Cyber Forces

1-30. During operations, the commander and staff's time and resources are balanced between four major activities in a continuous learning and adaptive cycle called the operations process which includes planning, preparing, executing, and continuously assessing the operation. The activities of the operations process are sequential but not discrete—all overlap and recur as circumstances demand. Refer to ADP 5-0 for more information about the operations process.

1-31. Commanders implement early information collection and security to help protect and prepare the force for operations. Defensive cyber force units often begin operations in the planning phase to shape preparation activities and execution.

1-32. Commanders take every opportunity to improve their situational understanding before execution of the mission. This requires defensive cyber forces to conduct aggressive and continuous information collection. Through information collection, commanders and staffs continuously plan, task, and employ defensive cyber forces to collect timely and accurate information to help meet commander's critical information requirements and other information requirements.

1-33. The force is often vulnerable to enemy cyber attacks during preparation, when forces are deploying into a theater of operations, or staging prior to operations. Cyber-related security tasks—screen, guard, and cover—are essential during preparation. Defensive cyber force units assigned cyber-related security missions often execute these missions while the rest of the force prepares for the overall operation.

1-34. Defensive cyber forces continuously conduct wide-area hunt against the threat, who may manifest in unexpected ways across the globe in their efforts to impact U.S. operations.

1-35. As in all defensive cyberspace operations, a defensive cyber force's higher headquarters typically leverages defensive cyber forces to gain situational understanding to—

- Inform commanders at echelon.
- Provide early warning and reaction time.
- Defeat enemy cyber reconnaissance efforts.
- Act as the lead defensive element.

1-36. Commanders task-organize defensive cyber forces with the combat power necessary to accomplish the mission, based on the mission variables of METT-TC (I). The USCYBERCOM unit of action is the mission element. Mission elements are made effective when tied to the authorities and assets of the cyber mission force. They often operate as part of a flexible response force that can grow to include cyber assets up to the battalion or brigade task force level. These task forces can include assets from across USCYBERCOM, ARCYBER, NETCOM, the Defense Information Systems Agency, the Department of Homeland Security, and others. Defensive cyber forces are further augmented by military intelligence units and the broader intelligence community.

HUNT CONSIDERATIONS AT ECHELONS ABOVE CORPS

1-37. Commanders at echelons above corps depend on situational understanding to seize and retain the initiative. To support the requirement for timely hunt and security at echelons above corps, the Army forces commander and staff will determine the missions and supporting technology dependencies that are critical to success. These missions may change by phase or decisive point in the overall operation. The preservation of these missions and their supporting technologies typically ties to the overall operation and is critical to the success of that operation.

HUNT CONSIDERATIONS AT ECHELONS CORPS AND BELOW

1-38. Corps and division commanders require similar situational understanding to seize and retain the initiative. However, how they experience enemy cyber activity is often different. Corps and divisional units operate inside the network umbrella of the Army forces commander for unclassified, classified, and mission partner networks. This means that threat tactics, techniques, and procedures enabled by computer-to-computer attacks are already defended in depth. However, units may be susceptible to electromagnetic attack, which may disrupt, degrade, or deny access to key operational assets and technology. While the defensive cyber forces addressed in this publication are not trained, manned, or equipped to counter threat electromagnetic warfare, understanding that such an attack may originate in the electromagnetic spectrum is a useful component of the larger mitigation strategy. Electromagnetic warfare forces are held as Service assets at ARCYBER, at theater level, and electromagnetic warfare companies and platoons organic to units at echelons corps and below.

1-39. The defensive cyber force's proficiency increases with time as leaders, Soldiers, and Department of the Army civilians become competent in their individual and collective tasks and adjust to the mission variables of METT-TC (I) that differ between areas of operations. Rotating the mission and designation between formations challenges the desired expertise gained by job qualification specialization and sustained operations on like terrain.

OPERATIONS STAFF AND DEFENSIVE CYBER FORCE EMPLOYMENT

1-40. Defensive cyber force commanders and staffs integrate operations and intelligence in the conduct of hunt tasks. A commander, through the G-3 or S-3, focuses combined signal, cyber, technical sustainment, and remote operations efforts to execute successful hunts and enable situational understanding.

1-41. The G-3 or S-3 at echelon coordinates and synchronizes hunt tasks and operations across their formation. The G-3 or S-3 allocates organic, attached, and supporting enablers while ensuring that hunt operations orient on assisting the commander and subordinate units in the accomplishment of key tasks consistent with the concept of the operation. In concert with higher echelon and subordinate staffs, the G-3 or S-3 ensures defensive cyber force operations are nested, complementary, and focused on mission accomplishment.

OTHER STAFF AND DEFENSIVE CYBER FORCE EMPLOYMENT

1-42. Defensive cyber force units establish coordination within the staff to synchronize. This cell might include the G-2 or S-2, technical directors from enabling and supporting staff directorates, analytic support

officers, cyber integration technicians, and G-6 or S-6 (remote operations) (see figure 1-1). At the same time, to achieve this intent, the defensive cyber force commander task organizes subordinate defensive cyber force units with the necessary combined arms, analytic, developer, and signal (remote operations) support to execute the mission. At the conclusion of mission analysis, the headquarters directing the defensive cyber force publishes hunt guidance and a fragmentary order to initiate hunt operations. An analytic support element is usually the lead hunt element in the brigade. Parallel and collaborative planning between the defensive cyber force and higher headquarters staffs is essential to timely execution of operations as well as the integration of intelligence.

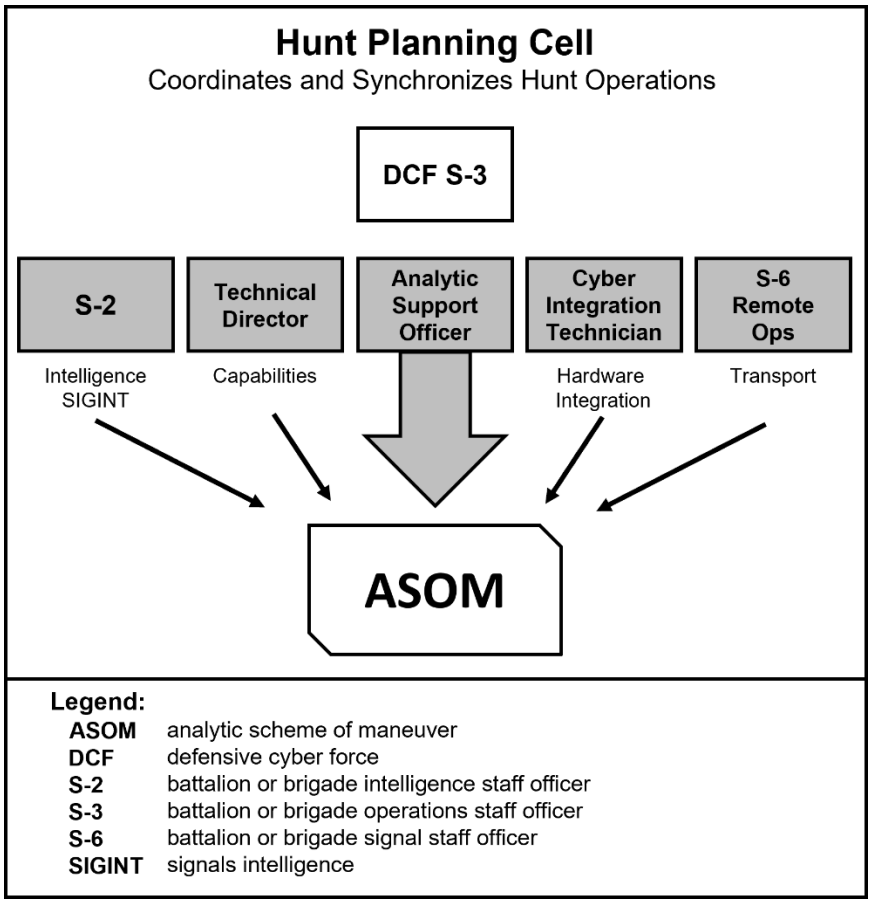


Figure 1-1. Defensive cyber force hunt planning cell

ORGANIZATIONS

1-43. Hunting is foundational to successful defensive cyberspace operations. Through effective analytic employment and continuous refinement and hunting, defensive cyber forces develop and sustain the necessary understanding to counter adaptive and determined threats. Hunt tasks help their supported command reduce and adapt to uncertainty. They are essential to understanding the tactical cyber environment, visualizing operations, developing the situation, and identifying or creating options for supported commanders to seize and retain the initiative. Defensive cyber force units provide flexibility, adaptability, and depth to the commander's operations, synchronizing and integrating cyber elements to seize and retain the initiative based on relevant understanding of the situation.

1-44. Defensive cyber force units provide information on enemy activity, disposition, early warning, and protection. Defensive cyber force hunt operations preserve the commander's freedom of maneuver. Successful hunt allows the commander to initiate operations under advantageous conditions to defeat the enemy and accomplish the mission.

DEFENSIVE CYBER BRIGADES

1-45. Defensive cyber brigades, which include the cyber protection brigades of all Army components, are the Army's fundamental cyber hunt force. In crisis, the combatant commander may build a joint task force around the defensive cyber brigade. The defensive cyber brigade includes units and capabilities able to meet specific mission requirements.

1-46. Battalions with defensive cyber forces are the main instrument of executing hunt tasks across the Army, each hunting a unique assigned area of operations or occupying an assigned battle position or observation post. Elements of Service cyber component commands, cybersecurity service providers, network enterprise centers, or signal support elements may be task organized to support forces in execution of hunt operations.

ROLES AND ORGANIZATIONS

1-47. The organizations in the defensive cyber brigade that conduct hunt operations consist of defensive cyber force battalion task forces and mission elements. Defensive cyber force battalion task forces and mission elements share most of the same capabilities and limitations.

Common Capabilities

1-48. Defensive cyber force battalion task forces and mission elements share certain capabilities:

- Fighting for information within unit capabilities.
- Gathering information about network-enabled threat cyber actors.
- Supporting tipping and cueing of other cyber forces across internal and external networks.
- Executing continuous, accurate, and timely broad area hunt for threats.
- Rapidly developing the situation.
- Reducing risk and generate opportunities by providing information that characterizes and neutralizes the threats' abilities in and through cyberspace.
- Assisting in shaping networks in the area of support by providing information and feedback to signal and cybersecurity professionals that enhance hunt operations.

Common Limitations

1-49. Defensive cyber force battalion task forces and mission elements share the following limitations:

- They require support from their parent unit and its ties to the analytic and intelligence elements of the cyber mission force to perform hunt operations as an economy of force role.
- They lack the ability to defend networks beyond a small tactical or temporal event without the support of more robust signal and cybersecurity assets.

Defensive Cyber Force Battalion Task Forces

1-50. Defensive cyber force battalion task forces conduct hunt and security operations through contact with threats and in conjunction with signal and cybersecurity professionals. They maintain contact with threats to fight for information while preserving their own freedom of maneuver. They shape the operational environment to create conditions favorable to friendly cyber forces while ensuring deterrence and enabling the supported commander to defeat the threat at a time and place of the commander's choosing.

Additional Capabilities

1-51. In addition to their capabilities in common with mission elements, defensive cyber force battalion task forces are capable of—

- Conducting collaborative and parallel planning that fully integrates with higher and adjacent units and optimizes employment of defensive cyber force assets to support operations.
- Enabling reestablishment of command and control by repelling a threat attack that caused a disruption.

Additional Limitations

1-52. In addition to their common limitations with mission elements, defensive cyber force battalion task forces—

- Have limited sustainment assets that frequently operate over extended distances.
- Lack the ability to defend networks beyond a small tactical or temporal event without the support of more robust signal and cybersecurity assets.

Mission Elements

1-53. Mission elements conduct hunt operations throughout the area of support of their parent unit. Mission elements use an analytic scheme of maneuver to synchronize and drive their tactical contributions to an accurate operational picture of the area of support. That operational picture can focus on any mixture of the mission variables of METT-TC (I) when necessary. However, to develop an accurate operational picture of more complex network terrain requires additional time.

1-54. The mission element's common operational picture helps form a battalion task force common operational picture in command nodes. This common operational picture allows commanders within, and external to, the parent unit to accurately assess the situation and inform course of action decisions.

1-55. In addition to hunt tasks, mission elements augment the supported unit's cybersecurity efforts in support of the analytic scheme of maneuver. Mission elements often develop the situation in close support with signal and cybersecurity forces. Refer to ATP 6-02.71 for more information on cybersecurity tasks.

1-56. Mission elements can conduct defensive tasks though they typically support higher-level offensive and defensive task completion through the conduct of hunt and cybersecurity tasks. The commander considers the mission element's capabilities and limitations before employing them in any specific mission.

1-57. As the eyes and ears of the battalion task force, the mission element is the battalion commander's primary information collection asset in cyberspace. Hunt operations provide combat information the commander needs to conduct better informed planning, to direct operations, and to visualize the area of support. Hunt operations collect information on threat location, disposition, composition, and intent. The information the mission element collects allows the commander to proactively shape the network and to accept or initiate contact at times and places of their choosing for intelligence gain or combat effect.

1-58. Mission elements conduct hunt operations throughout the battalion task force's area of operations. The mission element develops the situation by focusing on the hunt objectives outlined in the analytic scheme of maneuver.

1-59. In addition to their common limitations with battalion task forces, mission elements—

- Have no organic sustainment assets.
- Are incapable of broad area hunt or 24-hour operations without reachback support.

ANALYTIC SUPPORT CELLS

1-60. The analytic support cell conducts proactive (pull) hunt operations to satisfy the commander's critical information requirements and inform decisions regarding application of defensive cyber forces towards targeted hunts (pursuit). The analytic support cell provides operations support to mission elements with analytic planning and advanced analytic capabilities. Therefore, the analytic support cell is the single greatest combat multiplier and force integrator within the defensive cyber force. It synchronizes the execution of analytic schemes of maneuver at echelon in concert with the analytic support officers who dictate analytic priorities to mission elements. Analytic support cells conduct proactive hunt (pull method) and develop the situation so the commander has the necessary facts to employ the appropriate combat power in a targeted hunt (pursuit method). The analytic support cell consists of—

- Analytic support officer.
- Data engineer.
- Senior analysts.
- Master gunner.

Proactive Hunt

1-61. Proactive hunt is a hunt that determines which routes are suitable for maneuver, where the threat is strong and weak, and where gaps exist, thus pulling the main body toward and along the path of least resistance. This enables commanders to exercise initiative and agility. In proactive (pull) hunt operations, the commander uses the products of intelligence preparation of the operational environment and the analytic scheme of maneuver interactively and iteratively. The commander obtains combat information from available defensive cyberspace operations hunt assets to determine a preferred course of action for the tactical situation based on the mission variables of METT-TC (I).

Targeted Hunt

1-62. Targeted hunt (pursuit method) refines the common operational picture, enabling the commander to finalize the plan and support shaping and decisive operations. Targeted hunt is normally used once the commander commits to a scheme of maneuver or course of action. In targeted hunt, the commander uses the products of intelligence preparation of the operational environment and the analytic scheme of maneuver interactively with combat information from hunt assets to support a course of action.

Chapter 2

Hunt Methodology

The nature of cyberspace and the threat environment are evolving and dynamic. This requires continuous threat hunting, supplemented by intelligence to enable rapid target identification and characterization. In the absence of intelligence, defensive cyber forces collect and analyze data to develop situational understanding of the operational environment, including threat activity and intent. Often, information obtained through hunt operations is adequate for rapid detection and characterization of a wide variety of cyberspace threats. Once a threat actor is identified on the network, defensive cyber forces can take immediate action to eliminate the threat from the network and eliminate the exploited vulnerability.

COMPONENTS OF HUNT

2-1. Hunting has two components—characterization of malicious activity and hunt execution. *Malicious cyber activity* is activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communication systems, networks, physical or virtual infrastructure controlled by computers of information systems, or information resident thereon (NSA/CSS Policy 11-11). The components of hunting should be continuously updated based on new information about threats and the network. The flow of updates is visualized in figure 2-1, commonly called the V diagram. There are three layers of related activities, focusing on the malicious activity, analytic processes, and data processes.

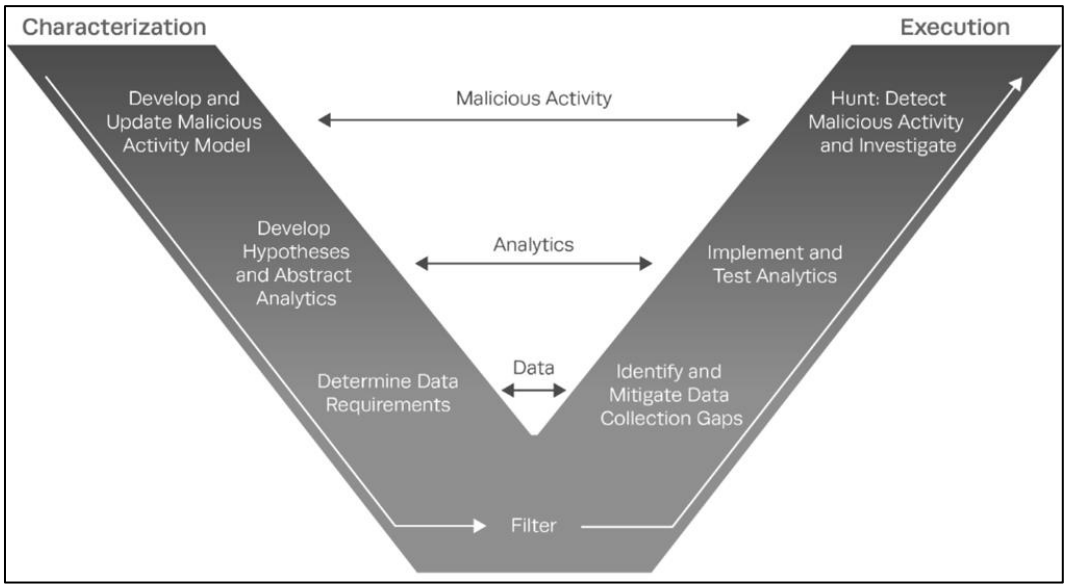


Figure 2-1. The components of proactive hunt (V diagram)

CHARACTERIZATION

2-2. Characterization of malicious activity starts with developing or updating the generic adversary model of behavior to identify all tactics, techniques, and procedures a threat may use—regardless of which threat group, environment, or targeted network. For each tactic, technique, or procedure identified in the model, an analyst proposes one or more detection hypotheses that are formulated as abstract analytics. These hypotheses and abstract analytics are used to determine what data is necessary to collect. For each hunt operation, the hunt element should filter these data collection requirements and analytics based on the specifics of the terrain and situation of that hunt. Characterization entails—

- Developing and updating a malicious activity model.

- Developing hypotheses and abstract analytics.
- Determining data requirements.
- Filtering.

2-3. The defensive cyber force conducts threat research, collects data, renders information, and leverages intelligence to characterize and develop situational understanding of threat behavior in cyberspace, including—

- Windows enterprise networks.
- Industrial control systems.
- Supervisory control and data acquisition systems.
- Infrastructure devices.

2-4. It is important during this analysis to consider which aspects of threat behavior are transient, or easy for the threat to change or mask, and which aspects of behavior are likely to remain constant or prove difficult for the threat to change (for instance, established tactics, techniques, and procedures). The focus is on information that can be converted into tactics, techniques, and procedures-based analytics rather than brittle indications of compromise such as file hashes, Internet Protocol addresses, or domain names (that is, focus on the top of the Pyramid of Pain). This information needs to be organized to enable filtering by dimensions in the analysis space by time, terrain, and behavior; by the threat; or by the phase of the threat's operation.

2-5. A common question asked at this stage is how to prioritize tactics, techniques and procedures for analytic development. There are many possible effective methods to prioritize analytic development. Because various scenarios require different approaches, no method is prioritized or given favor over another in all situations. Analysts should choose one of these analytic methods based on the situation and mission:

- **Based on threat tactics, techniques, and procedures**—a rough approximation would be to count distinct references on techniques and build a heat map on what is most prevalent across groups and software, either based on the examples already in the adversarial tactics, techniques, and common knowledge (ATT&CK®) framework or based on locally collected cyber threat intelligence or past incidents. For all of these usages, keep in mind previous reporting is probably only against a subset of usage, and it should be used with caution and an understanding of the biases in the data (for example, the data in the ATT&CK® framework itself is only based on openly reported incidents, while data from past incidents may not include attacks undetected at the time).
- **Based on currently available data**—analysts start with which data types are available and incorporate new sources as they become available. This is a very practical approach as collecting new data might require modifications to operational systems or purchasing new tools.
- **Based on the threat's lifecycle**—analysts focus first on early stages of the threat's lifecycle with initial access, execution, and discovery tactics. Detecting activity at this stage may have a greater benefit than detection during later stages when response actions might be too late.
- **Based on technique bottleneck**—analysts start with what needs to happen and what most threats are likely doing (for example, credential dumping or remote system discovery).
- **Based on differentiation between malicious behavior and benign behavior in the operational network**—there may be some threat tactics, techniques, and procedures which are known to be very unlikely to be used by the organization's intended users and system administrators. Indications of those behaviors should have very low false alarm rates.
- Based on a combination of the above approaches.

Hypotheses, Analytics, and Data Requirements

2-6. Based on threat behavior, defensive cyber force elements propose hypotheses to detect behaviors in the form of an abstract analytic. Hunting effectiveness is determined by data that adequately captures the activity of the threat from data sources and sensors properly located within the terrain to successfully observe it. Specific data requirements for hunting fall into two broad categories—collection requirements and modeling requirements.

2-7. To identify collection requirements, a list of required data and data sources should be created based on the set of abstract analytics developed. These data sets and sources should become more readily known and available as hunt elements mature their capability and familiarity with terrain.

2-8. Sensor and data source selection play a key role. It is helpful to consider the merits of which sensor or data source to select based on the amount of contextual information they provide the analyst balanced against the volume of data generated by each data source. It is generally true that more context equates to more volume (network bandwidth utilized for collection; storage, indexing, and analysis resources for processing), so analysts are unlikely to capture all possible data (full content collection from hosts and network devices) to support a hunt. By starting with an understanding of threat techniques and abstract analytics, an organization can reduce its data collection load by tailoring the collection strategy for the desired analytics. However, context is critical to effectively triage suspicious events and separate truly malicious activity from suspicious but ultimately benign activity. Therefore, it is important to collect sufficient data to enable analysts to make connections between analytic hits. An *event* is any observable occurrence in a network or system (NIST SP 800-61 Rev. 2). An analytic hit is an indication from an analytic tool that points to a possible event. Not all hits point to actual events or malign activity, they require analysis to characterize as either malicious or benign (see paragraphs 2-36 through 2-43).

2-9. Figure 2-2 illustrates the relationship between the amount of contextual information available from a data source, the generalized amount of data generated by the data source, and whether the data source is primarily host-based or network-based. The higher the data source is on the chart, the more likely it is to be able to capture the context needed for hunting. A successful hunt will involve correlating information from multiple data sources in multiple locations (host and network) to create a comprehensive understanding of the activities taking place on the network.

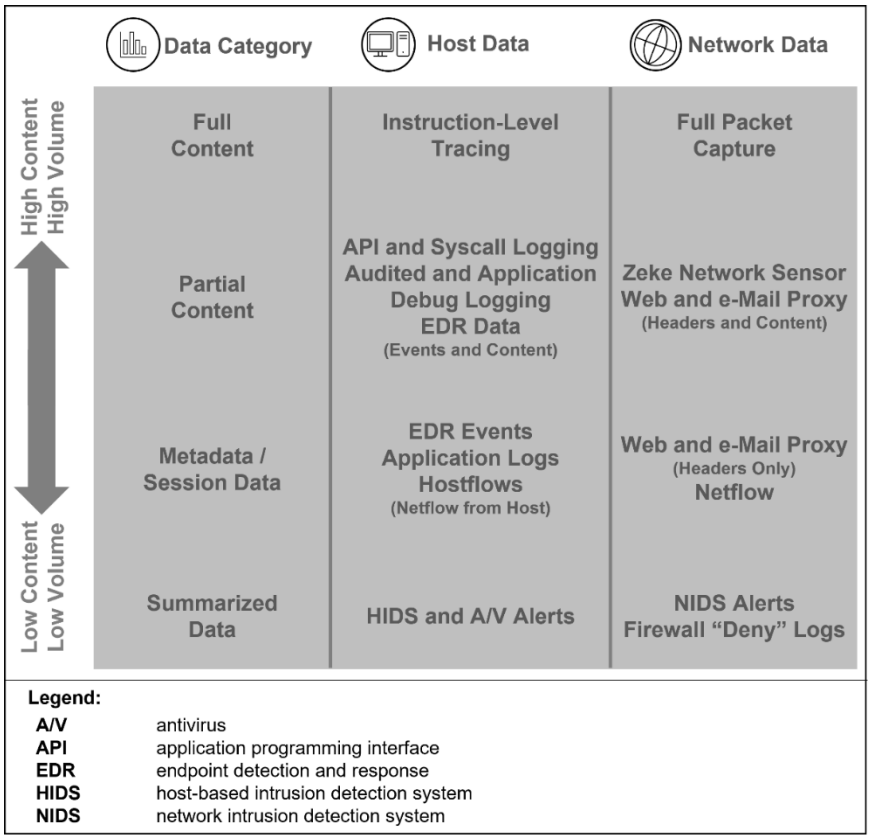


Figure 2-2. Information context for hunting

2-10. Sensors that provide continuous activity, event, or content data are preferred over signature and alert-based ones, as the nature of hunting requires examining activity that was not initially detected as malicious. Many traditional sensors, such as signature-based host or network intrusion detection systems, focus on detecting very specific, discrete information present in an attack (usually some highly identifiable malware attribute). These types of sensors are generally not useful for hunting, as they are focused on automated detection of well-known malicious activity—there is no hunting involved—and the data generated by these sensors is generally limited to specific alerts. They do not provide contextual event and activity data around

any suspicious activity being investigated. Host sensor selection will likely involve some combination of endpoint detection and response agents, application logs, and operating system event logs.

Filtering

2-11. The team needs to filter what they plan to analyze to hunt the threat. Essentially this is where the team initially constrains the analysis space to focus on what time, terrain, or behavior will enable them to start hunting the threat. Analysts can filter by—

- Time.
- Threat behavior.
- Ease of detection.
- Threat actor or group.

Time

2-12. Filtering on time is relatively straightforward—the team may have information that indicates a threat was operating within the target environment at a certain time, so the initial window should be bounded around that time period. Another possibility is to start from the present and retrospectively look backwards for a finite period (for example, two weeks prior to the start of the hunt activity). Often, the time window is automatically constrained by the retention period of the data storage and analysis system (security information and event management logs cover a rolling 30-day period).

Threat Behavior

2-13. The team can filter on behavior—specifically selecting which threat tactics, techniques, and procedures to detect within the environment. There are numerous ways to accomplish this, but two general approaches to use are: filter based on the likelihood that the tactics, techniques, and procedures will be easily identified as malicious relative to similar but benign behavior, or on the likelihood of a specific threat group known to target the environment using the tactics, techniques, and procedures.

Ease of Detection

2-14. Filtering on ease of detection requires knowledge about what activities are common within an environment and likely involve trial and error to reduce false positives. In a large enterprise network, there is significant variation in benign behaviors exhibited by users and system administrators in performing their duties, so what may be typical, benign activity for one user might be very unusual for another. Repeated hunting operations will help identify which behaviors are uncommon, and therefore more useful for detection within that environment.

Threat Actor or Group

2-15. Filtering on which threat groups are targeting an environment may be useful, with some caveats. It is unlikely that an organization or environment will be targeted by a single threat group, so filtering down to just known behaviors of that group may cause a hunt to miss the presence of another threat that has successfully compromised the environment. Additionally, threats can, and often do, adapt as new tactics, techniques, and procedures are identified. Filtering only on tactics, techniques, and procedures that were previously associated with a particular threat actor may allow the threat to escape detection. This type of filtering is likely to be beneficial in prioritizing which tactics, techniques, and procedures to search for first. However, analysts should not deselect tactics, techniques, and procedures from being considered during a hunt based on this filtering method. These methods of initial filtering will also be useful for tuning and refining analytical results during the hunt.

EXECUTION

2-16. Upon completion of characterization and identifying required analytics and data sources, hunt elements may begin to execute the hunt. Hunt execution entails—

- Identifying and mitigating collection gaps.
- Implementing analytic tools.

- Detection and pursuit.
- Detecting hits.
- Characterizing as either benign or malicious.
- Pursuing malicious hits.
- Responding and reporting.

Identify and Mitigate Collection Gaps

2-17. Analysts should conduct an initial analysis and iteratively reassess how well their data collection approach meets their information requirements. Analysts might need to determine whether the data are present, valid (free from configuration errors and threat tampering) and collected across the defended network continuously. Frequency analysis of event counts by Internet Protocol address or hostname can help identify coverage gaps across the terrain.

2-18. In hunting missions, there is commonly a lack of available data to observe threat activity from a part of the terrain that lacks sensor coverage. Hunt elements should assess what coverage is available within the environment and supplement that coverage with necessary configuration changes, centralized data collection, and deployment of additional sensors and capabilities to mitigate those visibility gaps. If, at any time before or during a hunt, significant gaps are detected between the desired and actual data collection, the team should assess how to handle each gap. When possible, new sensors should be deployed to fill the gap. The hunt team should also consider operations security in the deployment of new sensors and balance the value of the additional data collected with the visibility of that sensor to the threat.

2-19. Sensor deployment and data collection that starts post-compromise may be less effective in comparison to continuous, ongoing monitoring due to the issues in covering the time domain mentioned above. Additionally, sensors deployed on already compromised hosts may not be able to observe activity effectively due to anti-monitoring and anti-forensics capabilities of the threat's tools.

2-20. When deploying new sensors is not possible or practical, the team should assess whether other data collected can be used to fill the gap, perhaps with lower confidence or granularity of visibility. This can be done by mapping data sources to the analytics they enable. This mapping allows the team to assess the impact on the hunt operation due to the lack of a particular data source and adjust their analytics to adapt.

2-21. Knowing the blind spots with respect to terrain and time—which threat techniques are not visible due to a data gap and therefore have reduced analytic coverage—can help the team determine how to proceed and to communicate to the network owner about the impact. If certain threat techniques are no longer visible due to the gap, the hunt team may need to adjust its overall analytic approach as they seek initial detections and connections between detected threat behavior. This could include modifying which behaviors are included in initial detection analytics or increasing tolerance for missing evidence in linking suspicious events.

2-22. If certain areas of the terrain are not covered by existing data collection, analysts can increase their scrutiny on links between covered terrain and identified blind spots (for example, network connections made from covered systems to those without coverage). If certain windows of time lack data collection, links between events on either side of that window will be more tenuous. At a minimum, the hunt team should be aware of the visibility gaps and their impact on hunting results and should communicate them to network owners.

Implement Analytic Tools

2-23. The abstract analytic, the data model, and available data sources can now inform the creation of an analytic tool within the team's analysis system. The form of the analytic may vary depending on the specific system used. The analytic should be written to specifically identify the behavior noted in the tactics, techniques, and procedures and leverage the data model as much as possible.

2-24. The risk of writing analytic tools without modeling the data first is that the tool could be too specific to that environment's devices and configurations making it harder to re-apply to other configurations. The analytic tool becomes more useful across terrain types and data types—ideally, one analytic tool to run and

query regardless of terrain. This ideal may not be practical for all analytic tools but serves as a goal for implementation guidance.

2-25. It is important to note that analytic tools developed at this stage are not set in stone. Analytics development is an iterative process that requires frequent tuning and reevaluation of logic. Changes in the environment may cause certain analytic tools to be retuned, or new threat tactics, techniques, and procedures may need to be compensated for.

Detection and Pursuit

2-26. Hunting is an iterative process that requires creativity and flexibility. It is enabled by a core sequence of steps that provide a foundation for that flexibility. The iterative hunting process illustrated in Figure 2-3 on page 17 describes that core sequence. It begins with collected data and knowledge of malicious tactics, techniques, and procedures and illustrates fundamental processes to leverage that knowledge to filter the data efficiently and find the malicious activity. Once that activity is sufficiently understood, defenders can impose costs on the threat through—

- Coordination for defensive cyberspace operations-response actions through national-level cyber forces.
- Elimination of the threat's access to the defended network.
- Patching of the identified vulnerability.
- Exposure of threat tactics, techniques, and procedures to the public.

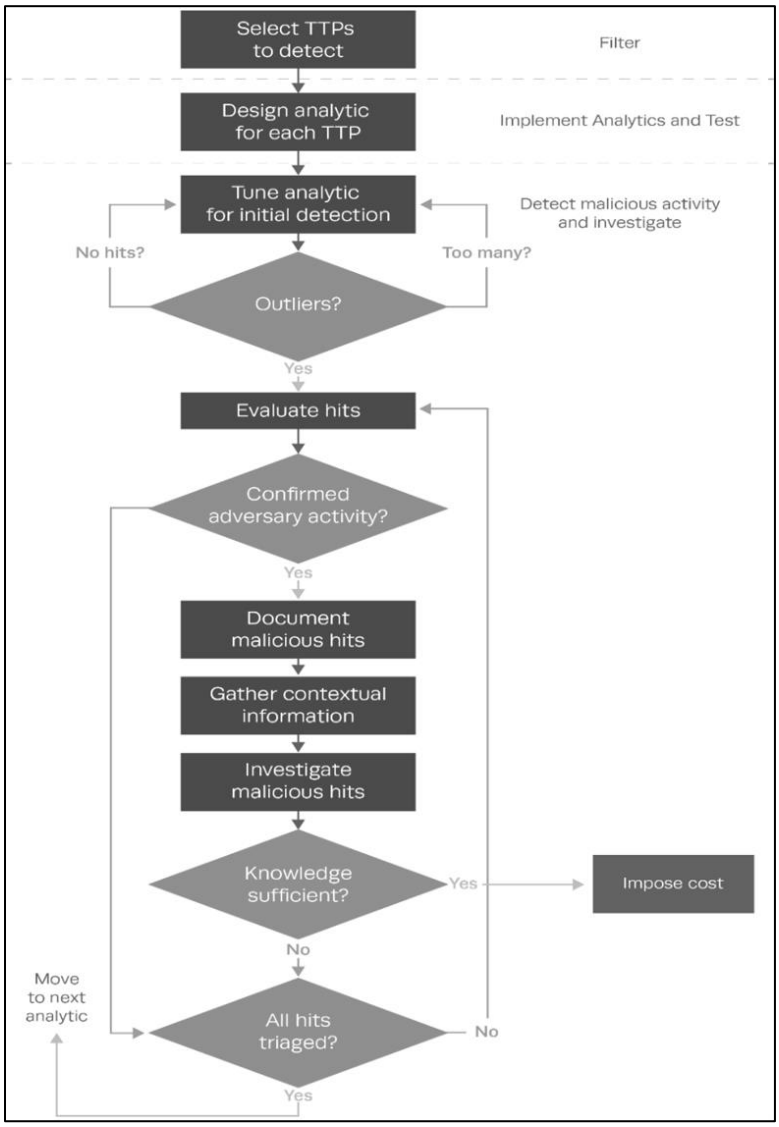


Figure 2-3. Iterative hunting process

2-27. Analysts tune the analytic tool to the subset of hits with malicious activity. It is common to start with analytic tools with relatively low false positive rates individually, however this is difficult to know in advance. Terrain-specific knowledge may inform the choice of analytic tools.

2-28. Once events (or hits) generated by a given analytic tool are reduced to a number small enough to devote some hunt element resources to pursuing each, the hunt element needs to resolve each of the hits returned. Events belonging to an outlier group are not necessarily malicious, so each one needs to be evaluated in depth. The methods used for evaluating results do not necessarily follow a prescribed order; the analyst decides which methods to pursue based on available information, experience, and expertise.

2-29. Once suspicious activity has been identified, widening the aperture (across time or numbers of devices) to generate a broader data set can help provide the context needed to determine whether the activity is malicious. Some events will require deeper inspection to make a determination regarding maliciousness. As a hunt element's processes mature, these cases will ideally decrease as the team becomes more familiar with the kind of data required by the analysts.

2-30. Contextual information is often needed to determine whether an event is malicious. Threats do not perform actions in isolation and thus the traces of activity they leave behind do not exist in isolation either.

There will be a chain of events an analyst can follow to connect seemingly disparate events. If an analyst can draw a direct connection between the event under investigation and another event or piece of intelligence that is known to be malicious, the certainty that this event is also malicious increases significantly.

Causes of False (Benign) Hits

2-31. Not all activity identified by an analytic tool is necessarily attributable to an external threat. Three possibilities to consider are—

- The activity is legitimate, if uncommon or unusual.
- The activity is caused by the hunt element itself.
- The activity may be an insider threat.

2-32. Analytic findings could be the result of legitimate, explainable activity. Administrators are also often responsible for deploying new software to the environment, which can cause unexpected events from both host-based and network data. Administrators are also often responsible for deploying new software to the environment, which can cause unexpected events from both host-based and network data. Ideally, these kinds of planned changes to the environment will be coordinated with the hunt team so that they are prepared when the deployments happen but that is not always feasible, so the analysts need to prepare for this eventuality. These kinds of issues may require the analyst to inquire about the activities of administrators or individual users to deconflict results.

2-33. System or service misconfigurations can cause false positives in hunting analytics, and often go unnoticed until the hunting activity uncovers them. The analyst needs to be prepared to identify instances where such is the case and to notify the party responsible so it can be addressed. This kind of issue could have the unintended side effect of changing the baseline of the environment, so any anomaly-based analytics in use may need to account for that fact.

2-34. Analysts must be cognizant of the possibility of detecting their own hunting activities or sensors rather than the threat, because various methods used by threats can be used by analysts to collect and aggregate data. For example, some teams may use PowerShell scripts running as administrators to collect data from endpoints or they might run a vulnerability scan to scan for misconfigurations or vulnerabilities on the network. For this reason, teams should be aware of their footprint in the environment so if they are the cause of what looks like an event it can be quickly dismissed. This use case also exemplifies the need for communication within the team so team members are aware of what each other are doing and can quickly deconflict results. Additionally, this could occur when there are multiple defensive teams operating within the same environment. An example of such a situation would be where an external team comes in to augment existing manpower. If the two teams are not properly coordinating activities with each other, they run the risk of both duplicating effort and tracking each other rather than the threat.

2-35. In rare cases, the activity may be related to an insider threat. In these cases, the defensive cyber force element might need to involve law enforcement or the organization's counterintelligence or insider threat tracking group. Behavior that may initially look like an insider threat, however, may come from a variety of motives, ranging from ignorance of accepted policies to an over-enthusiastic can-do attitude, or even pressure from management to willfully break from policy.

Determining Malicious Hits

2-36. Detected events determined to be malicious should be captured in such a way that the information can be shared between team members, higher headquarters, and eventually the terrain owner.

2-37. Contextual information can be extremely important, as outlined above, and for that reason collecting it is of utmost importance. Not only does it aid in understanding events that have been identified as malicious, but it can be used to drive direction for further investigation. Often, the most valuable information is that which can help to establish what caused the event in question, and what the event caused in turn. By capturing these pieces of information, the team can focus their efforts on events that are directly tied to a known bad event. Events that precede a known malicious event should be considered very suspicious and events that were caused by it should be considered malicious.

Pursuing Malicious Hits

2-38. To pursue a malicious hit, the hunt element should investigate both backwards and forwards to find the activity which caused the hit—ideally back to the initial malicious event—and subsequent activity to determine the scope and scale of the threat's actions.

2-39. Analysts begin pursuing the threat, by working backwards to find the causes of the detected event. This will help determine the full scope of the activity, attribute the events to a specific threat group, and gain the most useful knowledge for planning decisive response action.

2-40. If no causal events are found, the analyst will need to relax the requirement for finding evidence of each link in the causal chain. The analyst should consider the range of processes, systems, or other causes that could have resulted in the event under consideration.

2-41. In parallel with, or after sufficient information has been obtained regarding causally preceding events, the hunt element should investigate caused or related subsequent activity. Similar to the investigation of preceding events, analysts should look first for evidence of directly caused activity such as child processes, file creations, or opened network connections. When needed, the analyst should expand the investigation to include other machines exhibiting identical behavior and other suspicious files, processes, or activity on the same system.

2-42. Throughout these pursuits, analysts should continually refine the characterization of findings. As they gather more information, they should update a common knowledge repository (for example, textual reporting; graphical representation of activity) about the currently known chain of events, to include information regarding whether they are indicative of a specific set of threats, whether this activity is indicative of a certain stage in the cyber attack lifecycle, and threat intent. As new information is added to a shared repository, the team should also regularly determine what gaps in knowledge and visibility should be filled next and who or what could help fill them.

2-43. Looking for similar behavior across the broader network may reveal other instances of compromise that were initially missed. Hunt elements should employ high hit or effective analytics that may reflect the most dangerous threat course of action across the broadest network and data sources possible to broaden the pursuit and illuminate possible additional threat activity.

Responding and Reporting

2-44. Throughout hunt operations, the team must be mindful of the courses of actions possible for responding to the intrusion under consideration by the network owners and tailor the pursuit accordingly. Over time, the knowledge gained by the hunt will be sufficient to select a course of action. This may occur when the full extent of the threat activity is known, or when the defensive team's knowledge and ability to effectively defend and respond can render the threat's attack ineffective.

2-45. The commander must strike the right balance between waiting too long to act and acting prematurely. Too much emphasis on learning the full extent of the activity may hamper timely responsive action. Acting before sufficient knowledge is gained could result in tipping one's hand to the threat without significantly affecting their presence in the network or their ability to accomplish their objectives. This is a strategic decision which should incorporate an understanding of the threat activity, intent, and capabilities and the potential or actual impact to the defended network.

2-46. There are several reporting requirements that should be addressed as part of planning for, conducting, and concluding a hunting operation. When planning a hunt, communication and reporting channels will need to be created for all stakeholders. The stakeholder group includes the hunt element's chain of command and the network owner hunting on a network environment that is not owned by the hunt team's organization. Key items to report include—

- The general timeline for the hunt.
- What phase of the timeline the team is in.
- Confirmed presence of a threat.
- Systems affected—
  - Systems that are being investigated.

    - Known compromised systems.
- What damage or risk is currently posed by the threat.

2-47. Defensive cyber forces should establish regular update cycles, so commanders know when to expect new information. Reporting also entails knowing the purpose of the hunt—if the hunt is for remediation, reporting should be tailored towards informing stakeholders and remediation personnel where to pre-stage remediation capabilities and what the full scope and scale of the intrusion is to enable effective mitigation. The element conducting the hunt operation should establish communication channels separate from the network being hunted on to avoid alerting the threat and allowing them to react to hunting efforts. Figure 2-4 on page 21 illustrates a sample spot report-cyber (SPOT-C) for an observed data exfiltration incident on the Army network.

SPOT-C REPORT	
TEAM: 300 CPT	**CONTROL # (LEAVE BLANK)**
OPERATION: Operation VIGILANT TIGER	
NETWORK ACTIVITY REPORT (NAR)	
1. GENERAL INFO	
DTG OCCURRED: 011000FEB23	**LOCATION (COUNTRY):** Fort Bragg, NC, USA
DTG IDENTIFIED: 021500FEB23	**SENSOR LOCATION (VLAN):** 100
INDICATORS OF ACTIVITY:	
2. TECHNICAL DATA:	
BLUF: Credential data exfiltration through masquerading process	
DOMAIN: nase.ds.army.mil	
ORIGINATING SYSTEM	**DESTINATION SYSTEM**
LOCAL ASSET _X_ YES __NO	**LOCAL ASSET: YES ___ NO _X_**
IP ADDRESS:140.17.89.26	**IP ADDRESS:** 92.163.102.211
HOST NAME: BRAGA001DC-WIN2022 **OS VERSION:** Windows Server 2022 **MAC ADDRESS:** 70:98:FF:3E:A8:D1 **PORT(S):** 42689 **PROTOCOL(S):** HTTP **SERVICES:** PowerShell **WEBSITE/SERVER:** YES ___NO _X_ **IF YES URL:**	**HOST NAME:** N/A **OS VERSION:** Ubuntu LTS 22.04 **MAC ADDRESS:** 20:82:44:3D:2F:f3 **PORT(S):** 8080 **PROTOCOL(S):** HTTP **SERVICES:** N/A **WEBSITE/SERVER** YES _X_ NO ___ **IF YES URL:** customgear.site.ru
MITRE T-Codes Identified: T1555: Credentials from Password Stores; T1053: Scheduled Task/Job; T1020: Automated Exfiltration	
3. FILES AND ARTIFACTS	
List of Suspicious content: 01FEB-Dump.txt	
Location of Artifacts taken from system: Zeek extracted files log; local DDS-M kit.	
4. ANALYST COMMENTS: A Zeek connection log identified outbound HTTP POST request from a Fort Bragg domain controller to a Russian IP on a non-standard HTTP port at 011000FEB23. The associated Zeek HTTP log identified the extracted contents of the POST to be the 01FEB-Dump.txt file, which appears to be a set of plaintext user credentials. Examination of Windows events from the local domain controller identified process creation spawning a masquerading executable (smsss.exe) that dumped credentials and initiated the HTTP request prior to the Zeek log timestamp.	
ME: Report forwarded to battalion analytic support cell after verification of logs.	**ASC:** ASC corroborates outbound connection discovery using enterprise DODIN-A tools (Gabriel Nimbus).
FINAL ACTION TAKEN	
Mission element lead and team lead have notified the mission owner and recommended removal of the malicious process.	
ASC COMMENTS (POST SPOT-C COMPLETION)	
Russian IP is being analyzed at the DODIN-A enterprise level for other outbound U.S. connections.	

SAMPLE

Figure 2-4. Sample spot report-cyber

2-48. Typically, a cyber incident story board accompanies the SPOT-C. The story board facilitates visualization of the reported cyber incident. Figure 2-5 on page 22 illustrates a sample story board accompanying the SPOT-C in figure 2-4. The sample is unclassified, but the SPOT-C and story board are normally controlled unclassified information or classified secret or top secret, depending on the characterization and severity of the compromise and system or systems affected.

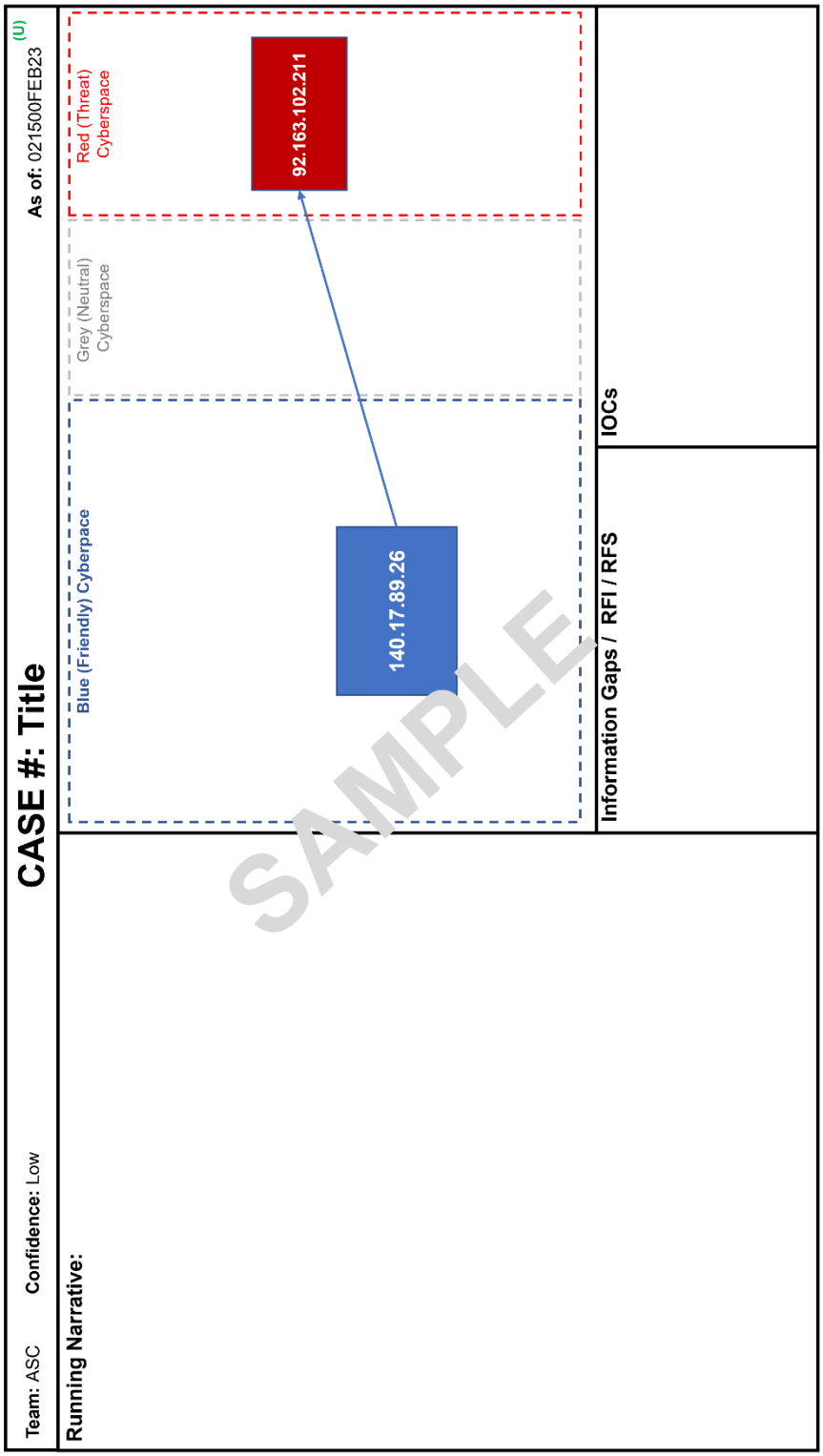


Figure 2-5. Sample cyber incident story board

HUNT TASKS

2-49. Defensive cyberspace operations hunt is primarily based on iterative application of the components of hunt. However, certain defensive cyber force mission-essential tasks contribute to hunt operations. These mission-essential tasks are available on the Army Training Network Website:

- 13-CO-9600—Conduct Cyber Hunt.
- 13-PLT-6010—Conduct Network Reconnaissance.
- 13-PLT-6050—Provide Support to Defensive Cyber Operations.
- 13-PLT-6060—Conduct an Analytic Scheme of Maneuver.

2-50. See paragraph 2-26 for details about defensive cyberspace operations hunt as an iterative process. See paragraph 2-1 to review the components of defensive cyberspace operations hunt.

This page intentionally left blank.

Chapter 3
Threat

Understanding threats—including enemies, adversaries, and criminal organizations—is essential for commanders to understand, visualize, describe, direct, lead, and assess operations. To develop and maintain running estimates as the basis for continuous adaptation, commanders and staffs consider their own forces in the context of the mission variables

UNDERSTANDING CYBERSPACE ACTORS

3-1. The various actors in any area of operations can qualify as threat, neutral, or friendly. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). Threats may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, states, or national alliances. Non-malicious actors in cyberspace may create risks or vulnerabilities without intent to cause harm. Defensive cyber forces must be prepared to engage adaptive threats and mitigate vulnerabilities while operating in complex terrain and adjacent to civilian equities.

3-2. Actors in cyberspace may include agents or forces of—

- Malicious actors—
  - Other states' cyber forces.
  - State-sponsored cyber actors.
  - Organized criminal and cyber mercenary actors.
  - Hacktivist and criminal groups motivated by political or social ends.
  - Lone criminals.
  - Lone-wolf hacktivists and vigilantes.
  - Insider threats.
  - Script kiddies driven by curiosity or prestige.
- Other actors—
  - National and multinational corporations.
  - International, national, and private cybersecurity organizations.
  - Joint, interorganizational, and multinational organizations.

ENEMIES, ADVERSARIES, AND NEUTRAL PARTIES

3-3. An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). An enemy is a combatant. U.S. forces may target combatants but in doing so must adhere to the law of war (refer to FM 6-27). An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0). A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements acting in concert to achieve mutually benefitting effects (ADP 3-0).

Note. The distinction between enemies and adversaries is critical in determining rules of engagement and proportional response in the physical domains. However, many threat actors calculate they can conduct offensive activities in cyberspace during competition without provoking an armed response. For the purposes of this training circular, most references to enemy or adversary actions will be to the more inclusive term threat to encompass actions across the competition continuum.

3-4. Neutral is an identity applied to a party whose characteristics, behavior, origin, or nationality indicate that it is neither supporting nor opposing friendly forces. Cyberspace operations are often complex and uncertain because threat, friendly, and neutral actors intermix and challenge Army forces' ability to classify them.

STATE AND NON-STATE ACTORS

3-5. Defensive cyber forces must be prepared to defeat determined state and non-state actors that combine conventional and unconventional tactics to avoid U.S. forces' strengths (rapid response, network surveillance, and advanced analytical capabilities) while exploiting perceived vulnerabilities (disparate network owners, seams in cybersecurity service provider coverage, and program of record systems and platforms). Threats combine a variety of means, to include traditional cyberspace attacks, espionage, sponsored criminal activity, and information warfare to accomplish objectives and attack U.S. forces. Threat actors exploit perceived U.S. and mission partners' military, political, social, economic, and information vulnerabilities as they seek to seize the initiative and dictate the terms and tempo of operations in their favor. Threats often rely on information technology networks to enable their operations as development, delivery, and command and control assets.

3-6. Threats employ countermeasures to limit U.S. forces' ability to develop the situation, avoid decisive engagements, and initiate contact under advantageous conditions. Threat organizations employ technological countermeasures to reduce their signatures in cyberspace and degrade U.S. forces' ability to detect, engage, and neutralize them. Many hostile states continue to procure cyber capabilities which are increasingly available to non-state threat organizations and hybrid threats. Threats also integrate emerging technologies such as machine learning, artificial intelligence, and quantum computing. Threats combine conventional and unconventional tactics to counter, evade and disrupt U.S. forces across the range of cyberspace operations.

3-7. Many threat organizations already have cyber weapons and access systems to employ them, for example, zero-day vulnerabilities and valid credentials. Threat organizations that do not have cyber weapons may attempt to proliferate, acquire, and employ them. While many threat organizations pursue the use of cyber weapons, many opt to use proxies or state-sponsored groups to launch attacks to avoid attribution.

3-8. Defensive cyber force commanders and staffs plan for countering cyber weapons by conducting control, secure, and isolate activities. They must understand the threat in context of the mission variables of METT-TC (I). Contextualized situational understanding allows commanders to identify emerging opportunities to seize, retain, and exploit the initiative.

NETWORKS AND ORGANIZATIONS

3-9. The defensive cyber force commander and staff determine a threat's objectives, strategies, and the multiple dimensions (physical, cognitive, informational, and political) in which they operate to defeat them. The defensive cyber force identifies and categorizes organizations, and networks that affect the mission as friendly, enemy, or neutral. The defensive cyber force supports friendly networks, influences neutral networks, and disrupts, neutralizes, or defeats threat organizations or networks. Assessment of networks and organizations is continuous and collaborative, integrating joint, interorganizational, and multinational partners whenever possible. At the tactical level, units develop an understanding of various networks through information collection and hunt. Considerations for network and organization assessment include—

- Objectives and strategy.
- Key individuals, groups, nodes, and their roles within a network or organization.
- Relationships between key individuals and nodes within networks and organizations.
- Flow of resources (such as access, capability, and data) across, into and out of networks.
- Where networks and organizations connect to other institutions, businesses, and entities.
- Network strength and vulnerabilities.

POTENTIAL THREAT GROUPS

3-10. Multiple threats may operate within a defensive cyber force's area of interest. Malicious cyber actors may include military forces of nation states, hacktivist organizations, transnational criminal organizations, and state sponsored cyber groups. These threat groups may form alliances based on mutual goals and common interests. As a result, defensive cyber forces must be prepared to defeat a complicated and often shifting array of threats. Understanding threat capabilities as well as their political, economic, or ideological aims is essential to seizing, retaining, and exploiting the initiative. Defensive cyber forces must qualify each cyber threat based on capability and intent to validate its relevance in continuous competition in cyberspace. Not all threat actors in the area of operations are participating in or contributing to state competition; depending

on the mission parameters and commander priorities, discovery of low-level threats may necessitate a recommendation for bypass. Specific malicious cyber actors can be categorized by a combination of their alignment, capabilities, and intent, as illustrated in figure 3-1.

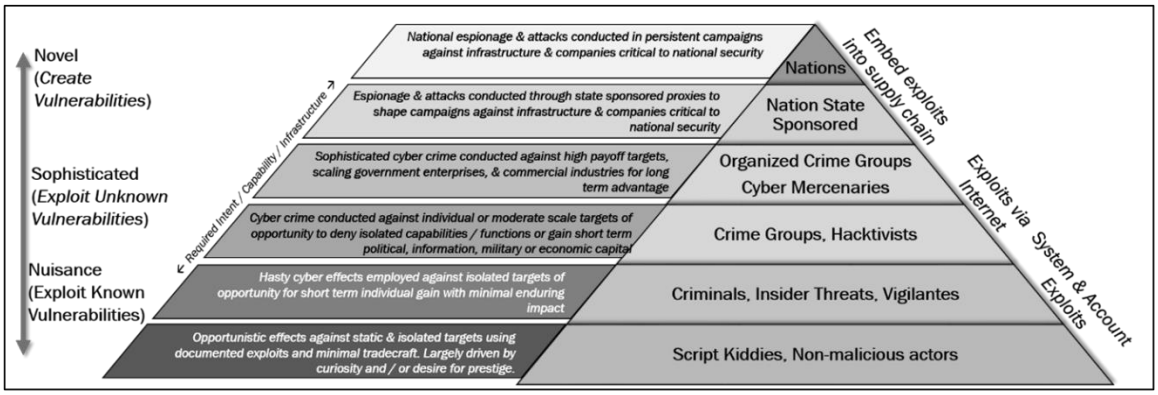


Figure 3-1. Sophistication of potential threat groups

STATE THREATS

3-11. State sponsored cyber actors operate on behalf of a nation's government, military, or leadership. Their capability is high due to their access to resources, personnel, and time not typically available to other actors. State actors conduct cyberspace operations to generate intelligence, set conditions for future operations, or create specific effects that support the political, economic, or military agenda of the state. Regional peer nations all have multiple different state sponsored cyber organizations, each tracked as a unique threat group. These threat groups can be a part of different government, intelligence, security, or military organizations, or aligned to different target sets. Each state's set of threat groups also have varying levels of capability and coordination with other cyber actors. State threats are the most dangerous threat groups potentially targeting the defensive cyber force's area of operations. However, there is a possibility the defensive cyber force may also discover state actors of allied or otherwise non-hostile nations. Analysts should contact their S-2 for the most up-to-date information on identified state threats. Examples of state threats include—

- Advanced persistent threat 29—Russian Foreign Intelligence Service aligned threat group responsible for the SolarWinds supply chain compromise in late 2020.
- Sandworm Team—Russian General Staff Main Intelligence Directorate group tasked with conducting destructive attacks such those targeting Ukrainian utilities in 2015, 2016, and 2022.
- Leviathan—Chinese Ministry of State Security's (MSS) group indicted in 2021 for stealing trade secrets in multiple sectors to include defense and government.
- Advanced persistent threat 38—North Korean Reconnaissance General Bureau threat group focused on cyberspace operations to enable financial theft.
- MuddyWater—Advanced persistent threat linked to the Iranian Ministry of Intelligence and Security that conducts cyber espionage targeting defense and governments.

3-12. Advanced persistent threat is a term often used interchangeably with state sponsored malicious cyber actors. However, advanced persistent threat only describes advanced threats focused on long-term access and does not necessarily denote state alignment. Advanced persistent threats have the technical capability to initiate and maintain access to support sustained operations against targeted networks. Advanced persistent threats can be either state or non-state actors. However, long-term persistence is resource-intensive, and the cost is unlikely to outweigh the benefit for non-state actors. Conversely, not all state actors are advanced persistent threats by their capability or intent. Certain state actors are focused on short-term achievable successes against targets of opportunity rather than on maintaining long-term access to specific networks.

NON-STATE THREATS

3-13. Non-state threats include organized criminal organizations and cyber mercenaries, violent extremist organizations, and cyber vigilantes. While these organizations are not formally aligned with a state threat, their goals may temporarily align with a threat state.

Organized Crime and Cyber Mercenaries

3-14. Many non-state malicious cyber actors are labeled as cyber criminals, ransomware gangs, or cyber mercenaries. These groups are generally monetarily motivated and conduct cyberspace operations for their own self-interest. State threats can formulate a relationship with these malicious cyber actors through monetary, legal, or social coercion in order facilitate cyber effects with reduced attribution and escalation. As a result, some non-state malicious cyber actors act as state proxies and respond directly to taskings and requirements to support the political, economic, or military agenda of a state threat. Examples of organized crime and cyber mercenaries include—

- Wicked Panda—a Chinese threat group that initially began as a financially motivated criminal organization and gradually shifted to take on cyber espionage on behalf of the Chinese Communist Party. CrowdStrike assesses this group as consisting of contractors.
- Evil Corp—a Russian cybercrime group that developed the Dridex malware responsible for over $100 million in theft. The organization now focuses on running ransomware operations. The Department of the Treasury assesses that Evil Corp's leader, Maksim Yakubets, was working directly for the Russian Federal Security Service as of 2017.

Violent Extremist Organizations

3-15. Violent extremist organizations may also have cyber branches within their organization to conduct disruptive or destructive effects in support of their political objectives. Malicious cyber actors can extend the limited physical reach of a violent extremist organization by affecting global targets to support information operations against governments, generate support, and create uncertainty in a target populace. Both ISIS and Hamas have employed cyber organizations in the past to conduct disruptive operations, however none have been identified since 2019.

Cyber Vigilantes

3-16. Colloquially called hacktivists, cyber vigilantes are politically- or socially-motivated malicious cyber actors comprised of loosely organized individual hackers who operate to further a cause or purpose. Cyber vigilantes coordinate via social media, web forums, or encrypted chat applications, and have varying degrees of capability and capacity depending on the level of internal support for the specific operation or agenda. Cyber vigilantes can also align directly to state agendas, depending on the situation or cause.

3-17. As with many other crowd sourced capabilities and socially motivated movements, cyber vigilantes are difficult to predict and can be difficult to template against. However, cyber vigilantes often announce their intent publicly ahead of time and self-identify successful cyberspace operations. Defensive cyber forces must be careful with this type of attribution, as it creates opportunities for false-flag cyberspace operations. The most notable cyber vigilante group is Anonymous, which in 2022 used its cyber capabilities to support Ukraine against Russia and Russia-aligned targets.

INDIVIDUAL OR SMALL GROUP THREAT

3-18. Individual or small group threats include hackers and security researchers, script kiddies, and insider threats. These malicious cyber actors do not operate as part of a larger state or non-state threat organization.

Hackers and Security Researchers

3-19. Hacker is a generalized description for individuals with the capability to generate cyber effects against computer systems or networks. Individuals or small groups of hackers likely lack the capacity to affect the end state of defensive cyber force hunt operations. However, these individuals may still impact the timing and tempo of defensive cyber force operations or become co-opted by more sophisticated malicious threat actors into a larger campaign.

3-20. The term hacker does not necessarily denote malicious intent. An ethical white-hat hacker or a security researcher can identify network or system vulnerabilities legally. While security researchers generally operate without malicious intent, they can affect defensive cyber force's area of operations depending on the asset or technology researched. A security researcher can also affect the timing and tempo of defensive cyber force operations by how and when they disclose identified vulnerabilities or exploits. One notable example

of a security researcher who has impacted defensive cyber forces in the past is the Taiwanese researcher Orange Tsai. Tsai famously disclosed vulnerabilities against Microsoft Exchange in 2021 that led to immediate patching but also immediate weaponization of the exploit by malicious cyber actors around the world.

Script Kiddies

3-21. Script kiddie is an unskilled individual who uses off-the-shelf cyber tools and exploits provided by others. Script kiddies find or purchase readily available exploits on GitHub or on the dark web and use them without an in-depth understanding of how the tool or exploit works. Script kiddies can operate with a wide range of intent, ranging from supporting a political cause to generating notoriety or for personal curiosity. Script kiddies still can impact a defensive cyber force hunt operation by contributing noise to observable activity in the area of operations, potentially obscuring other malicious cyber actors.

Insider Threats

3-22. An *insider threat* is a person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of United States military forces (AR 381-12). Insider threats may be contract, government, or military personnel with physical or close access to systems or network devices in an area of operations.

3-23. Insider threats can conduct reconnaissance physically or on network with credentialed access and exfiltrate data for espionage purposes. Insider threats can also potentially introduce malicious code, unauthorized access points, or connections directly onto a network. Insider threats can be lone wolf actors operating on their own initiative or they can be co-opted and equipped by state or non-state actors to enable a cyberspace operation. Insider threat motivations can range from personal financial gain, to political or religious alignment, to disillusionment with the U.S. government or their organization. The cyber personas and the physical and logical accesses of any identified insider threats will inform the defensive cyber force's hunt operations.

THREAT CHARACTERISTICS

3-24. Malicious cyber actor attribution and identification is difficult due to the degree of obfuscation and anonymity that can be achieved in cyberspace. Defensive cyber forces can characterize and deconstruct a threat by the various types of indicators that form their technical threat characteristics.

3-25. One representation of technical threat characteristics is David Bianco's Pyramid of Pain (see figure 3-2 on page 30). These categories provide the defensive cyber force indicators to detect and respond to. The pyramid also describes the level of cost imposed on the malicious cyber actor once the defensive cyber force denies those indicators.

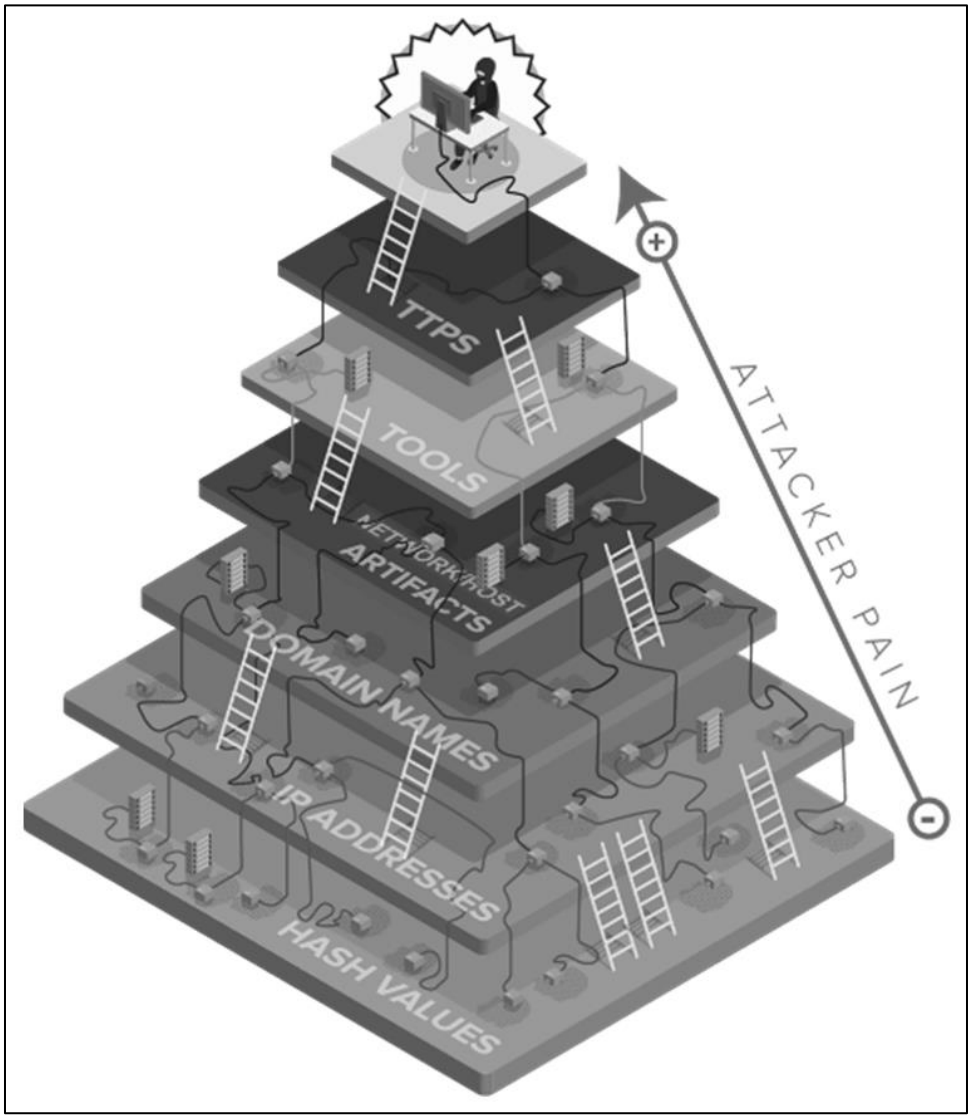


Figure 3-2. Pyramid of Pain for malicious cyber actor indicators

THREAT CAPABILITIES, TACTICS, AND TECHNIQUES

3-26. Tactics, techniques, procedures, and tools at the top of the Pyramid of Pain can provide insight into the level of sophistication and intent of the malicious cyber actor, as well as scope the defensive cyber force's analytic scheme of maneuver. The MITRE corporation's adversarial tactics, techniques, and common knowledge (ATT&CK®) is a knowledge base for modeling potential malicious cyber actor tactics, techniques, and procedures as they maneuver into and through the defensive cyber force's area of interest and area of operations. In the ATT&CK® framework, tactics represent the goal of the malicious cyber actor and techniques represent how a malicious cyber actor achieves a tactical goal. Each technique is identified with a unique T number.

3-27. Current ATT&CK® knowledge base tactics for enterprise networks include—

- Reconnaissance.
- Resource development.
- Initial access.
- Execution.
- Persistence.

- Privilege escalation.
- Defense evasion.
- Credential access.
- Discovery.
- Lateral movement.
- Collection.
- Command and control.
- Exfiltration.
- Impact.

3-28. The ATT&CK® framework is arranged in a linear fashion, but malicious cyber actors can execute tactics and techniques in any order suitable to the terrain and to their tradecraft.

3-29. Cybersecurity industry analysts have worked to map and analyze common tactics, techniques, and procedures observed among malicious cyber actors. The below findings likely contain confirmation bias and are not specific to the DODIN. These specific ATT&CK® techniques will provide the defensive cyber force a starting point absent a specific malicious cyber actor to target. They are annotated along with their ATT&CK® T number for reference.

3-30. Analysts combine tactics, techniques, procedures, and risks to U.S. and mission partner forces to develop intelligence assessments across the full spectrum of cyberspace operations (see figure 3-3). Commanders use these assessments to inform and refine hunt operations. Adversaries will often use less-novel techniques, including electromagnetic warfare and other radio frequency-enabled capabilities at the onset of conflict, reserving specialized cyberspace capabilities for decisive operations.

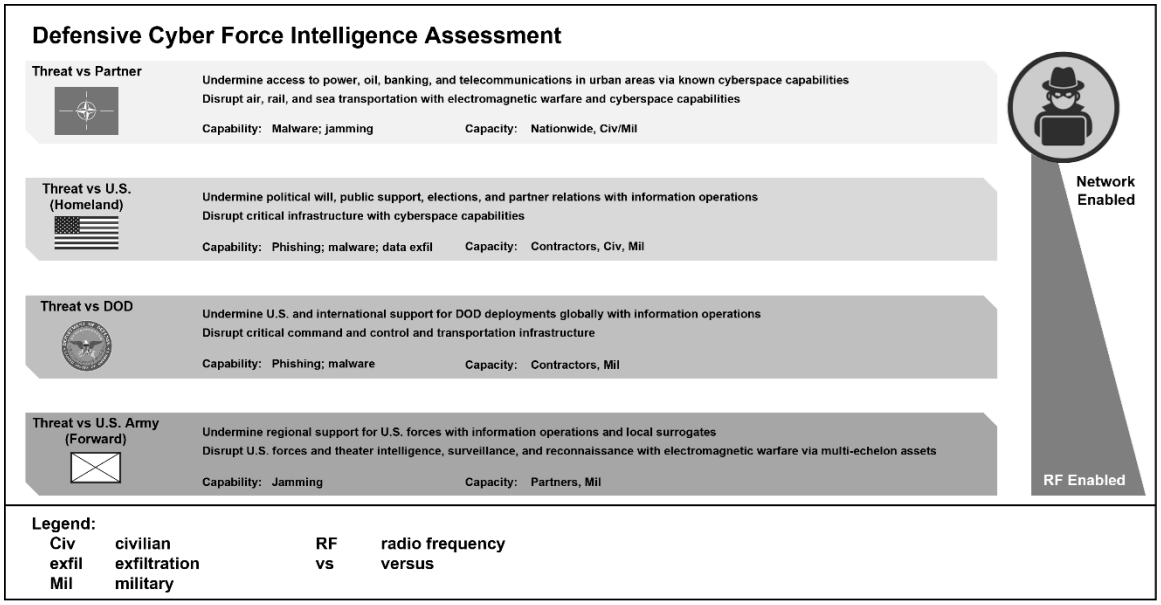


Figure 3-3. Sample defensive cyber force intelligence assessment

Threat Reconnaissance Techniques

3-31. Reconnaissance involves the threat's activities to either actively or passively gather information about a target and gain an understanding of the environment. Active reconnaissance takes the form of various scanning methods but could include physical surveillance. Passive reconnaissance includes gathering target information from publicly available sources, websites, or databases.

Threat Resource Development Techniques

3-32. Resource development includes all activities on the part of the threat to gather and stage the necessary infrastructure and capabilities required to execute a successful attack. Infrastructure can be natively developed and maintained by the threat but will likely be procured through hard-to-detect means meant to provide additional subterfuge. Likewise, a threat may acquire capabilities, both novel and commonplace, from various sources, including public repositories such as GitHub and Exploit Database.

Threat Initial Access Techniques

3-33. Initial access is a threat's means of ingress into an environment to gain their initial foothold. While the options for initial access vary widely, the techniques adversaries leverage to gain an initial foothold most often manifest as variations of phishing or exploitation of vulnerabilities in public-facing web servers. Any initial access is temporal in different measures, depending on the technique, and can change with conditions in the environment.

Threat Execution Techniques

3-34. Employment of techniques that result in threat-executable code running on a local or remote system constitutes execution. The adversarial code is often leveraged for various ends such as enumeration of the system or network and the defensive obstacles emplaced. An example is the threat running a script that conducts reconnaissance of the targeted local system to understand the local system environment and its suitability with their later-stage toolsets. The presence or lack of antivirus or end point detection and response tools on the system would inform their future employment of later stage toolsets.

Threat Persistence Techniques

3-35. Access to systems or networks that survives restarts, changed credentials, and other interruptions that could disrupt legitimate network access constitutes persistence. A threat solidifies their access by changing configurations, startup files, registry, or kernel level settings to maintain their foothold. An example would be to install a high privileged kernel level rootkit on a compromised system that would survive restart.

Threat Privilege Escalation Techniques

3-36. Techniques used to gain increased permissions on a system or network constitute privilege escalation techniques. While some threat actions may be achievable with unprivileged access, their objectives most often require elevated permissions. System or root accounts on the local system, domain and enterprise administrators within a domain, or global administrators at cloud service providers are all examples of high payoff permission levels for privilege escalation techniques.

Threat Defense Evasion Techniques

3-37. Any techniques used to subvert detection or bypass friendly defensive obstacles such as antivirus program constitutes defense evasion techniques. Modifying existing security software, carefully managing the parent-child process relationship of their malicious code, or abusing trusted processes are other examples of defense evasion techniques.

Threat Credential Access Techniques

3-38. Adversaries attempt to maintain or improve access by acquiring legitimate credentials from users in the targeted network. Complexity ranges from brute force password cracking to sophisticated adversary-in-the-middle attacks and authentication procedure manipulation.

Threat Lateral Movement Techniques

3-39. The act of pivoting from an initial access foothold to enter or control a remote system on a network is considered lateral movement. While an initial access foothold may have been opportunistic, lateral movement techniques are used to pivot through the network to a position of relative advantage to the target of interest. Lateral movement is where the threat incurs the highest amount of risk to their mission, so stealth is

paramount. Example means of lateral movement include installing remote access tools or abusing legitimate credentials with native network and system tools.

Threat Collection Techniques

3-40. Collection techniques represent a host of activities an adversary in a position of advantage may take to gain information or answer their information or intelligence requirements. These activities can range from simple activities such as data repository access to more sophisticated activities such as input capture and browser session hijacking.

Threat Command and Control Techniques

3-41. The overt or covert channels through which adversaries communicate with the systems subject to their control make up command and control channels. These channels most often are masked to exist below the noise floor of normal network and web traffic. Adversaries often establish persistent access long haul command and control that beacons infrequently with a certain degree of entropy. Long-haul command and control channels serve as a break-glass measure to maintain access if the threat's more active command and control channels are discovered. Access management for long-term campaigns holding friendly terrain at risk often involves hard to detect, covert command and control channels.

Threat Exfiltration Techniques

3-42. Threats may attempt to remove information of significant value from the network through automated, scheduled, and manual processes, including alternative protocols, or physical and Internet-based extraction.

Note. In Army doctrine, *exfiltrate* is a tactical mission task in which a unit removes Soldiers or units from areas under enemy control by stealth, deception, surprise, or clandestine means (FM 3-90). This differs from use of the term in cyberspace operations, where exfiltration describes a cyberspace attack in which data is clandestinely removed from an information technology network.

Threat Impact Techniques

3-43. Once a threat has a position of advantage over a network, they can affect friendly activities on and through that network, depending upon their access. Threats can deny, disrupt, destroy, or modify information or data traversing the affected network.

This page intentionally left blank.

Chapter 4

Shape, Engage, and Consolidate Gains

To win within all operational frameworks, defensive cyber forces must understand the operational environment, shape the operational environment through action, engage local defenders to influence the network, and consolidate gains to seize, retain, and exploit initiative. Commanders shape their operational environment by conducting missions and efforts to achieve a common goal and end state that nests with the higher command's objectives and desired end state.

UNDERSTANDING THE OPERATIONAL ENVIRONMENT

4-1. Commanders must understand competing interests within the operational environment to determine what is of value to competitive parties and entities within their area of operations. Understanding interests helps develop courses of action to engage leaders, enhance the security situation, and lead to mission success. Defensive cyber forces consolidate gains and favorable milestones to seize and exploit weaknesses, capitalize on opportunities, and further the interests of allies to secure stable political settlements and objectives complementary to desired outcomes.

4-2. Understanding cyberspace aspects of the operational environment is vital to cyber planners. Until a threat is identified, or an activity attributed, it is challenging to conclusively determine motivations of cyber actors, other than general intent. National- and theater strategic-level planners analyze the cyberspace environment to develop situational understanding, while policymakers view the cyberspace environment through the operational variables of political, military, economic, social, infrastructure, information, physical environment, and time (PMESII-PT).

4-3. Tactical defensive cyber forces analyze cyberspace through the mission variables of METT-TC (I), informed through hunt operations and information collection to enhance situational awareness and understanding of competing interests. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets and as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55).

4-4. Understanding competing interests within the area of operations allows the commander and staff to frame specific problems. Competing interests often manifest in the form of friction between maintaining availability and shaping the terrain to create a position of relative advantage (often restricting both friendly and threat avenues of approach). To operate effectively under conditions of complexity and in contact with threats, defensive cyber forces consider interests from multiple perspectives. Understanding friendly and threat interests assists commanders and staffs in planning defensive cyberspace operations that support modifying behaviors and further sustainable objectives.

SHAPING THE ENVIRONMENT

4-5. Commanders and staffs consider the competitive environment in their areas of operations and shape the operational environment to set conditions to seize and retain the initiative. Shaping the environment requires defensive cyber forces to develop situational understanding. This is an enduring process throughout all operations and not separated by phase.

4-6. Commanders actively seek to understand their areas of operations. The ability of defensive cyber forces to shape conditions favorable to future outcomes relates to their understanding of threat influences as well as their ability to develop the situation through hunt tasks to collect information requirements enhancing situational awareness and understanding. A thorough understanding of the threat is imperative to identifying information collection requirements that are developed through hunt and cybersecurity tasks. Defensive cyber forces actively seek answers to information gaps through the development of the information requirements that are satisfied through active hunt tasks on given cyberspace terrain. Through information collection and analysis, staffs develop options for the commander to further inform the populace, influence various actors, seize opportunities, and maintain initiative.

CONSOLIDATING GAINS

4-7. Consolidating gains is the combination and nesting of multiple objectives to unite military advantage and influence within the area of operations. Defensive cyber forces consolidate gains through the execution of tasks to accomplish objectives consistent with the commander's intent. Gains capitalize success in military operations to accomplish tactical, operational, and strategic objectives.

4-8. Consolidating gains occurs upon the capitalization of positive actions and objectives through information collection, hunt operations, and cyberspace defense improvement to bridge tactical success with operational and strategic objectives. Consolidating gains is tied to mass, a principle of war, though instead of accumulating forces or effects, it is a matter of accumulating positive impacts through security and defensive mechanisms. In essence, the consolidation of gains links positive contributing tactical actions with operational and strategic objectives.

4-9. Commanders and staffs tie complementary tactical objectives across multiple lines of effort to influence operational and strategic objectives with tactical actions. Defensive cyber forces conduct activities to ensure gains are sustainable. Commanders and staffs build friendly partner capacity through collaboration and empowerment that enhances the long-term defense of friendly networks. Defensive cyber forces gather information to assist in assessing the effectiveness of defensive cyberspace operations. Through continuous hunt, defensive cyber forces develop and reassess the situation and opportunities to maintain positive momentum and resultant tactical, operational, and strategic gains.

4-10. Defensive cyber forces collect information and develop situational understanding in cyberspace to understand, shape, and influence the operational environment and consolidate positive gains leading toward desired objectives. Shaping transcends phases and is continuous throughout all operations.

Chapter 5
Command and Control

Hunt operations are critical to the preservation of the command and control network. To make effective decisions in an uncertain environment, the defensive cyber force commander requires timely and accurate information from their hunt formations.

COMMAND AND CONTROL FOR HUNT OPERATIONS

5-1. *Command and control* is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of mission (JP 1). Command and control is fundamental to the art and science of warfare. No single activity in operations is more important than command and control. Command and control by itself will not secure an objective, destroy a target, or deliver supplies. Yet none of these activities could be coordinated towards a common objective, or synchronized to achieve maximum effect, without effective command and control. It is through command and control that the countless activities a military force must perform gain purpose and direction. The goal of command and control is mission accomplishment (ADP 6-0).

THE MISSION COMMAND APPROACH

5-2. *Mission command* is the Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation (ADP 6-0). Military operations are complex human endeavors characterized by continuous, mutual adaptations among all participants. U.S. forces will face capable, adaptable, and determined enemies who will resist our actions, employ countermeasures to our strengths and capabilities, and will seek to impose their will on all actors within the operational environment. At the same time, Army forces will conduct defensive cyberspace operations seeking to counter threat cyber attacks and minimize the threat's dwell time from initial infiltration to discovery or realized effects on friendly networks or capabilities. The result of the continuous process of interactions and dynamic nature of hardware and software security and vulnerabilities is an environment defined by uncertainty.

HUNT OPERATIONS

5-3. Hunt operations are critical for cyber force commanders to gain timely and accurate information to enable effective command and control for defensive cyberspace operations. To make effective decisions in an uncertain environment, the defensive cyber force commander requires timely and accurate information from their hunt formations.

5-4. Defensive cyber force commanders apply the mission command approach to develop the situation—possibly in close contact with the threat—to develop their understanding, visualization, and description of the operational environment, the terrain, local defensive posture, and the threat. Through effective information collection and continuous hunt tasks, defensive cyber forces develop and sustain the necessary tactical and operational understanding to counter adaptive and determined threats and set conditions to consolidate tactical gains. Hunt tasks improve situational understanding and help commanders to—

- Understand the tactical cyber dynamics within an area of operations.
- Visualize operations in the context of the mission variables of METT-TC (I).
- Describe the commander's decisive operations in time, terrain, and purpose with a greater degree of detail, accuracy, and fidelity.
- Direct the execution of decisive operations with higher degrees of flexibility, adaptability, synchronization, and integration.
- Lead the defensive cyber force to concentrate its strengths against threat weaknesses.
- Assess progress through continuous hunt, monitoring, and evaluation.
- Modify existing or developing plans and reallocate defensive cyber force assets based on changing tactical situations.
- Achieve tactical depth.
- Identify and create options to seize, retain, or exploit the initiative.

5-5. Based on their initial understanding of the operational environment and the tactical situation, defensive cyber force commanders generate information requirements for organic elements. Commanders visualize how defensive cyber force elements and other hunt assets, including local network defenders, inspection activities, cybersecurity service providers, and intelligence community assets, will work together, and describe how the defensive cyber force's activities will contribute to the success of higher, adjacent, and lower echelons. Defensive cyber forces are the primary assets used to develop the situation and provide friendly network information that will ultimately refine subsequent courses of action to inform decision making. As a result, defensive cyber force commanders and their staffs, including the brigade S-3 and cyber force battalion commanders, direct hunt and cybersecurity to answer the commander's information requirements and develop the situation to establish conditions conducive to mission success.

5-6. Effective hunt operations create opportunities that allow commanders to confirm or deny assumptions, make decisions, and act. Commanders establish the commander's critical information requirements, and continuously update information requirements based on changes in the mission variables of METT-TC (I). Commanders and their staffs identify information gaps and continuously assess, adapt, add, and delete requirements throughout the operation. As staffs identify requirements for successful execution, they recommend and assign tasks for defensive cyber force units to conduct hunt operations and provide answers that allow the commander to make timely and effective decisions. As they continuously plan, task, and employ assets to answer the commander's critical information requirements and other information requirements, commanders and their staffs—

- Develop and continuously update intelligence requirements.
- Identify and update the commander's critical information requirements.
- Tie the commander's critical information requirements directly to the analytic scheme of maneuver and decision points.
- Limit the commander's critical information requirements to only the most critical intelligence and combat information needs.
- Seek higher echelons' collection of—and answers to—information requirements.
- Ensure the commander's critical information requirements include the latest time information of value to ensure timely reporting and decision making.

5-7. Hunt operations provide flexibility, adaptability, and depth to the defensive cyber force commander's analytic scheme of maneuver by synchronizing and integrating other signal and cyber support assets to size, retain, and exploit the initiative based on a relevant understanding of the situation. By employing combined cyber and signal teams, the defensive cyber force commander fights for information and develops the situation against a broad range of threats throughout their area of operations. Hunt operations provide the defensive cyber force commander with tactical depth, freedom of maneuver, flexibility, and critical combat information regarding cyberspace.

5-8. Commanders conduct hunt operations continuously to protect the DODIN. The commander adjusts hunt priorities continuously—hunt tasks will vary as the cyberspace terrain dynamically changes and reacts to new threat avenues of approach. This minimizes the time available for troop leading procedures for the defensive cyber force element, including planning, rehearsal, pre-combat checks, pre-combat inspections, and maintenance. Missions without focus degrade the capabilities of the defensive cyber force element. Improper utilization of assets can leave threat persistence mechanism or other catastrophic threat undiscovered. The commander sets priorities in a warning order, establishing—

- Focus.
- Tempo.
- Engagement criteria.
- Disengagement criteria.
- Displacement criteria.

5-9. Hunt and cybersecurity tasks are most effective when integrated with other cyber and signal forces, enabled by the mission command approach. Hunt missions require quick dissemination and execution of orders. Leaders must be decisive, plan quickly, pass available information to subordinates, report to higher headquarters accurately and rapidly, and be responsive to changing conditions in the battlespace.

5-10. The following historical example illustrates the value of flexible defensive cyber forces at echelon that directly answered the commander's critical information requirements.

The Cyber Protection Brigade's Analytic Support Cell and Command and Control

Through cueing from partner agencies, the cyber protection brigade's analytic support cell identified an unknown avenue of approach to a group of domain controllers that would allow direct interaction with domain controller services from public devices. The analytic support cell was able to rapidly assess observed traffic and confirm an absence of successful malicious communication. This prevented the unnecessary re-allocation of a cyber protection team and, through a deliberate hunt handover with the cybersecurity service provider, enabled the rapid blocking of the avenue of approach.

THE EXERCISE OF COMMAND AND CONTROL

5-11. To function effectively and have the greatest chance for successful mission accomplishment, commanders, supported by their staffs, exercise command and control throughout the conduct of operations. The exercise of command and control encompasses how defensive cyber force and cyber battalion commanders and staffs apply the mission command approach, described above, using the operations process—planning, preparing, executing, and continuously assessing the operation.

5-12. The operations process and defensive cyberspace operations hunt tasks are mutually dependent. Just as planning, preparation, and assessment in the operations process inform and direct hunt tasks, the defensive cyber force and cyber battalions conduct hunt tasks during all phases of the operations process and provide the necessary information to complete plans, prepare, adjust the execution of the operation, and provide further assessments of the tactical situation and the operational environment.

5-13. The activities of the operations process are not discrete—planning, preparing, executing, and continuously assessing the operation overlap and recur as the circumstances of the tactical situation and operational environment demand. Planning starts an iteration of the operations process, yet upon completion of the initial order, planning continues as leaders revise the plan based on changing circumstances and timely reports from employed defensive cyber force elements. Preparing begins during planning and continues through execution. Execution puts a plan into action by applying combat power to accomplish the mission.

5-14. The command and control warfighting function tasks focus on integrating the activities of the other elements of combat power to accomplish missions. Commanders, assisted by their staffs, integrate numerous processes and activities within their headquarters and across the force through the command and control warfighting function (ADP 6-0). These tasks are—

- Command forces.
- Control operations.
- Drive the operations process.
- Establish the command and control system.

THE OPERATIONS PROCESS

5-15. Commanders and staffs use the operations process to integrate numerous tasks executed by the defensive cyber force's organic elements and subordinate units. Commanders must organize and train their staffs and subordinates as an integrated team to plan, prepare, execute, and assess operations. Defensive cyber forces conduct hunt tasks while simultaneously planning, preparing, and assessing defensive cyber force operations.

5-16. In addition to the mission command approach to command and control, commanders and staffs consider the following principles for effective employment of the operations process:

- Commanders drive the operations process.
- Commanders and staffs collaborate to plan, prepare, execute, and assess operations.

- Commanders and staffs build and maintain situational understanding.
- Commanders and staffs encourage collaboration and dialogue.

COMMANDERS DRIVE THE OPERATIONS PROCESS

5-17. The commander is the central figure in the operations process. While the staff performs essential functions that amplify the effectiveness of operations, the commander is ultimately responsible for accomplishing assigned missions.

5-18. Commanders encourage disciplined initiative through a clear commander's intent while providing enough direction to integrate and synchronize the force at the decisive place and time during hunt tasks. Early dissemination of intent is particularly important as hunt operations often can pull additional forces into the operation and create decisive points. The commander relies upon subordinates to respond quickly to mission-type orders and execute disciplined initiative.

Understand

5-19. Understanding is fundamental to the commander's ability to establish a situation's context and make effective decisions. Timely and accurate analysis of network data, threat activities in cyberspace, and defeat mechanisms presented in an easily understandable format enables the commander to establish decision dominance. The commander and staff, supported by the defensive cyber force S-3, analyze the mission variables of METT-TC (I) to develop situational understanding within their area of operations. Using their own training, experience, education, and inputs from others—including running estimates from the staff and mission partners—commanders continuously refine their situational understanding of the operational environment.

5-20. Defensive cyberspace operations hunt tasks are indispensable to building and improving the commander's understanding of the situation. As commanders refine their understanding, they must quickly formulate the commander's critical information requirements, keep them current, determine where to place key personnel, and arrange for liaison teams to contribute further to improving the commander's understanding. In short, greater understanding of the situation will enable commanders to make better decisions throughout the conduct of operations.

Visualize

5-21. As commanders begin to understand their operational environment and the tactical problem, they visualize potential solutions and their desired end state. The commander's visualization is the mental process of developing situational understanding, determining a desired end state, and envisioning an operational approach through which the force will achieve that end state. The process of commander's visualization applies to both the defensive cyber force's primary mission and the collective visualization of hunt tasks that influence the defensive cyber force's operation.

5-22. Visualization of the operational environment and terrain are a challenge in cyberspace operations. Often, no readily available map or set of maps is available for analysis to drive courses of action and shared understanding across the staff or across echelons. While local network defenders often have a schematic diagram of their portion of the network, it may be incomplete or too localized to drive planning. That is not to say that detailed network maps are not useful, but defensive cyber forces must often gather multiple sets of information, security information and event management details, an understanding of avenues of approach, and host disposition to support visualizing the environment. Often abstracting details into generalized blocks helps build a visualization that can operate as the base mission graphics and remain useful when describing tactical information to key leaders or supporting entities. Figure 5-1 on page 41 illustrates an example of a simple network abstraction.

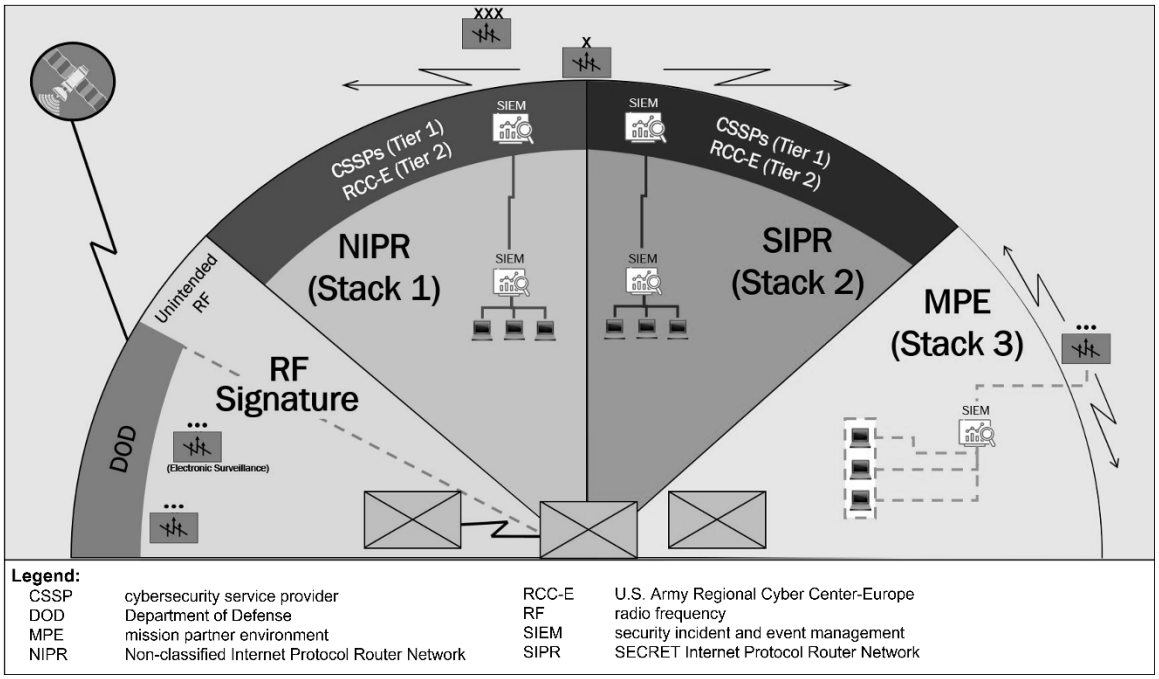


Figure 5-1. Simple network abstraction

5-23. Close collaboration between the defensive cyber force commander and subordinate leaders, as well as close synchronization between the defensive cyber force staff and the analytic support staff, are critical to developing the visualization of hunt tasks. Assigning missions focused on specific hunt objectives provides the focus for developing the commander's visualization that, in turn, provides the basis for developing plans and orders. During preparation and execution, the commander's visualization helps the commander and subordinates determine if, when, and what to decide as they adapt to changing conditions and the updated information reports produced through hunt operations.

Describe

5-24. After commanders visualize an operation, they describe it to their staffs and subordinates to facilitate a shared understanding and purpose. During planning, commanders ensure subordinates understand their visualization well enough to begin course of action development. During execution commanders describe modifications to their visualization, modifications informed by continuous hunt tasks, in updated planning guidance and directives resulting in fragmentary orders that adjust the unit's mission. Commanders describe their visualization in doctrinal terms, refining and clarifying their visualization as circumstances require. Commanders express their visualization in terms of—

- Commander's intent.
- Planning guidance.
- Commander's critical information requirements.
- Essential elements of friendly information.
- Hunt guidance.

Commander's Intent

5-25. The commander's intent is a clear and concise expression of the purpose of the operation and the desired military end state. Clear commander's intent provides focus to the staff. It helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned.

5-26. For defensive cyberspace operations hunt, the commander's intent statement describes what constitutes success for the hunt operation including the operation's purpose, key tasks, and the conditions that define the

end state. Intent links the mission, concept of operations, and tasks to subordinate units. A clear commander's intent facilitates a shared understanding and focuses on the overall conditions that represent mission accomplishment. During execution the commander's intent spurs disciplined initiative.

5-27. The commander's intent must be easy to remember and clearly understood by commanders and staff two echelons lower in the chain of command. The more concise the commander's intent, the easier it is to recall and understand. Commanders develop their intent statement personally using the following components:

- Expanded purpose.
- Key tasks.
- End state.

5-28. When describing the expanded purpose of the hunt operation, the commander's intent does not restate the why of the mission statement. Rather, it addresses the broader purpose of the operation and its relationship to the force as a whole. Often, the purpose incorporates how the operation relates to one or more of the fundamentals of hunt can clearly convey the expanded purpose of an operation.

5-29. Key tasks are those activities the force must perform as a whole to achieve the desired end state. Key tasks are not specified tasks for any subordinate unit; however, they may be sources of implied tasks. During execution, when significant opportunities present themselves or the concept of operations no longer fits the situation, subordinates use key tasks to keep their efforts focused on achieving the desired end state.

5-30. The end state is a set of desired future conditions the commander wants to exist when an operation concludes. Commanders describe the operation's end state by stating the desired conditions of the friendly force in relation to the desired conditions of the enemy, terrain, and other friendly forces. A clearly defined end state promotes unity of effort among the force and with interorganizational and multinational mission partners.

Planning Guidance

5-31. Commanders provide planning guidance to the staff based upon their visualization of the current situation, their experience, and their professional military judgment. Planning guidance reflects how the commander sees the operation unfolding with sufficient detail, context, and clarity. It broadly describes when, where, and how the commander intends to employ combat power to accomplish the mission within the higher commander's intent. Broad and general guidance gives the staff and subordinate leader's maximum latitude allowing both the defensive cyber force staff and battalion staff to develop flexible and effective options in parallel, simultaneous, and complementary efforts. Leaders within the defensive cyber force headquarters and the leaders of the defensive cyber force elements who will execute the hunt tasks in support of the supported commander, must clearly understand the defensive cyber force commander's planning guidance so they know what and when to report as they identify combat information, fill information gaps, and answer priority intelligence requirements.

Commander's Critical Information Requirements

5-32. A *commander's critical information requirement* is an information requirement identified by the commander as being critical to facilitating timely decision making (JP 3-0). The two key elements of commander's critical information requirements are priority intelligence requirements and friendly force information requirements.

5-33. Priority intelligence requirements identify the information about the enemy and the operational environment that the commander considers most important. Normally tied to either a named area of interest or a target area of interest, priority intelligence requirements become the central focus for the defensive cyber force organizations conducting the hunt tasks.

5-34. Friendly force information requirements identify the information about the mission, troops, support, and time available for friendly forces that the commander considers most important.

5-35. A commander's critical information requirements directly influence decision making and enable the successful execution of flexible military operations, or decision point tactics. Commanders decide to designate an information requirement as a commander's critical information requirement based on likely

decisions and their visualization of the course of the operation. During planning, staffs recommend information requirements for commanders to designate as commander's critical information requirements. During preparation and execution, staffs may recommend changes to commander's critical information requirements based on assessment. A commander's critical information requirement is—

- Specified by a commander for a specific operation.
- Applicable only to the commander who specifies it (or their subordinates executing hunt tasks in support of the commander).
- Situation dependent—directly linked to a current mission or a decision that will create a new mission, branch, or sequel to the current mission.
- Time-sensitive.

5-36. Commanders limit the number of commander's critical information requirements to focus the efforts of its organic defensive cyber force organizations or task-organized combined arms, cyber-signal teams that will conduct hunt tasks for the supported commander. With fewer prioritized commander's critical information requirements, subordinate units can apply greater concentrations of combat power and hunt focus to each information requirement. At the same time, fewer prioritized commander's critical information requirements facilitate timely and accurate reporting and provide the commander with the required information sooner.

5-37. Throughout an operation, the list of commander's critical information requirements will constantly change. defensive cyber force commanders, through their staffs, effective liaison teams, the tactical network, and direct communications with their subordinate commanders, constantly refine and develop their information requirements throughout the operations process as they add and delete commander's critical information requirements based on the information needed for specific decisions.

Essential Elements of Friendly Information

5-38. Commanders describe information they want protected as essential elements of friendly information. An *essential element of friendly information* is a critical aspect of a friendly operation that, if known by a threat would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection (ADP 6-0). Although essential elements of friendly information are not commander's critical information requirements, they have the same priority. Essential elements of friendly information establish elements of information to protect rather than ones to seek or collect. Identifying essential elements of friendly information is central to prioritizing units, information, or activities to focus security tasks. Figure 5-2 shows the various types of information requirement.

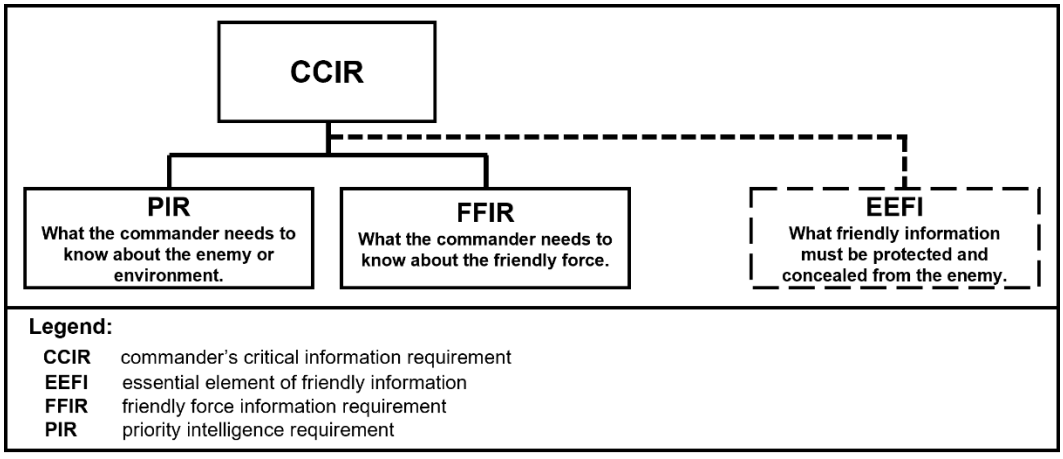


Figure 5-2. Information requirements

Hunt Guidance

5-39. Commanders provide clear hunt guidance that offers both freedom of action to develop the situation as well as adequate direction to ensure their organic defensive cyber force elements can accomplish stated hunt

objectives within the required timeframe. The commander's hunt planning guidance provides a clear understanding of the defensive cyber force organization's task, purpose, and objective. Hunt guidance explains focus, levels of detail required, levels of covertness, and guidelines for engagement, disengagement, and displacement of the organization. The commander develops their planning guidance based on the higher headquarters mission, timeline and intent in order to satisfy information requirements and identify opportunities to seize, retain, and exploit the initiative. The commander specifies different hunt guidance for each phase of an operation and adjusts the components of their guidance when appropriate. The commander's guidance consists of four elements:

- Focus.
- Tempo of hunt operations.
- Engagement and disengagement criteria (if any).
- Displacement criteria.

5-40. As with hunt guidance, commanders provide clear security guidance that offers freedom of action and direction to ensure that their defensive cyber force organizations can accomplish stated objectives within the required timeframe. The commander's security planning guidance provides a clear understanding of the defensive cyber force organization's task, purpose, and objective and the protection requirements of the security mission. The elements and purpose of security guidance are the same as hunt guidance. Figure 5-3 illustrates the process of developing hunt guidance.

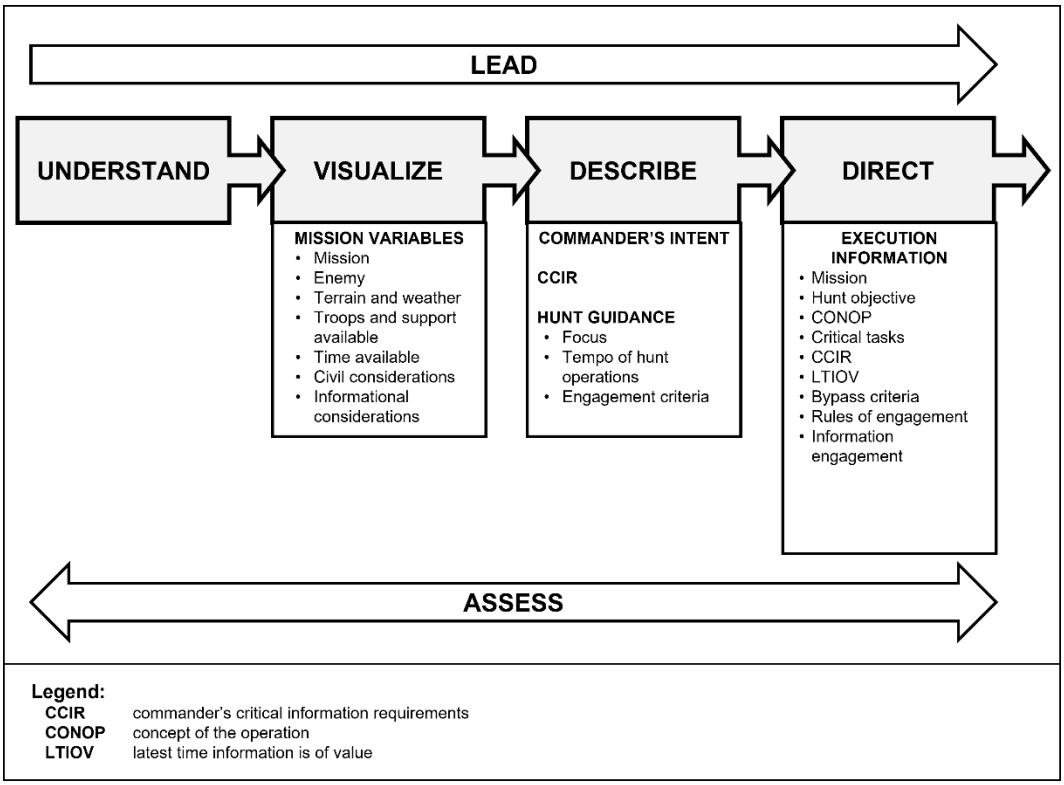


Figure 5-3. Development of hunt guidance

COMMANDERS AND STAFFS COLLABORATE TO PLAN, PREPARE, EXECUTE, AND ASSESS

5-41. The operations process consists of the major command and control activities performed during operations—planning, preparing, executing, and continually assessing. Commanders drive the operations process, while remaining focused on the major aspects of operations. Staffs conduct the operations process—they assist commanders in the details of planning, preparing, executing, and assessing.

5-42. The continuous nature of the operations process—and the critical combat information and timely and accurate reports provided during hunt tasks—allows commanders and staffs to adjust plans to enable agile and adaptive forces. Commanders, assisted by their staffs, integrate activities and operations throughout the

defensive cyber force and subordinate elements as they exercise command and control. Throughout the operations process, they develop an understanding and appreciation of the operational environment and the tactical situation. They formulate a plan and provide purpose, direction, and guidance to the defensive cyber force. Commanders then adjust operations as changes to the operational environment and the tactical situation occur, allowing commanders to seize, retain, and exploit the initiative to gain a position of relative advantage over the enemy.

5-43. Throughout the entire operations process, the staff supports the commander and subordinate commanders in understanding situations, decision making, and implementing decisions throughout the conduct of operations. The staff does this through three primary tasks:

- Conduct the operations process (plan, prepare, execute, assess).
- Conduct knowledge management and information management.
- Conduct analytic support operations.

Plan

5-44. *Planning* is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Army leaders plan to create a common vision among subordinate commanders, staffs, and unified action partners for the successful execution of operations. Planning results in an order that clearly communicates a commander's vision and directs actions to synchronize forces in time, space, and purpose for achieving objectives and accomplishing missions.

- Understand and develop solutions to problems.
- Anticipate events to adapt to changing circumstances.
- Task-organize the force and prioritize efforts.

Understand and Develop Solutions

5-45. The commander and staff conduct conceptual planning (using the Army design methodology) to understand, visualize, and describe the operational environment and the operational approach to the problem. The Army design methodology entails framing an operational environment, framing a tactical problem, and developing an operational approach to solve the problem. The Army design methodology results in an improved understanding of the operational environment, a problem statement, initial commander's intent, commander's hunt guidance, and an operational approach that serves as a link between conceptual and detailed planning. Based on their understanding and learning gained during Army design methodology, commanders issue planning guidance, including an operational approach, to guide more detailed planning using the military decision-making process. The defensive cyber force and subordinate elements' detailed planning efforts use the military decision-making process to produce a synchronized plan that provides mission type orders to subordinate units, including the analytic support cell and defensive cyber force elements.

5-46. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The military decision-making process integrates the activities of the commanders, staffs, subordinate headquarters, and unified action partners to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operations order for execution. The military decision-making process helps leaders apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions. The military decision-making process helps commanders, staffs, and others to think critically and creatively while planning and results in an improved understanding of the situation and an order that guides the force through preparation and execution.

5-47. The military decision-making process consists of seven steps. Each step of the military decision-making process has various inputs, a method (step) to conduct, and outputs. The outputs lead to an increased understanding of the situation and to facilitating the next step of the military decision-making process.

5-48. The military decision-making process facilitates collaboration and parallel planning. The defensive cyber force headquarters solicits input and continuously shares information concerning future operations through planning meetings, warning orders, operations orders, and fragmentary orders. Commanders

encourage active collaboration to build a shared understanding of the situation, participate in course of action development and decision making, and resolve conflicts before publishing the order.

5-49. The military decision-making process also drives preparation. Since time is a factor in all operations, commanders and staffs conduct a time analysis of their planning and preparation activities early in the planning process. Time analysis may require the commander to direct subordinates through a series of warning orders to start necessary movements, change task-organization, begin hunt tasks, and execute other preparation activities before completing the plan. For example, to support hunt tasks, the defensive cyber force commander and staff must conduct parallel planning simultaneously with the higher headquarters defensive cyber force staff.

5-50. The commander is the most important participant in the military decision-making process. More than simply a decision maker in the process, commanders use their experience, knowledge, and judgment to guide staff planning efforts. During the military decision-making process, commanders focus their activities on understanding, visualizing, and describing.

5-51. The staff's efforts during the military decision-making process focuses on helping the commander understand the situation, make decisions, and synchronize those decisions into a fully developed plan or order. Staff activities during planning initially focus on mission analysis. The products that the staff develops during mission analysis help commanders understand the situation and develop the commander's visualization. The mission analysis products also define the staff's input into the initial phases of the hunt tasks.

Anticipate Events and Adapt to Changing Circumstances

5-52. Defensive cyber force elements are the eyes and ears of the defensive cyber force organization and the commander. The commander and staff must be able to assist the higher headquarters commander in understanding, visualizing, and describing the area of operations and the tactical situation. The defensive cyber force's primary purpose in operations is to answer the higher commander's priority intelligence requirements.

5-53. To this end, outputs of intelligence preparation of the operational environment (such as the enemy situational template, the event template, and the defensive cyber force commander's critical information requirements) are critically important to assisting the defensive cyber force in anticipating events and adapting to changing situations. As commanders articulate their information requirements, the defensive cyber force staff further refines the information requirements into specific hunt operations and information collection plans.

5-54. Priority intelligence requirements drive decision points. For example, the defensive cyber force commander could establish priority intelligence requirements concerning enemy capabilities and disposition and civil considerations in conjunction with a series of friendly force information requirements about the defensive cyber force:

- Priority intelligence requirements are information about the enemy which drives decision points. For example—
  - Is the enemy scanning focused on certain ports or protocols?
  - What is the scope of enemy persistence mechanisms?
  - Does enemy command and control use common web protocols?
- Friendly force information requirements are the things we need to know about ourselves. For example—
  - Completion and status of defensive preparations.
  - Loss of communications with endpoint detection and response agents.
  - Loss of data feed or impact to data retention.

5-55. The defensive cyber force staff will further refine the defensive cyber force commander's priority intelligence requirements into essential elements of information. And the defensive cyber force staff and subordinate commanders and analytic support officers, will, in turn, designate essential elements of information that nest with the higher commander's priority intelligence requirements. After establishing essential elements of information, the defensive cyber force staff may establish indicators. In intelligence

usage, an *indicator* is an item of information that reflects the intention or capability of an enemy and/or adversary to adopt or reject a course of action (JP 2-0). After doing analysis of likely threat accesses, given the terrain, subsequent essential elements of information for their respective area of operations could include—

- Brigade echelon essential elements of information—
  - Does the threat have privileged access to the domain controller?
  - Have we observed lateral movement to identified key terrain?
  - Has the threat breached the operational technology network?
- Battalion echelon essential elements of information—
  - Has the threat conducted privilege escalation?
  - Is there a viable connection between area of operations Beta and area of operations Delta?
  - Is there communication between the information technology and operational technology networks?
- Mission element analytic scheme of maneuver indicators—
  - Have we observed Windows Event log 4672 on user accounts?
  - Do the network device configurations include routes between area of operations Beta and area of operations Delta?
  - Have we observed traffic between the human-machine interface and the information technology network?

5-56. The defensive cyber force staff has a supporting relationship to the higher headquarters hunt mission and will often operate on a parallel planning timeline with the higher headquarters staff during the operations process.

Task Organize the Force and Prioritize Efforts

5-57. Task organization is a temporary grouping of forces designed to accomplish a particular mission. Commanders task-organize their forces by establishing command and support relationships in accordance with their analysis of the mission variables of METT-TC (I).

5-58. Defensive cyber forces task-organize and assign command relationships for their formations to execute cyberspace operations to accomplish their assigned mission in their anticipated operational environment. The defensive cyber force establishes conditions for hunt tasks by enabling the defensive cyber force elements with additional intelligence collection assets (to include partnering with and access to joint and national-level intelligence assets), mobility, countermobility, and general network engineering support, increased sustainment capacity, increased communications capabilities for extended operational timelines, as well as additional analytic combat power in the form data engineers and analytic support personnel. The more sufficient the task organization, the more capable the defensive cyber force organization is to develop the situation through action, especially in an unclear operational environment.

5-59. When task-organizing, commanders and staffs should clearly define the command and support relationships between organizations. The type of command relationship will relate to the nature of the operation and the expected duration of the organization. Refer to ADP 6-0 for detailed descriptions of command and support relationships. Command and support relationships include—

- Organic.
- Assigned.
- Attached.
- Operational control.
- Tactical control.

5-60. Additional combat power enhances the defensive cyber force's ability to gain and maintain contact, execute hunt operations, conduct battle handover, and provide an increased capability to defeat threat counterreconnaissance and react to chance encounters. Task-organizing additional combat power with the defensive cyber force can give the unit a marked advantage during decisive operations.

5-61. Although properly task-organized defensive cyber force organizations can produce effects that outweigh the diversion of combat power from other elements—achieving an economy of force—the

commander should consider that dedicating these additional capabilities to the battalion echelon comes at the expense of capability for potential follow-on operations. Therefore, commanders should carefully consider the risks of executing hunt tasks as an economy of force.

Prepare

5-62. Preparation consists of activities performed by units and Soldiers to improve their ability to execute an operation. Preparation creates conditions that improve friendly forces' opportunities for success. Preparation requires commanders, staffs, and units to ensure that the force is trained, equipped, and ready to execute operations. Preparation activities help commanders, staffs, and units understand a situation and their roles in upcoming operations.

5-63. During preparation, commanders take every opportunity to improve their situational understanding prior to execution of their decisive operations. The defensive cyber force and its organic elements must be prepared to execute aggressive and continuous hunt tasks during the preparation phase of the operations process.

5-64. At the same time, the defensive cyber force is often most susceptible to surprise and unobserved threat activity during preparation, when forces might be in planning or in transit. Leaders are away from their units and concentrated together for rehearsals: part of the force could be moving to task organize. Required supplies may be unavailable or being repositioned. As a result, security tasks are essential during this phase of the operations process.

5-65. Commanders and staffs must revise and refine their initial plan during preparation. The commander's situational understanding will change over the course of the operations process—threat actions will require revision of the plan and the ongoing hunt tasks will generate both applicable combat information and unforeseen opportunities. During preparation, assumptions made during planning are confirmed or denied. Significant new information—either priority intelligence requirements or friendly force information requirements that are answered by effective hunt tasks—will require commanders to revise and refine their operational plan.

5-66. Finally, commanders and staffs conduct confirmation briefs and rehearsals. A confirmation brief is a briefing that subordinate leaders give to the higher commander immediately after the operation order. It is the leaders' understanding of the commander's intent, their specific tasks—to include the defensive cyber force commander's hunt guidance—and the relationship between their mission and the other units in the operation. Ideally, the commander conducts confirmation briefs in person with selected staff members. A rehearsal is a session then which the commander and staff or unit practices expected actions to improve performance during execution. Both confirmation briefs and rehearsals are essential to ensure that subordinate commanders and staffs understand the concept of operations and the commander's intent. Rehearsals and confirmation briefs allow leaders to practice synchronizing operations at times and places critical to mission accomplishment. Effective rehearsals and confirmation briefs solidify the sequence of the operation's key actions and improve mutual understanding throughout the unit. During preparation, commanders and staffs must ensure that the defensive cyber force and the analytic support elements are—

- Assessing data availability and accesses.
- Conducting aggressive hunt operations to improve commanders' situational understanding.
- Revising, refining, and rehearsing the operational plan.
- Integrating, organizing, and configuring their task-organized, combined-arms, cyber-signal teams.
- Ensuring forces and resources are ready for execution.

5-67. The cyber protection brigade and battalion should also conduct a reconnaissance and security rehearsal to ensure the hunt plan meets the commander's intent and is synchronized across the defensive cyber force. The commander, executive officer, S-2, S-3, analytic support officer, element lead, intelligence support lead, and other staff cells (for example, sustainment, and remote operations) should attend. The rehearsal should last no longer than one hour and should focus on rehearsing hunt tasks that address each priority intelligence requirement and their associated named areas of interest.

Execute

5-68. Hunt and cybersecurity tasks, by their nature, are combined arms, cyber and signal operations providing the commander with information and intelligence that help reduce uncertainty and enable rapid decision making. Moreover, the same combined arms, cyber-signal teams can present threat forces with multiple forms of disruption, forcing the threat to react continuously. Signal assets provide critical complementary effects to defensive cyber force's organic elements during hunt operations. Specifically, signal assets provide organic defenses and extensive observation capabilities, and facilitate the rapid movement of data during hunt operations. Additionally, signal assets can quickly employ deliberate defensive measures within the defended network or as identified during hunt and cybersecurity tasks. Cybersecurity elements can provide additional observation to assist the defensive cyber force organization in maintaining contact.

Cyber-Signal Operations

5-69. Cyber-signal operations consist of the simultaneous or synchronized employment of defensive forces to retain the initiative. Effective cyber-signal operations are built upon relationships, mutual trust, and a common understanding of the operational environment, operation, and mission. They require detailed planning, coordination, and synchronized employment of cyber maneuver and network effects to achieve the commander's objectives and ensure freedom of movement and action. Cyber-signal operations require detailed planning of synchronized timelines, signal element task and purpose, and Soldier work-rest cycles.

5-70. Key to implementing cybersecurity assets into hunt operations is early integration into the supported commander's operations process. The supported commander and their staff must understand the capabilities and limitations of the signal unit and the types of defenses available, along with the doctrinal missions and roles which signal can support. Regardless of the type of hunt mission, integrating signal elements into the early stages of planning allows the supported commander, their staff, and subordinates, to leverage the capabilities and deconflict issues critical to the effective use and synchronization of signal in a combined arms environment. The signal commander's plan must be nested and deconflicted with the cyber scheme of maneuver. Signal-specific information includes the location of network observation points, battle positions, domain controllers, ingress and egress paths and routes, and other network management control measures. These locations and assets must be viewed with respect to the analytic scheme of maneuver, cyber force observation points and sensor positions, and other network restrictions to ensure they do not interfere with network administration, maneuver by cyber units, or signal use. Coordinating cyberspace for the rapid and efficient use of cyber and signal is essential and must be planned early and reviewed often. Once planning is complete, all cyber and signal units must use the same common operational picture to prevent fratricide and efficiently conduct operations.

5-71. The defensive cyber force combined arms cyber-signal teams operate and move dispersed over wide areas to evade threat detection and achieve surprise. Cyber units are quickly able to reconnoiter terrain that is not well-mapped or to observe the dead-space between signal observation points and battle positions. Defensive cyber units are ideally suited to execute hunt tasks due to the superior speed, mobility, and analytic power inherent to defensive cyber force elements. Cyber analytic support cells have advanced always-on observation and analysis systems, enhance analytic development capabilities, and can integrate with intelligence community assets for awareness and information collection. Hunt operations allow the defensive cyber force to concentrate rapidly against decisive points to exploit threat weaknesses, block the threat from sources of ingress, or disrupt the threat from unexpected directions.

Execute Decision Point Tactics

5-72. The commander and staff's ability to anticipate changing conditions in the battlespace is key to mission success—commanders and their staffs must see themselves and other friendly forces, the terrain, vulnerabilities, threats, and the user base. Hunt tasks allow commanders to accurately anticipate changing conditions. Defensive cyber force organizations confirm or deny the commander and staff's initial anticipatory assumptions. For example, during course of action analysis, commanders and staffs focus on critical events that directly influence mission accomplishment. In addition, it is during these identified critical events that the commander may identify priority intelligence requirements that answer their decision points. The decision support matrix coupled with the decision support template are results of a commander and

staff's ability to visualize the battlespace and identify critical points where transitions or decisions must occur.

5-73. A *decision point* is a point in space and time when the commander or staff anticipates making a key decision concerning a specific course of action (JP 5-0). A decision support template depicts decision points, timelines associated with movement of forces and the flow of the operation, and other key items of information required to execute a specific course of action. A decision support matrix is a written record of a war-gamed course of action that describes decision points and associated actions at those decision points.

5-74. The decisions commanders and staffs must make during operations are either execution decisions or adjustment decisions. Execution decisions involve options anticipated in planning and outlined in the operation order. Adjustment decisions involve options that commanders did not anticipate—they respond to unanticipated opportunities and threats and require implementing and synchronizing unanticipated operations. Adjustment decisions may include a decision to develop an entirely new plan.

5-75. The employment of defensive cyber force organizations ties directly to answer decision points in support of higher echelon's course of action and provides the commander the flexibility necessary for mission accomplishment. During mission execution the staff constantly updates their critical facts and assumptions based on reports from hunt tasks. This technique of using decision points to influence critical events in the area of operations highlights the imperative for continuous reporting during mission execution.

5-76. The location of commanders and their tactical command posts should facilitate the rapid and effective decision making under the anticipated tactical and operational decisions contained within the decision support matrix, the decision support template, and updated assessments of the situation. To create, identify, and seize fleeting opportunities, defensive cyber force commanders must be capable of commanding remotely and take advantage of DOD networks to confirm combat information and update their understanding, visualization, description, direction, assessment, and leadership of cyberspace operations to make timely and effective tactical and operational decisions.

Assess

5-77. Defensive cyber force commanders and their staffs prioritize data and information collection activities by providing their hunt guidance and intent early in the planning process, establishing commander's critical information requirements, and updating information requirements based on changing conditions in the operational environment as reported by their defensive cyber force elements. While doing so, commanders and their staffs must ensure that the commander's critical information requirements directly inform decisions associated with their analytic scheme of maneuver to provide flexibility and agility as they develop the situation and determine the disposition, intent, and capabilities of threat organizations. Commanders and staffs must aggressively seek higher echelons' collection of, and answers to, the information requirements as well as identify the time sensitivity of their commander's critical information requirements with the latest time information is of value to ensure timely decision making.

COMMANDERS AND STAFFS BUILD AND MAINTAIN SITUATIONAL UNDERSTANDING

5-78. Success in operations demands timely and effective decisions based on applying judgment to available information provided by effective hunt tasks. As a result, commanders and staffs must build and maintain situational understanding throughout the operations process. Situational understanding is the product of applying analysis and judgment to relevant information to determine the relationships among the operational variables (PMESII-PT) and the mission variables of METT-TC (I) to enable decision making. Building and maintaining situational understanding is essential to establishing the situation's context, developing effective plans, assessing operations, and making quality decisions throughout the operations process.

COMMANDERS AND STAFFS ENCOURAGE COLLABORATION AND DIALOGUE

5-79. Throughout the operations process, commanders encourage continuous collaboration and dialogue among the staff and with mission partners. Collaboration and dialogue aids in developing shared understanding throughout the force. To accomplish the requisite degree of collaboration and dialogue and to assist the defensive cyber force commanders to plan, execute, and assess hunt operations, the defensive cyber force staff should organize into an operations and intelligence working group.

5-80. The operations and intelligence working group comprises designated staff officers that coordinate and integrate information collection activities and provide the commander and the defensive cyber force S-3 with recommendations. The operations and intelligence working group develops and refines the information collection plan as part of the defensive cyber force's hunt tasks.

5-81. The S-3 directs the operations efforts of coordinating and special staff officers, integrating and synchronizing plans and orders, and supervising management of the commander's critical information requirements. The S-2 prepares the information collection plan by working in concert with the entire staff to identify information collection requirements for inclusion. The analytic support and intelligence staff determines collection requirements, develops the analytic collection matrix with input from the staff representatives, and continues to work with the staff planners to develop the plan. The S-2 identifies those intelligence assets and resources that can provide answers to the commander's critical information requirements, including human intelligence or signals intelligence.

5-82. The intelligence cell manages counterintelligence and human intelligence operations in support of the overall unit mission. The intelligence cell works with the G-2 or S-2 for information collection planning and assessment by taking developed counterintelligence and human intelligence requirements and identifying the proper assets to answer the requirements.

5-83. The S-3 is the primary information collection tasking and directing staff officer within the unit, tasking the organic and assigned assets for execution. Before publishing the information collection plan, the S-3 coordinates it with other command post staff to ensure synchronization with the other elements of the operation order. The operations and intelligence working group is represented by—

- S-3 technical director.
- Cyberspace network management representative.
- Signal liaison officer.
- Defensive cyber force battalion S-3.
- Defensive cyber force battalion S-2.
- Analytic support officer.
- Chief, remote operations (signal officer).
- Senior cyber integration technician.
- Cyber sustainment representative.
- Staff judge advocate (if required).
- Public affairs officer (if required).

5-84. The operations and intelligence working group will directly support the commander in the execution of command and control of hunt operations by performing command and control warfighting function tasks. The operations and intelligence working group conducts—

- The operations process—plan, prepare, execute, and assess.
- Knowledge management and information management.
- Synchronization of cyber and other information functions.
- Analytic and data collection prioritization.

INTEGRATING PROCESSES AND CONTINUING ACTIVITIES

5-85. Throughout the operations process, commanders and staffs integrate the warfighting functions to synchronize the force in accordance with the commander's intent, their hunt focus, the concept of operations, and the updated combat information provided by the defensive cyber force's hunt operations. The integrating processes for hunt tasks are:

- Intelligence preparation of the operational environment.
- Gap analysis and requirement development.
- Timely reporting and situational understanding.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

5-86. Hunt operations begin with developing and adapting the staff's intelligence preparation of the operational environment, including understanding threat capabilities, visualizing threat courses of action, and developing associated decision support matrixes and templates.

5-87. Intelligence preparation of the operational environment is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. The entire staff participates in intelligence preparation of the operational environment to develop and sustain an understanding of the enemy, terrain and weather, and local user considerations. Intelligence preparation of the operational environment helps identify options available to friendly and threat forces.

5-88. Intelligence professionals and analytic support officers supporting defensive cyber forces employ traditional intelligence community resources as well as commercial intelligence feeds to close technological information gaps. Vulnerabilities and risks to DOD networks are often shared across the globe by government and private entities, thus providing opportunity to understand threat capabilities, tactics, techniques, and procedures by observing their activities outside the DOD network. Commercial partners are well-positioned to supply data and trends that inform hunt operation planning.

GAP ANALYSIS AND REQUIREMENT DEVELOPMENT

5-89. Through intelligence preparation of the operational environment and development of the analytic scheme of maneuver, the team may identify gaps in data or in analytic capabilities. In some instances, these gaps can be resolved with other data or capabilities. Data engineers become responsible for the data gaps and analytic support officers are responsible for analytic (capability) gaps that are identified in the planning process. Capability gaps for crucial indicators or evidence often suggest that a commander's critical information requirement cannot be answered, and therefore the unit cannot effectively complete the mission.

5-90. Resolving analytic capability gaps is a core function of an analytic support officer. This function occurs during all phases of an operation, including recovery and training phases. The analytic support officers work with other cyber professionals to develop analytical methods and analytic solutions to fill the existing capability gaps. While network and host analysts are expected to develop queries using simple methodologies, analytic support officers are expected to apply advanced statistical analytic methods to one or multiple datasets. These advanced analytic solutions are geared at identifying anomalous and malicious cyber activity or understanding the operational environment.

5-91. When the unit assigned to the mission is unable to resolve a capability gap, the analytic support officer is responsible for providing the technical information necessary for a higher echelon or external organization to work on resolving the gap. While an analytic support officer can serve as the point of contact for this coordination, it will generally serve the mission element best if the support element lead manages it and works with the analytic support officer when necessary.

TIMELY REPORTING AND ASSESSMENT

5-92. During mission planning execution, defensive cyber force organizations provide timely and accurate combat information through cyber hunt operations and their associated reports. These reports allow the staff and the defensive cyber force commander to update their running estimates based on the most recent and accurate reports generated through hunt operations. At the same time, analytic support operations execute assigned missions while the rest of the force prepares for the overall operation. Security tasks (such as screening boundaries) and analytic development are essential during preparation.

5-93. Commanders take every opportunity to improve their situational understanding before execution of the mission. Improving situational understanding requires aggressive and continuous information collection from the defensive cyber force. Through information collection, commanders and staffs continuously plan, task, and employ collection assets and forces to collect timely and accurate information to help satisfy the commander's critical information requirements and other information requirements.

5-94. The commander and staff's ability to anticipate changing conditions in the area of operations is key in seizing, retaining, and exploiting the initiative. To be effective, the S-2 and S-3 staffs base the information collection plan on the initial intelligence preparation of the operational environment and modify it as the

intelligence running estimate changes. Other staff sections' running estimates may contain requirements for inclusion into the information collection plan. Additionally, the staff plans synchronization into the analytic scheme of maneuver and adds updates as that scheme changes. Properly synchronized information collection planning begins with developing and updating the intelligence preparation of the operational environment, including threat characteristics, enemy templates, enemy course of action statements, and an enemy event template or matrix.

5-95. During course of action analysis, the staff focuses on critical events that directly influence mission accomplishment. It is during these critical events the staff may identify priority intelligence requirements to answer decision points. The decision support matrix coupled with the decision support template is a result of a staff's ability to visualize the operational environment and identify potential points of friction. The employment of defensive cyber force organizations should be tied directly to answer these decision points in support of higher headquarters' course of action and provide the commander the flexibility necessary for mission accomplishment. During mission execution, the staff constantly updates critical facts and assumptions based on reports from hunt elements. Using decision points to influence critical events highlights the imperative for continuous reporting during mission execution.

5-96. As execution of the plan progresses, decision point timelines used as the basis for the latest time information is of value are refined. The staff stays alert to the need for recommending changes in the information collection plan due to refinements. As the need for change arises, the S-2 staff coordinates with the appropriate staff sections to update the products required to refine the information collection plan.

Cue Hunt Organizations and Analysis Assets to Other Requirements

5-97. The S-2 and S-3 staffs at the defensive cyber force headquarters track the status of analysis or collection assets, cross-cueing them as needed, and teaming assets together as appropriate, to answer priority intelligence requirements. For example, if an analyst reports an increase in anomalous activity to a public-facing Internet Protocol address, the staff, primarily the analytic support officer, could recommend redirecting intelligence assets or other surveillance means to monitor the address for potential threat.

Eliminate Satisfied Requirements

5-98. As the operation continues, the operations and intelligence cell tracks the status of each analysis task, analyzes specific information requirements, and monitors tasks for satisfaction of information requirements. The staffs pay particular attention to assets not producing required results, which may trigger adjustments to the analytic scheme of maneuver or the reallocation of analytic assets.

5-99. The operations and intelligence staff eliminates satisfied requirements and irrelevant requirements from the analytic scheme of maneuver, even if unsatisfied. In this case, the operations staff, in coordination with the intelligence staff, relieves the analysis assets of further responsibility to analyze information on the original task.

Re-Task Defensive Cyber Force Organizations and Assets

5-100. As the situation changes, or when defensive cyber force organizations meet the initial information requirements, the commander and the staff should redirect the focus of hunt tasks. Re-tasking is assigning an analysis asset or a defensive cyber force unit a new, modified, or refocused task and purpose.

5-101. Re-tasking is generally accomplished at the battalion level through a fragmentary order published by the S-3. Re-tasking occurs—

- Upon completion of its initial requirement.
- When an original task becomes irrelevant.
- On order, after the latest time information is of value, and having not satisfied the original analysis requirement—adjusting the latest time information is of value may be required.
- As planned to support a branch or sequel.
- To respond to changes in the tactical or operational situation

Develop and Add New Requirements

5-102. As the operation progresses and the threat situation develops, commanders generate new requirements. The S-2 staff begins updating requirements planning by identifying and prioritizing new requirements, evaluating resources based on priorities, and making appropriate recommendations to the commander and operations officer.

Transition

5-103. Updating analytic scheme of maneuver taskings may result in a change of focus for several defensive cyber force assets. Defensive cyber force assets may require rest and refit, or lead time for employment to effectively transition from one mission or operation to another.

UPDATE THE ANALYTIC SCHEME OF MANEUVER

5-104. The staff updates the data collection plan as the hunt assets answer information requirements. Evaluation of reporting, production, and dissemination identifies the need for focus or refocus and assigning or reassigning defensive cyber force assets. As the tactical situation changes, adjustments are made to the overall data collection plan to keep analysis tasks synchronized.

5-105. These steps are collaborative efforts by the S-2 and analytic support staffs. Some steps predominately engage the S-2 staff, others the S-3 and analytic support staff, and some steps may require coordination with other staff sections.

SCREEN REPORTS

The staff screens incoming reports to determine whether the collected data will satisfy the following criteria:

- **Relevance**—does the information address the analysis task? If not, use this information to satisfy other requirements.
- **Completeness**—is essential information missing? (Refer to the original analysis task.)
- Timeliness—has the asset reported, by the latest time information is of value, as established in the original task?
- **Opportunities for cueing**—can this asset or another asset take advantage of the new information to increase the effectiveness and efficiency of the overall information analysis effort?

CORRELATE REPORTS TO REQUIREMENTS

5-106. Correlating and evaluating intelligence and analysis reports to the original requirement is a key to effective requirements management. Timely requirements management includes dissemination and receipt of reports and related information to the original requesters and other users.

5-107. The staff tracks which specific analysis task originates from which requirement, ensuring the analyzed information provided to the original requester (and to all who need the information) is timely. For efficiency and timeliness, the staff ensures they receive the proper analysis assets to determine which requirements have been satisfied and which require additional analysis or analytic support.

5-108. The staff address the following potential challenges:

- Large volumes of information that could overwhelm the analytic support section.
- Reports that partially satisfy analysis tasks.
- Assets reporting information without referring to the original tasking.
- Circular reporting or unnecessary message traffic.

5-109. Subordinate defensive cyber force elements maintain clear and precise reporting throughout the hunt. Reporting that no evidence of priority intelligence requirements was observed during analysis can be a significant indicator when combined with data available to the higher echelon and adjacent unit hunt information.

PROVIDE FEEDBACK AND REVISE ANALYTIC SCHEME OF MANEUVER

5-110. Commanders should schedule assessments before and after each engagement to update information collection guidance and increase their own understanding of the situation. Feedback is essential for maintaining effectiveness and alerting leaders of deficiencies.

5-111. Following each assessment, staff sections should work together to tailor the information collection plan, making it as seamless as possible by removing information sharing barriers. Feedback reinforces whether collection or production satisfies the original task or request, provides guidance if it does not and aids in the redistribution of assets to capitalize on opportunities or fill identified voids.

5-112. Defensive cyber forces must conduct effective cyber-signal operations to engage partners and key actors, and establish security conditions to defeat threat organizations, shape environments, and consolidate gains. They require detailed planning, coordination, and synchronized employment of analytic maneuver to achieve the commander's objectives and ensure freedom of movement and action. Hunt tasks simultaneously confirm the commander and staff's initial understanding and visualization of the environment and further develop the situational understanding of the defensive cyber force.

5-113. The steps for updating the analytic scheme of maneuver are—

- Distill a new priority intelligence requirement.
- Determine valid indicators that could confirm or deny the requirement.
- Assess data sources that could provide evidence of indicator.
- Validate access to data source.
- Develop and validate analytics to apply to data.
- Action analytics across the data set.
- Record changes to the analytic scheme of maneuver.

This page intentionally left blank.

Chapter 6
Hunt

Cyber formations conduct hunt operations to determine threat composition and disposition as well as to gather information on terrain and cyber-personas. Hunt tasks enable units to seize, retain, and exploit the initiative across the range of cyberspace operations by identifying, creating, and capitalizing on opportunities, providing commanders with information to enable decision making, and the enabling concentration of unified efforts against decisive points.

FUNDAMENTALS, METHODS, AND MANAGEMENT

6-1. Hunt is a mission to obtain, by technical observation or other detection methods, information about the activities and resources of a threat, or to secure data and control of a particular network. Conducting hunt before and during other cyberspace operations provides information for the commander to confirm, deny, and modify their concept of operations. Within defensive cyber forces, the defensive cyberspace operations battalion is the principal reconnaissance organization. The fundamentals that govern planning and executing hunt tasks are—

- Ensure continuous reconnaissance.
- Do not keep reconnaissance forces in reserve.
- Orient on reconnaissance objectives.
- Report all information rapidly and accurately.
- Retain freedom of maneuver.
- Gain and maintain threat contact.
- Develop the situation rapidly.

ENSURE CONTINUOUS HUNT

6-2. Defensive cyber forces require continuous information collection throughout all phases and critical events of all operations. Commanders direct information collection throughout all operations and task-organize defensive cyber force assets to collect required information leading to more informed identification of execution of branches and sequels. Continuous hunt provides commanders with a constant flow of information to identify and control key terrain; confirm or deny threat activity, disposition, and likely courses of action; and provides reaction time and maneuver space for unpredicted threat actions.

DO NOT KEEP HUNT FORCES IN RESERVE

6-3. Continuous and focused collection efforts require an efficient mix and redundancy of hunt assets; however, this does not mean to employ all assets simultaneously. Commanders maximize employment of their hunt assets to answer their commander's critical information requirements. Defensive cyber forces task and position hunt assets at the appropriate time, place, and in the right combination (mission element, analytic support, data engineering, or enterprise cybersecurity surveillance means) to maximize their impact, allow for timely analysis of information, and aid decision making at the appropriate echelon. Sustainable readiness must also be considered as the nature of cyber competition and warfare often requires defensive cyber forces to train and execute operations simultaneously to retain perishable skills and be prepared for surge operations in crisis.

ORIENT ON HUNT OBJECTIVES

6-4. Commanders direct hunt efforts by establishing hunt objectives, with specific tasks, purpose, and focus. Hunt objectives can be a combination of terrain, enclaves, threat, or mission functions that provide commanders the necessary information to answer priority intelligence requirements. Defensive cyber force formations, task-organized to effectively accomplish their objectives, develop their analytic schemes of maneuver to maximize their capability to collect the required information within assigned objectives.

REPORT ALL INFORMATION RAPIDLY AND ACCURATELY

6-5. Commanders develop plans and make decisions based upon the analysis of information collected by subordinate units. Quick and accurate reports are required for the commander to make informed decisions on the proper application of their forces. Rapid reporting allows staffs maximum time to analyze information and make timely recommendations to the commander. Information requirements tied to decision points with a latest time information is of value date-time group provide focus for units collecting information and ensure units report information to enable timely decisions.

RETAIN FREEDOM OF MANEUVER

6-6. Tactical analytic mobility and maneuver fundamentally drive the success of hunt tasks. Commanders and staffs consider task-organization, movement techniques, and analytic schemes of maneuver to retain the unit's ability to execute its analytic mission. Hunt tasks confirm or deny assumptions about terrain and enemy made during mission analysis and intelligence preparation of the operational environment to identify opportunities for the command to seize, retain and exploit the initiative. Commanders change analytic techniques and employ multiple assets to ensure the appropriate echelon can bring effects to bear when the threat is identified. Commanders retain freedom of maneuver by providing early warning to operate and other defend forces, while preparing to take decisive action and develop the situation further—consistently balancing the requirement to maintain contact with retaining flexibility in response action. Hunt elements left to persistently observe a target outside of the analytic scheme of maneuver lose their ability to freely maneuver to new areas of emphasis.

GAIN AND MAINTAIN THREAT CONTACT

6-7. Defensive cyber forces find and sustain contact with the threat in preparation for either disrupting threat access or maintaining overwatch while intelligence gain-loss is evaluated. Commanders and staffs plan for and integrate available organic network and defensive cyber force sensors, signals intelligence, big data sets, and unified platforms to gain technical contact with the threat using the appropriate element. Intelligence units can provide a wide array of support to assist defensive cyber forces in detecting and tracking threats such as—

- Neutral space monitoring tools.
- Sensitive intelligence information.
- Other intelligence and counterintelligence resources.

6-8. Once units make contact, defensive cyber forces maintain contact until specific orders are given, a change of mission occurs when disengagement or displacement criteria dictate, or the unit conducts hunt handover with another unit. Maintaining contact with the threat provides real-time information of the threat's disposition, persistence, and activities that allows staffs to analyze and make recommendations to the commander based on current intelligence.

DEVELOP THE SITUATION RAPIDLY

6-9. Defensive cyber forces act instinctively and urgently to increase the commander's situational awareness of the terrain, threat, and network functionality. Effective defensive cyber forces understand how time impacts analysis and how timely data collection and analysis impact the commander's decisions. The analytic scheme of maneuver and tempo match the requisite urgency to answer the necessary information requirements. Defensive cyber forces collect data on directed hunt objectives in close contact with supporting operate forces while hunting and characterizing threat forces to determine likely intent, disposition, persistence, and the next action in their attack campaign.

HUNT TECHNIQUES

6-10. There are two hunt techniques commanders employ to answer information requirements—proactive (pull) and targeted (pursuit method). Commanders employ these techniques based on their level of understanding of the operational environment combined with the time available to refine their understanding. In selecting one technique over the other, the commander considers the—

- Degree of the situational understanding of the threat.
- Time available to collect the information.

- Leadership ability of subordinate commanders.
- Proficiency of subordinate units to plan and rapidly react for uncertain situations.

PROACTIVE (PULL)

6-11. Proactive (pull) hunt is used when commanders are uncertain of the disposition of threat forces in their areas of operations, information concerning terrain is vague, and time is limited. In these cases, hunt assets initially work over a broad area to develop the threat situation. As they gain an understanding of threat weaknesses, they then pull the main body to positions of tactical advantage. Proactive hunt knowingly emphasizes opportunity at the expense of a detailed, well-rehearsed plan and unity of effort. Commanders' base plans on several viable branches or courses of action triggered by decision points that hunt assets operate to answer associated commander's critical information requirements.

6-12. Leaders at all levels must understand and rehearse branches and sequels. Analytic support cells proactively hunting within Army big data platforms to detect probable threat behavior, are the most effective hunt asset that can be brought to bear by the defensive cyber force battalion commander for the proactive hunt. The proactive hunt will often leverage analytics to detect atomic malicious cyber activity to develop the situation and inform the Commander's decision to employ a mission element for a targeted hunt to further characterize and illuminate the threat campaign.

TARGETED (PURSUIT METHOD)

6-13. Targeted (pursuit method) hunt is used when commanders have a relatively thorough understanding of the operational environment. In these cases, commanders target hunt assets into specific portions of their areas of operations to confirm, deny, and validate planning assumptions impacting operations. Targeted hunt emphasizes detailed, well-rehearsed planning. Mission elements employed to observe and track threat behavior for intelligence gain or to enable incident response are the most effective hunt asset that can be brought to bear by the defensive cyber force battalion commander for the targeted hunt. The targeted hunt is used to fully characterize and illuminate the extent of a threat campaign or attack flow. Figure 6-1 on page 60 illustrates the hunt operations framework.

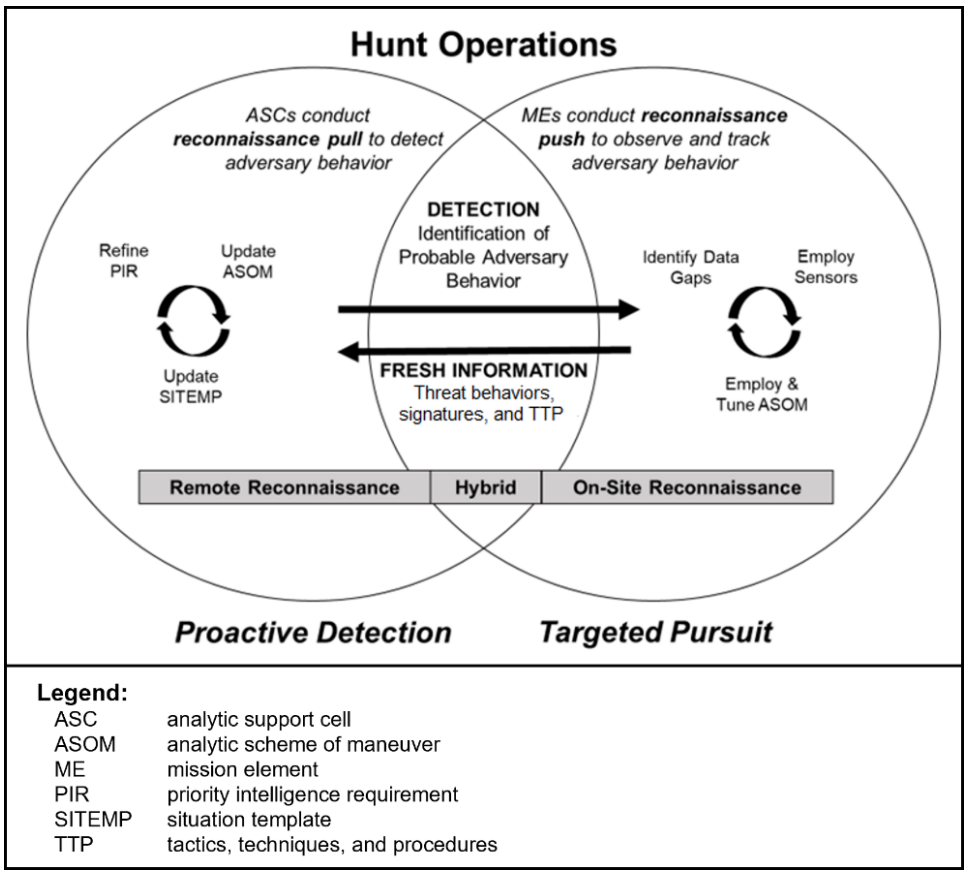


Figure 6-1. Hunt operations framework

HUNT METHODS

6-14. Hunt tasks use appropriate combinations of remote, on-site, and hybrid hunt to accomplish their mission. No method is mutually exclusive of another as the greater number of assets applied to information collection increases the effectiveness of the operation.

REMOTE HUNT

6-15. Remote hunt enables a more rapid tempo while increasing the flexibility of analytic efforts. Remote hunt should take advantage of existing enterprise and network surveillance sensors and data, as well as big data and unified platforms to find and observe the threat without the need for physical deployment. This increases defensive cyber forces' speed of response and enables them to execute the analytic scheme of maneuver across broader swaths of terrain. Some hunt tasks may mix on-site and remote methods, based on the threat situation and time available. The commander considers remote hunt when—

- Data is readily available to inform the analytic scheme of maneuver or can be made available in time available.
- The area of operations is not well-known and initial hunt to characterize network areas and understand enterprise surveillance data collection is preferred before any on-site force employment.
- Stealth and operations security are primary concerns.
- Threat activity is widespread and on-site hunt would not be possible in the time available.

6-16. Remote hunt is a form of hunt that involves a directed effort to obtain detailed information on data sets as informed by the analytic scheme of maneuver, but with the primary analysis being conducted from the defensive cyber force's local power projection platform with enrichment from access to intelligence and big data platforms. Any defensive cyber force element can perform a remote hunt through remote connection support and planning lead time. Commanders assign a remote hunt when the threat situation does not dictate

an on-site deployment and existing sensor architecture contains enough requisite network data to satisfy the requirements of the analytic scheme of maneuver. Commanders may require specific information or data to develop or refine their course of action before deploying forces on-site. In this regard, a remote hunt operation may orient follow-on elements' sensor strategy or data collection plan.

6-17. A remote hunt mission can be initiated rapidly, often prior to the completion of mission analysis helping to drive course of action development and ascertain the need for on-site hunt forces. The commander must work to balance available time with critical data collection to ensure that defensive cyber force units provide the necessary information for their higher commander. To do this, commanders deliberately focus analysis requirements and adjust their hunt techniques to increase the overall tempo. Commanders choose to task-organize defensive cyber forces to mitigate risks associated with an increased operating tempo and provide defensive cyber force organizations with an increased ability to develop the situation through action before committing combat forces to an on-site hunt operation.

6-18. The primary tasks associated with remote hunt are—

- Assess available data to ensure analysis can satisfy the analytic scheme of maneuver.
- Plan for last-mile connectivity to remotely emplaced defensive cyber force sensors.
- Request the alternation, tuning, or shifting of existing sensors in the area of operations to cover data gaps.
- Identify and report avenues of approach and impact on key terrain in cyberspace.
- Identify and report all threat activity within the area of operations according to the analytic scheme of maneuver.
- Based on engagement and bypass criteria, address threat persistence in the area of operations within the capability of the unit conducting reconnaissance.
- Report hunt information

6-19. The vignette on page 62 outlines a historical example of a remote hunt operation conducted on a global scale.

Remote Hunt Operations at Global Scale

Following the public release that a technology company suffered a supply-chain attack in their software patch; software that was in wide use across the DOD network. Army cyber leaders were immediately concerned with the risk posed to the network and wanted to determine the scope and disposition of threat infiltration and persistence. Early reports indicated that the threat's access was incredibly widespread across much of the logical and geographical Army footprint.

In response, ARCYBER tasked the U.S. Army Cyber Protection Brigade to conduct a hunt operation across the Department of Defense information network-Army to identify the systems infected with the threat's malware and the extent to which the threat had infiltrated adjacent terrain. Due to both the logical and geographic dispersion of terrain needing reconnoitered, defensive cyber forces initiated a remote hunt operation using available enterprise data in Army, joint, and interorganizational data platforms.

Developing an analytic scheme of maneuver while leveraging cyber threat emulation to learn more about the malware, the defensive cyber force determined that Domain Name System records and specific host artifacts were the most important data sets within the analytic scheme of maneuver. A battalion analytic support cell was tasked to execute the analytic scheme of maneuver, while coordinating sub elements to remotely reconnoiter certain network boundaries to develop the situation. Defensive cyber force elements maneuvered through Domain Name System logs, while others worked with local system administrators to obtain host artifacts from the infected, but now isolated systems.

All host artifacts were transported to a consolidated bucket within the Army's big data platform, enabling distributed and remote analysis. Domain Name System log analysis led to the discovery of previously unknown infected systems, and the Army's defensive cyber force triaged hundreds of infected machines without deploying any of their deployable defensive cyberspace operations systems or physically deploying personnel to any on-site location.

Operating within the deliberately developed and validated analytic scheme of maneuver, Army defensive cyber forces were able to quickly assess risk to the Army network based on the characteristics and disposition of identified infected systems. The analytic scheme of maneuver served as operational control of data analysis, ensuring disciplined maneuver through required data sets without duplication, with unit analytic support officers serving as synchronizers and aggregators of analysis findings. By remaining within their power projection site, defensive cyber forces maintained a well-integrated relationship with Army signal forces to clear infected systems, and intelligence community enablers helping to scope the situation for DOD and government leaders.

ON-SITE HUNT

6-20. On-site hunt is the most time-consuming method used by defensive cyber forces, but may permit the most detailed information collection about the threat, terrain, user base, and supported functionality. The commander considers using on-site hunt when—

- Adequate data does not exist in existing sensor platform or big data storage and time requires immediate data collection and forgoing reengineering the existing sensor infrastructure.
- Threat control of the area of operations is suspected to be such that existing sensor data is likely manipulated or sabotaged.

- The analytic scheme of maneuver requires data that can only be collected by emplacing sensors directly on-site.
- The area of operations is a closed-restricted network, such as an industrial control system network, where remote data acquisition would require breaking an air gap.
- Network infrastructure supporting the route to the area of operations is so unstable or contested that any remote sensor connectivity is likely to consistently degraded or denied.
- The area of operations is not a part of the unified network.

6-21. On-site hunt is a form of hunt that focuses on obtaining detailed network and host information about terrain or threat activity by deploying analysts to the data, often employing additional defensive cyber force sensors to collect analytic scheme of maneuver-required data sets. On-site hunt allows for detailed hunt in specific locations that answers priority intelligence requirements and develops the situation to provide the commander options. The commander assigns an on-site hunt when there are no available means of acquiring data for remote analysis, or when the threat situation is limited and direct coordination with local defensive cyber forces may be required to provide more detailed information than can be acquired remotely. In most instances, on-site hunt is used as an initial phase pending coordination for and implementation of remote reconnaissance.

6-22. The primary tasks associated with an on-site hunt are—

- Establish and occupy sensor positions for data collection.
- Coordinate for local sensor tuning and network defense configuration.
- Execute the analytic scheme of maneuver and report hunt information.

6-23. Other tasks include—

- Pursue remote hunt capability over a defensive cyberspace operations mission network.
- Characterize network avenues of approach and associated access controls.
- Seek to develop engagement areas based on the threat doctrinal template in preparation for contact.
- Report misconfigurations and bypassed anomalous or threat activity to local network defenders for remediation.

HYBRID HUNT

6-24. Hybrid hunt is a combination of both remote and on-site hunt. It is the most common form of hunt as data sets mature and normalize in remote analysis platforms. The commander considers using hybrid hunt when—

- Early, remote analysis identifies a need for on-site data collection.
- Some data required by the analytic scheme of maneuver is available in enterprise big data platforms, but more granular data is required and only available by collecting on-site.
- An on-site hunt element successfully establishes remote connectivity or data streams to big data platforms allowing other elements to support analytic scheme of maneuver remotely.
- A higher headquarters commander has directed the use of an on-site hunt as a show of force.

6-25. In hybrid hunt, defensive cyber force commanders must ensure analytic support officers and leaders understand who executes assigned analysis according to the analytic scheme of maneuver, since defensive cyber forces working the same analytic scheme of maneuver may not be co-located or in regular communication via secure communications. Tasks and planning considerations are a combination of those required for executing remote and on-site hunt missions.

HUNT MANAGEMENT

6-26. The defensive cyber force unit commander and staffs manage assets by cueing, mixing and validating hunt information. Hunt management allows the unit to collect the most critical information with multiple perspectives at the appropriate time. The S-3 manages and synchronizes all assets in support of defensive cyber force analytic and element execution. Cueing, mixing, and validating are used to maximize hunt efforts and allow primary focus on hunt objectives likely to yield the threat's disposition.

- **Cueing** is the integration of one or more types of hunt systems to provide information that directs follow-on collecting of more detailed information by another system. These systems may signal

other defensive cyber force or security assets to investigate specific areas to confirm, deny, or verify information.

- **Mixing** is using two or more different assets to collect against the same data requirement. Employing different systems is always desirable if the situation and available resources permit. This method increases the probability of collection and tends to provide information that is more complete. Mixing can help defeat deception attempts by highlighting discrepancies in information reported by different collection assets.
- **Validating** is using an additional hunt element to verify hunt findings and objectively review the analytic scheme of maneuver outcome to confirm conclusions. Validating reduces the likelihood of false positives, however it may slow analytic scheme of maneuver progress or consume combat power from the commander's available forces.

6-27. The defensive cyber force commander task-organizes with additional assets from within or outside the defensive cyber force unit to increase the effectiveness of a defensive cyber force asset. For example, the defensive cyber force task-organizes a hunt element with the cyber threat emulation cell or additional data engineers to validate sensor placement, ingest, and defensive measures in established engagement areas.

HUNT ASSETS AND SYSTEMS

6-28. Although the defensive cyber force hunt element directly executing the analytic scheme of maneuver is the commander’s most tactical asset, the commander maximizes use of all analysis and collection assets to assess the threat and the effects of the terrain on threat and friendly forces. Besides knowing the capabilities and limitations of these systems, commanders and staffs must understand all systems are susceptible to downtime, misconfiguration, and threat countermeasures.

6-29. Sensors, enterprise data platforms, and signals intelligence assets and systems integrate into the hunt data collection effort through cueing, mixing, and validating. These assets provide the commander's most critical information with the fewest assets at the appropriate time.

SENSORS

6-30. Deployable defensive cyberspace operations systems, whether modular, garrison based, or part of cybersecurity service provider or Defense Information Systems Agency enterprise sensors allow flexibility in economizing hunt assets. Since hunting threats often is aided by distilling an event timeline from threat activity by going back in time, often, the sensors with the best historical record of past activity are most useful in terms of executing the analytic scheme of maneuver.

6-31. Defensive cyber force commanders use their organic sensors to observe areas without adequate coverage, or when local sensors are likely to be compromised. Sensors afford the defensive cyber force element a means to collect data as part of the analytic scheme of maneuver over time, increasing the likelihood of detecting threats spanning multiple phases of the ATT&CK® matrix. The commander considers sensor hunt to expand the scope of coverage as required, conduct missions of extended duration, often remotely, or while local defenders tune or acquire their own sensors to sustain suitable observation.

ENTERPRISE DATA PLATFORMS

6-32. Enterprise level data and big data platforms afford defensive cyber force commanders an ability to hunt widescale areas without emplacing their limited deployable sensors. Big data platforms consolidate data feeds and metadata from the Defense Information Systems Agency, cybersecurity service providers, and other organizations and assets allowing for a more holistic and expedient way to hunt across vast portions of the DODIN.

6-33. The preferred form of hunting is often conducted by leveraging existing data in big data platforms, while developing and executing innovative analytics to detect novel threat tactics, techniques, and procedures. Combined with a robust open-source intelligence threat feed and vulnerability disclosures, defensive cyber force elements often are most effective at hunt and security tasks by working within the existing big data platform and unified platform data sets.

6-34. Hunting through the big data platform is most effective across large areas of operation. Cued by intelligence information, analytic support cells and defensive cyber force elements provide excellent hunt capabilities. Big data platforms enable analytic support cells to—

- Identify threat activity earlier in their campaign to minimize their dwell time and disrupt their operation.
- Assist other defensive cyber force elements in characterizing a large area prior to their employment within a smaller, nested area of operations.
- Locate and help determine threat forces, disposition, and activity.
- Maintain contact with threat forces through observation.
- Provide threat information with enough accuracy to enable immediate target handover to offensive cyber forces for counterattack and local defenders for clearing operations.
- Provide or enhance existing enterprise analytics.
- Provide information to employed defensive cyber force elements, increasing their ASOM effectiveness.
- Reduce or eliminate the necessity of on-site hunt efforts, preserving flexibility and combat power in anticipation of decision operations.
- Support mission duration beyond those of manned, on-site systems.
- Provide digital connectivity and sharing of analytics and data that enables rapid dissemination, collaboration, and reporting.

6-35. While big data platforms offer increased data visibility for effective hunt operations, they require contact with local defenders and cybersecurity service providers to deliver disruptive effects to threat activity. Remote, enterprise defensive capabilities exist, but are currently not integrated or controlled by defensive cyber hunt forces.

SIGNALS INTELLIGENCE

6-36. Defensive cyber forces use information developed by the signals intelligence systems that are organic or task-organized to the defensive cyber force. Signals intelligence systems can monitor or scan for activities that help to cue defensive cyber forces before or during missions.

6-37. Defensive cyber forces use commercially available data sets containing a collection of trends across the globe to inform technological information gaps. As new tactics, techniques, procedures, and capabilities are observed around the world, defensive cyber forces can evolve their hunt planning and threat detection techniques.

FORMS OF HUNT

6-38. Defensive cyber forces conduct two types of hunt that are analogous to forms of reconnaissance—zone reconnaissance and area reconnaissance. *Zone reconnaissance* is a form of reconnaissance operation that involves a directed effort to obtain detailed information on all routes, obstacles, terrain, and enemy forces within a zone defined by boundaries (FM 3-90). *Area reconnaissance* is a form of reconnaissance operation that focuses on obtaining detailed information about the terrain or enemy activity within a prescribed area (FM 3-90).

ZONE HUNT

6-39. Commanders assign a zone hunt when the threat situation is vague or when information related to terrain, infrastructure, or friendly disposition is limited. Commanders use zone hunt to refine their understanding at scale when specific information about a technology, indicator, or vulnerability is required to refine course of action development. Zone hunt can be defined by physical or logical boundaries or by technology.

6-40. The level of detail required during a zone hunt makes these operations a deliberate and time-consuming process. The commander must work to balance available time with critical collection requirements to ensure that they provide the necessary information for their higher commander. To do this, commanders deliberately focus collection requirements and adjust the hunt techniques to increase the overall tempo. However, as speed increases so does the associated risk to zone hunt and follow-on operations. Commanders may task-organize

the hunt force to mitigate risks associated with an increased operating tempo and provide defensive cyber force organizations an increased ability to develop the situation through action in close contact with the threat.

Tasks

6-41. A zone hunt may be executed either on-site or remotely and often starts remotely during mission analysis, based on initial hunt guidance. Based on the time available and the commander's intent, the commander may direct the hunt towards specific information requirements only. The commander should provide hunt focus in the commander's intent paragraph and list the tasks in the specific instructions. The primary tasks associated with a zone hunt are—

- Find and report threat activity within the zone, according to bypass and engagement criteria.
- Find and report all occurrences of a specific technology or indicator within a zone.
- Reconnoiter specific terrain within the zone.
- Report hunt information.

6-42. Other zone hunt tasks include—

- Reconnoiter all the terrain within the zone.
- Verify organic network sensors and data sets, recommending modification to improve local defender visibility.
- Characterize and validate host and network log collection and normalization to improve future hunt.

Planning Considerations

6-43. The planning considerations for a zone hunt include the defensive cyber force's intelligence preparation of the operational environment that supports the determination of speed, element size, and hunt method. Depending on the size or scope of the zone, the commander decides the appropriate element size required to reconnoiter the objective. The larger the hunt zone, associated data sets, or technology proclivity, the more important a detailed and well-rehearsed analytic scheme of maneuver to ensure analytic forces focus on priority intelligence requirements and can reduce extraneous analysis.

6-44. An essential part of zone hunt is understanding and characterizing the threat avenues of approach. Despite initial diagrams of the cyberspace terrain, defensive cyber forces must ensure they are aware of other potential avenues of approach that may enable threat forces to subvert established means of observation and detection.

6-45. The size and scope of a zone hunt require constant reporting and refinement of data and terrain characterization, which should lead to continuous refinement of the analytic scheme of maneuver. As hunt elements locate new information of value, they report their findings through analytic support officer channels to ensure the analytic scheme of maneuver remains current, improving the defensive cyber force element's chances of identifying threat activity.

6-46. Zone hunt often increases the liaison requirements of the defensive cyber force headquarters, as multiple network owners, mission owners, and user groups may be responsible for the network and data within the prescribed area. During mission analysis, commanders and staffs should initiate coordination with the zone's local security and defense forces to ensure defensive cyber force requirements, actions, and scheme of maneuver are deconflicted and clear lines of communication established.

AREA HUNT

6-47. An area hunt can obtain, verify, confirm, or deny extremely specific information for the commander. The commander assigns an area hunt either as a discrete mission or as a specified task. Area hunt missions provide commanders detailed information about very specific terrain or data to prevent surprise, determine risk posed by a threat, and to confirm or deny staff estimates and assumptions made during the operations process.

Tasks

6-48. Certain tasks are required during an area hunt, unless otherwise directed by the commander. These tasks are not a checklist or arranged sequentially, as some may not be necessary for mission accomplishment.

When time is limited, the commander directs hunt only toward specific information requirements. The tasks associated with area hunt are—

- Find, report, and—based on engagement criteria—disrupt threat capabilities that can influence the point of the hunt.
- Reconnoiter and determine the avenues of approach to the point.
- Reconnoiter all terrain the threat can use to affect the point.
- Identify lateral movement to and from the point.
- Identify threat command and control from the point along their lines of communication.
- Identify forms of threat persistence within the point, or undefended areas that could afford the threat to reconstitute rapidly within the point of hunt.

Planning Considerations

6-49. The planning considerations for area hunt are similar to those for zone hunt, with some unique considerations. When a defensive cyber force element conducts an area hunt of a single point or data set, an additional defensive cyber force element may operate adjacently by reconnoitering a zone or boundary that may include terrain that dominates or influences the area hunt. The commander initially determines areas of high risk and the nature of potential threat in deciding how much area (or data) around the area to reconnoiter. The defensive cyber battalion then determines the task-organization and command relationships of any combined arms attachments based on intelligence preparation of the operational environment and mission analysis.

6-50. When a defensive cyber force element conducts an area hunt of multiple discrete points in a noncontiguous battlespace where threat contact is likely, additional elements may prepare to serve as follow-on forces if the element locates an entrenched and determined threat. Close collaboration between cyber and signal elements often allows a faster and more complete hunt operation. The defensive cyber force element uses the analytic scheme of maneuver to direct and control sub-elements' analysis and complete the hunt. Upon completion of the analytic scheme of maneuver and required reporting, defensive cyber force elements should prepare to broaden their hunt or execute a hunt handover.

GENERAL HUNT PLANNING AND EXECUTION CONSIDERATIONS

6-51. The commander integrates cyber, signal, and other technical assets to enable either a faster or more detailed hunt. The commander orders remote zone hunt when the mission needs to be completed quickly. When time is limited, remote area hunt is essential to determine which areas contain threat activity and to cue on-site or area hunt operations.

6-52. The commander establishes the priority of analytics and bypass and engagement criteria to ensure disciplined execution of the analytic scheme of maneuver. Preapproved actions and defensive (engagement) actions should be planned and coordinated with local defense forces to ensure defensive cyber forces are well-aware of intent and potential effects of actions.

6-53. If the commander requires detailed information beyond the capacity of the assigned defensive cyber force element, forensics and malware analysis may be coordinated to deliberately assess critical points or data faster than the defensive cyber force element. If the unit commander anticipates the requirement for forensics and malware analysis, forensics and malware analysis or cyber threat emulation assets must be task-organized to the battalion.

FOCUS

6-54. Hunt focus—derived from the commander's intent and defined by specific hunt objectives—allows subordinate defensive cyber force organizations and commanders to prioritize tasks to accomplish, and the assets used to accomplish them. Hunt focus defines the defensive cyber force organization's area of emphasis and consists of—

- Threat.
- Available sensor data.
- Terrain effects.
- Host activity.

6-55. The higher echelon commander's intent and the commander's initial assessment of information requirements and information gaps serves as the basis for establishing hunt focus. Focus helps the defensive cyber force organization narrow the scope of operations to get the most important information to develop the situation for future operations.

6-56. Commanders and staffs can further focus hunt efforts by assigning specific hunt objectives. A hunt objective the most important result desired from that specific hunt effort. The objective should directly support the commander's desired end state.

6-57. For example, the defensive cyber force could address information gaps concerning terrain—collecting information on terrain features and avenues of approach that might affect friendly forces, the threat's disposition, and the various courses of action the defensive cyber force commander might develop during their planning. The information developed by terrain- or threat-focused hunt helps update templated threat courses of action as part of the continuous intelligence preparation of the operational environment assessment.

6-58. Additionally, a hunt objective may include gaining an awareness of how the local user base affects military operations and the impact of cyberspace operations on those users. Defensive cyber force organizations may conduct hunt to gather information on the size, location, composition, and life patterns of the local user base. Such hunt focuses on developing an understanding of the human factors that affect friendly populations, such as work hours, software used, login methods, or remote workforce. Furthermore, defensive cyber force hunt of the local network seeks to determine what native capabilities exist to enable hunt operations. Regardless of its focus on terrain, the threat, capabilities, or local user considerations, the hunt objective clarifies the intent of the hunt effort by stating the most important result of the hunt effort.

TEMPO

6-59. Tempo of hunt refers to the level of detail and covertness required of the defensive cyber force organization to best accomplish hunt or security tasks. Tempo is described as rapid, deliberate, stealthy, or forceful. Rapid and deliberate indicate levels of detail and are mutually exclusive in all cases; a hunt cannot be both rapid and deliberate. However, defensive cyber force organizations can vary between rapid and deliberate from phase to phase or even within sub-phases of an operation. Stealthy and forceful tempos indicate mutually exclusive levels of covertness (see figure 6-2 on page 69). Commanders choose the appropriate hunt tempo to accomplish the mission based on the mission variables of METT-TC (I).

- **Rapid tempo** dictates that the level of detail for the hunt operation is limited to a certain prescribed list of tasks or priority intelligence requirements. Rapid tempo is appropriate when time is of the essence and only a limited number of information requirements are necessary to accomplish the mission.
- **Deliberate tempo** implies all tasks of the mission must be accomplished to ensure mission success. Deliberate tempo allows the organization more time to answer all information requirements. Detailed and thorough hunt and security tasks require time-intensive, comprehensive, and meticulous data acquisition and analysis efforts to observe hunt objectives and develop the situation.
- **Stealthy tempo** emphasizes avoiding detection and prioritizing operations security when a threat is suspected. Stealthy hunt typically takes more time than aggressive hunt and utilizes passive sensor collection to take maximum advantage of cover and concealment to reduce signatures that lead to friendly compromise. Stealthy hunt is used when time is available, detailed hunt and stealth are required, or threat forces are likely in a specific area.
- **Forceful tempo** develops the situation through action by employing active and passive hunt methods, technical means, and aggressively fighting for data sets to rapidly develop the situation. Forceful hunt often requires elevated credentials on local terrain, or close coordination with network owners, aggressive exploitation of action on contact, operations security, and training to accomplish the mission. Forceful hunt is appropriate when time is limited, detailed hunt is not required, and terrain is easily observed by existing sensors.

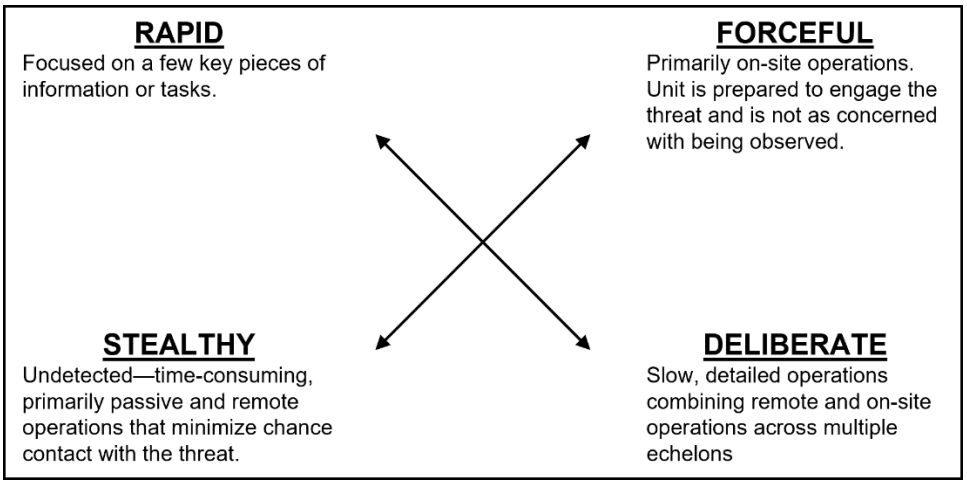


Figure 6-2. Hunt tempo

ENGAGEMENT AND BYPASS CRITERIA

6-60. Engagement criteria specify those circumstances for initiating engagement with a threat force. They can be either restrictive or permissive. The defensive cyber force battalion commander visualizes engagement criteria through analysis of the mission variables of METT-TC (I).

6-61. The commander must define the size or type of threat force he expects their subordinate units to engage or avoid which drives planning for direct and indirect fires, as well as establishment of bypass criteria. The defensive cyber force commander must consider intelligence gain loss and communication with network and system owners when engaging with effects that may have cascading impact across the network.

6-62. Merely defining engagement criteria using terms such as ‘aggressive’ or ‘discreet’ is not sufficient. Engagement criteria should be defined using precise doctrinal terms. The defensive cyber force commander issues specific planning guidance to clearly define the engagement criteria. The staff and subordinate commanders refine that guidance into specific execution information. Examples include—

- Engagement criteria.
- Guidance for actions on contact.
- Bypass criteria.
- Hunt handover criteria.
- Priority of analytics.
- Rules of engagement, if applicable.
- Analytic coordination measures.
- Endpoint detection and response agent control status.

DISPLACEMENT CRITERIA

6-63. Displacement criteria define triggers for planned withdrawal, passage of lines, or hunt handover between units. As with engagement and bypass criteria, the conditions and parameters set out in displacement criteria integrate the commander’s intent with tactical feasibility. Conditions are either event driven (for example, associated priority intelligence requirements being met, threat contact not expected in the area, or observed named areas of interest or avenues of approach denied to the threat); time driven (for example, latest time information of value triggers are met); or threat driven (observation posts or defensive cyber force sensors have been compromised). Failure to specifically dictate conditions of displacement, nested within the higher scheme of maneuver, will likely result in ineffective hunt operations. Figure 6-3 on page 70 shows an example of a commander’s hunt guidance.

Phase #: Control Mission Thread Terrain
Focus: Focus for phase # reconnaissance is on traffic within defined key terrain in cyberspace and in and out of mission thread terrain.

Tempo: Cyber protection forces should deliberately, yet stealthily develop their understanding of the mission thread terrain and how each subnet interacts in order to establish tailored, effective control of the mission thread terrain.

Engagement Criteria: All malicious cyber activities will be reported to 2d Cyber Battalion to be adjudicated by the analytic support cell and the commander. Cyber protection forces should prepare to engage malicious cyber activity within the mission thread terrain or terrain that poses risk to mission thread terrain functionality (including availability). If engagement is ordered, it should be aggressively executed to prevent threats from reconstituting in the cleared area.

Disengagement Criteria: Cyber protection forces will disengage when malicious cyber activity is cleared from mission thread terrain and continue to develop engagement areas and obstacles to control the mission thread terrain.

Displacement Criteria: Cyber protection forces will not displace from key terrain in cyberspace until control of mission thread terrain is achieved and transition to phase #.

Bypass Criteria: All malicious cyber activity outside the mission thread terrain should be reported and kept under observation, but bypassed until key terrain in cyberspace is controlled or until told to initiate clearing operations by the 2d Cyber Battalion tactical operations center.

Figure 6-3. Example hunt guidance with engagement, disengagement, displacement, and bypass criteria

HUNT HANDOVER

6-64. Hunt handover occurs between two elements to coordinate the transfer of information and responsibility for observation of potential threat contact, or the transfer of an assigned area from one hunt element to another. Hunt handover occurs between defensive cyber force elements, cybersecurity service providers, local defenders, and responsible network owners.

6-65. Hunt operations require the unit conducting the handover to coordinate with higher, lower, and adjacent units. Planning for these operations requires the hunt handover coordination to start at the higher echelons and execute at the lower element. Hunt handover ensures information requirements are transferred between units to maintain initiative and tempo, and to ease transitions. Well-planned and executed hunt handover eases transitions in plans, phases, and priorities of effort and mitigates information gaps between units.

6-66. Planning for hunt handover takes place as a part of a change of mission before or during operations. When planning an operation, commanders review the completed plan for layered, redundant hunt using all available assets. Commanders and staff use the analytic scheme of maneuver as a control measure to describe iterative analysis efforts or potential coordination points to facilitate shared understanding of terrain and the analytic scheme of maneuver. A hunt handover point is a designated point in time, space, or operational objectives where hunt responsibility transitions from one element to another and includes a shared understanding of continued iteration of the approved analytic scheme of maneuver until completion of the mission.

6-67. Hunt handover is typically associated with a trigger, coordination point, or time in phase designated as the hunt handover point to ensure positive control and chain of custody from the initial force to a force assuming responsibility and control. Hunt handover prevents gaps or seams from emerging that the threat can exploit. Once handover is complete, the force transferring control may maintain access or remote overwatch in preparation for having to rapidly reinforce the assuming unit or resume the analytic scheme of maneuver as part of a future hunt phase.

6-68. Hunt handover involves transferring documentation and technical observation in varying combinations. Assets such as network sensors and log data may transfer. Hunt handover is similar to battle handover in that its conduct is in conjunction with other tasks such as relief in place, linkup, and sensor retrograde.

6-69. Leaders and planners at all levels coordinate and execute hunt tasks, considering—

- Redundant observation mechanisms to assist in maintaining threat contact.
- Time, location, and criteria for hunt handover.
- A communications plan between handover elements.
- Exchanging the analytic scheme of maneuver and defensive control plan.
- Exchanging intelligence information.
- Contact points and reporting channels.
- Co-locating command posts.
- Transfer and acceptance of command between units.
- Rehearsals.
- Sensor and data transfer and recovery.

This page intentionally left blank.

Chapter 7
Security

Security operations are operations undertaken by a commander to provide early and accurate warning of threat operations, to provide the force being protected with time and maneuver space within which to react to the threat, and to develop the situation to allow the commander to effectively use the protected force. Security is inherent in all operations and is always the first task in the priority of work. Continual hunt and the development of information requirements are the means to provide security.

SECURITY OPERATIONS

7-1. The main difference between security operations and hunt operations is that security operations orient on the protected force or facility, while hunt is threat and terrain oriented. However, security operations cannot be divorced from hunt missions as one of the fundamentals of security is to perform continuous hunt.

7-2. Security operations prevent threat hunt assets from determining friendly locations, strengths, and weaknesses. A review of history repeatedly demonstrates that to preserve the striking power of an organization and preclude unnecessary attrition or premature culmination, each tactical echelon requires a specially-trained organization capable of executing security missions to preserve freedom of action for the main force.

7-3. Security operations ensure early and accurate warning of threat activity and provide reaction time and maneuver space to develop the situation and determine the most effective use of capability to neutralize or defeat threat forces. Each form provides varying levels of protection to the main network. The commander selects the appropriate type of security operation by weighing the operational variables (PMESII-PT) and the mission variables of METT-TC (I) and the desired end state.

PURPOSE

7-4. Security operations provide information about the threat and terrain and preserve the combat power of friendly forces. Security operations provide information about the size, composition, location, and likely intent of threat forces. Reaction time and maneuver space gained by information collected allows the supported mission commander to respond to disrupt or engage the threat. Security prevents the larger network from surprise by the threat, which allows the commander to preserve the capability and function the network provides and enable friendly freedom of maneuver in cyberspace.

7-5. Security along a common boundary with another friendly unit is the responsibility of the unit assigned to that zone or sector. Liaison with the protected network is critical during security missions. Constant communication and liaison ensure both security force and protected force remain informed of the full situation and maintains synchronized operations.

FUNDAMENTALS OF SECURITY

7-6. The fundamentals of security, like the fundamentals of hunt, provide a framework for security operations. Hunt operations, because they are continuous throughout all operations to develop the situation through information collection, are essential to successful security operations. The fundamentals of hunt are applicable to security operations and are necessary to ensure successful execution. The following fundamentals guide defensive cyber force security tasks.

Provide Early and Accurate Warning

7-7. The defensive cyber force or protecting unit detects, orients upon, and observes threat activity that can influence the DODIN or other defended network. Early detection and warning through rapid reporting enables the defensive cyber force commander to make timely and well-informed decisions for the proper application of their forces on the observed threat.

Provide Reaction Time and Maneuver Space

7-8. As with provide early and accurate warning, the ability for the defensive cyber force battalion to gain and maintain contact and report accurately and rapidly affords the supported network owner the time and space to make an informed decision to employ additional defensive forces. Reaction time and maneuver space relate to decision points driven by information requirements and indicators given the latest time information is of value to enable the commander to make decisions that place maximum defensive controls and capability at the decisive point in a timely manner.

Orient on the Protected Force, Network, of Terrain

7-9. While hunt operations orient on the hunt objective, security operations focus on the protected network by understanding their critical mission and function. By understanding the protected network's mission and function, the defensive cyber force element can best provide reaction time to prevent disruption of protected capabilities.

Perform Continuous Hunt

7-10. Defensive cyber force battalions continuously seek the threat and reconnoiter mission-relevant cyber terrain. Through continuous hunt, forces continue to gain and maintain threat contact, develop the situation, report rapidly and accurately, and retain freedom of maneuver to provide early and accurate warning and provide reaction time to the protected network owner.

Maintain Threat Contact

7-11. Accurate, real-time information requires defensive cyber force elements to gain and maintain contact with the threat to rapidly report their activity and provide reaction time and options. Like the hunt fundamental of gain and maintain threat contact, maintaining threat contact through one or more of the forms of contact enables the staff to make recommendations to the commander, generate options, identify opportunities, and seize, retain, and exploit the initiative.

COMMANDER'S SECURITY GUIDANCE

7-12. The defensive cyber force commander's guidance should consist of the security focus, duration, engagement and disengagement criteria. In providing this guidance, the commander describes, shapes, and prioritizes how he envisions the security effort supporting the overall scheme of maneuver and the specific roles of the defensive cyber force unit. As with the commander's hunt guidance, this guidance, and the importance of accomplishing the mission, must be understood at echelon.

Security Objective

7-13. The commander provides focus to the protecting force's efforts to best accomplish the mission. As an example, the security objective may constitute—

- Locating and defeating threat hunt activity.
- Confirming or denying the commander and staff's initial assessment.
- Providing early warning and reaction time to the protected network.
- Protecting a critical capability from threat disruption and engagement.

7-14. The security objective clarifies and prioritizes the tasks for the defensive cyber force unit nested within the defensive plan of the protected commander and network.

Defensive Cyber Force Focus

7-15. The focus of security tasks defines what to defend and why. In other words, the focus describes the expected result of the security operation. Security tasks orient on the threat, terrain, or friendly mission. Examples of focus in security tasks include threat terrain (key terrain, routes, and avenues of approach; network choke points; defensible terrain), the friendly mission or capability (the defended mission thread), and local user population.

7-16. Defining the focus of security tasks allows the commander to determine specific critical tasks, their priority, and their relation to the commander's intent and desired end state. Focus allows subordinate commanders to narrow their operations to acquire the information most important to their higher headquarters and defend the most critical activities.

7-17. Named areas of interest provide a graphical method to label data sets and focus defensive cyber force organizations as they execute security tasks. Significantly named areas of interest link the most likely and most dangerous threat activities to data where those activities may be observable. Given the named areas of interest, subordinate commanders can prioritize the deployment and employment of their forces and assets to provide the most effective observation and coverage throughout the area of operations as they develop their analytic scheme of maneuver and observation plans.

Tempo of Security

7-18. Clearly articulating the tempo of security tasks allows the commander to establish associated time requirements that will drive security tasks planning such as the method of establishing observation (sensors), data rollover thresholds, and required logistical and communications support needed to execute the mission. Tempo can also relate to depth, especially in screen missions, as time is needed to properly ensure data from multiple screen lines are accessible to achieve the required depth throughout the area of operations. When articulating the security tempo, commanders consider—

- Tasks.
- Commander's critical information requirements.
- The latest time information is of value.
- Tactical risk.
- Data analytic techniques.
- Hunt methods (stealthy or forceful, onsite or remote, or appropriate combinations of both).
- Defensive cyber force elements.

Duration of Observation Points

7-19. Tempo affects whether defensive cyber force units will employ short- or long-duration observation points (sensors) in their security tasks.

Short Duration

7-20. Defensive cyber force organizations employ short duration observation points for periods less than 30 days. Defensive cyber force units use short duration observation points to answer commander's critical information requirements when on-hand or available data sets cannot provide necessary visibility. They may also employ short-duration observation points when organic data observation capabilities in an area of operations may be suspect or compromised. In parallel, defensive cyber force units should pursue longer-term solutions for network and host data collection through more enduring security information and event management and data storage solutions.

Long Duration

7-21. Defensive cyber force organizations employ long-duration observation points for periods greater than 30-days. Long-duration observation points significantly impact the defensive cyber force commanders' flexibility and ability to displace or retrograde, as local defense forces become comfortable with defensive cyber force support and expertise. Historical analysis shows tactical network sensors begin to degrade when used for more than 90 days in-system. Long-duration observation points degrade combat power by requiring units to manage deliberate rotation schedules, rest plans, and adequate resupply for extended periods of time.

Engagement and Bypass Criteria for Security Operations

7-22. Just as the commander issues guidance concerning engagement and displacement criteria in their hunt guidance, the same criteria apply to security tasks. When assigning a security mission and employing a security force, commanders should consider—

- Mission or network enclave to secure and defend.
- Physical and logical location and disposition of the security area
- Initial location and organic types of observation points and sensors, if applicable.
- Time allocated to establish the security operation.
- Criteria for transitioning from the security operation to defensive cyber force decisive operations.
- Task organization and augmentation of security forces.
- Reporting requirements.
- Threat considerations—
  - Bypass criteria.
  - Engagement criteria.
  - Threat capability to influence friendly mission activities.

COUNTERRECONNAISSANCE

7-23. *Counterreconnaissance* is a tactical mission task that encompasses all measures taken by a unit to counter enemy reconnaissance and surveillance efforts. (FM 3-90). The purpose of counterreconnaissance is to disrupt, defeat, or repel all threat reconnaissance efforts with capabilities and following engagement criteria. It denies the threat the ability to conduct reconnaissance and develop their situational understanding. Successfully countering threat reconnaissance is the first and probably most important step in ensuring the DODIN enables friendly operations.

7-24. Counterreconnaissance is active and passive and includes action to disrupt or repel threat reconnaissance activities from gaining persistence in friendly terrain or obtaining information of value from friendly forces. Units organize to disrupt threat reconnaissance without requiring reinforcement. Commanders consider threat reconnaissance capabilities to determine whether additional defensive cyber force maneuver elements are required.

7-25. Counterreconnaissance elements must be task-organized to accomplish their mission against the threat. Whatever option the commander employs, the counterreconnaissance fight should be firmly controlled, monitored at the higher headquarters level, coordinated early, and deliberately rehearsed. Effective counterreconnaissance blunts the threat information collection efforts, forcing the threat to act without accurate information on the friendly network. Effective counterreconnaissance imposes costs on threat forces, delaying their campaign and impacting their decision making.

TYPES OF SECURITY OPERATION

7-26. Leaders categorize security operations in terms of the degree of security provided and the amount of combat power required. There are five defined types of security operation—

- Screen.
- Guard.
- Cover.
- Area security.
- Local security.

7-27. The different types of security operation provide varying levels of protection to the protected force and are dependent upon the size of the unit conducting the security operation. All forms of security provide protection and early warning to the protected force, which, in turn, provides reaction time and maneuver space to the commander and preserves freedom of action.

7-28. Defensive cyber force organizations are organized and equipped to perform screen, guard, area security, and local security missions. They can also participate in cover operations as part of a larger element with external assets traditionally leading the effort and perform guard operations with signal or cybersecurity service provider augmentation.

Note. The nature of a cover mission in defensive cyberspace operations requires the ability to create effects in commercial or neutral cyberspace. This is outside the capabilities and legal authorities of DOD defensive cyberspace operations forces.

7-29. Security missions at echelons above brigade are carried out primarily by cybersecurity service providers and joint or DOD agencies.

SCREEN

7-30. *Screen* is a type of security operation that primarily provides early warning to the protected force (ADP 3-90). The primary purpose of a screen is to provide early warning to a supported network or mission. Screens provide less protection than guards or covers. Screen missions are defensive in nature and accomplished by establishing a series of observation points to ensure observation of the protected network terrain. The screen force gains and maintains threat contact consistent with the fundamentals and disrupts threat reconnaissance activity by conducting counterreconnaissance. The depth of the screen is critical to allow reconnaissance handover from one element to another without duplicity in observation points. Depth provides friendly forces the ability to conduct counterreconnaissance to delay, impede, and disrupt the threat activity to prevent them from identifying, penetrating, and exploiting the screen.

7-31. Screen missions are appropriate when intelligence as to the threat's capabilities and intent are not well understood, gaps exist between adjacent or nested networks, or when required to provide early warning over gaps not critical enough to require security in greater strength. The defensive cyber force commander maximizes security efforts where contact is expected.

General Description

7-32. Screens, even for a protected network, are active observations of which observation points and surveillance assets are only part of the overall mission. A screen may require employment of remote and on-site defensive cyber force elements, and sophisticated analytics employed over massive data sets and collection points in depth. Inactivity in a screen yields identifiable and exploitable gaps for the threat.

Commander's Guidance

7-33. The defensive cyber force commander provides purpose and guidance to the employed screening force. The commander states why the screen is important to the protected mission and network and how it fits into the defensive cyber force's scheme of maneuver.

Depth

7-34. Depth provides the defensive cyber force commander with more time to react to threat activity and allows for hunt handover from one element to another with minimal downtime. Depth prevents the threat from easily identifying and penetrating the screen, prevents gaps from occurring when observation points falter, and facilitates the disruption of threat reconnaissance elements without compromising critical observation points. Units employ depth by positioning observation points and other information collection assets between the network boundary and critical protected assets.

Width

7-35. The wider the area to secure, the less the security force can take advantage of increased depth, because it has fewer forces to position in depth. Once the defensive cyber force has determined the width and depth of the security area, the initial screen line and likely avenues of approach, the security force orients on the protected network, mission, or capability.

Note. When the term screen line is used, it describes the trace along which the protecting unit is providing security, not the logical or physical position of defensive cyber force assets.

Displacement

7-36. Displacement of the screen elements to subsequent observation points is event-driven. The approach of an identified and specified threat element, detection by a threat force, relief by a friendly unit, or a change in the disposition of the protected network may dictate displacement. Collapsing the screen, executed by well-rehearsed drills performed at all levels, provides security and maintains contact for the unit as it

displaces. The defensive cyber force commander can place a time requirement on the duration of the screen if the intent is to provide a higher level of security, or to provide a tentative period for subordinate unit planning and follow-on missions.

Critical Tasks

7-37. Execution considerations guide screen planning. Execution considerations for a screen include—

- Analytic effectiveness to identify and detect threat activity.
- Maintaining continuous surveillance of all avenues of approach that affect the protected network's mission.
- Conducting counterreconnaissance to disrupt all threat reconnaissance activity, within the capabilities and according to engagement criteria.
- Seeking to locate command and control mechanisms that indicate the threat's disposition, and persistence and phase of ATT&CK® campaign when facing an echeloned threat force.
- Determining the path of threat advance, maintain contact and report threat activities, even while displacing.
- Impeding and disrupting the threat within capabilities without becoming decisively engaged and while displacing to provide the protected for commander with additional time to respond.
- Detecting and reporting all threat activity attempting to pass through the screen to provide the protected network owner early warning of threat activities.

***Note*.** To enhance the effectiveness and depth of the screen, the squadron's subordinate elements conduct hunt handover or battle handover to pass contact from one element to another. In this way, the methods of hunt management (cueing, mixing, and redundancy) and task organization maintain threat contact and protect the main effort following the commander's intent.

Planning Considerations

7-38. When planning the screen, the defensive cyber force battalion, commander and staff consider the number of observation points and elements needed (depth, width, duration, and orientation of the screen), time needed to occupy the observation points and establish the screen, and the ability of defensive cyber forces to rapidly bring defensive control measures (effects) to bear to provide the level of security to the protected network or mission (often requiring coordination with cybersecurity service providers and network owners). The defensive cyber force commander and staff consider conditions to facilitate hunt handover or battle handover with follow-on forces, to include time required to conduct the handover along with time and observation needed for subordinate elements to displace to their next mission.

7-39. Defensive controls and observation points must be known and coordinated between defensive cyber force echelons to ensure that screening forces are able to observe data to inform the analytic scheme of maneuver and threat detection. As network owners at echelon shift and alter terrain and security controls, these actions should be coordinated with supporting screen forces to ensure data analytics remain relevant and appropriate to observed data. For example, the screen force is observing Domain Name System logs to identify likely threat command and control channels, and higher echelon network owner sinkholes known malicious Domain Name System queries, rendering the defensive cyber force analytic and observation point moot.

Stationary Screen

7-40. A defensive cyber force executing a stationary screen mission requires the following guidance:

- General trace of screen and time it should be established.
- Scope of the screened sector.
- Identification of the screened network, mission, or capability.
- Decision points for deploying on-site forces.
- Possible follow-on missions.

7-41. The tasks required of a screening unit are minimal compared to other security missions. Therefore, the screening force may have wide coverage. Units are normally deployed abreast, with subordinate units established in depth.

7-42. A phase line placed along identifiable network boundaries (logical terrain) indicate the forward line of observation of the screening unit. A boundary depicts the rear limit of the screen. The screening force is responsible for the area between the screened assets and the rear screen boundary. The boundary may serve as a battle handover line or a hunt handover line. Other phase lines are detailed in the analytic scheme of maneuver to coordinate reporting and orientation within the overall screen.

7-43. Given the higher commander's guidance (security objective, focus, duration, engagement criteria, and displacement criteria), commanders and staffs consider the following during planning:

- Logical location of initial screen.
- defensive cyber force occupation technique to achieve screen (remote / on-site).
- Assigned areas of operations and analytic schemes of maneuver for subordinate elements.
- Cyber and signal integration.
- Surveillance and observation assets.
- Defensive controls and preapproved actions.
- Command and control.
- Sustainment.
- Disposition of alternate and subsequent observation points.
- Hunt handover between screening elements.

Initial Screen

7-44. The defensive cyber force establishes the general location of the initial screen. With permission from the defensive cyber force commander, the screening element can adjust the initial screen to address changing mission variables. Time available and the threat situation determine the method of occupying the screen either remotely, on-site or hybrid. Remote area hunt is the preferred method to occupy a screen as it provides useful information and intelligence regarding the terrain and maximizes the opportunity to identify threat activities enroute to the screen line.

Areas of Operations for Subordinate Elements

7-45. The screening unit commander designates areas of operations for subordinate elements, including responsibility for named areas of interest and target areas of interest. Sensors and signals intelligence systems are positioned to provide additional depth. Reduced depth is a trade-off when screening extended frontages. Screening high-bandwidth avenues of approach may require adjusting defensive cyber force equipment and data storage capabilities. Screening plans should include hunt management (cueing, mixing, and validation) to maximize coverage and effectiveness.

7-46. National strategic assets, such as cyber national mission force elements may conduct hunt forward of friendly defensive cyber force elements to add depth and extend the capabilities of the blue space screen. These elements may make contact with threat elements before the screen line and provide supporting early warning to screening forces and protected assets.

7-47. When using their own organic surveillance and sensor assets, the screening unit develops a plan to provide early warning on the most likely avenues of approach. Nonorganic, higher assets (such as boundary sensors and big data platforms) provide an earlier indication of threat activity to cue unit assets.

7-48. Local security and defensive assets aid the screening unit when it is collapsing the screen or to assist in regaining contact with the threat if contact is lost. If the defensive cyber force screens extended frontage, these assets can operate in an economy of force role; conducting periodic surveillance on less likely areas the threat may use, maximizing defensive cyber force combat power along more likely avenues of approach.

7-49. Defensive measure planning includes the integration of established hardware, software and instrumentation to disrupt threat activity. The commander's intent drives the screen's purpose—to report, disrupt, delay, or deny specific threat actions. The staff plans observation and chokepoints along avenues of approach in areas where the threat movement may be restricted or severely restricted. Commanders designate

engagement areas to help focus defensive measures along likely avenues of approach where the measures have the greatest likelihood of achieving desired effects. It is critical the higher headquarters clearly identifies the command and or support relationship of the supporting cybersecurity service provider and local defenders available to the screening force.

7-50. Sensor operators (gunners) and data engineers provide engineering and maintenance support to ensure operational readiness of emplaced observation. Obstacles may be planned and prepared but are not emplaced until the commander's emplacement criteria are met. Generally, an endpoint detection and response agent or on-call firewall rule are used as obstacles because they can rapidly disrupt threat activity and be easily rolled back. In screening operations, situational obstacles disrupt and delay the threat to protect elements of the protected network.

Command and Control

7-51. Commanders and command posts are positioned to support mission command over disparate analytic schemes of maneuver and elements and to maintain robust communications and enabler integration. Defensive cyber force commanders place themselves in positions that maximize their ability to command their units and to gain and maintain situational awareness.

Sustainment

7-52. Defensive cyber forces prepare sustainment assets for operation in both time and space. Units reliant on their organic sensors may require priority for technical and data engineering support. This requirement should be determined early in the planning process to allow the supporting sustainment element to plan, coordinate, and posture assets and support to provide sustainment to the screening units.

Displacement

7-53. Besides phase lines, checkpoints control displacement. The screen's analytic scheme of maneuver, engagement, disengagement, and displacement criteria nested within the defensive cyber force plan defines the event or time criteria triggering displacement. Displacement of a screening unit is a decision point that marks a transition from security operations to offensive or defensive operations. The vignette on page 6-9 illustrates a successful defensive cyber force screen operation.

Screen Vignette

Following the successful disruption of a supply-chain attack that led to infected host systems across a vast portion of the DODIN, threat forces escalated hostilities against a partner nation. In response, U.S. and allied forces began preparing for conflict (an escalation from competition), during which the coalition forces land component commander identified deficiencies in a key command and control network. The network owner, the theater Army commander, requested defensive cyber forces to screen their network for threat activity to provide early warning to their local defense forces, while they worked to harden their posture and improve their security architecture.

The defensive cyber force assigned the screening mission began a remote area hunt immediately to characterize the assigned area of operations and begin to identify avenues of approach. Heightened concerns by senior leaders led to an element being tasked with an on-site network hunt operation, while a supporting element continued the remote area hunt during occupation of their screen line.

The on-site element immediately occupied the assigned terrain, establishing their organic sensor observation points and working with the local defenders to tune and improve their own perimeter and monitoring capabilities. The on-site defensive cyber force element worked with its higher headquarters and supported command to establish a remote connection from their forward sensors (in theater) back to the defensive cyber force's home station workspace.

At this point, the defensive cyber force commander declared the screen line had been established, using both available enterprise data, and remotely available and more granular data from the defensive cyber force's forward sensors. After holding the screen line while the network owner worked to improve the defensive posture of the network, a theater-based defensive cyber force was tasked to relieve the screening unit. Close coordination between the screening unit and inbound screening force executed a deliberate hunt handover between screening elements, leading to the retrograde continental United States-based defensive cyber force.

GUARD

7-54. *Guard* is a type of security operation done to protect the main body by fighting to gain time while preventing enemy ground observation of and direct fire against the main body (ADP 3-90). A guard differs from screen by the fact that the defensive cyber force must have control of the terrain and defensive measures to disrupt threat activity. This control in rare cases may be assumed by defensive cyber forces on undefended or in-duress networks. Most often, a guard is executed by task-organizing cybersecurity service providers and local defense forces to the defensive cyber force commander. Commanders assign guard missions when they expect contact or require greater, more responsive protection than a screen can provide. The guard force conducts hunt, defends, and delays as needed to provide reaction time and maneuver space to the protected asset.

7-55. A defensive cyber force battalion supported by a responsive cybersecurity service provider typically perform guard missions. A guard force operates within the range of protected assets. It accomplishes all the tasks of a screen, but it deploys over a narrower front to permit the concentration of analytic power, and rapidly employ defensive controls to disrupt identified threat activity.

7-56. Battalion-sized elements or higher generally conduct guard missions due to the protection and assets required, as well as the increased coordination and liaison requirements necessary to employ defensive effects while protecting sensitive assets.

7-57. Staffs consider augmenting the guard force based on the anticipated threat and tasks for the guard force. Depending on defensive cyber force specialization, the guard force has different capabilities than the assets or network it protects. Additionally, defensive cyber force commanders consider and plan for the integration of assets and enablers across warfighting functions.

7-58. The guard force also differs from a screen in that the guard force contains sufficient combat power to disrupt, deny, or fix threat elements before they can engage protected assets. A guard force is appropriate when contact is expected, when there are transitions that impart risk to network or mission, or when there is a requirement for greater protection than a screen can provide.

Tasks

7-59. Defensive cyber force elements conducting a guard perform certain tasks and staffs consider whether subordinate units conducting a guard mission require augmentation to execute their mission. Within their capabilities, the guard force disrupts threat activity before it can adversely affect protected assets or missions. Guard forces maintain surveillance of avenues of approach into the area of operations or protected asset. Cybersecurity service providers and local defenders assist the guard force by bringing their organic network management, control, and intrusion prevention capabilities to bear on identified threat activity.

Planning Considerations

7-60. Defensive cyber force commanders, or higher echelon commanders conducting a guard, may augment the guard force with internal and external assets. Commanders and staffs analyze requirements and notify the higher headquarters of tasks they will be unable to accomplish based on their ability to employ defensive measures. The protected mission commander then task-organizes support and augmentation or provides guidance on the prioritization of guard tasks.

COVER

7-61. Cover operations protect the network or mission from threat observation and effective threat massing of long-range capabilities (such as circuit denial of service). Defensive cyber force elements constrained to operate within blue space are unable to cover, however strategic national assets are possible of cover missions. Cover missions are currently not performed by Service defensive cyber force elements, because these elements lack the depth of observation, maneuverability in neutral cyberspace, and commercial partnerships to cover DODIN assets.

AREA SECURITY

7-62. *Area security* is a type of security operation conducted to protect friendly forces, lines of communications installation routes, and actions within a specific area (FM 3-90). Defensive cyber forces conduct area security to preserve the commander's freedom of maneuver in cyberspace, posture for response to threat contact, enable support unit command and control, and deny threats from holding friendly capabilities at risk. Area security degrades the threat's ability to affect friendly capabilities in a specific area by denying the threat's activity or access to an area for its own purposes. Area security is essential to all operations, particularly in competition, where threat forces maneuver to gain advantage over friendly cyberspace.

7-63. The commander may task subordinate units to conduct the following in support of area security operations:

- Area or point hunt.
- Screen.
- Defensive tasks (within capabilities).
- Security of high-value assets.

Execution Considerations

7-64. When conducting an area security mission, the security force prevents threat reconnaissance elements from disrupting friendly activities within the area being secured. Within capabilities, the security force prevents threat forces from penetrating the defensive perimeters.

7-65. The commander can have the subordinate element employ a variety of techniques such as observation points, battle positions, sensor grids, and remote overwatch to accomplish this security mission. A reserve or quick reaction force enables the commander to react to unforeseen contingencies.

7-66. The mission variables of METT-TC (I) dictate the required augmentation for the defensive cyber force element. Early warning of threat activity is paramount in area security missions and provides the commander with time and space to react to threats. Failure to conduct continuous hunt may create a vulnerable seam where the threat can execute an infiltration or attack.

7-67. A unit establishes a perimeter when it secures an area where the defense does not have a supporting defensive cyber unit. Perimeters vary in scope, security, and monitoring capability. A probable method of attack based on the threat most likely and most dangerous courses of action as determined in intelligence preparation of the operational environment may require the massing of combat power in that portion of the perimeter to disrupt an attack or infiltration.

7-68. When a perimeter is not feasible due to lack of proper network architecture, the defensive cyber force element secures the area by conducting hunt tasks throughout the area. Defensive cyber force elements may focus their security on critical data, network nodes, and other high-value assets, while requesting signal forces conduct operations to establish adequate perimeters and monitoring. The commander positions reaction forces to respond to threat activity as required, to enable the securing force to continue hunt of a poorly secured area.

High-Value Asset Considerations

7-69. High-value assets are those whose disruption by threat forces could decisively change the course of military operations. Security missions to protect high-value assets are an important component of the area security across the competition continuum. Examples of high-value assets to be secured in large-scale combat operations include—

- Command and control networks.
- Nuclear command and control infrastructure.
- Sustainment networks and nodes.
- Industrial complexes critical to war.

7-70. High-value assets to be secured in competition include—

- Likely threat avenues of approach to the DODIN that would enable infiltration.
- Modernization, research and development data and organizations.
- Gaps and seams between cybersecurity service providers.
- Industrial complexes critical to war.
- National strategic assets that provide the United States economic and military advantage in conflict.

7-71. Considerations the security force should address when it tasks subordinate elements to secure high-value assets include—

- Internet Protocol address range of high-value assets and dependencies.
- Avenues of approach within the network to high-value assets.
- Planned changes in location or disposition of assets (for instance, moving to cloud infrastructure).
- Duration of mission, and sensor and data sustainment considerations.
- Other friendly forces in the area, and their task and purpose.
- Triggers for change of mission from security to hunt or defensive action (for example, is there an implied reserve mission?).
- Ability of the security force to maintain communications with its higher headquarters.

LOCAL SECURITY

7-72. Local security includes local measures that prevent or interdicts threat efforts. Local security is an enduring priority of work, is essential to maintaining initiative, and prevents units from being surprised. Local security involves avoiding detection or deceiving the threat about friendly actions, positions, and intent. It includes protecting friendly defensive cyberspace infrastructure through active and passive means.

Continuous monitoring and hunt are active measures that help provide local security. Passive measures include—

- Obfuscating friendly sensor names and Internet Protocol addresses.
- Minimizing noise and actions that would tip the threat to defensive cyber force occupation of an area.
- Using operations security and secure communications.
- Working through local defenders' pattern of life when changing or improving security.

Chapter 8
Sustainment

This chapter discusses sustainment of defensive cyber force operations. It begins with a discussion of logistics, then discusses sustainment of hunt operations and sustainment planning.

LOGISTICS

8-1. Logistics consists of supply, field services, maintenance, transportation, operational contract support, general engineering support and distribution. Not all of these will apply in defensive cyberspace operations, due to the remote and garrison environment in which most operations take place, however, cyber professionals will be required to ensure proper logistics planning to seize, retain, and exploit the initiative.

8-2. Supply operations consider all classes of supply. For units conducting hunt tasks, supply may provide items to ensure proper analog tracking can take place, as well as coordinate for other classes when in a field type or forward-deployed (theater-of-war) environment.

8-3. Field maintenance is the level of maintenance that occurs in units conducting hunt tasks. *Field maintenance* is on system maintenance, repair and return to the user including maintenance actions performed by operators (FM 4-30). Field maintenance is accomplished by operators and technicians organic to the maneuver unit and by the next higher level of deployable defensive cyberspace operations system sensor support. Maintenance management is accomplished by the unit S-4 and company executive officers and may have to be executed due to the long duration of some hunt tasks.

8-4. Transportation for units conducting temporary duty (forward) hunt and security tasks is coordinated through unit resource managers and handled according to unit standard operating procedure. The S-4 should be prepared to coordinate for more unique transportation into theaters of war using military aircraft, if needed.

HUNT SUSTAINMENT

8-5. Hunt operations present unique challenges for analytic support and sustainment planners. Planners need to consider many factors as they develop their concepts of support. Challenges include the terrain and threat situation, friendly situation, type of hunt operation, level of covertness and duration of the operation. Planners consider positioning low-density assets based on decisive points and on-order requirements. Planners need to consider primary, alternate, and contingency means of analytic support and sustainment.

8-6. Over the course of a unit's execution of hunt operations, analytic repositories will become robust, and distribution should enable the initiation of most hunt tasks without a large burden on analytic support requirements. History has shown that as threat techniques and terrain change, emerging analytic requirements may be discovered during planning or mission execution.

8-7. The analytic support planning cell ensures integration of analytic support plans in the operations process. The analytic support planning cell consists of—

- Analytic support officer.
- Data engineer.
- Senior analysts.
- Master gunner.

8-8. The lead sustainment planner in the defensive cyber force battalion is the battalion S-4, assisted by the battalion cyber integration technicians, master gunner, mission element gunner, remote operations cell, and capabilities manager. Representatives from these elements form the sustainment and capabilities planning cell to ensure integrated hardware, software, and data stream sustainment plans in operational planning.

SUSTAINMENT PLANNING

8-9. Analytic support and defensive cyber force sustainment are integrated into all operational planning, with the concept of analytic support and other sustainment synchronized with other areas of the concept of operations. Planning is continuous and concurrent with ongoing support execution. Key support and sustainment personnel (such as the analytic support officer, S-4, cyber integration technician, master gunner, and capabilities manager) actively participate in the unit's planning process, to include course of action development and war-gaming. The goal is to ensure support during all phases of the operation.

8-10. The unit standard operating procedure is the basis for support and sustainment operations, with planning conducted to determine specific requirements and prepare for contingencies. Orders should address only specific support matters for the operation. The planning process addresses deviations from standard operating procedure sustainment planning early in the planning process. In some situations, sustainment and support planning begin before receipt of mission, as part of the ongoing process of refining the support and sustainment estimate.

8-11. To provide effective support, sustainment planners and operators understand the mission statement, commander's intent, and concept of operations. During the military decision-making process, the S-4 produces paragraph 4 (Sustainment) of the operation order, which includes—

- Commander's hunt priorities.
- Priority of analytic support by type and unit.
- Sustainment overlay.
- Supply routes (as required for on-site missions).
- Maintenance plan and collection points.
- Sensor, software license, and hardware resupply during mission, if necessary.
- To predict support requirements, sustainment planners determine—
- Type of support and sustainment required.
- Quantities of support required.
- Priority of support by type and unit.

8-12. After determining these support requirements, sustainment planner assess—

- Sustainment resources available (organic and supporting).
- Status of the sustainment resources (location, maintenance, and personnel status).
- Time sustainment resources are available to the unit.
- Configuration of resources and methods of distribution available.

8-13. Based on facts and assumptions, planners develop the support plans for the operation. The sustainment estimate is the formal, detailed process of analysis that supports sustainment planning and used when time is available. During execution, use a running estimate to support recommendations to the commander.

8-14. To enable rapid planning, information required to address many of these considerations should be readily available through routine reports. The S-4 should actively maintain an accurate picture of where defensive cyber force hardware and software are employed, their time in-system, maintenance status, and plan for refreshment based on priority of support. Supplemented by their actual operational experience, sustainment planners take advantage of—

- Running estimates, status charts, and estimate tools.
- Updated status reports when the commander issues a warning order.
- Established planning factors, historical data and data tailored for their unit.
- Procedures and organizations specified in the unit standard operating procedure.

ECHELONS ABOVE BATTALION SUSTAINMENT SUPPORT

8-15. Support for units conducting hunt missions may require sustainment from echelons above sustainment elements, particularly in maintenance and engineering support on their deployable defensive cyberspace operations systems. Echelons above battalion support is normally provided by a technical support element or contracted armory. In almost all circumstances, the completion of hunt tasks results in the need for updates and refresh of unit deployable defensive cyberspace operations systems, which may include exchanging expired equipment for new equipment through the defensive cyberspace operations armory.

Source Notes

This division lists sources by page number. Where material appears in a paragraph, it lists the page number followed by the paragraph number.

Page 11. Figure 2-1. *TTP-Based Hunting*, MITRE and Roman Daszczyszak et al., March 2019. This work is reproduced and distributed with the permission of the MITRE Corporation.

Page 12, Paragraph 2-4. Bianco, David J., *The Pyramid of Pain*, 17 January 2014, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

Page 12. Paragraph 2-5. *MITRE ATT&CK® Matrix*, MITRE Corporation. This work is reproduced and distributed with the permission of the MITRE Corporation.

Page 17. Figure 2-3. *TTP-Based Hunting*, MITRE and Roman Daszczyszak et al., March 2019. This work is reproduced and distributed with the permission of the MITRE Corporation.

Page 29. Paragraph 3-25. Bianco, David J., *The Pyramid of Pain*, 17 January 2014, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

Page 30. Paragraphs 3-26 and Figure 3-2. Bianco, David J., *The Pyramid of Pain*, 17 January 2014, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

Page 30. Paragraphs 3-26 and 3-27. *MITRE ATT&CK® Matrix*, MITRE Corporation. This work is reproduced and distributed with the permission of the MITRE Corporation.

Page 31. Paragraphs 3-28 and 3-29. *MITRE ATT&CK® Matrix*, MITRE Corporation. This work is reproduced and distributed with the permission of the MITRE Corporation.

Page 64. Paragraph 6-31. *MITRE ATT&CK® Matrix*, MITRE Corporation. This work is reproduced and distributed with the permission of the MITRE Corporation.

Page 78. Paragraph 7-37. *MITRE ATT&CK® Matrix*, MITRE Corporation. This work is reproduced and distributed with the permission of the MITRE Corporation.

This page intentionally left blank.

Glossary

Use chapter intro style for glossary introduction.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine Publication
AR	Army regulation
ARCYBER	United States Army Cyber Command
ATT&CK	adversarial tactics, techniques, and common knowledge
CNSSI	Committee on National Security Systems instruction
DODIN	Department of Defense information network
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
METT-TC (I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations
NETCOM	United States Army Network Enterprise Technology Command
NIST	National Institute of Standards and Technology
PMESII-PT	political, military, economic, social, infrastructure, information, physical environment, and time
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-4	battalion or brigade logistics staff officer
S-6	battalion or brigade signal staff officer
SP	special publication
SPOT-C	spot report-cyber
TC	training circular
USCYBERCOM	United States Cyber Command

SECTION II – TERMS

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

area reconnaissance

A form of reconnaissance operation that focuses on obtaining detailed information about the terrain or enemy activity within a prescribed area. (FM 3-90)

area security

A type of security operation conducted to protect friendly forces, lines of communications, installation routes, and actions within a specific area. (FM 3-90)

command and control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of mission. (JP 1)

commander's critical information requirement

An information requirement identified by the commander as being critical to facilitating timely decision making. (JP 3-0)

counterreconnaissance

A tactical mission task that encompasses all measures taken by a unit to counter enemy reconnaissance and surveillance efforts. (FM 3-90)

decision point

A point in space and time when the commander or staff anticipates making a key decision concerning a specific course of action. (JP 5-0)

Department of Defense information network

The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. **Also called DODIN.** (JP 6-0)

enemy

A party identified as hostile against which the use of force is authorized (ADP 3-0)

essential element of friendly information

A critical aspect of a friendly operation that, if known by a threat would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. (ADP 6-0)

event

Any observable occurrence in a network or system. (NIST SP 800-61 Rev. 2)

exfiltrate

A tactical mission task in which a unit removes Soldiers or units from areas under enemy control by stealth, deception, surprise, or clandestine means. (FM 3-90)

field maintenance

On system maintenance, repair and return to the user including maintenance actions performed by operators. (FM 4-30)

friendly force information requirement

Information the commander and staff need to understand the status of friendly forces and supporting capabilities. (JP 3-0)

guard

A type of security operation done to protect the main body by fighting to gain time while preventing enemy ground observation of and direct fire against the main body. (ADP 3-90)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements acting in concert to achieve mutually benefitting effects. (ADP 3-0)

indicator

In intelligence usage, an item of information that reflects the intention or capability of an enemy and/or adversary to adopt or reject a course of action. (JP 2-0)

information collection

An activity that synchronizes and integrates the planning and employment of sensors and assets and as well as the processing, exploitation, and dissemination systems in direct support of current and future operations. (FM 3-55)

insider threat

A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of United States military forces. (AR 381-12)

malicious cyber activity

Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communication systems, networks, physical or virtual infrastructure controlled by computers of information systems, or information resident thereon. (CNSSI 4009)

military decision-making process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0)

mission command

The Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation. (ADP 6-0)

operational environment

The aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

planning

The art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. (ADP 5-0)

priority intelligence requirement

The intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support. (JP 2-0)

screen

A type of security operation that primarily provides early warning to the protected force. (ADP 3-90)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADP 3-0)

zone reconnaissance

A form of reconnaissance operation that involves a directed effort to obtain detailed information on all routes, obstacles, terrain, and enemy forces within a zone defined by boundaries. (FM 3-90)

This page intentionally left blank.

References

All URLs accessed on {DATE}.

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

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

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

JP 1, Volume 2. *The Joint Force*. 19 June 2020.

JP 2-0. *Joint Intelligence*. 26 May 2022.

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

JP 5-0. *Joint Planning*. 1 December 2020.

JP 6-0. *Joint Communications System*. 15 June 2015.

ARMY PUBLICATIONS

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

ADP 3-0. *Operations*. 31 July 2019.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-0. *Mission Command: Command and Control of Army Forces*. 31 July 2019.

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

AR 381-12. *Threat Awareness and Reporting Program*. 1 June 2016.

ATP 6-02.71. *Techniques for Department of Defense Information Network Operations*. 30 April 2019.

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

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

FM 3-55. *Information Collection*. 3 May 2013.

FM 3-90. *Tactics*. 1 May 2023.

FM 4-30. *Ordnance Operations*. 1 April 2014.

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

OTHER PUBLICATIONS

Committee on National Security special publications are available online: https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

CNSSI 4009. *Committee on National Security Systems (CNSS) Glossary*. 2 March 2022.

NIST SP 800-61 Rev. 2. *Computer Security Incident Handling Guide*. August 2012. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

TTP-Based Hunting, MITRE and Roman Daszczyszak et al., March 2019. https://www.mitre.org/news-insights/publication/ttp-based-hunting.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

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

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

Index

Entries are by paragraph number.

A

actors
- cyber vigilantes, 28
- hackers, 28
- individual or small group, 28
- non-state, 26
- organized crime, 28
- script kiddie, 29
- security researcher, 28
- state, 26
- violent extremists, 28

adversary, 25

analytic scheme of maneuver, 54

analytic support cell, 9

analytics, 12

area security, 82

ATT&CK, 30

C

capabilities and limitations, 8

combined arms, 3

command and control, 37, 39

considerations
- corps and below, 6
- echelons above corps, 6

consolidating gains, 36

counterreconnaissance, 76

cyberspace actors, 25

D

data platforms, 64

defensive cyber force employment, 4

defensive cyber forces
- re-tasking, 53
- role, 1

E

economy of force, 4

enemy, 25

F

false hits, 18

filtering, 14

G

G-2 or S-2, 6

G-3 or S-3, 6

G-6 or S-6, 6

gap analysis, 52

H

hunt
- area, 66
- assets, 64
- components, 11
- execution, 14
- forms, 65
- fundamentals, 57
- guidance, 43
- handover, 70
- management, 63
- methods, 60
- techniques, 58
- zone, 65

hunt operations, 37

I

integrating processes, 51
- intelligence preparation of the operational environment, 52

intelligence collection, 2

L

logistics, 85

M

malicious hits, 18

mission command approach, 37

N

neutral, 25

O

operational environment, 35
- shaping, 35

operations process, 39
- assess, 50
- execute, 49
- plan, 45
- prepare, 48

organizations
- battalion task force, 8
- defensive cyber brigade, 8
- mission element, 9

P

pursuit, 16

R

reporting and assessment, 52

roles, 8

S

security, 73
- fundamentals, 73
- guidance, 74
- objective, 74
- tempo, 75

security operations
- cover, 82
- guard, 81
- local security, 83
- screen, 77

sensors, 64

SIGINT. *See* signals intelligence

signals intelligence, 65

situational understanding, 50

sustainment
- planning, 86
- support, 86

T

techniques
- collection, 33
- command and control, 33
- credential access, 32
- defense evasion, 32
- execution, 32
- exfiltration, 33
- impact, 33
- initial access, 32
- lateral movement, 32

Entries are by paragraph number.

persistence, 32
privilege escalation, 32
reconnaissance, 31
resource development, 32
threat
  capabilities, 30
  characteristics, 29
  groups, 26
  insider, 29
  networks, 26
  non-state, 27
  state, 27

TC 3-12.2.98

02 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
2403102

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

This page intentionally left blank.

PIN: 217001-001