ADP 3-37
PROTECTION

January 2024

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes ADP 3-37, dated 31 JULY 2019.

HEADQUARTERS, DEPARTMENT OF THE ARMY

*ADP 3-37

Army Doctrine Publication
No. 3-37

Headquarters
Department of the Army
Washington, DC, 10 January 2024

Protection

Contents

Page

PREFACE ..... **iii**

INTRODUCTION ..... **vii**

Chapter 1 **PROTECTION FUNDAMENTALS** **1-1**
Protection 1-1
Operational Environment 1-2
Threats and Hazards 1-3
The Role of the Protection Warfighting Function 1-5
Protection Principles 1-7
Protection Challenges 1-9

Chapter 2 **PROTECTION DURING OPERATIONS** **2-1**
Army Operations 2-1
Protection Within the Operational Framework 2-4
Protection During Competition Below Armed Conflict 2-5
Protection During Crisis 2-8
Protection During Armed Conflict and Large-Scale Combat Operations 2-12

Chapter 3 **PROTECTION CAPABILITIES INTEGRATION** **3-1**
The Operations Process 3-1
Protection Planning 3-2
Protection Preparation 3-23
Protection Execution 3-27
Protection Assessment 3-29
Measures of Effectiveness and Performance 3-31
Lessons Learned Integration 3-31

Chapter 4 **PROTECTION CELLS** **4-1**
Roles and Responsibilities 4-1
Echelons Above Brigade Protection Cells 4-4
Staff Coordination 4-7
Protection Cell Participation 4-11

Appendix A **PROTECTION WARFIGHTING FUNCTION PRIMARY TASKS** **A-1**

SOURCE NOTES ..... **Source Notes-1**

GLOSSARY **Glossary-1**

REFERENCES **References-1**

*This publication supersedes ADP 3-37, dated 31 July 2019.

INDEX Index-1

Figures

Introductory figure 1. ADP 3-37 logic chart viii
Introductory figure 2. Protection across the strategic contexts ix
Figure 1-1. Examples of key protection considerations by echelon 1-7
Figure 2-1. Operational categories and the spectrum of violence 2-2
Figure 2-2. Example of protection considerations within a corps area of operations during large-scale combat operations 2-4
Figure 2-3. Army Protection Program 2-8
Figure 2-4. Notional protection measures during large-scale combat operations 2-14
Figure 2-5. Example of increased security of a specific area for a main supply route 2-26
Figure 3-1. Integration of protection throughout the operations process 3-2
Figure 3-2. Protection planning 3-3
Figure 3-3. Example criticality, vulnerability, and probability values 3-10
Figure 3-4. Example of shifts in protection priorities 3-14
Figure 3-5. Example protection running estimate 3-18
Figure A-1. Risk matrix example during large-scale combat operations A-3

Tables

Introductory table 1. Rescinded Army terms x
Table 2-1. Protection responsibilities during deployment 2-11
Table 3-1. Example division protection working group activities and participants 3-4
Table 3-2. Example protection risk analysis table 3-10
Table 3-3. Example protection prioritization list 3-11
Table 3-4. Protection integration to MDMP 3-19
Table 3-5. Protection cells input to a synchronization matrix tool example 3-22
Table 3-6. Examples of change indicators 3-29
Table A-1. Force health protection primary preventive tasks by function A-23

Preface

ADP 3-37 expands on doctrine for protection described in the Army capstone manual ADP 3-0. It describes how Army forces at every echelon employ protection. The primary focus of ADP 3-37 is on how commanders and staffs integrate, synchronize, and employ protection capabilities and proactive measures to prevent or mitigate detection, threat effects, and hazards. Effective protection preserves combat power and enables freedom of action.

ADP 3-37 is applicable to all members of the profession of arms: leaders, Soldiers, and Army civilians. The principal audience for ADP 3-37 is commanders and staffs within theater armies, corps, divisions, and brigades. This publication provides the foundation for training, curricula, and future capabilities development across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

To comprehend the doctrine contained in ADP 3-37, readers must first understand the Army mission, organization, and roles described in ADP 1. They must understand the operations process, operational art, and other warfighting functions (command and control, intelligence, fires, movement and maneuver, and sustainment) described in ADP 3-0. Readers must understand Army operations discussed in FM 3-0, tactics described in ADP 3-90, and stability operations covered in ADP 3-07.

Army leaders must understand joint doctrine and use it when communicating and coordinating directly with the joint force. Prerequisite reading of joint doctrine includes JP 3-0. When conducting multinational operations, readers must be familiar with FM 3-16. AJP-01 establishes the capstone doctrine for North Atlantic Treaty Organization military operations, and AJP-3.14 establishes allied joint doctrine for force protection.

ADP 3-37 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ADP 3-37 is the proponent publication (the authority) are italicized in the text and are marked with an asterisk (*) in the glossary. Terms and definitions for which ADP 3-37 is the proponent publication are boldfaced and italicized, and the definitions are boldfaced. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition.

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

The proponent of ADP 3-37 is the Maneuver Support Center of Excellence (MSCOE). The preparing agency is the Fielded Force Integration Directorate (FFID), Doctrine Division, Maneuver Support Center of Excellence. Send comments and recommendations on Department of the Army (DA) Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Director, FFID, Doctrine Division, MSCOE, ATTN: ATZT-FFD, 14000 MSCOE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929; by email to usarmy.leonardwood.mscoe.mbx.mpdoc@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Acknowledgements

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

Quotes reprinted courtesy Dictionary of Military and Naval Quotations, compiled by Robert Debs Heinl, Jr. (Annapolis, MD: United States Naval Institute, 1966).

This page intentionally left blank.

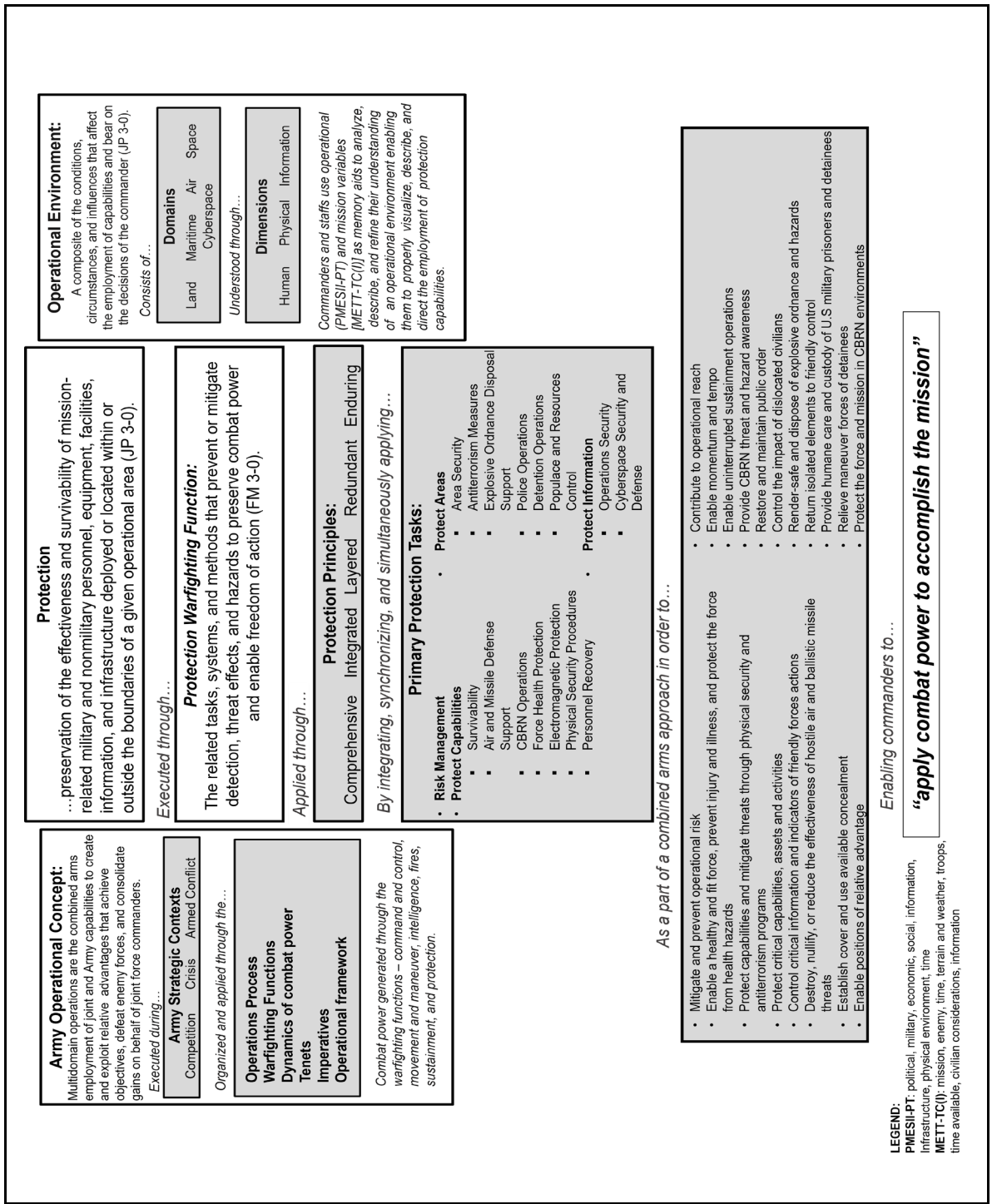
Introduction

Protection is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (JP 3-0). Protection is not linear; it is a continuous and enduring process that is planned, prepared, executed, and assessed throughout Army operations and encompasses everything that makes Army forces hard to detect, disrupt, and destroy. From individual Soldier tasks to the integration of the Army protection warfighting function and the Army protection program, protection is a wholistic outcome that stems from many activities—not only from specific staff sections or Army units, but also from each and every Soldier.

The foundation of protection starts with the individual Soldier and units conducting tactical-level operations. Soldiers must be proficient in common Soldier tasks and field crafts. Leaders and Soldiers must understand the threat, operational environment, and all forms of enemy contact—and account for being under constant observation—to enhance survivability. *Survivability* is a quality or capability of military forces which permits them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission (ATP 3-37.34). To increase survivability, units employ security operations, modify tempo, take evasive action, maneuver to gain positional advantages, decrease electromagnetic signatures, and disperse forces. Dispersed formations improve survivability by complicating targeting and making it more difficult for enemy forces to identify lucrative targets. Tactical units integrate procedures for the use of camouflage, cover, concealment, and conducting electromagnetic protection—including noise and light discipline.

The *protection warfighting function* is the related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action (FM 3-0). Protection as an Army warfighting function is not limited to a specific domain, nor is it branch- specific; it includes capabilities from all domains. Units must be able to preserve themselves, be resilient, and withstand enemy attack. When units are unable to protect themselves, commanders coordinate with higher command for protection support. Commanders and staffs must understand their Soldiers, the enemy, and the operational environment at each echelon to prioritize protection for applying critical resources and coordinating support in the conduct of combined arms operations. The protection warfighting function complements, reinforces, and overlaps with the Army Protection Program in support of Army operations.

ADP 3-37 is the Army's primary doctrinal publication for the protection warfighting function and remains consistent with previous protection doctrine. The logic chart for ADP 3-37 is shown in introductory figure 1, page viii, and is read from out to in. It begins on the left, which illustrates how the Army's operational concept of multidomain operations is conducted across the Army's strategic context (competition below armed conflict, crisis, and armed conflict) and organized and applied through the operations structure (operations process, operational framework, and combat power [generated through the warfighting functions]). The right side of the logic map describes the operational environment as consisting of five domains (land, maritime, air, space, and cyberspace) and is understood through three dimensions (human, physical, and information). The logic map concludes down the center. It describes protection and how it is executed through the protection warfighting function, enabling the commander to apply combat power and achieve mission success.

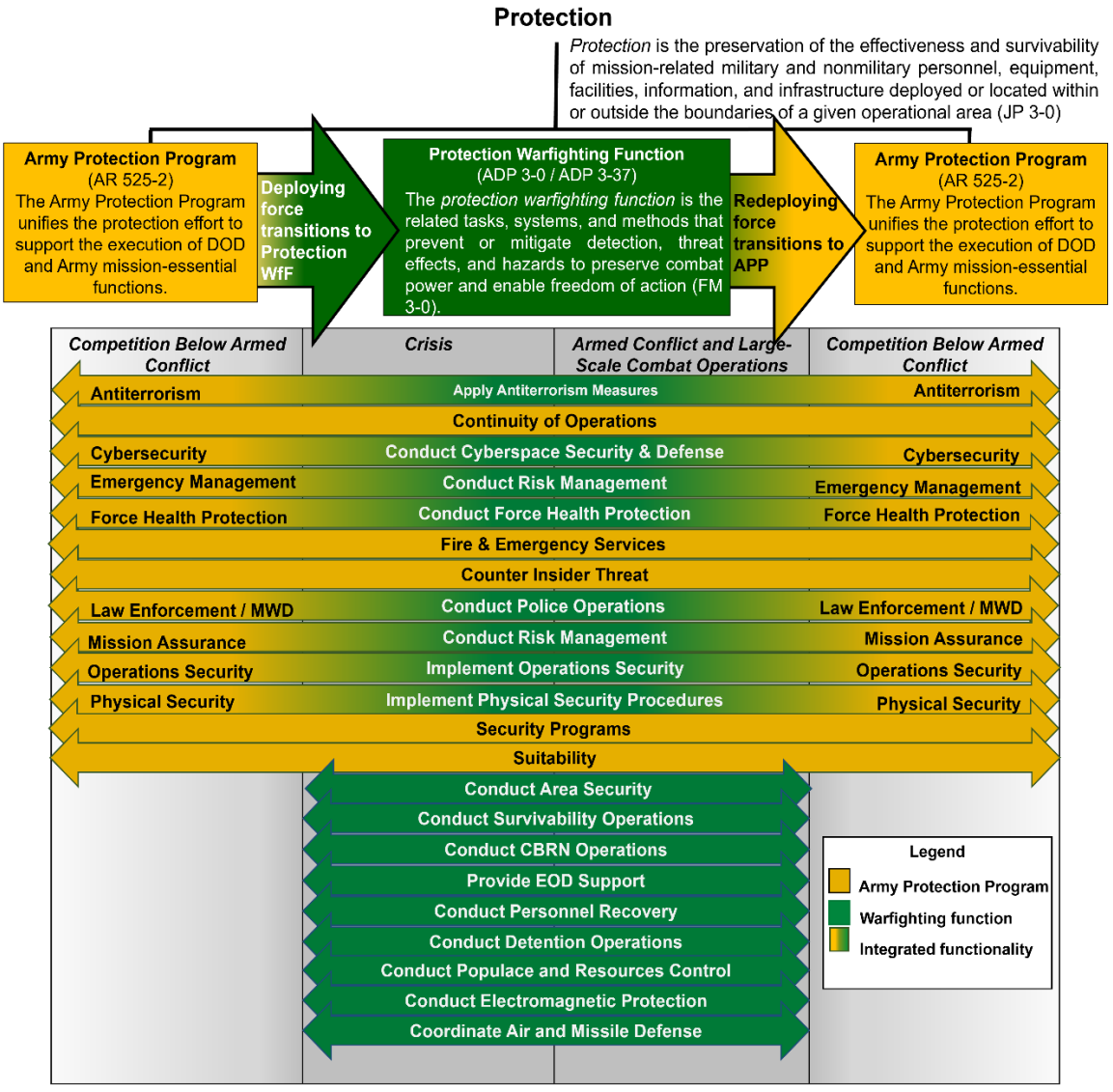


Legend:

CBRN	chemical, biological, radiological, and nuclear
FM	field manual
JP	joint publication
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
METT-TC(I)	mission, enemy, time, terrain and weather, troops, time available, civilian considerations, and informational considerations

Introductory figure 1. ADP 3-37 logic chart

The Army Protection Program manages risks relative to the safety and security of Soldiers, civilians, family members, contractors, facilities, infrastructure, and information on U.S. Army installations. The Army Protection Program enables commanders to build and project combat power in support of Army operations throughout the strategic context. The Army Protection Program cannot eliminate the risks of threats and hazards, but it does seek to prevent, prepare for, protect against, mitigate, respond to, and recover from an event to minimize the impact to the execution of DOD and Army missions. It integrates, coordinates, synchronizes, and effectively prioritizes the efforts and resources of the Army Protection Program functions with their associated programs and processes (see AR 525-2 for additional information on the Army Protection Program). Introductory figure 2 illustrates the overlapping and reinforcing capabilities of the Army Protection Program and the Protection Warfighting Function.



Legend:

ADP	Army doctrine publication	EOD	explosive ordnance device
APP	Army Protection Program	FM	field manual
AR	Army regulation	JP	joint publication
CBRN	chemical, biological, radiological, and nuclear	MWD	military working dog
		WfF	warfighting function
DOD	Department of Defense		

Introductory figure 2. Protection across the strategic contexts

A shared understanding of the joint protection function (see JP 3-0) and joint allied force protection (see AJP 3.14) enables Army leaders and staffs to integrate and synchronize the protection warfighting function with unified action partners. Army leaders must anticipate that joint support is limited in large-scale combat operations and must protect the force by utilizing a combination of measures. The joint protection function focuses on preserving the joint force fighting potential in four primary ways:

- Active defensive measures to protect friendly forces, civilians, and infrastructure.
- Passive defensive measures to make friendly forces, systems, and facilities difficult to locate, strike, and destroy when active measures are limited or unavailable.
- The application of technology and procedures to reduce the risk of fratricide.
- Emergency management and response to reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters.

The doctrine described in this publication nests with ADP 3-0 and FM 3-0. ADP 3-37 builds on the collective knowledge and wisdom gained through recent operations, numerous lessons learned, and doctrine revisions throughout the Army. It is rooted in time-tested principles and fundamentals, while accommodating new technologies and organizational changes.

ADP 3-37 consists of four chapters and one appendix:

Chapter 1 discusses the role of protection, protection in support of multidomain operations, the effects of threats and hazards throughout the operational environment, and protection challenges, and it identifies the principles of protection.

Chapter 2 expands on the discussion of protection integration throughout the operational framework in support of Army operations.

Chapter 3 describes the integration and layering of protection through the operations process.

Chapter 4 establishes the roles and responsibilities of the protection cell at corps echelon and below, identifies the sections that make up the protection cell, and discusses the protection cell relationship with other key staff sections and working groups in which the protection cell must participate.

Appendix A defines and examines the protection warfighting function and the primary tasks associated with protection.

Based on current doctrinal changes, certain terms for which ADP 3-37 is the proponent have been added, rescinded, or modified for purposes of this publication. The glossary contains acronyms and defined terms. See introductory table 1 for specific term changes.

Introductory table 1. Rescinded Army terms

Term	*Remarks*
critical asset security	Rescinded.
movement corridor	Rescinded.

Chapter 1
Protection Fundamentals

"It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible."

Sun Tzu

Protection determines the degree to which potential threats or hazards can disrupt operations and initiates active and passive measures to prevent and mitigate those disruptions. When commanders understand the operational environment and their protection capabilities, they coordinate, integrate, and synchronize protection capabilities to reduce risk, mitigate identified vulnerabilities, and create windows of opportunity. This chapter discusses the role of protection and the effects of threats and hazards throughout the operational environment, identifies the principles of protection, and provides discussion on protection challenges.

PROTECTION

1-1. Protection is an outcome that is essential to the success of large-scale combat operations against peer threats. It determines the degree to which potential threats and hazards can disrupt operations and encompasses everything that makes Army forces hard to detect and destroy. Peer threats are able to rapidly detect and destroy Army forces by employing space-based capabilities, unmanned systems, and massed and precision fires. Their standoff approaches contest the joint force through all domains and increase risk to Army forces attempting to operate within adversary-denied areas. A *domain* is a physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills (FM 3-0). Current threats are the most evenly matched forces the Army has faced in decades, amplifying the importance of protection and making it the responsibility of all leaders and units during all operations.

1-2. Protection is essential to preserving critical capabilities, areas, and information against threats in all domains; preventing or mitigating detection and the effects of threats and hazards; enabling the generation of combat power; and enabling freedom of action. *Protection* is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (JP 3-0).

1-3. Protection efforts always encompass threats and hazards from all domains and through the depth of the operational environment. Protection is not a linear activity—planning, preparing, executing, and assessing protection is a continuous and enduring process. Commanders and staffs continue to update their priorities based on transitions, evolving understanding of the threat, and the gaps and seams that create vulnerabilities. A commander's intent and guidance should be clear to ensure that proper integration of protection capabilities is considered throughout the entire operation.

Protection requires commanders and staffs to understand the threat and identify likely avenues of approach and methods of attack; prioritize critical capabilities, areas, and information and understand the dependencies between them; and be willing to assume greater risk in areas that may be more exposed but are of less significance or are less likely to be targeted.

1-4. Commanders and staffs must understand that the operational environment includes the totality of factors, specific circumstances, and conditions that impact the conduct of operations. Understanding the operational environment enables leaders to better identify problems and anticipate potential outcomes to properly direct, coordinate, and synchronize active and passive protection efforts as part of a combined arms approach. Anticipating protection requirements demands that leaders understand all hazards and potential threats in the operational environment.

1-5. Commanders identify and characterize the threat to employ protection capabilities. Protection includes active and passive measures. Leaders apply active and passive protection measures proactively, anticipating protection requirements and taking appropriate action as early as possible. Active protection measures involve the interception or destruction of the delivery systems, sensors, and data of threats and hazards before they can inflict damage on their intended targets. Passive protection measures include protecting personnel and equipment from detection and the effects of threats and hazards. A unit implements passive protection measures by changing tempo or taking evasive action. Formations often derive protection through dispersion and by exploiting terrain and weather conditions or by using the cover of darkness to mask movement. Cyber activities remain constant throughout all operations.

Commanders should attempt to make initial contact with sensors and unmanned systems, incorporating them into movement techniques and the scheme of protection.

1-6. The employment of protection capabilities creates a comprehensive, integrated, layered, redundant, and enduring effect that prevents or mitigates detection, threat effects, and hazards and enables freedom of action. The ability to protect and preserve the force and secure the assigned area is vital to achieving agility, convergence, endurance, and depth during operations. See FM 3-0 for additional information on the tenets of operations and methods of warfare.

OPERATIONAL ENVIRONMENT

1-7. Within the broader strategic security environment, Army forces conduct operations in specific operational environments. 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). For Army forces, an operational environment includes portions of the land, maritime, air, space, and cyberspace domains and is understood through three dimensions (human, physical, and information). The land, maritime, air, and space domains are defined by their physical characteristics. Cyberspace, a man-made network of networks, connects the other domains. See FM 3-0 for additional information on the domains and dimensions in an operational environment.

1-8. Commanders and staffs who are charged with providing or ensuring protection must begin with a thorough understanding of the operational environment, risks, and opportunities that area present and the ways and means available that prevent or mitigate detection and threat effects. Protection cells use information and intelligence to understand enemy or adversary capabilities. Intelligence capabilities contribute to protection by collecting, storing, analyzing, and disseminating detailed, timely, relevant, accurate, and predictive information and intelligence about threats and the operational environment. See FM 2-0 for additional information on intelligence support to protection.

1-9. Army doctrine also recognizes the eight operational variables (political, military, economic, social, information, infrastructure, physical environment, and time [PMESII-PT]) for analyzing and understanding any operational environment. To support military plans, missions, and orders, relevant information from these operational variables can be filtered into the categories of the Army mission variables of mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and integrated into the other variables, informational considerations (METT-TC [I]). (See FM 5-0 for more information on operational and mission variables.) Understanding of the operational environment helps identify current, developing, and potential hazards and threats that enable commanders to direct, coordinate, and synchronize protection capabilities and proactive measures to mitigate or prevent the effects of threats and hazards. See ATP 2-01.3 and ATP 3-05.20 for additional information.

THREATS AND HAZARDS

1-10. The protection warfighting function prevents or mitigates detection, threat effects, and hazards to preserve combat power and enable freedom of action and survivability of the force by providing protection from threats and hazards. Threats and hazards have the potential to cause personal injury, illness, or death; equipment or property damage or loss; or mission degradation. Hazards lead to risk when people interact with equipment or their environment. Hazards exist in all types of environments and activities, including combat, stability, base support, training, garrison activities, and off-duty activities. Commanders and protection cells analyze the following potential threats and hazards:

- **Hostile actions.** Threats from hostile actions include any capability that enemy forces or criminal elements can use to inflict damage on personnel, physical assets, or information. These threats may include direct and indirect fires; unmanned aircraft systems; explosive hazards; suicide bombings; network attacks; asset theft; air attacks; cyberspace networks and other forms of electromagnetic attacks; or chemical, biological, radiological, and nuclear (CBRN) weapons.
- **Nonhostile activities.** Nonhostile activities include hazards associated with Soldier duties within their occupational specialty, Soldier activities while off duty, and unintentional actions that cause harm. Examples include on- and off-duty accidents, operations security (OPSEC) violations, network compromises, equipment malfunctions, unexploded ordnance, or CBRN hazards.
- **Environmental conditions.** Environmental hazards associated with the surrounding environment could degrade readiness or mission accomplishment. Common examples include weather, natural disasters, complex terrain, and diseases. Weather effect knowledge is critical to the commander's situational understanding and decision making. By exploiting this knowledge, commanders can minimize the impact of environmental threats to friendly forces while simultaneously capitalizing on environmental conditions that maximize their advantage while operating at the limits of their capabilities. The staff also considers how military operations may affect noncombatants in the area of operations. Such considerations prevent unnecessary collateral damage and consider how civilians may affect the mission.

1-11. Commanders use the METT-TC (I) mission variables to describe the characteristics of the area of operations, including threat- and accident-based hazards that may impact protection. In most cases, they can obtain relevant information from an ongoing analysis of the operational environment by using the PMESII-PT operational variables.

THREATS

1-12. Land operations are often complex because actors intermix with each other, with no easy means to distinguish one from another. The various actors in any area of operations can qualify as a threat, an enemy, an adversary, or a neutral:

- 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 are, by nature, hybrid. Threats may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, nation-states, or national alliances. When threats execute their capability to do harm to the United States, they become enemies. See ADP 3-0 for additional information on threat and adversary methods.
- An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). An enemy is also called a combatant and is treated as such under the law of war.

- 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 peer threat is an adversary or enemy with the capabilities and capacity to oppose U.S. forces across multiple domains worldwide or in a specific region where they have a position of relative advantage. Peer threats possess roughly equal combat power in geographical proximity to a conflict area with U.S. forces. See FM 3-0 for additional information on peer threats.
- 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).
- A neutral is an impartial or unbiased country or person that neither helps nor supports either side in a conflict or disagreement.

HAZARDS

1-13. A *hazard* is a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation (JP 3-33). Hazards are usually predictable and preventable and can be reduced through effective risk management efforts. Commanders differentiate hazards from threats and develop focused schemes of protection and priorities that match protection capabilities with the corresponding threat or hazard. However, hazards can be enabled by the tempo or friction or by the further complacency that sometimes develops during extended military operations. For additional information on hazards, see ATP 3-34.20 and TM 3-11.91.

LEVELS OF THREAT

1-14. There are three levels of threat: Level I, Level, II, and Level III. These different levels provide commanders with general descriptions and categorizations of threat activities and identify protection requirements to preserve combat power; enable the freedom of action; and identify, prevent, or mitigate the effects of threats and hazards.

1-15. Commanders and staffs should consider the sizes and types of potential threats to friendly forces when determining and describing levels of threat. Threat levels should be based on the activity, capability, and intent of enemy agents or forces. They can be further described by looking at mission impact. A Level I threat may require only a routine response by assembly area, base camp, or base cluster security forces and have a negligible impact on the mission, or a Level I threat may have a catastrophic impact. For example, on 21 December 2004, a suicide bomber killed 14 and injured 72 in the Forward Operating Base Marez dining hall. According to the chart, it was a Level I threat; however, the attack was catastrophic. A Level III threat could cause mission failure and requires a tactical combat force response. The following are descriptions of the levels of threat:

- **Level I threats.** Level I threats include enemy agents, terrorists, and criminals whose primary missions include espionage, sabotage, assassination, and subversion. These include a potential for insider attacks by elements or individuals of host-nation partners and security forces.
- **Level II threats.** Level II threats include small-scale forces that can cause serious harm to military forces and civilians. Attacks by Level II threats can cause significant disruptions to military operations and the orderly conduct of local governments and services. Forces constituting Level II threats are capable of conducting well-coordinated, but small-scale, hit-and-run attacks; improvised weapons attacks with roadside or vehicle-borne improvised explosive devices; raids; and ambushes. Level II threats may also include special operations forces.
- **Level III threats.** Level III threats have the capability of projecting combat power by air, land, or sea or anywhere into the area of operations. Specific examples include airborne, heliborne, and amphibious operations; large, combined-arms, ground-force operations, or penetrations; and infiltration operations involving large numbers of individuals or small groups. Level III threats are beyond the capability of support and rear area forces and can only be effectively defeated by a tactical combat force or other significant forces.

THE ROLE OF THE PROTECTION WARFIGHTING FUNCTION

1-16. The *protection warfighting function* is the related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action (FM 3-0). The protection warfighting function preserves the commander's critical capabilities, areas, and information. It disrupts enemy targeting of friendly forces and enables freedom of action to expand exploitable opportunities at each echelon and through the depth of the operational environment during competition below armed conflict, crisis, and armed conflict (see Chapter 2). Protection represents a diverse array of tasks—some of them performed by specialized units and personnel. However, all leaders bear continuous protection responsibilities for their forces and their mission. See Appendix A for a description of the primary protection warfighting function tasks.

Protection Warfighting Function Primary Tasks:

- **Risk Management**
- **Survivability**
- **Air and Missile Defense Support**
- **CBRN Operations**
- **Electromagnetic Protection**
- **Area Security**
- **Operations Security**
- **Cybersecurity and Defense**
- **Physical Security Procedures**
- **Antiterrorism Measures**
- **Explosive Ordnance Disposal Support**
- **Personnel Recovery**
- **Police Operations**
- **Detention Operations**
- **Populace and Resources Control**
- **Force Health Protection**

1-17. Commanders integrate protection to preserve combat power without impeding mission accomplishment. Commanders consider the fundamentals of protection to ensure the proper integration of protection capability necessary in time and space. The primary protection tasks fall into four categories:

- **Conduct risk management.** *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0). It focuses on both the mission and the force.
- **Protect capabilities.** Protecting capabilities are measures taken to prevent or mitigate detection or the impact of enemy action by intercepting, defeating, or mitigating threats and hazards before they can degrade Army capabilities. Protecting capabilities includes—
  - Survivability (protect against detection and lethal fires).
  - Air and missile defense (coordinate for protection against air and missile threats).
  - CBRN operations (protect against CBRN effects).
  - Force health protection (protect against threats and hazards to health).
  - Electromagnetic protection (protect against electromagnetic spectrum threats).
  - Physical security (protect personnel, resources, and information).
  - Personnel recovery (protect isolated personnel).
- **Protect areas.** Protecting areas prevents, mitigates, and disrupts the enemy's ability to gain positions of advantage; maintain freedom of action; destroy friendly critical capabilities, assets, and activities; and influence third-party actors, surrogates, proxies, and irregular criminal threats across the operational environment, including force projection and generation platforms in the homeland and abroad. A *critical asset* is a specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively (JP 3-26). Protecting areas includes—
  - Area security (secure areas, lines of communication, and defense of critical assets from threats).
  - Antiterrorism (protect personnel, property, and resources).
  - Explosive ordnance disposal (EOD) (protect against explosive hazards).

- Police operations (protect forces, populations, critical infrastructure, and assets and enable stability).
- Detention operations (protect forces by detaining enemy threats).
- Populace and resources control (protect people and their economic resources).

- **Protect information.** Protecting information requires enduring measures that protect and defend friendly information and information systems. These measures are designed to conceal information from, and deny information to, the threat; protect information from unauthorized modification; protect information from unauthorized destruction; and enable information advantage. Protecting information includes—
  - OPSEC (protect critical information and indicators of friendly force actions).
  - Cyberspace security and defense (protect networks).

1-18. Protection is an enduring requirement. Defense and security operations have temporary objectives. Defensive operations typically last until a formation can resume the offense. Reconnaissance and surveillance operations typically transition at a time during the battle to best support the commander's objectives. In contrast, protection is a continuous requirement that serves one dominant purpose—the preservation of combat power. Preserving combat power includes protecting personnel (combatants and noncombatants) and physical assets of the United States, unified action partners, and host nations.

1-19. Army forces consolidate gains, sustain, and exploit control over land to deny its use to an enemy. They use combined arms formations that possess combat power to defeat an enemy and establish control of areas, resources, and populations. The protection warfighting function, when properly integrated with the intelligence, maneuver, fires, sustainment, and command and control warfighting functions, enables commanders to sustain, maintain, and generate combat power to apply against the enemy. *Combat power* is the total means of destructive and disruptive force that a military force that a unit/formation can apply against an enemy at a given time (JP 3-0).

1-20. Combat power is the means for conducting warfare and consists of five dynamics (leadership, firepower, information, mobility, and survivability). Each dynamic is interdependent and enabled by the protection warfighting function. Survivability is both a primary task of the protection warfighting function and a dynamic of combat power. In both uses, survivability is a quality or capability of military forces that permits them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission. As a primary task of the protection warfighting function, survivability includes supporting tasks that enhance a formation's ability to avoid or withstand an enemy's actions by providing or improving camouflage, cover, and concealment; controlling electromagnetic emissions; and increasing personal protective posture (adding small arms protective insert plates, adding mission-oriented protective posture, or hardening command facilities).

1-21. Protection considerations are not the same at every echelon or in every area of operations (see figure 1-1). While some multidomain protection considerations, such as cybersecurity and defense, are executed at a strategic level across the operational framework, protection priorities diverge based on the time and proximity to different threat capabilities and capacities. Protection prioritization changes are anticipated and assets are reassessed as transitions occur throughout operations, changes to the commander's priorities occur, or decision criteria is met.

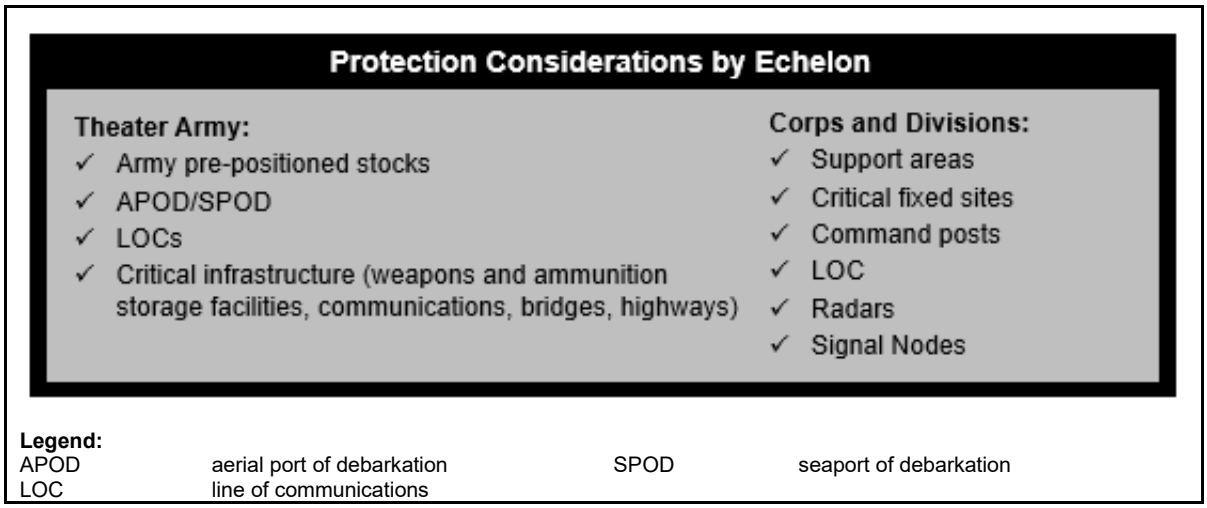


Figure 1-1. Examples of key protection considerations by echelon

1-22. Commanders establish protection priorities and develop a scheme of protection for each phase of an operation or major activity. They integrate protection-enabling operations and capabilities to reduce risk, mitigate vulnerabilities, and act on opportunity. Commanders strive to counter enemy threats and hazards from each domain that can influence an operational environment. They account for threats from space, cyberspace, and entities outside their assigned area of operations as they develop protection measures. When properly integrated, the tasks and systems that comprise the protection warfighting function effectively preserve the force.

1-23. Individuals are protected at the lowest level by awareness, personal protective equipment, an understanding of the rules of engagement, and fratricide avoidance measures. By implementing additional protection measures in the area surrounding an individual (fighting positions, vehicles, collective protection, and force health protection measures taken against accidents and disease), the force then provides a layering of protection. Enhancing survivability measures, applying active and passive defense operations, and implementing antiterrorism and physical security measures add to the next layer of a comprehensive, integrated, layered scheme of protection. Implementing protection tasks and utilizing protection systems in a comprehensive, layered scheme of protection preserve the commander's priorities throughout the range of military operations in any operational environment.

PROTECTION PRINCIPLES

Protection Principles:
- **Comprehensive**
- **Integrated**
- **Layered**
- **Redundant**
- **Enduring**

1-24. A *principle* is a comprehensive and fundamental rule or an assumption of central importance that guides how an organization approaches and thinks about the conduct of operations (ADP 1-01). The five principles of protection—comprehensive, integrated, layered, redundant, and enduring—summarize the characteristics of successful coordination and synchronization. These principles provide a context for applying the protection warfighting function, developing schemes of protection, and allocating resources. Each principle complements and enables the others. Leaders consider each principle when developing protection options and integrating protection into operations.

COMPREHENSIVE

1-25. Army formations require an all-inclusive approach to preventing or mitigating detection, threat effects, and hazards. Commanders and protection cells develop and execute a comprehensive scheme of protection that integrates all complementary and reinforcing protection tasks, systems, and methods available to a commander. This comprehensive approach creates layered, redundant, and enduring effects that preserve combat power and enable freedom of action. A comprehensive scheme of protection and/or protection

priorities can vary from mission to mission but, in most cases, they should be based on the degree to which potential threats and hazards can disrupt Army operations.

1-26. One of the first steps in developing a comprehensive scheme of protection and establishing protection priorities is to collect data on existing threats and hazards. The protection cell and working group uses information from the commander's guidance, intelligence preparation of the operational environment, risk management, friendly forces information requirements, warning order, mission analysis, and initial assessments to develop a comprehensive plan. When executed, the scheme of protection provides a holistic approach to preserving critical capabilities, assets, activities, critical missions, the supporting effort, and/or the main effort. As transitions occur or as the commander's priorities change, the protection cell makes the necessary adjustments required to achieve a unified approach to protection, enabling mission success.

INTEGRATED

1-27. The integration of protection capabilities provides strength and structure to the overall protection effort. Integration occurs vertically and horizontally and includes unified action partners throughout the operations process. When properly integrated, protection capabilities achieve a comprehensive, layered, redundant, and enduring effect that enhances the effectiveness and endurance of Army formations during operations.

1-28. All military activities have some inherent or organic protection characteristics (for example, survivability, antiterrorism measures, local and area security). Understanding those characteristics helps leaders employ protection capabilities in complementary and reinforcing ways:

Protection must be integrated by planners at echelon in both the operations and targeting process throughout competition, crisis, and armed conflict.

- **Complementary.** Complementary protection capabilities protect the weakness of an organization with the protection capabilities of a different organization.
- **Reinforcing.** Reinforcing capabilities combine similar protection capabilities within the same organization to increase its overall protection capabilities.

1-29. Commanders and staffs should be familiar with protection capabilities and the characteristics of each to understand how they complement and reinforce each other to increase the probability of mission success. In addition to the primary protection warfighting function tasks, commanders and staffs integrate and simultaneously apply the protection enabling tasks and programs (intelligence support, combat identification/fratricide, security operations, Army protection program) that preserve combat power at each subordinate echelon.

LAYERED

1-30. Protection capabilities are deliberately arrayed to prevent or mitigate the risk of detection, threat effects, or hazards. Layering protection capabilities achieves a comprehensive, integrated, redundant, and enduring effect. For example, protection capabilities may be layered in support of route security to enhance the overall protective posture. All units conduct local security for self-protection. Incorporating additional protection capabilities in support of movement (such as route clearance, convoy escorts, CBRN reconnaissance and surveillance, and response force operations) enhances survivability, providing multiple layers of active and passive protection. Coordinating air and missile defense support and defensive counter air operations layer protection. *Air and missile defense* is direct [active and passive] defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile air and ballistic missile threats against friendly forces and assets (JP 3-01). Air and missile defense actions are conducted by air defense artillery personnel, forces, and systems. Layering protection tasks, systems, and methods preserves combat power and enables freedom of action. A screening force, employment of unmanned aerial systems on flanks, employment of obstacles, employment of overhead cover, and implementation of electromagnetic radiation masking procedures are also examples of layering protection capabilities and tasks against the risk of effective enemy surprise attacks.

REDUNDANT

1-31. Redundancy ensures that critical capabilities, areas, and information have secondary or auxiliary protection measures that reduce their vulnerability. Redundant capabilities overlap with other capabilities and reduce seams in protection. Protection efforts are often redundant and overlapping when vulnerability, weakness, or failure is identified or expected. Redundancy may not be achieved for all protection priorities based on available protection assets.

1-32. Commanders and staffs ensure that redundant protection measures improve the probability of success against detection, threat effects, or hazards. Commanders and staffs conduct assessments to ensure the redundancy of protective measures and to account for the possibility that some protection priorities are more vulnerable to attacks than others.

ENDURING

1-33. The protection principle of enduring is directly related to the Army tenet of endurance discussed in FM 3-0. Endurance is the ability to persevere over time throughout the depth of an operational environment (see FM 3-0 for additional information on endurance). Endurance enhances the ability to project combat power and extends operational reach. Endurance is about resilience and preserving combat power while continuing operations for as long as necessary to achieve the desired outcome.

1-34. In terms of protection, the principle of enduring refers to an ability to prevent or mitigate detection and the effects of threats and hazards for an extended period. Endurance also includes a protection asset's ability to resist over an extended duration. Endurance involves anticipating transitions and making the most effective and efficient use of protection resources.

PROTECTION CHALLENGES

1-35. Operational environments present unique challenges that Army forces must be prepared to overcome during competition below armed conflict, crisis, and armed conflict (see FM 3-0 for more information about competition, crisis, and armed conflict). An operational environment is broader than a specific area of operations; it also involves interconnected influences from the global or regional perspective that impact operations. Adversaries use a combination of military and nonmilitary capabilities in all domains, requiring commanders and staffs to continually assess and reassess protection priorities and the employment of protection capabilities within their assigned areas of operations.

1-36. Operational environments may include dense urban terrain, large and dynamic populations, traditional and critical information infrastructure, adversary information warfare, and other factors that challenge military forces. Enemy capabilities enable them to conduct operations within the homeland, against power-projection capabilities, in the support areas, and into the deep maneuver and fire support areas of the battlefield. Their disruptive effects may occur at unit home stations and ports of embarkation, while in transit to the theater, and upon arrival at ports of debarkation. Army forces may not have the capability nor the authority to preempt these attacks.

1-37. Commanders must be aware of personnel within their own force who have authorized access to Department of Defense (DOD) facilities and systems who may want to disrupt operations or support a criminal, extremist group, insider threat, or terrorist organization. Adversaries will also create or leverage conditions intended to fracture partnerships, stress the will of friendly actors, and flip friendly force advantages in multiple areas to the side of the adversary.

1-38. Operational environments can be marked by rapid change and a wide range of threats and hazards that significantly challenge military forces. During armed conflict, Army forces face peer enemies that are capable of contesting them in all domains. The fluidity and rapid tempo of large-scale combat operations pose challenges for the protection of friendly assets.

1-39. Long-range lethal and nonlethal capabilities allow the enemy to target rear areas and lines of communication. Securing and protecting bases, command and control nodes, and other infrastructure are essential to compete and win. The use of bases for intermediate staging, sustainment, and related activities is required to conduct large-scale combat operations. Commanders must be able to establish staging areas and

enable access for onward movement and sustainment of forces. Due to their size, immobility, concentration of friendly forces, and material, base camps are considered high-value targets for enemy attacks.

1-40. In large-scale combat operations with a peer or near-peer threat, force health protection personnel and organizations may not be able to conduct assessments or move freely due to enemy actions. Soldiers will be challenged to maintain hygiene and sanitation. Commanders and leaders must ensure that force health protection measures such as hygiene and sanitation are enforced.

Chapter 2
Protection During Operations

"Nine times out of ten, an Army has been destroyed because its supply lines have been severed."

General Douglas MacArthur, 1950

The protection function manifests itself differently at each echelon, through competition below armed conflict, crisis, and armed conflict. Operations from strategic support areas in the United States to the close area face a wide range of threats. Their disruptive effects may occur at unit home stations, ports of embarkation, while in transit to the theater, and upon arrival at ports of debarkation. Adversaries seek to gain an advantage through combat action and their ability to identify friendly vulnerabilities. As the violence and intensity of conflict increase, the ability to protect combat power and associated elements without hindering maneuver and stifling initiative becomes increasingly complex. As operations transition to large-scale combat operations, the increase in violence and intensity creates gaps and seams in friendly forces protection posture. Commanders must assess each mission and develop a scheme of protection that applies protection capabilities and proactive measures to protect the force and enable mission success. This chapter discusses protection across the operational framework in support of Army operations.

ARMY OPERATIONS

2-1. The Army's primary mission is to organize, train, and equip its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas. The Army accomplishes its mission by supporting the joint force in four strategic roles: shaping operational environments, countering aggression on land during crisis, prevailing during large-scale combat operations, and consolidating gains. The strategic roles clarify the overall purposes for which Army forces conduct multidomain operations on behalf of joint force commanders across the competition continuum in the pursuit of a stable security environment and other policy objectives that are favorable to the United States. (See ADP 3-0 for more information on the Army's strategic roles.) *Multidomain operations* is the combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders (FM 3-0). Success in fulfilling the strategic roles requires national-level leaders to orchestrate all instruments of national power throughout the entire government and coalition and across the competition continuum.

2-2. Army forces achieve objectives through the conduct of operations. An *operation* is a sequence of tactical actions with a common purpose or unifying theme (JP 1 Volume 1). Operations across the range of military operations vary in many ways (see figure 2-1, page 2-2). They occur in all kinds of physical environments, including urban, subterranean, desert, jungle, mountain, maritime, and arctic. They also take place anywhere along a spectrum of violence, from competition below armed conflict up to armed conflict. Operations vary in scale of forces involved and in duration. Operations change the physical, information, and human factors of an environment.

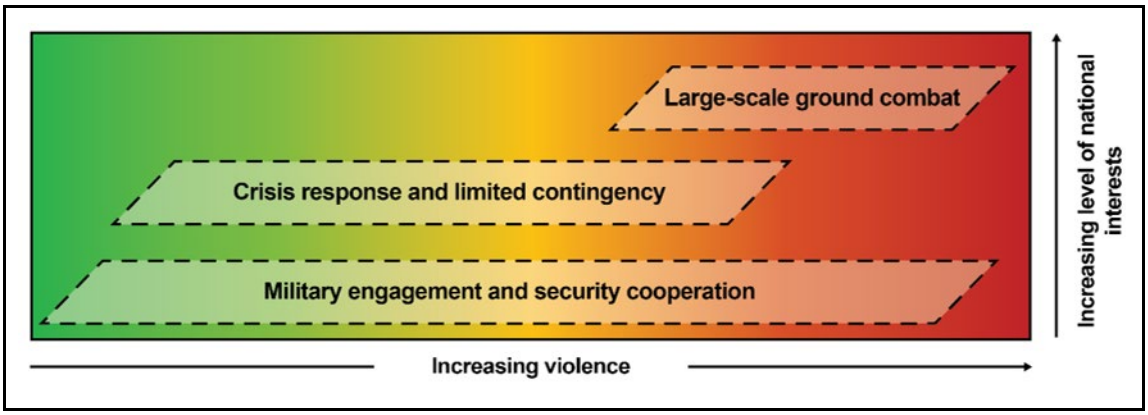


Figure 2-1. Operational categories and the spectrum of violence

2-3. All operations involve risk, and commanders must take protection into consideration across the range of military operations. The protection of combat power from the effects of threats and hazards is essential. Army forces must consider protection requirements for assets such as aerial ports of debarkation, seaports of debarkation, lines of communication, and critical infrastructure at the theater level, and for assets such as support areas, lines of communication, command posts, and signal nodes at corps and division levels.

2-4. Commanders and staffs must be able to integrate and synchronize protection capabilities and proactive measures to prevent or mitigate detection, threat effects, and hazards. When units are unable to protect themselves, commanders will coordinate with their higher echelons for support. Commanders at each echelon prioritize protection by coordinating support for and applying resources to their most critical capabilities, areas, and information.

THEATER ARMY

2-5. The theater Army's mission is the most diverse and complex of any Army echelon. It provides enabling capabilities appropriate to theater conditions, such as intelligence, sustainment, signal, fires, information activities, civil affairs, engineer, medical, and protection. Theater protection capabilities focus on protecting the joint security area and setting conditions for follow-on operations. The theater Army requires a multifunctional capability to provide operational and campaign-quality planning, synchronization, integration, and command and control of protection capabilities in support of joint forces land component command requirements during competition below armed conflict, crisis, and armed conflict. See JP 3-10 for information on theater Army joint security and protection responsibilities when the theater Army commander is designated as the joint force land component commander.

2-6. The theater Army secures and protects ports, lines of communication, critical facilities, and the flow of forces and materials. It also coordinates support with national technical capabilities (space operations, cyberspace operations, the electromagnetic spectrum) to enable protection. The theater Army facilitates the linkage to interagency and host-nation support to protect critical capabilities, areas, and information to expedite operations. The theater Army coordinates with national level assets, ensuring access to critical domain-specific technical capabilities to protect the force and operations.

2-7. Commanders in theaters with significant aerial threats require continuous land-based air defense capabilities to protect critical assets and areas. Defending the force from air and missile threats is a critical task, especially in the early phases of a major operation. Air and missile defense planning begins at the theater level and addresses the various aspects of air and missile defense capabilities and airspace requirements.

CORPS

2-8. The corps is the most versatile echelon above brigade due to its ability to operate at both the tactical and operational levels of warfare as a cohesive formation. During large-scale combat operations, a corps headquarters normally functions as a tactical headquarters under a joint or multinational land component. The corps is the echelon best positioned and resourced to achieve convergence with Army and joint capabilities. The corps shapes an operational environment and sets conditions for tactical actions by the division and lower echelons.

2-9. The corps continuously shapes operations for its divisions by attacking and countering enemy networked detection and long-range fires capabilities that threaten the divisional brigade combat team's close operations. It coordinates, integrates, synchronizes, and monitors military, civilian, joint, and multinational protection capabilities throughout the corps' area of operations. The corps secures areas, units, supplies, and activities through its protection capabilities and enabling operations and tasks, and it task-organizes protection and security capabilities to support division operations. The corps ensures that the division has engineer, military police, medical, personnel recovery, air, and missile defense, CBRN, cyberspace, electromagnetic spectrum protection, and EOD capabilities as needed.

2-10. The corps also integrates with special operations forces to deny irregular warfare in the rear areas and to identify and locate enemy systems that will affect the protection of friendly operations from the deep areas. It coordinates access to the space and cyberspace domains, electromagnetic spectrum, and information environment to overcome the adversary's information narrative, assure communications, and conduct denial activities.

DIVISION

2-11. The division is the Army's principal tactical formation during large-scale combat operations and serves as a tactical headquarters commanding brigades. It conducts operations in an area assigned by its higher headquarters—normally a corps. It task-organizes subordinate forces according to the mission variables required to accomplish its mission. A division typically commands between two and five brigade combat teams, a mix of functional and multifunctional brigades, and a variety of smaller enabling units. The division is typically the lowest tactical echelon that employs capabilities from multiple domains to achieve convergence during large-scale combat operations. Winning battles and engagements remain the division's primary purpose. As a tactical headquarters, a division uses the operational framework of deep, close, and rear operations. It shapes enemy forces in the deep area, synchronizes subordinate forces in the close area, and coordinates and protects friendly activities in the rear and subordinate support areas.

2-12. Division commanders allocate protection resources and establish protection priorities in support of the division's main and supporting efforts. Protection priorities may change with transitions or phases of an operation, but the division should preserve unity of effort throughout its area of operation at all times. Divisions conduct combined arms operations that synchronize fires with maneuver and enable brigade combat teams to rapidly exploit opportunities. In support of close operations, the division also synchronizes the maneuver of brigade combat teams with mobility, countermobility, and protection capabilities by modifying the task organization and support relationships of the units under division control. It further allocates protection capabilities such as air defense artillery, personnel recovery, and engineer and military police units to mitigate threats against the friendly forces in close and rear areas. *Air defense artillery* are weapons and equipment for actively combating air targets from the ground (JP 3-01). Protection of division rear and subordinate support areas requires planning considerations equal to those in the close areas.

BRIGADE COMBAT TEAM AND BELOW

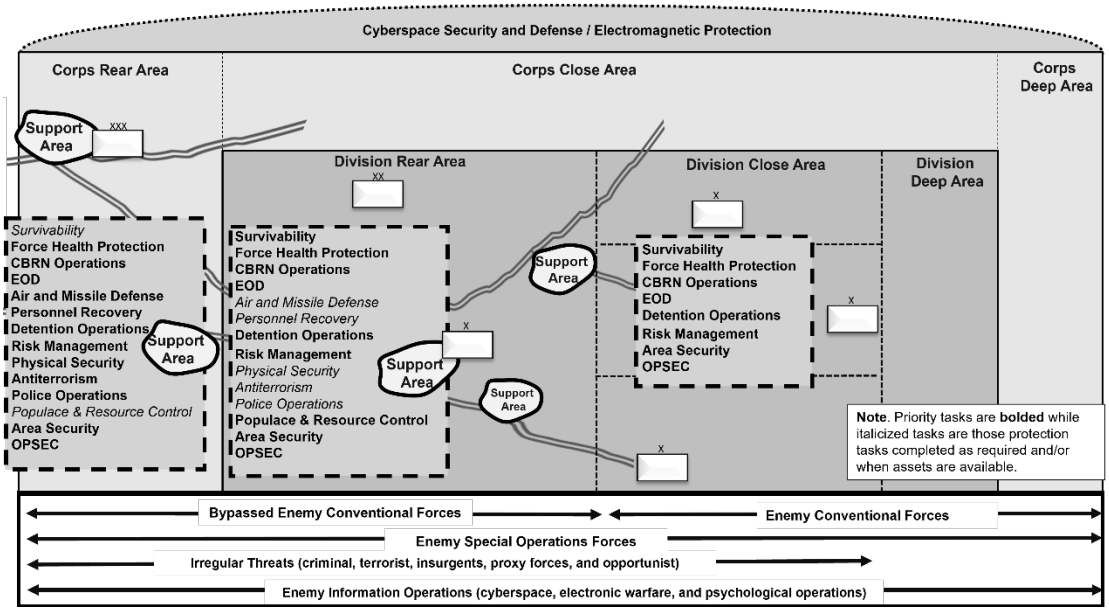
2-13. At the brigade combat team and below, each echelon takes protection measures within its capability. These measures usually include cover, concealment, and camouflage; electromagnetic control measures; and local security. Divisions use the mutual support that exists between contiguous and noncontiguous units to improve the protection of the whole formation. Divisions allocate additional required resources to the brigade combat teams that are needed for the duration of the mission based on weighting of the main effort and supporting efforts. Divisions shape the close area and corps shape deep areas to enable brigade combat teams to maneuver while preserving their freedom of action.

2-14. Brigade combat teams operate dispersed, moving, and integrating protection capabilities in a manner that takes advantage of enemy vulnerabilities to apply maximum combat power needed to achieve its objectives. The presence of the brigade combat teams during competition below armed conflict and in the transition to armed conflict provides value at preserving critical capabilities, assets, and activities at the division echelon and below.

PROTECTION WITHIN THE OPERATIONAL FRAMEWORK

Protection encompasses everything that makes Army forces hard to detect and destroy.

2-15. Commanders must emphasize the importance of planning and expanding protection priorities across the operational framework during competition below armed conflict, crisis, and armed conflict. The *operational framework* is a cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations (ADP 1-01). The coordination, synchronization, and integration of protection capabilities and resources are essential throughout the operational framework (see FM 3-94 for additional information on the operational framework). Commanders continuously assess the mission, threats, and hazards during operations and adapt protection when necessary to thwart enemy action and enable freedom of action. However, each echelon typically considers a general set of protection requirements within its area of operations (see figure 2-2).



Legend:

CBRN	chemical, biological, radiological, and nuclear
EOD	explosive ordnance disposal
OPSEC	operations security

Figure 2-2. Example of protection considerations within a corps area of operations during large-scale combat operations

2-16. At the tactical level, areas of operations are often designated and assigned based on factors in the operational environment and unit capability. Unit boundaries, fire control restrictions, and graphic control measures help create engagement areas and kill zones for friendly forces that help commanders reduce the likelihood of fratricide or accidental damage. Rules of engagement and warning systems protect the force and populations through the controlled application of lethal and nonlethal action.

2-17. An important aspect of protection planning involves the support areas. A support area is where units position, employ, and protect base sustainment assets and lines of communications required to sustain,

enable, and control operations. If conditions in the support area degrade, it is detrimental to the success of operations. A degraded support area inhibits the ability to shape the deep area for the brigade combat teams involved in close operations. Therefore, the protection of support areas requires planning considerations equal to those in the close areas.

PROTECTION DURING COMPETITION BELOW ARMED CONFLICT

2-18. Competition below armed conflict is a state of tension that exists when most of a specific adversary's national interests are incompatible with U.S. interests, and it is willing to actively pursue them. While neither side desires, at least initially, to use military force as the primary method to resolve differences, the adversary is willing to employ national instruments of power, including military forces, below the threshold of actual armed conflict to achieve its aims.

Improving protection capabilities during competition below armed conflict preserves combat power during armed conflict.

2-19. Operations during competition below armed conflict include security cooperation and military engagement that encompass training and operations to build the cohesion and large-scale combat readiness of the United States and its allies and partners. U.S. forces, allies, and partners conduct operations during competition below armed conflict with forward-stationed forces to promote mutual interests. Regionally aligned and engaged Army forces are essential to achieving objectives to strengthen the global network of multinational partners and prevent conflict. However, these forces often operate within the range of adversary capabilities and should ensure the synchronization and integration of protection.

2-20. Army operations during competition below armed conflict bring together all of the activities intended to promote regional stability and to set conditions for a favorable outcome of a military confrontation. Operations during competition are intended to deter malign adversary action, set conditions for armed conflict on favorable terms when deterrence fails, and shape an operational environment with allies and partners in ways that support U.S. strategic interests and policy aims. Commanders require an understanding of common adversary methods and objectives to effectively plan, prepare, execute, and assess protection capabilities in support of Army operations. Army forces can protect the force by understanding and effectively preventing and mitigating adversary threats and hazards.

2-21. Leaders consider protection throughout every Army operation. Military engagement and security cooperation require commanders and their staffs to consider protection measures commensurate with potential threats and hazards, even in a permissive environment. Threats and hazards may include protests, dislocated civilians, terrorist attacks, criminal and illegal activity, kidnapping, social media interference, false narratives, offensive cyberspace, electromagnetic warfare activities, and the employment of unmanned aircraft systems to collect information. Commanders and staffs mitigate and prevent threats and hazard effects by directing, coordinating, and synchronizing protection capabilities in support of Army operations during competition below armed conflict that—

- Harden key facilities, including fighting positions, bomb shelters, command and control nodes, motor pools, and other critical infrastructure that may be vulnerable during crisis and armed conflict.
- Incorporate mitigation measures to reduce operational risk to missions (risk management).
- Implement measures to enable a healthy and fit force, preventing injury and illness and protecting the force from health hazards (force health protection).

- Establish defensive measures to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian law enforcement. These programs also include personal security and defensive measures to protect Service members, high-risk personnel, civilian employees, family members, DOD facilities, information, and equipment (antiterrorism).
- Integrate physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and safeguard against espionage, sabotage, damage, and theft (physical security).
- Identify, control, and protect critical information and indicators that would allow enemies and adversaries to identify and exploit friendly vulnerabilities (OPSEC).
- Conduct security operations to protect friendly forces, lines of communications, and activities within a specific area (area security).
- Protect information networks (cyberspace and electromagnetic protection).
- Maintain a safe and secure environment by countering criminal, terrorist, and hybrid threats, reducing crime, establishing order, preserving readiness, and enforcing the Rule of Law (police operations).
- Safeguard and preserve Army resources (to include Soldiers, DA Civilians, and Army property) against accidental loss.
- Provide for public safety incidents during Army operations and activities.
- Protect civilian networks or groups identified by Army forces as critical in facilitating the provision of essential services and overall governance (populace and resources control).
- Establish security measures and deception measures to protect indigenous natural and man-made materiel resources of a nation-state, deny threats access to resources, and detect and reduce the effectiveness of criminal activity. This includes protection of U.S. assets to deny or defeat enemy and criminal activities against them (populace and resources control).
- Prepare for and execute the recovery and reintegration of isolated personnel (personnel recovery).
- Conduct activities to protect against air and missile threats, including threats from small, unmanned aircraft systems using active or passive measures (air and missile defense support).
- Correct misinformation and counter disinformation (public affairs).
- Assess threat CBRN capabilities and potential hazards.
- Implement protection measures to reduce risk (CBRN defense).

2-22. During competition below armed conflict, protection considerations also include unit home station activities, such as maintaining operational readiness, training, and contingency planning. Combined exercises and training, military exchange programs, and foreign military member attendance at Army schools are examples of home station shaping activities. At home stations, commanders employ force protection measures. These measures, along with the primary protection tasks and the synchronization and integration of the Army Protection Program, maintain safe and secure environments. They further enable commanders to generate and preserve combat power during training and deployment tasks that are associated with Army sustainable readiness requirements that are in support of multidomain operations.

FORCE PROTECTION

2-23. Military activities and operations are inherently hazardous. Commanders and leaders conducting Army operations accept prudent risks every day based on the significance of the mission, the demand of the operation, and opportunity. Commanders carefully determine risks, analyze, minimize as many hazards as possible, and accept risk to accomplish the mission. In warfare, this reality defines the sacred trust that exists between leaders and Soldiers regarding mission accomplishment and force protection.

2-24. *Force protection* is preventive measures taken to mitigate hostile actions against Department of Defense personnel (including family members), resources, facilities, and critical information (JP 3-0). A commander's inherent duty to protect the force should not lead to risk aversion or inhibit the freedom of action necessary for maintaining initiative and momentum or achieving decisive results during operations. Leaders should balance these competing responsibilities and make risk decisions based on experience, ethical and analytical reasoning, knowledge of the unit, available resources, and the situation.

2-25. During competition below armed conflict, adversaries seek to degrade and disrupt operations. Adversaries employ cyberspace attacks to inflict power outages at home station, target transportation, and pipeline networks to delay the shipment of resources, conduct social media attacks on Service or family members, and instigate protests that lower popular support for Army forces. They also employ direct action through agents, criminals, or proxies, and they have the means to employ lethal effects against Army forces within the United States.

2-26. Commanders and staffs must develop and incorporate force protection preventive measures commensurate with the level of risk. These measures must prevent or mitigate enemy and other threat actions directed against DOD personnel (to include family members and contractor personnel), resources, facilities, and critical information. Force protection must include physical security and antiterrorism measures, personnel recovery, and active information efforts to counter adversary efforts that misinform and otherwise influence Soldiers, family members, and supporting organizations.

PROTECTION IN SUPPORT OF HOMELAND DEFENSE

2-27. Commanders and staffs use information and intelligence regarding an enemy's or adversary's capabilities against personnel and resources, as well as information regarding force protection measures. Foreign and domestic law enforcement agencies can contribute to force protection through the prevention, detection, response, and investigation of crime and by sharing information on criminal and terrorist organizations. The U.S. government employs all instruments of national power to continuously detect, deter, prevent, and defeat threats to the homeland. *Homeland defense* is the protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President (JP 3-27). The strategy for homeland defense calls for defending U.S. territory against attack by state and nonstate actors through an active, globally integrated layered defense that aims to deter and defeat aggression abroad and simultaneously protect the homeland. The DOD is the lead federal agency for defending against traditional external threats or aggression (such as nation-state conventional forces or weapons of mass destruction attacks) and against external asymmetric threats that are outside of the scope of homeland security operations.

2-28. During homeland defense, Army forces work closely with federal, state, territorial, tribal, local, and private agencies to enable protection of the homeland. Homeland defense support may include support to civil law enforcement, antiterrorism, force protection, counterdrug, air and missile defense, CBRN operations, explosive hazards, and defensive cyberspace operations (see ADP 3-28, ATP 3-28.1, and JP 3-27 for additional information on homeland defense).

ARMY PROTECTION PROGRAM

2-29. The Army Protection Program complements, reinforces, and overlaps with the protection warfighting function in support of Army operations. This program is established to better manage risks relative to the safety and security of Soldiers, civilians, family members, contractors, facilities, infrastructure, and information. The Army Protection Program is the overarching framework for coordinating, synchronizing, integrating, and prioritizing policies, decisions, and resources of its primary functions, subordinate functions, and enabling functions (see figure 2-3, page 2-8).

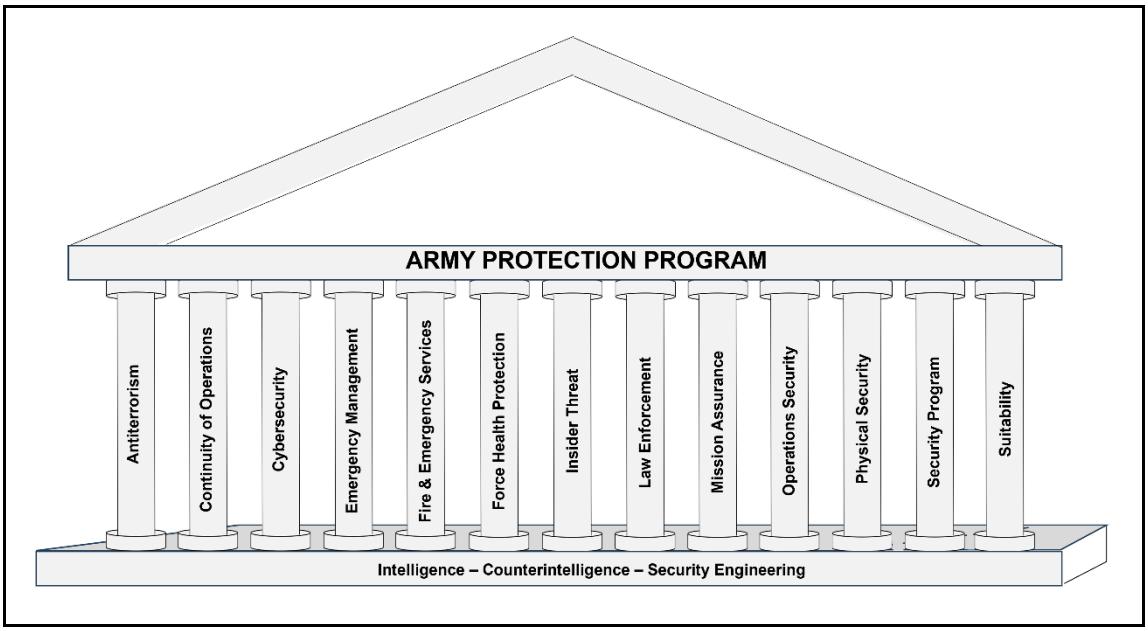


Figure 2-3. Army Protection Program

2-30. The Army Protection Program unifies the protection effort to support the execution of DOD and Army mission-essential functions. The Army Protection Program cannot eliminate the risks of threats and hazards, but it does seek to prevent, prepare for, protect against, mitigate, respond to, and recover from an event to minimize the impact to the execution of DOD and Army missions. It integrates, coordinates, synchronizes, and effectively prioritizes the efforts and resources of the Army Protection Program functions with their associated programs and processes (see AR 525-2 for additional information on the Army Protection Program).

PROTECTION DURING CRISIS

2-31. A *crisis* is an emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives (JP 3-0). A crisis can end as quickly as it begins with a return to competition below armed conflict, escalate to armed conflict, or endure for an extended period of time. A crisis occurs when an adversary takes actions, or when there are indications and warnings that an opponent is likely to do something contrary to U.S. interests that is serious enough to warrant a military response. It requires a rapid crisis response by U.S. forces to deter further actions or aggression. See FM 3-0 for additional information on operations during a crisis.

2-32. Army operations during a crisis are those activities designed to deter an adversary's undesirable actions. They are designed to prevent opportunities for the adversary to further exploit positions of relative advantage by raising the potential costs of continuing unwanted actions or aggression. Commanders are generally focused on actions to protect friendly forces, assets, and partners and to indicate U.S. intent to execute subsequent phases of a planned operation.

2-33. Army protection capabilities support operations to prevent armed conflict during mobilization, during the transit of Army forces and cargo, along movement routes, at initial staging areas, and at subsequent assembly areas where uncertain threat conditions require a delicate balance between protection and building combat power. Corps and division protection cells coordinate closely with staff personnel to identify information and assets that need protection and to apply appropriate protection and security measures consistent with the collective threat analysis.

2-34. Army operations to consolidate gains during a crisis correspond with, stabilize, and enable the civil authority phases of a joint operation. Commanders continuously consider the coordination, synchronization, and integration of protection capabilities necessary to consolidate gains and achieve the desired end state. Consolidate gains activities include populace and resources control, security cooperation, law and order reestablishment, humanitarian assistance, and critical infrastructure protection and restoration. See FM 3-0 for a discussion on consolidate gains.

FORCE PROJECTION

2-35. Force projection is particularly important during a crisis. *Force projection* is the ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations (JP 3-0). Force projection encompasses mobilization, deployment, employment, sustainment, and redeployment. Army forces project combat power from the homeland when required to augment forward stationed forces and quickly transition to set conditions for a favorable outcome.

2-36. Force projection activities do not occur out of contact with the threat. Adversary capabilities can reach the continental United States. Peer and near-peer threats possess technological capabilities in all domains, the electromagnetic spectrum, and the information environment. Enemy forces will likely detect force projection activities through space, cyberspace capabilities, and human and open-source intelligence collection efforts and enable them to conduct operations within the homeland during force projection. Adversaries target mobilization, force generation, deployment, and sustainment capabilities, including public- and private-sector enablers. They will launch cyberspace attacks against critical infrastructure and information networks to destroy or degrade command and control. See FM 3-0 for additional information on conducting deployment operations contested by a peer threat.

2-37. The coordination, synchronization, and integration of protection measures are critical during force projection activities from home station to reception in theater, and to integration into the area of operation. The efforts of Army forces to provide necessary protection effects during crisis is increasingly complex due to changing political, cultural, and technological factors and increasing private sector partners. The expanded battlefield and the complexity of the operational space also increases protection requirements. Therefore, risk management, the protection of information, the disciplined use of social media, the dispersion of forces, deception operations, antiterrorism measures, police operations, and the physical security of forces are critical planning considerations during force projection.

Predeployment Activities

2-38. Mobilization and predeployment activities begin at the home station. *Mobilization* is the process by which the Armed Forces of the United States, or part of them, are brought to a state of readiness for war or other national emergency (JP 4-05). During predeployment activities through the fort-to-port phase, the U.S. Army Installation Management Command is a critical protection and force projection enabler. Securing and protecting installations and infrastructure is essential during predeployment activities.

2-39. Installation commanders are charged with protecting deploying forces as they conduct force projection. Installation provost marshals (with military police) protect assets as the unit prepares to deploy. Safety, medical, and information management personnel protect personnel and information. Units preparing for deployment interact with the installation staff through corps and division protection cells and the installation antiterrorism working group to identify which information and assets to protect and to apply appropriate protection and security measures that are consistent with the threat analysis.

2-40. These groups and cells work as forums to involve installation protection personnel with federal, state, and local law enforcement officials. Together, they identify potential threats to the installation and improve interagency communications. Before deployment, division and corps protection cells coordinate with the installation staff to develop protective measures as required by the local threat assessments. In addition, coordination may be required with port security personnel and the combatant commander for protection requirements in the area of operations.

2-41. OPSEC and the protection of information are also key during mobilization. Effective OPSEC keeps adversaries from exploiting friendly deployment and staging information. Commanders also ensure that their rear detachment commanders and family readiness groups take appropriate OPSEC measures.

2-42. Commanders consider the antiterrorism element of protection during predeployment activities. All units, battalion and above, will have a Level II antiterrorism officer appointed in writing. This individual must have completed a service-sponsored certification course. The deploying unit commander (assisted by the antiterrorism officer) ensures that antiterrorism plans are integrated into movements through high-threat areas. Before deployment, units assess risk by conducting threat, criticality, and vulnerability assessments. Units conduct the assessments far enough in advance of deployment to allow for the development of necessary protection measures for deploying assets.

2-43. Reserve component forces have several additional considerations during mobilization. They are normally located across wide areas and are often isolated from other DOD facilities. Commanders should assess risk that may impact mobilization by conducting threat, criticality, and vulnerability assessments of their unit areas and mobilization sites. Units must ensure that OPSEC is employed to prevent threats from disrupting the mobilization process.

Movement to and Activities at the Port of Embarkation

2-44. Deploying units traditionally focus protection efforts on their impending overseas operations. However, during movement to the port of embarkation, unit commanders, unit movement section, and the protection cell rely on their installation and deployment centers to provide the latest threat assessment along the route of travel and to coordinate with law enforcement to reduce the likelihood of domestic terrorist attack or civil protest. Adversaries possess the capability to delay force projection activities through cyberspace capabilities; criminal, terrorist, or proxy forces; or disinformation. Commanders and staffs introduce the protection principles into the operations process, risk management, and mission orders to prevent or mitigate threat effects and hazards to preserve combat power and enable freedom of action. Commanders ensure safety and establish security measures by identifying rest stops, refueling locations, and safe havens along the route.

2-45. The unit commander establishes in-transit standard operating procedures to the movement order, which outlines security measures that mitigate or reduce suspected vulnerabilities during movement. The unit movement section and the protection cell reviews in-transit security requirements, helps develop the standard operating procedures, and recommends appropriate security measures for movement. The unit then files its request for movement authorization (movement credit), coordinates for security support from local authorities (as required), executes the movement once approval is obtained, and coordinates for additional security at the port of embarkation (as required).

2-46. Although transportation organizations and activities may provide limited organic protection, the deploying unit commander also plans protection measures for rail and highway movements. The unit movement section and the protection cell, in coordination with the Surface Deployment and Distribution Command, continually assesses the assets and carriers. It also provides additional protection measures consistent with the threat and sensitive-cargo requirements. These measures may include the use of contract security personnel or unit guards to protect unit assets, but the commander makes the final determination based on security requirements. The unit movement section and the protection cell coordinates with the installation transportation officer (U.S.) or movement control team (overseas) and authorized railroad or commercial truck carriers on guard and escort matters.

2-47. Protection responsibilities for Army units deploying through commercial seaports are divided among joint and interagency organizations. These organizations include the U.S. Army Materiel Command, Surface Deployment Distribution Command, Army Contracting Command, Army Sustainment Command, U.S. Transportation Command, Military Sealift Command, U.S. Northern Command, and U.S. Army Forces Command. Because the protection tasks that the Army may conduct outside its installations are limited, unit movement section and the protection cell works closely with federal, state, and local agencies. Together, they ensure that adequate protection measures exist and that they are executed during deployments through strategic seaports.

2-48. The unit movement section and the protection cell coordinate with the port readiness committee at each strategic port. These committees provide deploying unit commanders with common coordination structures for DOD, the U.S. Coast Guard, and other federal, state, and local agencies at the port level. When military equipment is being moved, the committees act as principal interfaces between DOD and other officials at ports.

2-49. In coordination with other DOD activities and port authorities, the U.S. Transportation Command and Surface Deployment and Distribution Command administer the DOD transportation security program. This program provides standardized transportation security measures, constant oversight, and central direction. In the United States, commanders plan protection measures for units and equipment enroute to the port, while the Surface Deployment and Distribution Command coordinates security at the port.

2-50. During some phases of deployment, DOD transfers custody of its military equipment to non-DOD entities, including foreign-owned ships crewed by non-U.S. citizens. The unit movement section and protection cell ensure that contract processes for transportation movements meet DOD security requirements. Table 2-1 identifies various deployment activities and the agencies responsible for them.

Table 2-1. Protection responsibilities during deployment

Activity	***Load Material***	***Protection***
Responsibility	Installation	Installation – Military Police
	Unit	Unit guards
Activity	***Transportation by Land***	***Protection***
Responsibility	Commercial rail and moving carriers	Commercial carriers
	Surface Deployment and Distribution Command	Local law enforcement
	Unit	Unit guards
Activity	***Stage Cargo and Load Vessel***	***Protection***
Responsibility	Port readiness committee	Port authority U.S. Coast Guard
	Unit	Unit guards
Activity	***Transportation by sea***	***Protection***
Responsibility	U.S. Navy	U.S. Navy
	Commercial carriers	Commercial carriers
	Maritime administration	Unit guards
Note. The unit movement section and the protection cell must assess the assets and carriers and, in coordination with the Surface Deployment and Distribution Command, provide additional protection measures consistent with threat and sensitive-cargo requirements.		

2-51. Depending on the threat assessment, units may guard equipment while at the installation, at railheads, or enroute to ports of embarkation. Units may consider assigning supercargoes with defensive capabilities to accompany the equipment during transit from the seaport of embarkation to the seaport of debarkation. The Department of the Army Criminal Investigation Division also supports force projection and protection operations by providing logistics security to prevent theft, misappropriation, and other criminal acts.

2-52. DODD 4500.09 specifies governing requirements for moving sensitive military cargo. It establishes various levels of required protection and monitoring based on risk categories. Protection and monitoring measures range from simple seals used in shipping to continuous cargo surveillance. The regulation establishes protection requirements for cargo and outlines the transportation protective services available to meet them. The cargo sensitivity and means of transportation determine how the Surface Deployment and Distribution Command protects military cargo.

Reception, Staging, Onward Movement, and Integration

2-53. Reception, staging, onward movement, and integration is the process that delivers combat power to the joint force commander in a theater of operations or a joint operations area. During crisis involving a peer adversary, this process must occur rapidly in as many dispersed locations as possible to complicate adversary targeting. It requires a logistics infrastructure provided by the host nation or deployed sustainment assets.

2-54. Reception is the first and most critical step of reception, staging, onward movement, and integration. It marks the end of the strategic leg of deployment and the beginning of the operational use of forces. Reception, staging, onward movement, and integration aims to build the combat power necessary to support the combatant commander's concept of operation. Protection for units undergoing reception, staging, onward

movement, and integration falls under the unit movement section and the protection cell of the theater supporting the combatant commander.

2-55. Planners carefully consider the threat assessment in the operational environment of reception, staging, onward movement, and integration operations. A threat assessment gives commanders details of potential threats that can disrupt, delay, or block operations. The assessment also provides the level of infrastructure transportation and protection assets available to assist with onward movement. Commanders use this information to establish their protection priorities.

2-56. When establishing protection priorities, protection planners consider how changes in the tactical situation can create an urgent need for newly arrived units. Some units may be tasked for immediate employment. Heavy-equipment transport, military police, engineers, fuel support, and other assets necessary to move or protect equipment and personnel may become critical to mission success.

2-57. In a permissive environment, the host nation may be able to provide services and facilities to support protection. These services can lessen the requirement for U.S. forces to provide equivalent capabilities, thereby reducing the U.S. logistics footprint.

2-58. Reception, staging, onward movement, and integration operations can provide enemies with numerous opportunities to inflict serious casualties. These operations can delay the buildup of combat power by exploiting the vulnerability of units in transit from the theater staging base to the theater assembly area.

2-59. Units undergoing reception, staging, onward movement, and integration present enemies with high-value, high-payoff targets. Any damage or destruction could result in serious delays in force closure. Military police, air defense artillery, or other forces designated for area security become critical targets. Air defense artillery forces add a layer of protection against enemy air surveillance and attack platforms. Advanced deployment of CBRN capabilities may be required to mitigate CBRN hazards (see ATP 3-35 and JP 3-35 for a discussion of factors and considerations associated with the conduct of reception, staging, onward movement, and integration).

TRANSITION

2-60. There are two outcomes of a crisis; a de-escalation to competition below armed conflict or an escalation to armed conflict. If Army forces are successful in deterring armed conflict as part of larger joint force and national efforts, the Army should seek to improve its positions of relative advantage to increase its ability to compete. This increased ability to compete will help national and joint leaders deter further aggressive acts. As part of this effort, the Army should anticipate the need to maintain an enhanced force posture for a period of time after the crisis to assure allies and demonstrate resolve to adversaries (see FM 3-0 for discussion on transition back to competition or armed conflict).

2-61. Commanders, the unit movement section, and protection cells develop a scheme of protection for the transition of each phase of an operation or major activity. Transitions mark a change of focus between phases or between the ongoing operation and execution of a branch or sequel. Shifting protection priorities between offensive, defensive, and stability operations also involves a transition. Transitions require planning and preparation well before their execution so that a force can maintain the momentum and tempo of operations. A force is vulnerable during transitions. Commanders and staffs identify potential threats and hazards during planning and identify protection priorities during transition and follow-on operations.

PROTECTION DURING ARMED CONFLICT AND LARGE-SCALE COMBAT OPERATIONS

2-62. Armed conflict encompasses the conditions of a strategic relationship in which opponents use lethal force as the primary means for achieving objectives and imposing their will on the other. During armed conflict, operations can reflect combinations of irregular warfare and conventional warfare. Irregular warfare can include counterinsurgency and unconventional warfare. Leaders apply the doctrine of large-scale combat operations during limited contingencies that require conventional warfare approaches (see ADP 3-05 for more information on irregular warfare, see ATP 3-05.1 for more information on unconventional warfare, and see FM 3-24 for more information on counterinsurgency).

2-63. Large-scale combat operations are the focus of Army readiness. They are extensive joint combat operations in terms of the scope and size of forces committed and the destructive violence involved. Large-scale combat introduces levels of complexity, lethality, ambiguity, and speed to military activities not common in other operations. The high tempo of large-scale combat operations creates gaps and seams that generate both opportunities and risks as enemy formations disintegrate or displace.

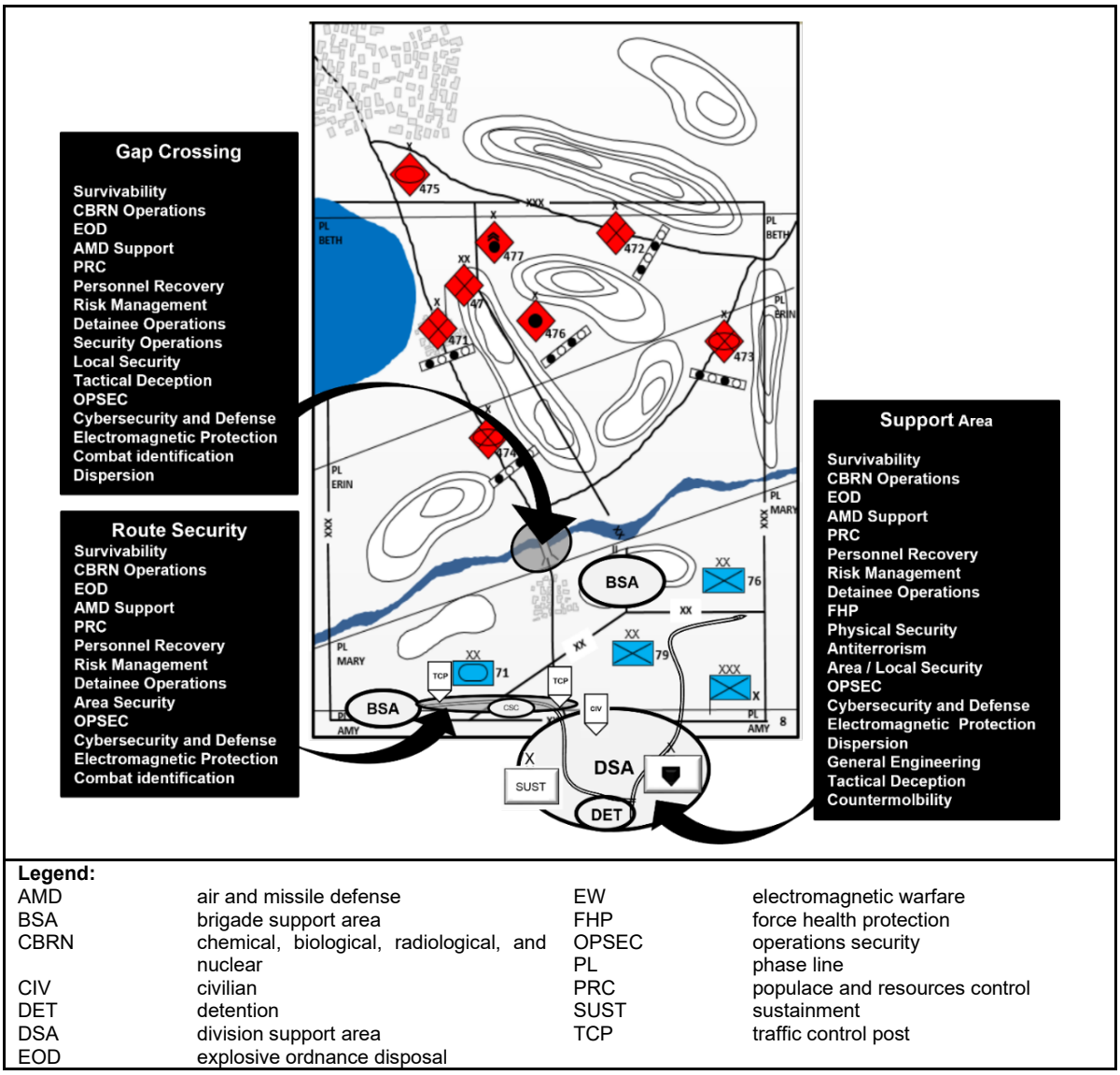
2-64. Large-scale combat operations occur in circumstances usually associated with state-on-state conflict, and they include combat between large formations of divisions and corps operating in all domains. A peer enemy can contest the joint force during large-scale combat. Their integrated air defense and long-range fires systems; cyberspace and electromagnetic warfare capabilities; CBRN weapon capabilities; and intelligence, surveillance, and reconnaissance networks can create parity across all domains. Army forces focus on the defeat and destruction of enemy ground forces as part of the joint team during large-scale combat operations and continuously consolidate gains to accomplish objectives that support a desirable political outcome.

2-65. During large-scale combat operations Army leaders must anticipate that joint support will be limited and must use a combination of measures to protect the force. Commanders and staffs deliberately plan and integrate protection capabilities to preserve combat power, mitigate identified vulnerabilities, and exploit opportunity.

2-66. Protection can be derived inherently from combat operations (such as security operations), or it can be deliberately applied as commanders direct, coordinate, and synchronize tasks and systems that comprise the protection warfighting function to apply maximum combat power. Leaders also implement protection measures to complicate the targeting of their units during armed conflict by moving irregularly, using camouflage, and maintaining dispersion. They coordinate, synchronize, and integrate enabling operations and enabling tasks with the primary protection tasks to prevent or mitigate detection, threat effects, and hazards.

2-67. Information activities throughout the range of military operations may deter enemy actions, prevent escalation of tensions, and prevent the civilian populace from participating in a resistance when a military intervention occurs. Effective information activities are essential to protection efforts from competition below armed conflict to conflict to ensure the protection of the force and the protection of the populace.

2-68. Commanders continuously direct, coordinate, and synchronize protection capabilities necessary to consolidate gains and achieve the desired end state (see figure 2-4, page 2-14). Protection capabilities are focused on security tasks to stabilize the area and protect the force, routes, sustainment assets, and critical infrastructure. Consolidate gains activities also include minimum-essential stability operations tasks (populace and resources control, detainee operations, law and order reestablishment, foreign humanitarian assistance, and critical infrastructure protection and restoration).



Legend:			
AMD	air and missile defense	EW	electromagnetic warfare
BSA	brigade support area	FHP	force health protection
CBRN	chemical, biological, radiological, and nuclear	OPSEC	operations security
		PL	phase line
CIV	civilian	PRC	populace and resources control
DET	detention	SUST	sustainment
DSA	division support area	TCP	traffic control post
EOD	explosive ordnance disposal		

Figure 2-4. Notional protection measures during large-scale combat operations

Operations and Tasks That Enable Protection During Armed Conflict and Large-Scale Combat Operations

2-69. As part of combined arms operations, commanders and staffs synchronize operations and tasks from other warfighting functions that complement and reinforce protection of critical assets. Below is a list of operations and tasks that enable protection:

- Security operations.
- Countermobility.
- Tactical deception.
- Intelligence support to protection.
- Combat identification/fratricide avoidance
- General engineering.
- Local security.
- Countering explosive hazards.

- Forensics and biometrics.
- Army space operations.

Security Operations

2-70. One of the most common methods of providing protection for ground combat forces during Army operations is through security operations. *Security operations* are those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy, and to develop the situation to allow commanders to effectively use their protected forces (ADP 3-90). The ultimate goal of security operations is to protect the force from surprise and reduce the unknown in any situation. The protected force may not always be a military force; it can also be a civilian population, civil institutions, and civilian infrastructure in the unit's area of operations. The following are four types of security operations:

- *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).
- *Cover* is a type of security operation done independent of the main body to protect them by fighting to gain time while preventing enemy ground observation of and direct fire against the main body (ADP 3-90).
- *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).
- *Screen* is a type of security operation that primarily provides early warning to the protected force (ADP 3-90).

2-71. Commanders use all four types of security to protect the force during operations; however, screen, guard, and cover are typically associated with combat formations specifically organized for combined arms operations. For this reason, screen, guard, and cover tasks are under the movement and maneuver warfighting function, while area security is a primary task within the protection warfighting function.

2-72. Area security operations usually focus on the formation, asset, or location they are protecting and do not normally focus on the enemy force. Area security operations take advantage of the various local security measures being performed by all units in the area of operations.

2-73. Cover, guard, and screen operations reflect increasing levels of protection that require different levels of combat power. The primary purpose of a screen operation is to provide early warning, thereby preventing surprise. Screens provide less protection than guards or covers. Screen missions are defensive, and they are accomplished by establishing a series of observation posts and patrols to ensure observation of the assigned area of operations. Military police are also capable of conducting a screen in support of operations throughout the rear area. Guard and cover operations involve maneuver forces in combat, fighting to gain time with differing levels of capability and autonomy for independent action (see ATP 3-90.8 for additional information on security operations).

Countermobility

2-74. The primary purposes of countermobility are to shape enemy movement and maneuver and to prevent the enemy from gaining a position of advantage. *Countermobility* is a set of combined arms activities that use or enhance the effects of natural and man-made obstacles to prevent the enemy freedom of movement and maneuver (ATP 3-90.8). Subsequently, countermobility supports the execution of offensive and defensive tasks and enables a commander's ability to protect critical capabilities, areas, and information.

2-75. In support of offensive tasks, countermobility is conducted to isolate objectives and prevent enemy forces from repositioning, reinforcing, and counterattacking. It is also conducted to enable flank protection as the fight progresses into the depth of enemy defenses to provide general flank security as an integrated economy-of-force effort. Countermobility tasks may be required to defend a lodgment and protect selected sites and positions from which combat power must be generated and sustained, such as a staging area or a base or base cluster in the support area.

2-76. In support of defensive tasks, countermobility is conducted to disrupt enemy attack formations and assist friendly forces in defeating the enemy in detail, channel attacking enemy forces into an engagement

area or areas throughout the depth of the defense, and protect the flanks of friendly counterattack forces. They are also conducted to shape engagements, maximize the effects of fires, and provide close-in protection around defensive positions to help defeat the final assault of the enemy and to prevent and warn of intrusion into critical fixed sites such as tactical assembly areas, base camps, base clusters, and sustainment sites (see ATP 3-90.8 for additional information on countermobility).

Tactical Deception

2-77. Tactical deception can be a key aspect of protection. *Tactical deception* is a friendly activity that causes enemy commanders to take action or cause inaction detrimental to their objectives (FM 3-90). Commanders conduct tactical deception to influence military operations to gain a relative, tactical advantage over the enemy; obscure vulnerabilities in friendly forces; and enhance the defensive capabilities of friendly forces. When commanders integrate OPSEC and other information-related capabilities, tactical deception can be a decisive tool in altering how the enemy views, analyzes, decides, and acts in response to friendly military operations and can potentially yield large payoffs for friendly forces on the battlefield. These payoffs include reducing operational risk to the force and preserving combat power (see FM 3-13.4 for additional information on military and tactical deception).

Intelligence Support to Protection

2-78. Intelligence supports operations and enables commanders and staffs to have situational understanding of the threat, terrain and weather, civil considerations, and other aspects of the operational environment. The use of intelligence to see and understand each domain can reduce the risk to friendly forces and enhance success during chaotic and high-tempo operations. Situational understanding enables commanders and staffs to implement protection measures that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action (see ADP 2-0 for additional information on intelligence).

2-79. Intelligence support to protection enables commanders to plan, integrate, and synchronize protection capabilities to mitigate detection and the effects of threats and hazards from enemy forces. It also provides intelligence that supports recovery from threat actions. Intelligence support includes analyzing the threats, hazards, and other aspects of an operational environment and utilizing the intelligence preparation of the operational environment process to describe the operational environment and identify threats and hazards that may impact protection. Intelligence support develops and sustains an understanding of the enemy, terrain and weather, and civil considerations that affect the operational environment (see Chapter 3 for more information on protection planning).

Information Collection

2-80. Information collection can complement or supplement protection tasks. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations (FM 3-55). Through information collection, commanders and staffs continuously plan, task, and employ collection assets and forces. These forces collect, process, and disseminate timely and accurate information to satisfy the commander's critical information requirements (CCIRs) and other intelligence requirements. When necessary, information collection assets (ground, air, and space-based reconnaissance and surveillance activities) focus on special requirements, such as personnel recovery (see FM 3-55 for additional information on information collection).

Counterintelligence

2-81. Army counterintelligence serves as an integral part of the multidiscipline approach to intelligence operations, with the goal of facilitating situational understanding and supporting the commander's decision making. It detects, identifies, deters, disrupts, exploits, or neutralizes foreign intelligence entity ability to conduct intelligence collection and terrorist activities against the United States. *Counterintelligence* is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (JP 2-0).

2-82. Commanders make decisions on acceptable risk and provide guidance to employ protection capabilities and resources. Counterintelligence elements perform various assessments to support protection planning. As the subject matter experts for foreign intelligence entities collection and targeting capabilities, counterintelligence special agents are integral in developing protection assessments. These assessments are used to determine foreign intelligence entities capabilities, friendly force vulnerabilities, protection prioritization, countermeasures, and available resources to protect critical assets (see ATP 2-22.2-1 for additional information on counterintelligence).

Combat Identification/Fratricide Avoidance

2-83. Supporting commands conduct combat identification before and during target engagement. The destructive power and range of modern weapons, coupled with the high intensity and rapid tempo of large-scale combat operations, increase the potential for fratricide. ***Fratricide*** **is the unintentional killing or wounding of friendly or neutral personnel by friendly firepower.** The primary preventive measures to limit friendly fire incidents are combat identification training, command emphasis, disciplined operations, coordination measures, close coordination among component commands, rehearsals, reliable and interoperable coordination systems, battle tracking, and enhanced situational awareness. Risk management is also fully integrated with planning and executing operations. Commanders identify and assess situations that increase the risk of friendly fire incidents.

2-84. Combat identification gives U.S. forces the ability to avoid fratricide and differentiate among friendly, enemy, neutral, and unknown personnel and objects. *Combat identification* is the process of attaining an accurate characterization of detected objects in the operational environment sufficient to support an engagement decision (JP 3-09). Units achieve combat identification by applying situational awareness and target identification capabilities and by adhering to doctrine, tactics, techniques, and procedures and approved rules of engagement that directly support a Soldier's engagement decision against objects in an operational environment. Combat identification attempts to avoid fratricide and unnecessary collateral damage. Proper identification provides an accurate characterization of potential targets to allow engagement decisions to be made with high confidence. Combat identification is not hardware-dependent; its capability combines the following:

- **Situational awareness.** Situational awareness provides the immediate knowledge of operation conditions, constrained geographically and in time.
- **Target identification.** Target identification provides the accurate and timely characterization of detected personnel and objects as friendly, neutral, enemy, or unknown. It is time-sensitive and directly supports a Soldier's target engagement decision. Quick and accurate target identification involves training and technology to maximize correct identification.
- **Doctrine.** Sound doctrine provides a source of shared understanding and enables interoperability. This knowledge directly contributes to a Soldier's ability to distinguish between friendly, neutral, or enemy.
- **Tactics, techniques, and procedures.** Tactics, techniques, and procedures for combat identification provides Soldiers the ability to identify a target, engage it while maintaining awareness of unknown targets, and avoid fratricide. Inadequate tactics, techniques, and procedures or the failure to rehearse them can cause hesitation, fratricide, and unnecessary collateral damage.
- **Rules of engagement**. *Rules of engagement* are directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered (JP 3-84). The rapid, accurate identification of potential targets is critical to the rules of engagement. Rules of engagement are standardized throughout the area of operations to comply with higher headquarters guidance. If too restrictive, rules of engagement could reduce combat effectiveness and put the force at greater risk. However, if rules of engagement are too lax, they can lead to unnecessary collateral damage and fratricide. The greater the Soldier's ability to distinguish unknown personnel and objects as friendly, neutral, or enemy, the less restrictive the rules of engagement become. The military authority developing the rules of engagement should consider combat identification capabilities when defining engagement criteria.

General Engineering

2-85. General engineering is an engineer discipline primarily focused on providing construction support. *General engineering* consists of those engineering capabilities and activities, other than combat engineering, that provide infrastructure and modify, maintain, or protect the physical environment (JP 3-34). It supports the commander's ability to protect critical capabilities, areas, and information against detection, threats, hazards, and military weapons effects. General engineering also enables protection with structural damage surveys and vulnerability and protection assessments at fixed facilities and forward-deployed sites.

2-86. General engineering enhances and supports protection measures associated with area security, antiterrorism, survivability, detention operations, physical security, and risk management through the planning, design, construction, maintenance, and hardening of facilities (see ATP 3-34.40 for additional information on general engineering). General engineering tasks in support of protection may include—

- Constructing field fortifications.
- Hardening critical infrastructure and facilities.
- Preparing protective positions.
- Emplacing protective obstacles around critical fixed sites, such as tactical assembly areas, base camps, base clusters, and sustainment sites.

Local Security

2-87. Local security measures performed by all units (regardless of their location) and support area security activities should be linked to the broader area security activities. *Local security* is the low-level security activities conducted near a unit to prevent surprise by the enemy (ADP 3-90). It is closely associated with unit force protection efforts and is typically performed by a unit for self-protection, but it may also be provided by another unit when the security requirements are greater than the unit security capabilities.

2-88. Local security includes any local measure taken by units that protect against threat actions. It involves avoiding enemy detection or deceiving the enemy about friendly positions and intentions. Local security prevents a unit from being surprised, and it is an important part of maintaining the initiative. The requirement for maintaining local security is an inherent part of all operations.

2-89. Units use active and passive measures to provide local security. Active patrolling and continuous reconnaissance are active measures that help provide local security. Passive measures include using camouflage, movement control, noise and light discipline, proper communications procedures, ground sensors, night-vision devices, and daylight sights. Commanders also avoid enemy detection by maintaining physical dispersion, concealing electromagnetic-based signatures through deliberate emission control procedures, and developing and implementing counter-small, unmanned aircraft system techniques.

Dispersion

2-90. Commanders can employ many ways to achieve dispersion. At the operational level, commanders maintain dispersion by employing multiple staging areas and multiple lines of communication. At the tactical level, commanders maintain dispersion by increasing the distance between subordinate formations and among the elements in those formations. In the attack, they use multiple routes and longer march intervals between formations to the objective and only concentrate forces enough to mass effects or generate favorable force ratios during close combat. In the defense, formations maximize dispersion by using terrain and employing the maximum supporting ranges and distances within acceptable risk criteria.

Electromagnetic Emissions Control

2-91. Army forces employ many capabilities that emit electromagnetic radiation that can be detected and targeted by enemies. Peer threats have well-developed capabilities to locate electromagnetic signatures of command posts, sensors, vehicles, and weapon platforms using ground-based or manned or unmanned aerial electromagnetic warfare platforms. Observable signatures increase an enemy's likelihood of successfully detecting, collecting information about, and targeting units and critical command and control nodes. As risk to the force increases, leaders increase the level of their electromagnetic control measures.

2-92. Commanders and staffs select electromagnetic hardening measures, electromagnetic masking techniques, electromagnetic spectrum operations, and emission control procedures that minimize the unit's electromagnetic signature. Commanders must also consider the use of personal electronic devices by Soldiers, such as smart phones, that present significant OPSEC risks. Enemies and adversaries may target personal electronic devices for information warfare activities or to locate friendly units. Recent experience shows that personal cell phones and electronic smart devices present a serious vulnerability. To mitigate these vulnerabilities, commanders should consider plans to ban cell phone use, or even confiscate personal electronic devices before operations during crisis and armed conflict (see ATP 3-12.3 for more information about electromagnetic protection).

Counter-Small Unmanned Aircraft Systems

2-93. Adversaries will use commercial-off-the-shelf unmanned aircraft systems to gain a tactical advantage over U.S. forces. During local security, commanders account for enemy capabilities and likely reconnaissance objectives as they develop their counter-small, unmanned aircraft systems plan. Commanders and leaders implement techniques and procedures for countering enemy small, unmanned aircraft systems based on their organic capabilities, attached capabilities, and the mission variables.

2-94. Commanders must ensure that their Soldiers are appropriately trained and equipped and that they understand counter-small, unmanned aircraft system operations. This understanding should translate into a quick reference guide or precombat checklist to focus the unit on these operations. A technique that may be established at unit level is to identify Soldiers to act as observers (air guards) throughout all phases of an operation. Local security is complemented by employing observer techniques. An observer assists with mitigating the threat of unmanned aircraft systems' capabilities to conduct reconnaissance, surveillance, and intelligence-gathering operations and their execution of attacks on friendly forces.

2-95. Units must avoid detection and observation from small, unmanned aircraft systems. If a small, unmanned aircraft system is detected near a unit position, the unit is likely compromised and under enemy observation. Within constraints of the rules of engagement and weapons control status, units should attempt to engage and destroy the unmanned aircraft system while simultaneously displacing. Units may use small arms fires and other organic means and implement other passive defensive measures. In some cases, units may be equipped with counter-small, unmanned aircraft capabilities to identify and defeat small, unmanned aircraft. These capabilities may include electromagnetic and/or direct fire capabilities (see ATP 3-01.8 and ATP 3-01.81 for additional information on counter-small, unmanned aircraft systems).

Countering Explosive Hazards

2-96. Countering explosive hazards reduces casualties and damage and enables the commander's freedom of action. An *explosive hazard* is any material posing a potential threat that contains an explosive component (JP 3-15). Engineers and EOD enhance protection through the execution of countering explosive hazards. Engineers enhance protection through route clearance patrols, and breeching and clearing obstacles enables freedom of movement and maneuver. EOD enhances protection through the identification, render safe, exploitation, and disposal of explosive hazards, weapons systems, and related materiel. Countering explosive hazards by render-safe procedures allows for the development of tactics, techniques, and procedures to counter the threat and the technical and forensic exploitation to obtain information to support targeting, improve force protection, identify material sourcing, and classify different weapon signatures (see ATP 4-32 for additional information on EOD's role in countering explosive hazards).

Forensics and Biometrics

2-97. Forensics, biometrics, and document and media exploitation provide the foundation for identity intelligence contributing to the discovery of unknown potential threat actors and associate individual actors to other persons, places, and events. Additionally, forensically derived information and biometric data can feed answers to commanders' critical information gaps. The joint force has employed forensics for decades through site exploitation, document and media exploitation, technical exploitation, and cyber forensics. Today, forensic and biometric techniques and technologies are used to bolster protection and directly support Army operations.

- **Antiterrorism, physical security, and risk management.** Forensics and biometrics can help identify known and potential threats to people or facilities. This enables proactive posture and more robust antiterrorism, physical, operational, and area security measures and countermeasures.
- **Police and detention operations.** Collected forensic and biometric information supports criminal investigations and prosecutions by providing material evidence attributing a person to a crime. Forensics also supports criminal intelligence in identifying offenders and networks, war crimes, crimes against humanity, and crimes committed by enemy combatants, criminal actors, or insider threats.
- **Force health protection and populace and resources control.** Forensics and biometrics supports medical findings and identification of remains through the Armed Forces Medical Examiner System, and also enhances preventative medical countermeasure decisions related to potential epidemics, known or potential disease threats, and emerging diseases. Additionally, forensics and biometrics can be employed to identify and account for civilians during humanitarian assistance, disaster relief operations, and noncombatant evacuation operations.
- **Personnel recovery.** Forensics and biometrics, in conjunction with planning efforts, can be used to identify people, attribute a person to a location, determine a person's medical/physical condition, better prepare rescue efforts, and develop a timeline and sequence of events leading to the time of isolation.
- **Survivability.** Forensic material collection and exploitation can provide information for prevention and mitigation strategies and ensure appropriate levels of protection against CBRN and other threats.
- **Cyberspace security and defense.** Forensics supports the range of cyberspace operations, including offensive and defensive operations, intrusion detection, tracking, targeting, and attribution. This may include counter-unmanned aircraft systems and remote operator tracking.
- **Intelligence support.** Forensic and biometric information injects vital data and identity information, which can be analyzed and organized into knowledge, facilitate action against threats and networks, and enable corresponding action.
  - **Counterintelligence and human intelligence.** Forensics and biometrics supports the collection and aggregation of information that feeds and influences various intelligence activities such as interrogations, surveillance, sourcing, and targeting. Forensically derived information and biometric identification may be used to establish profiles, patterns of life, vulnerabilities, risk matrices, target values, and other operationally relevant packages.
  - **Targeting.** Forensics and biometrics provides accurate information on threats to inform joint targeting processes. Forensics information details physical, functional, cognitive, and environmental characteristics of threats in support of joint targeting.

ARMY SPACE OPERATIONS

2-98. Army space operations provide Army and joint forces with a global combat advantage by using highly technical capabilities to create multiple dilemmas for threat actors on the battlefield. Army operations rely on the advantages provided by space capabilities and effects to enhance the effectiveness of combat forces. Space capabilities permit enhanced situational understanding; provide global communications; enable precise and accurate fires; support the conduct of joint expeditionary entry, movement, and maneuver operations; enable protection; and provide a conduit for cyber electromagnetic operations in support of Army operations (see FM 3-14 for additional information on space operations).

2-99. During large-scale combat operations, space capabilities enhance the Army's ability to communicate, navigate, accurately target the enemy, protect, sustain our forces, and enable intelligence preparation of the operational environment. While the Army is dependent on Army space operations, it is sometimes difficult to observe the effects or direct impact of space operations because the desired effect may be difficult to observe. Space operations enable protection by—

- Informing friendly forces of adversary satellites when they are in position to view and record ground activity.
- Assisting in personnel recovery operations.
- Identifying threats such as minefields, obstacles, and other potential hazards.

- Providing timely dissemination of friendly force unit locations and dispositions, which prevents fratricide.
- Identifying space-based missile launch locations, predicting missile impact points, and warning forces within the footprint of the predicted impact area to take protective actions.
- Assisting in the determination of scatter patterns for chemical, biological, and radiological agents and in the modeling of hazard predictions based on weather and terrain models.
- Identifying potential decontamination sites, water sources, drainage areas, routes, cover and concealment, and imagery of environmental disasters.
- Providing surveillance and reconnaissance, enabling access to denied areas.

PROTECTION CONSIDERATIONS DURING THE DEFENSE

Types of Defensive Operations:
- **Area defense**
- **Mobile defense**
- **Retrograde**

2-100. A *defensive operation* is an operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations (ADP 3-0). The inherent strengths of the defense are the defender's ability to occupy positions before an attack and to use the available time to improve those defenses. A defending force stops improving its defensive preparations only when it retrogrades or begins to engage enemy forces. A defending force continuously takes opportunities afforded by lulls in action to improve its positions and repair combat damage during execution of the defense. Characteristics of the defense include disruption, flexibility, maneuver, mass and concentration, depth, preparation, and security.

2-101. A defending force preserves control over land, resources, and populations and protects lines of communications and critical capabilities against attack. Commanders can use the defense to gain time and economize forces so that offensive operations can be executed elsewhere. A defending force—

- Creates conditions for the offense that allows Army forces to regain the initiative.
- Retains decisive terrain or denies a vital area to an enemy.
- Attrits or fixes an enemy as a prelude to the offense.
- Increases an enemy's vulnerability by forcing an enemy commander to concentrate subordinate forces.

2-102. Regardless of which defensive operation is performed (area, mobile defense, or retrograde), the survivability of command and control systems and key communications nodes in the defense is critical to its success. Survivability and antiterrorism tasks and plans are essential during the defense and may require a deliberate and detailed approach to ensure that combat power is apportioned where it is most needed. Commanders may use decision support tools and analysis to assess critical assets and key vulnerabilities (see FM 3-0 for additional information on defense).

Survivability

2-103. Defensive operations typically demand the most effort and resources for survivability. Activities in the defense include constructing survivability positions for critical assets such as command posts, artillery and air defense artillery systems, and equipment and supplies. Soldiers prepare individual and crew-served fighting positions and combat vehicle fighting positions. Survivability efforts must consider conventional threats (direct and indirect fires and unexploded ordnance) and unconventional threats (suicide bombings, vehicle-borne improvised explosive devices, unmanned systems, and CBRN hazards). The relative amount of survivability effort placed against these threats depends on the threat analysis and available resources.

2-104. Area defensive patterns require the placement of obstacles and the deliberate development and preparation of fighting and support-by-fire positions, engagement areas, and kill zones. Units emplace obstacles and harden defensive positions with overhead protection. Both thermal sheeting and overhead cover are critical to survivability. Engineer personnel and units have additional capabilities to support such tasks. They also assure the mobility of striking forces that support mobile defenses and reserve forces that support area defensive plans (see Appendix A for additional information on survivability).

Air and Missile Defense

2-105. In the defense, air defense artillery forces optimize the protection of Soldiers by providing coverage over designated critical assets. They proactively engage air and missile threats before they attack or surveil. Dedicated air defense artillery forces perform other tasks in the defense such as providing and disseminating early warning and situational awareness of the airspace and contributing to targeting information by determining and reporting enemy missile launch and impact points.

2-106. Air defense artillery commanders integrate air defense artillery sensors and certain intelligence capabilities into a comprehensive network to provide effective early warning of an aerial attack to friendly forces. They develop or contribute to an airspace control plan that assists friendly forces in identifying and engaging enemy aerial targets and protecting friendly air assets. The deployed air and missile defense systems defend friendly forces and critical assets from aerial attacks. Commanders enforce the employment of passive air and missile defense measures in support of survivability efforts (see Appendix A for additional information on air and missile defense).

Chemical, Biological, Radiological, and Nuclear Operations

2-107. Units develop, train, and rehearse a CBRN defense plan to protect personnel and equipment from CBRN threats or hazards. CBRN threat assessments help determine initial, individual protective equipment levels and the positioning of decontaminants. Force health protection personnel conduct medical surveillance of personnel by monitoring strength information for anomalies in force health trend data.

2-108. Defensive operations also provide the enemy or sympathizers the opportunity to release toxic industrial materials in proximity to U.S. forces. A survey of local toxic industrial material storage that assesses the potential for intentional or inadvertent release is a key element of CBRN defense (see Appendix A for additional information on CBRN operations).

Electromagnetic Protection

2-109. Electromagnetic protection remains constant during defense. Electromagnetic protection is a command responsibility, but it is only effective when everyone in an organization understands its importance and can readily identify opportunities to implement protection activities. Electromagnetic operations also applies to offensive operations and stability (see Appendix A, ATP 3-12.3, and FM 3-12 for additional information on electromagnetic protection operation and techniques).

Area Security

2-110. In the defense, commanders protect forces and critical assets by conducting area security operations. Forces conducting area security in the defense can deter, detect, or defeat enemy reconnaissance while creating standoff distances from enemy direct- and indirect-fire systems. Area security operations can be used to protect the rapid movement of combat trains or to protect cached commodities until needed (see Appendix A for additional information on area security).

Operations Security

2-111. Effective and disciplined OPSEC protects essential elements of friendly information, mitigating enemy reconnaissance and other information collection capabilities from gaining an advantage through identifiable or observable pieces of friendly information or activities. This is key to maintaining essential secrecy and preventing surprise during defensive operations. OPSEC, cyberspace, and electromagnetic warfare activities work together to deny the enemy access through emission control; however, they do so from slightly different angles.

2-112. Electromagnetic protection capabilities control these emissions and prevent an attacking enemy from using the electromagnetic spectrum to degrade, neutralize, or destroy friendly combat capabilities. During OPSEC, the emissions can be considered indicators. Indicators are data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities (see JP 3-13.3). From an adversary perspective,

friendly forces can establish signatures, associations, profiles, contrasts, and exposure, which are types of indicators (see Appendix A and ATP 3-13.3 for additional information on OPSEC).

Cybersecurity and Defense

2-113. The network allows commanders to leverage information to gain understanding of the operational environment, influence behavior, support decision making, and synchronize warfighting functions. The Army secures and defends the network through a defense-in-depth approach, incorporating layered security and defenses. Cyber security and defense also applies to offensive operations and stability. (see Appendix A and FM 3-12 for additional information on cybersecurity and defense).

Explosive Ordnance Disposal Support

2-114. During defensive operations, EOD provides support through the identification, exploitation, and disposal of explosive ordnance and weapons systems threatening critical infrastructure, terrain, materiel, and nodes necessary for force generation, to consolidate gains, and prepare for future operations. *Explosive ordnance* is all munitions and improvised or clandestine explosive devices, containing explosives, propellants, nuclear fission or fusion materials, and biological and chemical agents (JP 3-42). Based on METT-TC (I), defensive operations provide time and resources for EOD to—

- Conduct deliberate exploitation of counterexplosive captured enemy ammunition and weapons systems.
- Render safe and dispose of unexploded ordnance preventing sustainment of friendly materiel.
- Perform limited clearance operations required to improve movement.
- Perform hasty clearance of critical terrain, facilities, and nodes required for current or future support areas, command and control nodes, and other operations (see Appendix A and ATP 4-32 for additional information on EOD support).

Personnel Recovery

2-115. Personnel recovery moderates the loss of personnel and capabilities due to combat operations, isolating events, accidents, health threats, hazards, and natural disasters during the defense. This creates a reactive posture, while personnel recovery provides support to operations that did not go as planned. Personnel recovery also applies to offensive operations and stability (see Appendix A for additional information on the personnel recovery).

Detention Operations

2-116. Commanders must be prepared to capture detainees in the defense. The treatment and proper handling of detainees can directly affect mission success and could have a lasting impact on U.S. strategic military objectives. All Soldiers must follow the fundamental principles of detainee operations (see Appendix A and FM 3-63 for additional information on detention operations).

Populace and Resources Control

2-117. Actual conflict or fear of conflict could cause civilians to leave their homes or places of habitual residence. The first objective is to implement an integrated plan to inform, influence, and control civilian movement to ensure that they do not impede the movement and maneuver of military forces and to protect them from avoidable hazards. Populace and resource control also applies to offensive operations and stability (see Appendix A for additional information on populace and resources control).

Force Health Protection

2-118. Defensive operations could potentially have dramatic results on the mental and behavioral health of unit personnel. Soldiers can become combat-ineffective due to the close proximity of heavy direct and indirect fire, even if exposure is only for a short duration. Systems for combat stress identification and treatment are deliberately emplaced to reduce the return-to-duty time of affected personnel.

2-119. Force health protection enables the prevention of disease and nonbattle injuries through surveillance, risk analysis, protective measures, and corrective actions to conserve the fighting force. The main force health protection priorities target personal hygiene, food and water safety, and environmental factors (including climatic injuries, infectious diseases, disease vectors and their control, education, injuries during training, behavioral health assessments, and dental hygiene). Force heath protection measures can be overlooked due to stress and fatigue. The need for continued assessment by leaders is key to preventing avoidable nonbattle injuries. Combat conditions and operational stress can quickly take their toll on organizations and leaders engaged in prolonged operations. Behavioral health expertise provides preventative and restorative methods for identifying, treating, and restoring the effectiveness of personnel who are exposed to prolonged stress. Force health practitioners monitor offensive running estimates for the evidence of a deliberate or incidental epidemic.

2-120. Personnel rest and recovery plans, leader experience, and skill levels are safety considerations that influence risk management decisions during Army operations. Preventable accidents can thwart mission success during combat operations. Leaders must continue to assess the environment and routine activities for evidence of hazards that can lead to the preventable loss of combat power through disease and injury. Force health protection also applies to offensive operations and stability (see Appendix A for additional information on force health protection).

Fratricide Avoidance/Combat Identification

2-121. Protection through fratricide avoidance is critical during defensive operations and is accomplished with planning and preparation. Mobile defense is characterized by a high degree of movement and maneuver; therefore, they seek fratricide avoidance in a manner similar to the offense—through solid land navigation and position reporting, combat identification, and positive control. Area defense involves the deliberate structure of the defensive pattern that emphasizes preparation, identifiable engagement areas and kill zones, engagement criteria, and mutually supporting positions. The commitment of the reserve force during an area defense operation may create the conditions for a fratricide event; therefore, they are typically well-rehearsed. Air and missile defense operations are regulated by rules and directives to mitigate the potential for fratricide of friendly and neutral air platforms. The area air defense commander and the airspace control authority establish measures and procedures to positively identify all airborne assets. Protection measures and tasks are applied throughout the principles of protection in the defense.

PROTECTION CONSIDERATIONS DURING THE OFFENSE

2-122. Offensive operations impose the commander's will on the enemy or adversary. An *offensive operation* is an operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers (ADP 3-0). Against a capable, adaptive enemy or adversary, the offense is the most direct and sure means of seizing, retaining, and exploiting the initiative to gain physical and psychological advantage over an enemy or adversary and achieve decisive results. If that operation does not destroy the enemy or adversary, operations continue until enemy or adversary forces disintegrate or retreat to where they no longer pose a threat. Executing offensive operations compels the enemy or adversary to react, creating or revealing additional weaknesses that the attacking force can exploit.

Types of Offensive Operations:
- **Movement to contact**
- **Attack**
- **Exploitation**
- **Pursuit**

2-123. Characteristics of the offense include audacity, concentration, surprise, and tempo. Effective offensive actions capitalize on timely, relevant, accurate, and predictive intelligence and other relevant information regarding enemy forces, weather, and terrain. The commander maneuvers forces to advantageous positions before contact. Protection tasks keep or inhibit the enemy from acquiring accurate information about friendly forces (see ADP 3-90). On the offense, leaders must balance the need for caution with the potential significance that opportunity offers, and they must weigh their decision in favor of initiative and action.

2-124. During offensive operations, the preservation of combat power enables endurance and delays culmination. Commanders consider the impacts of committing time and resources to protection efforts

against the need to weight the main effort. Integrating and synchronizing protection tasks make protection more efficient and effective.

2-125. Commanders frequently face competing demands for limited protection capabilities. They resolve these competing demands by establishing protection priorities. One way in which commanders establish priorities is by designating, weighting, and protecting critical capabilities, areas, and information supporting the main effort. The *main effort* is a designated subordinate unit whose mission at a given point in time is most critical to overall mission success (ADP 3-0). Commanders shift resources and protection priorities as circumstances require. Commanders may shift the protection priorities several times during an operation.

Survivability

2-126. The protection of critical combat power systems requires survivability assets that alter the physical environment to provide or improve camouflage, cover, concealment, military deception, protective obstacles, emissions control, obscuration, and CBRN defensive measures. Such terrain modifications may require significant time. The protection of mobile assets can include measures such as survivability moves, the maximum use of existing terrain, obscuration, and military deception. EOD focuses on the elimination or reduction of the effects of explosive ordnance to preserve combat power (see Appendix A for additional information on survivability).

Air and Missile Defense

2-127. During offensive operations, air defense artillery units can provide vital protection from aerial threats while contributing to the freedom of maneuver of friendly forces. Air defense artillery commanders coordinate and synchronize air and missile defense coverage over maneuver forces and their critical assets, to include denying surveillance by threat air platforms. Air defense artillery units also protect forward-based infrastructure (such as lines of communications and command nodes or attacking friendly units moving beyond their short range air defense coverage) from aerial attack, provide early warning and surveillance, and determine and report ballistic missile launch and impact points (see Appendix A for additional information on air and missile defense).

Chemical, Biological, Radiological, and Nuclear Operations

2-128. An enemy force uses CBRN capabilities to delay, divert, or defeat friendly forces. Friendly CBRN reconnaissance and surveillance assets must be positioned and synchronized to provide commanders an early CBRN detection, identification, and avoidance capability. This enables rapid and decisive movement and maneuver, adjustments of mission-oriented protective posture levels, and informed decisions for decontamination to limit the spread of contamination. CBRN individual and collective protection measures protect the force while allowing it to maintain the initiative. Force health practitioners monitor running estimates for evidence of an endemic disease or biological attack (see Appendix A for additional information on CBRN operations).

Operations Security

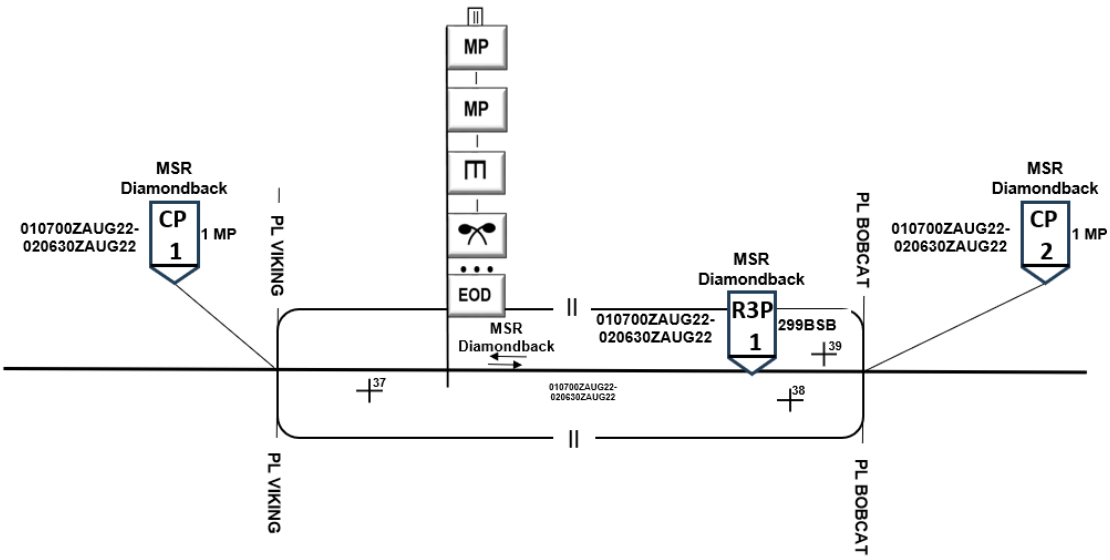
2-129. Offensive operations are enabled through disciplined OPSEC and the physical security of weapons, devices, sensitive items, codes, passwords, and other sensitive or classified material and information. OPSEC is used to deny enemy force critical information about friendly capabilities, intentions, and current operations. All organizations must deny access to information that can be used by the enemy to prevent or impede mission accomplishment.

2-130. Offensive operations and protection posture are further enabled through information advantage activities and the synchronization of information-related capabilities that attack enemy information warfare capabilities combined with those that protect friendly decision making and shared understanding (see FM 3-13 for additional information on information advantage activities). Measures taken to protect networks and computers from disruption and degradation can support and sustain tempo and allow leaders greater awareness through the uninterrupted access to information. Information assurance helps authenticate the identity of information users and sustains the availability of access by authorized users only (see Appendix A and ATP 3-13.3 for additional information on OPSEC).

Area Security

2-131. Area security operations support offensive operations by providing a response capability to assembly areas and sustainment areas and to designated geographical areas such as routes, bridge sites, or lodgments. Additionally, area security operations allow commanders to provide protection to critical assets without a significant diversion of combat power. During the offense, various military organizations may be involved in conducting area security operations in an economy-of-force role to protect lines of communications, convoys, or critical fixed sites and radars.

2-132. Urban areas typically contain structured and prepared routes, roadways, and avenues that can canalize traffic. Control measures (such as establishing traffic patterns) could alleviate traffic concerns, but they may also expose vulnerabilities that enemies and adversaries can exploit. This can lead to predictable friendly movement patterns that can easily be exploited. Commanders may gradually apply additional protection measures to protect movement along an area of a specific route due to increased threats (see figure 2-5).



Legend:	
BSB	brigade support battalion
CP	check point
EOD	explosive ordnance disposal
MP	military police
MSR	main supply route
PL	phase line
R3P	rearm, refuel, and resupply point

Figure 2-5. Example of increased security of a specific area for a main supply route

2-133. Tactical assembly areas utilize local security measures; however, they may be vulnerable to attack from bypassed enemy forces, which requires a response that exceeds the assembly area capabilities. In these support areas, commanders conduct area patrols and damage control to prevent and/or respond to enemy or adversary actions that can diminish combat power (see Appendix A for additional information on area security).

Explosive Ordnance Disposal Support

2-134. During offensive operations, EOD mission requirements vary based on the echelon of the supported unit. At division and below, EOD may support offensive operations through the direct integration of EOD teams and platoons into maneuver and other elements conducting kinetic operations. EOD enables freedom of maneuver through the identification, render safe, and disposal of explosive ordnance threatening critical infrastructure, nodes, and key terrain, thereby reducing the immediate operational risk created by unexploded

ordnance and weapons systems. EOD companies and battalions conduct hasty technical intelligence of munitions, weapons systems, and other material to answer priority intelligence requirements and to help identify protection requirements for the force (see Appendix A and ATP 4-32 for additional information on EOD support).

Detention Operations

2-135. Offensive operations conducted during large-scale combat operations may result in large numbers of detainees, categorized as enemy prisoners of war. Entire enemy units separated and disorganized from shock and intense combat may be captured. These large numbers of detainees place a tremendous burden on maneuver forces. Military police enable Army forces to defeat enemy organizations, control terrain, protect populations, and preserve joint force by conducting detainee operations. Military police take control of detainees from maneuver units as far forward as possible to ensure the freedom of movement and maneuver and the safe and humane treatment of detainees under U.S. control (see Appendix A and FM 3-63 for additional information on detention operations).

Fratricide Avoidance/Combat Identification

2-136. Converging non-contiguous forces can lead to combat identification errors and fratricide. Commanders and leaders down to the lowest echelons take deliberate precautions to prevent and mitigate friendly fire incidents through positive and procedural control mechanisms, standard unit marking schemes and patterns, and sound navigation and reporting procedures.

PROTECTION CONSIDERATIONS DURING STABILITY

2-137. As hostilities end, Army forces transition to stability operations and prepare for a transition to the host nation or other provisional governments if required. A *stability operation* is an operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADP 3-0). Army forces play a key role in enabling the joint force to establish and conduct military governance until a civilian authority or government can be restored.

Army Stability Tasks:

- **Establish civil security**
- **Support to civil control**
- **Restore essential services**
- **Support to governance**
- **Support to economic and infrastructure development**
- **Conduct security**

2-138. When conducting stability operations, protection is essential for success at all operating levels of warfare. The most sustainable protection success for the force in stability operations (same as in offensive and defensive operations) is achieved by integrating and synchronizing protection capabilities. Loss, damage, injuries, and casualties can influence the will of participating populations to sustain operations. The long-term nature of stability operations may require a scheme of protection that is more resource-intensive and more prescribed than typical security operations (see FM 3-07 for additional information on stability).

Air and Missile Defense

2-139. Air defense artillery units continue to protect forces and critical assets from aerial threats, such as unmanned aircraft surveillance or rocket attacks, during stability operations. Protection is extended over civilian areas and assets to facilitate civil security. Air defense artillery units also support security force assistance and continue partnerships with multinational air and missile defense forces (see Appendix A for additional information on air and missile defense).

Electromagnetic Protection

2-140. Electromagnetic protection remains constant during stability. Electromagnetic protection is a command responsibility but is only effective when everyone in an organization understands its importance

and can readily identify opportunities to implement protection activities (see Appendix A, ATP 3-12.3, and FM 3-12 for additional information on electromagnetic protection operation and techniques).

Area Security

2-141. Urban areas typically contain structured and prepared routes, roadways, and avenues that can canalize traffic. Control measures (such as establishing traffic patterns) can alleviate traffic concerns, but they may also expose vulnerabilities that enemies and adversaries can exploit. This can lead to predictable friendly movement patterns that can easily be contemplated by the enemy or adversary. Commanders may gradually apply protection to protect movement along a route (see Appendix A for additional information on area security).

Operations Security

2-142. Information advantage activities are a key protection enabler. These activities assist the commander in engaging the local population to inform friendly audiences and influence neutral audiences, enemies, and adversaries. This can include measures such as improving local information programs, improving populace and infrastructure security, defeating explosive hazards (including improvised explosive devices, bomb-making, and expertise-funding efforts), and defeating insurgent or terrorist recruitment efforts. Civil affairs organizations help develop formal and informal relationships. Military leaders and Soldiers conduct Soldier and leader engagements or other activities to facilitate the delivery of friendly messages (matched by actions on the ground) to key leaders and population groups (see Appendix A and ATP 3-13.3 for additional information on OPSEC).

Physical Security

2-143. The goal of physical security systems is to employ security in depth to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage, or other criminal activity. Establishing access control measures; installing concrete barriers, fences, exterior security lighting, concertina wire, and guard towers; and conducting aggressive security patrols during stability can deny enemy access to the area immediately surrounding friendly forces.

Antiterrorism

2-144. Antiterrorism must be integrated into all Army operations and always considered during stability. Awareness must be built into every mission, every Soldier, and every leader. Typical Army antiterrorism programs are composed of several adjunct and information programs, including tasks for specialized, nonprotection military occupational specialties.

Explosive Ordnance Disposal Support

2-145. During stability, EOD continues to provide the same support functions to the protection warfighting function as it did during offense and defense operations. The intensity and emphasis of each task varies based on the operational environment and priorities of the supported commander. Upon the transition to stability operations, EOD may also assume responsibilities for physical security, stockpile management, mine action (humanitarian), and other activities to secure, inspect, and dispose of explosive ordnance and weapons systems threatening the stability of the host nation and civil populations. These activities support the return of displaced populations, return land and infrastructure to their prewar uses, and aid in the overall effort to return an area to civil rule (see Appendix A and ATP 4-32 for additional information on EOD support).

Police Operations

2-146. Stability operations tend to be of long duration compared to offensive and defensive operations. Assessment includes determining the level of the civil Rule of Law in the policing and corrections services and identifying significant infrastructure and base development construction projects for police stations, training centers, and corrections institutions.

2-147. Adversaries often blend in with the local populace and are difficult to identify, making heightened levels of awareness the norm. The conduct of police intelligence operations and the use of biometrics collection devices in conjunction with identity activities supports population control by identifying criminals and combative individuals who seek to blend into the population.

Detention Operations

2-148. Detention operations in support of stability requires complex and sustainable systems, solutions, and facilities. Long-term custody and control requirements are often augmented with structured rehabilitative and reconciliation programs, increased access to medical treatment, and visitation opportunities, and they conclude with some form of guarantor or sponsor-based release or supervised system. These operations are resource-intensive and should receive a priority commensurate with their strategic significance (see Appendix A and FM 3-63 for additional information on detention operations).

Populace and Resources Control

2-149. Stability operations require commanders to balance protection needs between military forces and civil populations. Because U.S. forces and the local population frequently interact, planning for their protection is both important and difficult. Threats attack to weaken U.S. resolve and promote their individual agendas. Such enemies, who may be nearly indistinguishable from noncombatants, view U.S. forces and facilities as prime targets. An additional planning consideration during stability operations is to protect the force while using the appropriate force necessary, consistent with the approved rules of engagement. The rules of engagement must be flexible enough to change with local threat conditions and limit collateral damage. Collateral damage caused by military operations can negatively impact the mission and can support enemy or adversary provocation tactics. Overly restrictive rules of engagement should be avoided because they can limit the freedom of action and the ability to protect the force.

2-150. Army units should account for the protection of civilians from other hazards, in addition to their own direct and indirect fires. Particularly in counterinsurgency and when executing stability operations tasks, population support may be the center of gravity; it is unlikely that support can be achieved if the population is not protected. Army units may be expected to take measures that protect civilians from enemy or adversary actions. Antiterrorism measures should also account for the protection of civilians because they are likely to become incidental casualties by deliberate attacks against soft and populated targets.

2-151. Civilian casualty mitigation is similar to fratricide avoidance because both are intended to avoid casualties on an unintended target. The mitigation of civilian casualties is more challenging because there tends to be a high density of civilians throughout the area, in unexpected locations, and outside the command chain. In addition, Army forces are obligated to distinguish between military objectives and civilian people and objects and are obligated to take feasible precautions in planning and conducting attacks to reduce the risk of harm to civilians and other protected persons and objects. In many cases, civilians are virtually indistinguishable from the enemy or adversary. In the same way that Army units continually consider the possibility of fratricide and take measures to mitigate its risk, they should adopt a similar mindset regarding the avoidance of civilian casualties.

2-152. Stability operations and irregular warfare often involve armed conflict between nonstate actors who possess limited conventional forces. For this reason, some Army functional capabilities are often retasked from their primary function to conduct or reinforce protection efforts such as fratricide avoidance, OPSEC, and antiterrorism based on METT-TC (I).

2-153. The scheme of protection for stability operations often begins by determining where the current situation is best described along the stability framework and then applying protection capabilities to the most significant military and civilian vulnerabilities. Primary stability tasks reflect a host of subtasks within the range of military operations and throughout the five stability sectors. Protection measures are applied during vulnerability assessments focused on the primary stability tasks (see Appendix A and ADP 3-07 for additional information on populace and resources control).

Force Health Protection

2-154. The close proximity between civilians and Soldiers can also promote force health protection issues (such as communicable disease) through close contact with local civilians, detainees, animals, or local foods. Stability operations are often enduring and can lead to complacency among Soldiers and result in an increase in accidents. Disciplined risk reduction efforts require effective leadership and should be continually monitored and assessed from the beginning to the end of an operation or deployment (see Appendix A for additional information on force health protection).

Chapter 3

Protection Capabilities Integration

"It is always necessary to shape operations plans…on estimates of the weather, and, as this is always changing, one cannot imitate in one season what has turned out well in another."

Frederick the Great: Instructions for His Generals, iii, 1747

Protection task integration throughout the operations process helps establish control measures against potential threats and hazards. The layering of protection tasks (some redundant) ensures a comprehensive scheme of protection. The layered approach of protection provides strength and depth. Units use available capabilities to defend in a layered approach against the destructive effect of threats and hazards. This chapter describes the integration and layering of protection through the operations process.

THE OPERATIONS PROCESS

3-1. Commanders and staffs use the operations process to determine protection requirements and priorities and direct, coordinate, and synchronize protection efforts and capabilities across all domains to reduce risk, mitigate identified vulnerabilities, and create windows of opportunity to achieve mission success. The *operations process* is the major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0).

3-2. The major components of the operations process are planning, preparing, executing, and continuously assessing the operation. Planning normally begins upon receipt of orders from a higher echelon headquarters and continues through the execution of the operation. The commander and staff revise the plan and make adjustments as needed through fragmentary orders. Commanders, assisted by their chief of staff or executive officer, drive the preparation for an operation by allocating time, prioritizing resources, and supervising preparation activities (such as rehearsals) to ensure that their forces are ready to execute operations. During execution, commanders and staffs focus their efforts on translating plans into direct action to achieve objectives according to higher echelon headquarters' intent. The commander and staff continually assess operations throughout planning, preparation, and execution (see ADP 5-0 for more information on the operations process and FM 6-0 for more on the role of commanders in operations).

3-3. Army leaders are responsible for clearly articulating their visualization of operations in time, space, purpose, and resources. The commander's inherent responsibility to protect and preserve the force and secure the area of operations is vital in seizing, retaining, and exploiting the initiative (see figure 3-1, page 3-2). Protection must be considered continuously throughout the operations process to—

- Identify threats and hazards.
- Implement control measures to prevent or mitigate unnecessary exposure to threats or hazards or enemy or adversary freedom of action.
- Preserve critical capabilities, areas, and information.
- Enable freedom of action.
- Manage capabilities to mitigate effects and preserve time to react or maneuver against the enemy to gain superiority and retain the initiative.

Figure 3-1. Integration of protection throughout the operations process

PROTECTION PLANNING

3-4. Planning is the first step toward effective protection. Commanders consider the most likely threats and hazards and then decide which personnel, physical assets, and information to protect. They establish protection priorities for each phase or critical event of an operation. Mission analysis provides commanders a better understanding of the situation and problem. Commanders and protection cell planners identify what the command must accomplish, when and where it's done and, most importantly, why it must be carried

out—the purpose for the operation. This understanding of the situation and problem allows commanders to identify and analyze threats and hazards and develop a scheme of protection.

3-5. The keys to protection planning are establishing a protection working group; identifying threats and hazards; assessing the threats and hazards to determine the risks; developing preventive measures; directing, coordinating, and synchronizing protection capabilities; and enabling operations and protection capabilities into a comprehensive scheme of protection that includes mitigating measures (see figure 3-2). Integrating planning considerations from all warfighting functions into the scheme of protection and the integration of protection into the planning of all other warfighting functions provide common critical capabilities available to commanders and staffs at all echelons. Commanders integrate and synchronize capabilities of one warfighting function with other warfighting functions to achieve objectives and accomplish missions. These grouped and related capabilities and activities help commanders and staffs integrate, synchronize, and direct operations. Commanders and staffs use warfighting functions to ensure that major groupings are accounted for in every operation and to conceptualize and apply capabilities to accomplish the mission through synchronizing forces and warfighting functions in time, space, and purpose.

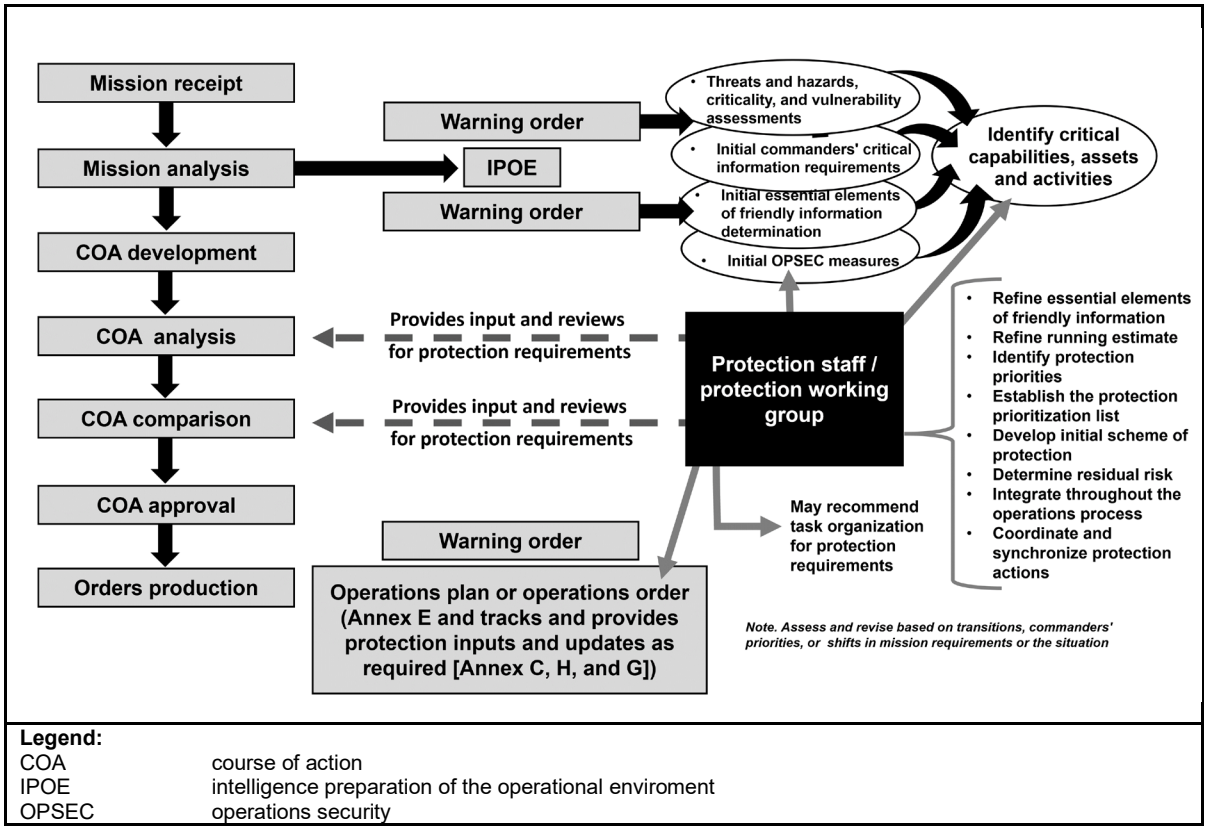


Figure 3-2. Protection planning

PROTECTION WORKING GROUP

3-6. *Working group* is a grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function (FM 6-0). Their cross-functional design enables them to coordinate and synchronize contributions from multiple command post cells and staff sections. For example, the protection working group brings together representatives of all staff elements concerned with protection. It coordinates and synchronizes the contributions of all staff elements with the work of the protection cell. It also integrates protection with future operations and current operations integration cells.

3-7. The protection cell forms the core membership of the protection working group, which includes other agencies, as required. Protection cell and protection working group members differ in that additional staff officers are brought into the working group. These additional officers meet operational requirements for threat and hazard, criticality, and vulnerability assessments and protection priority recommendations. The protection working group calls upon existing resources from the staff as required. The echelon chief of protection leads the protection working group.

3-8. Protection working group meetings have similar purposes, regardless of the echelon. Protection functions at different echelons of command differ mostly in the size of the area of operations and the number of available protection capabilities. Commanders augment the team with other unit specialties and unified action partners, depending on the operational environment and unit mission. The chief of protection determines the working group agenda, meeting frequency, composition, input, and expected output. Each protection working group meeting should have a unique purpose. For example, protection working group meetings during the military decision-making process (MDMP) may focus on threat, hazard, and risk analysis while conducting mission analysis; on criticality and vulnerability analysis and initial scheme of protection development during course of action (COA) development; or on refining the scheme of protection and mitigating additionally identified risk during COA analysis. Table 3-1 shows an example of the purpose, agenda, and composition of a protection working group, including staff inputs and outputs.

Table 3-1. Example division protection working group activities and participants

Purpose and Frequency	**Purpose:** • Determines likely threats and hazards and provides updates on enemy tactics, the environment, and accidents. • Determines vulnerabilities as assessed by the vulnerability assessment team. • Establishes and recommends protection priorities. • Reviews and provides recommendations for the protection prioritization list. • Reviews, coordinates, and synchronizes unit protection measures. • Recommends force protection conditions and random antiterrorism measures. • Makes recommendations to commanders on protection issues that require a decision. • Performs tasks required for a force protection working group and a threat protection working group. • Assesses assets and infrastructure that are designated as critical by higher headquarters. • Analyzes and provides recommendations for the protection of civilians in the area of operations. • Considers incorporating host-nation and constabulary forces into the scheme of protection. • Develops and refines the protection running estimate. • Develops a scheme of protection, ensuring that it nests with the operational concept. • Establishes the personnel recovery coordination center. • Determines organic personnel recovery capabilities at each echelon, tracks open personnel recovery events, and disseminates isolated personnel guidance. • Provides input and recommendations for defensive cyber operations. • Identifies risks to the mission. • Provides input and recommendations on protection-related training. **Frequency**: At least daily or as required.

Table 3-1. Sample protection working group activities and participants (continued)

Participants	**Chair: Chief of protection** **Attendees:** • Air and missile defense • Antiterrorism • CBRN • Engineer • Cyber electromagnetic activities • Explosive ordnance disposal • Fire support • Operations security • Provost marshal • Safety • Intelligence • Civil affairs • Unified action partners • Public affairs • Staff judge advocate • Chaplain • Surgeon • Medical • Veterinary • Subordinate unit liaison • Operations planner • Area contracting • Cyber • Information • Logisticians • Personnel recovery • Space operations	
Inputs and Outputs	**Inputs:** • Commanders' guidance and intent • Operations and warning orders • Friendly forces information requirements • Commanders' critical information requirements • Echelon sync matrix • Decision support matrix • Current scheme of protection • Threat and hazard assessment • Vulnerability assessment • Criticality assessment • Risk assessment • Status of personnel recovery assets and open events	**Outputs:** • Updated protection assessment • Updated scheme of protection • Updated protection running estimate • Protection prioritization list • Recommended force protection conditions • Recommended protection guidance and mitigation measures • Recommended changes to essential element of friendly information • Update to isolated personnel guidance and alert status or repositioning/prepositioning of personnel recovery assets
Agenda	• Roll call • Intelligence/operations update (G-2/G-3) • Protection prioritization list assessment/update (chief of protection) • New vulnerabilities–next 72 hours (chief of protection) • Mitigation measures (chief of protection) • Recommendations–security posture adjustments, information engagement, resource allocation, required training (chief of protection) • Guidance (G-3) • Conclusion (chief of protection)	
Legend: CBRN G-2 G-3	 chemical, biological, radiological, and nuclear assistant chief of staff, intelligence assistant chief of staff, operations	

INITIAL ASSESSMENTS

3-9. Initial protection planning requires various assessments to establish protection priorities. Assessments include threats, hazards, vulnerability, and criticality. These assessments determine which assets must be

protected given no constraints and which assets can be protected with available resources. There are seldom sufficient resources to simultaneously provide all critical assets the same level of protection. For this reason, commanders make decisions on acceptable risks and provide guidance to the staff so they can coordinate and synchronize protection capabilities based on the protection priorities.

3-10. Protection planning is a continuous process that must include an understanding of the threats and hazards that may affect operations from the deep area back to the strategic support area. Protection capabilities are aligned to protect critical capabilities, areas, and information and mitigate effects from threats and hazards. The protection cell and protection working group must prioritize protection during competition below armed conflict, crisis, and armed conflict.

3-11. During competition below armed conflict, the focus is on cooperation, prevention, and deterrence. Within planning, the protection cell conducts continuous assessments to understand the environment; cooperate with and support partners to build a network of protection; and safeguard the force through active and passive measures, training, and exercises.

3-12. During crisis, the main purpose is to deter adversary actions. The protection cell estimates the protection assets necessary for future operations and the increased threat according to the commander's priorities, force availability, and adversary assessment. Units prioritize protection capabilities and align them to defend critical capabilities, areas, and information. It is imperative to conduct information advantage activities to deny adversaries the ability to obtain information.

3-13. During armed conflict, planning prioritization considerations includes efforts to—

- Preserve combat power.
- Protect critical facilities, nodes, lines of communication networks, routes, and areas.
- Counter enemy fires and maneuver by placing personnel, systems, and units in locations or positions that are difficult to locate, strike, and destroy.
- Gain air, space, and electromagnetic spectrum superiority.
- Proactively target enemy systems.
- Use defensive information advantage activities.
- Recover and reintegrate isolated personnel.

3-14. Success in consolidating gains is obtained through setting the conditions for a stable environment. Staffs should weigh the prioritization of protection capabilities throughout defensive, offensive, and stability operations required to support the consolidation of gains.

Threat and Hazard Assessment

3-15. Personnel from all staff sections and warfighting functions help conduct threat and hazard analysis starting during mission analysis. This analysis comprises a thorough, in-depth compilation and examination of information and intelligence that address potential threats and hazards in the area of operations. The integrating processes (intelligence preparation of the operational environment, information collection, targeting, risk management, and knowledge management [see ADP 5-0]) provide an avenue to review and refine knowledge of threats and hazards. Threat and hazard assessments are continuously reviewed and updated as the operational environment changes.

3-16. The threat and hazard assessment results in a comprehensive list of threats and hazards and determines the likelihood or probability of occurrence of each threat and hazard. Protection considerations for the threat and hazard assessment include—

- Hostile actions.
- Environmental conditions.
- Nonhostile activities.
- Criminal activities.
- Civil unrest.

Criticality Assessment

3-17. The criticality assessment provides the commander a list of key assets and infrastructure based on the necessity for mission success. An asset's criticality is determined by the impact of its loss on the mission. A criticality assessment addresses the impact of a temporary or permanent loss of key assets on the unit's ability to conduct the mission. For installation, garrison, area support, and similar commands, a criticality assessment should include high-density population facilities (recreational centers, theaters, sports venues) that may not be mission-essential. Echelons above corps should consider urban population centers in their criticality assessments. They examine the costs of recovery and reconstitution, including time, expense, capability, and infrastructure support. The staff gauges how quickly a lost capability can be replaced before providing recommendations to the commander. The general sequence for a criticality assessment is—

- **Step 1.** List the key assets and capabilities.
- **Step 2.** Determine if critical functions or combat power can be substantially duplicated with other elements of the command or an external resource.
- **Step 3.** Determine the time required to substantially duplicate key assets and capabilities in the event of temporary or permanent loss.
- **Step 4.** Set priorities for the response to threats toward personnel, physical assets, and information.

3-18. The protection cell and working group continuously update criticality assessments during the operations process. As the staff develops or modifies a friendly COA, information collection efforts confirm or deny information requirements. As the mission or threat changes, initial criticality assessments may also change, increasing or decreasing the subsequent force vulnerability. The protection cell members monitor and evaluate these changes and begin coordination among the staff to implement modifications to the protection concept or recommend new protection priorities. Priority intelligence requirements, running estimates, measures of effectiveness (MOEs), and measures of performance (MOPs) are continually updated and adjusted to reflect the current and anticipated risks associated with the operational environment.

Vulnerability Assessment

3-19. A vulnerability assessment is an evaluation (assessment) to determine the magnitude of a threat's or hazard's effect on a critical capability, asset, or activity by phase of an operation. It identifies areas of improvement required to withstand, mitigate, or deter acts of an enemy attack. Commanders must understand their vulnerabilities to being attacked in each domain and develop mitigations to protect the force. The protection cell continually assesses the risk to friendly forces. When assessing friendly force vulnerabilities and weaknesses, the protection cell views the target that the force presents through the eyes of an enemy targeting analyst. The cell addresses who or what is vulnerable and how it is vulnerable against threats. They consider ways to reduce vulnerability and determine the appropriate protection capabilities to prevent and mitigate detection and the effects of threats and hazards.

3-20. The vulnerability assessment identifies physical characteristics or procedures that render critical capabilities, areas, and information vulnerable to known or potential threats and hazards. Vulnerability evaluation criteria may include the degree to which an asset may be disrupted, the quantity of the asset available (if replacement is required due to loss), dispersion (geographic proximity), and key physical characteristics. When a vulnerability is identified and assessed, commanders ensure that capabilities, assets, and activities critical for operations are aligned with the protection principles and priorities to accomplish the mission.

3-21. The general sequence of a vulnerability assessment is—

- **Step 1.** List assets and capabilities and the threats against them.
- **Step 2.** Determine the common criteria for assessing vulnerabilities.
- **Step 3.** Evaluate the vulnerability of assets and capabilities.

Note. DOD has created several decision support tools to perform criticality assessments in support of the vulnerability assessment process, including mission, symbolism, history, accessibility, recognizability, population, and proximity and criticality, accessibility, recuperability, vulnerability, effect, and recognizability. See ATP 3-37.2 for additional information.

PROTECTION PRIORITIES

3-22. Criticality, vulnerability, and recuperability are the most significant considerations in determining protection priorities that become the subject of commander guidance and the focus of area operations. The scheme of protection is based on the mission variables and should include protection priorities by area, unit, activity, or resource.

3-23. Although all military assets are important and all resources have value, the capabilities they represent are not equal in their contribution to overall mission accomplishment. Determining and directing protection priorities may involve the most important decisions commanders make. Prioritization of protection capabilities is situationally dependent and resource informed. There are seldom sufficient resources to simultaneously provide the same level of protection to all assets.

3-24. Most prioritization methodologies assist with differentiating important protection priorities from urgent protection priorities. In protection planning, the challenge is to differentiate between critical assets and important assets and between the main effort and supporting efforts, and to further determine what protection is possible with available protection capabilities.

3-25. Event-driven operations may be short in duration, enabling a formidable protection posture for a short time; condition-driven operations may be open-ended and long-term, requiring an enduring, sustainable, and revised scheme of protection. In either situation, commanders must provide guidance on prioritizing protection capabilities and categorizing important assets.

3-26. The protection cell and working group use information derived from the commander's guidance, the overall concept of the operation or COA, the intelligence preparation of the operational environment, information collection, targeting, risk management, knowledge management, warning orders, and mission analysis to prioritize critical capabilities, areas, and information. Critical capabilities, areas, and information at each command echelon must be determined and prioritized.

PROTECTION PRIORITIZATION LIST

3-27. Protection prioritization lists are organized through the proper alignment of critical assets and activities. The commander's priorities and intent determine critical assets and activity or operation for protection by the assets available. Critical assets can be people, property, equipment, activities, operations, information, facilities, or materials. For example, bridging companies might be identified as critical to the execution of military operations and, therefore, receive additional protection. The lack of a replacement may cause a critical asset to become a top priority for protection. A critical activity or operation could be a gap crossing or command post displacement.

3-28. The protection prioritization list is a key protection product developed during mission analysis, but it cannot be completed until the COA development step during MDMP. The protection cell and working group assess criticality, vulnerability, and probability of surveillance or attack to prioritize identified critical assets. Once the protection working group determines which assets are critical for mission success, it recommends protection priorities and establishes a protection prioritization list. It is continuously assessed and revised throughout each phase or major activity of an operation.

- Criticality is the degree to which an asset or area is essential to accomplish the mission. It is determined by assessing the impact that damage to—or the neutralization, disruption, or destruction of—the asset will have on the success of the operation. Damage to an asset may prevent, significantly delay, or have no impact on the success of the plan.
  - **Catastrophic.** Complete mission failure or the inability to accomplish the mission, the loss of major or mission-critical systems or equipment, major property or facility damage, mission-critical security failure, or unacceptable collateral damage.
  - **Critical.** Severely degraded mission capability or unit readiness; extensive damage to equipment or systems; significant damage to the environment; security failure; or significant collateral damage.
  - **Marginal.** Degraded mission capability or unit readiness; minor damage to equipment or systems, property, or the environment.
  - **Negligible.** Little or no adverse impact on mission capability, slight equipment, or systems damage (remaining fully functional or serviceable), or little or no collateral damage.
- Vulnerability measures the susceptibility of an asset to any action by any means through which its effectiveness is diminished. Asset vulnerability is greater if a lower-level threat (Level I) can create damage or destruction that would result in mission failure or severely degrade its mission capability. If an asset can withstand a Level I or Level II threat, its vulnerability ability is less and it may not require additional protection depending on the asset's criticality. The following mitigating factors must be considered when assessing the vulnerability of a target: survivability (the ability of the critical asset to avoid or withstand hostile actions by using camouflage, cover [hardening], concealment, and deception), the ability to adequately defend against threats and hazards, mobility and dispersion, and recuperability (the time required for the asset to be restored, considering the availability of resources).
  - **Level I Threat.** Enemy agents, terrorists, and criminals.
  - **Level II Threat.** Small tactical units. Irregular forces may include significant standoff weapons threats.
  - **Level III Threat.** Large tactical force operations including airborne, heliborne, amphibious, infiltration, and major air operations.
- Probability assesses the frequency an asset will be targeted for surveillance or attack by a capable threat. Determinations of the intent and capability of the threat are key in assessing the probability of attack.
  - **Frequent.** Occurs very often; known to happen regularly.
  - **Likely**. Occurs several times; a common occurrence.
  - **Occasional.** Occurs sporadically but is not uncommon.
  - **Seldom.** Remotely possible; could occur at some time.
  - **Unlikely.** Rarely occur, but not impossible.

3-29. Protection cells and working groups may develop criticality, vulnerability, and probability values to help prioritize critical assets. Figure 3-3, page 3-10, provides an example of how criticality, vulnerability, and probability values can help determine risk. Table 3-2, page 3-10, provides an example of a protection risk analysis table that identifies the risk analysis total for a critical asset, activity, or operation.

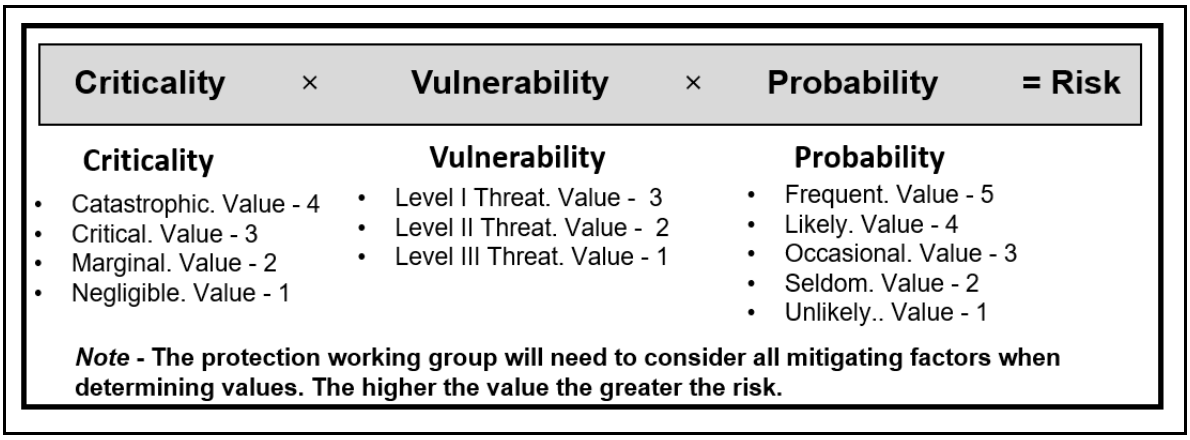


Figure 3-3. Example criticality, vulnerability, and probability values

Table 3-2. Example protection risk analysis table

Asset	*Criticality (1–4)*	*Vulnerability (1–3)*	*Probability (1–5)*	*Risk Analysis Total Criticality x Vulnerability x Probability*
Command post	4	2	4	32
Signal nodes	3	2	4	24
Route security – Main supply route Viking	2	2	4	16
Population center	2	3	2	12

3-30. The protection prioritization list helps Army commanders to identify or assess assets that require protection prioritization within their assigned areas. Not all assets listed on the protection prioritization list receive continuous protection. Some critical assets only receive protection assets based on available resources. It is the responsibility of the protection cell and working group to provide the assessment and recommended protection prioritization list to the commander for approval (see table 3-3, page 3-11).

Table 3-3. Example protection prioritization list

Priority	Critical Asset / Activity	Location (Grid / Proximity)	Notes	Threats	Units Tasked	Mitigation
1	DIVARTY Q53 (Radar)	DL43562765 / PL Bobcat	Critical for Counterfire missions, 4x	ENY Air, IDF(G-6, 9A51, 9A52, 2S19), SPF, EW Jamming	SPF, A, 3-265 ADA 1-172 CAV 1/233 MP CO	Survivability Position; Active / Passive Air Defense; Area Security
2	DIVARTY Q36 (Radar)	DL43682779 / PL Bobcat	Critical for Counterfire missions, 3x	ENY Air, IDF(G-6, 9A51, 9A52, 2S19), SPF, EW Jamming	A, 3-265 ADA 1-172 CAV 2/233 MP CO	Survivability Position; Active / Passive Air Defense; Area Security
3	DIVARTY Q37 (Radar)	DL44172960 / PL Bobcat	Critical for Counterfire missions, 3x	ENY Air, IDF(G-6, 9A51, 9A52, 2S19), SPF, EW Jamming	B, 3-265 ADA 1-172 CAV 3/233 MP CO	Survivability Position; Active / Passive Air Defense; Area Security
4	3-197 MLRS	DL43562765 / PL Bobcat	BN assigned to DIVARTY, 16x	IDF(G-6, 9A51, 9A52, 2S19), Chemical Attack	B, 3-265 ADA B, 1BCT (-) 2/333 MP CO(-)	Survivability Position; Active / Passive Air Defense; Area security
5	2-18 HIMARS	DL43682779/PL Bobcat OBJ Viking	BN assigned to DIVARTY, 16x	IDF(G-6, 9A51, 9A52, 2S19), Chemical Attack	C, 3-265 ADA B, 1BCT (-) 1/333 MP CO(-) 1MP CO(-)	Survivability Position; Active / Passive Air Defense; Area Security
6	1-201FA BN	DL44172960 / PL Bobcat	Fires support DIVARTY, M109A6 BTYs	Enemy Air, IDF(G-6, 9A51, 9A52, 2S19)	1-172 CAV	Survivability Position; Passive Air Defense; Area Security
7	1-82FA BN, 1-7FA BN	DL44172960/With organic BDE	Fires support to Maneuver Units, M109A6 BTYs	Enemy Air, IDF(G-6, 9A51, 9A52, 2S19)	3/1MP CO(-)	Survivability Position; Passive Air Defense; Area Security
8	CL III, V, & VII Re-supply Missions	PL Giants	TACON for Convoy Security	SPF, IDF(G-6, 9A51, 9A52, 2S19)	7 MP CO	Passive Air Defense; Area Security
9	Division Support Area	DL47683879/PL Bobcat With 404MEB	Open additional GLOC	SPF, IDF(G-6, 9A51, 9A52, 2S19)	1MP CO(-)	Passive Air Defense; Area Security

Protected Asset List – those critical assets protected by active defense measures

Critical assets with units designated to provide additional security beyond self-secure.

Legend:

ADA	air defense artillery	FA	field artillery
BCT	brigade combat team	GLOC	ground lines of communication
BDE	brigade	HIMARS	high mobility artillery rocket system
BN	battalion	IDF	indigenous forces
BTY	battery	MEB	maneuver enhancement brigade
CAV	cavalry	MLRS	multiple launch rocket system
CO	company	MP	military police
CL	class	OBJ	objective
DIVARTY	division artillery	PL	phase line
ENY	enemy	SPF	special purpose forces
EW	electromagnetic warfare	TACON	tactical control

SCHEME OF PROTECTION DEVELOPMENT

3-31. The scheme of protection describes how protection tasks and systems support the commander's intent and concept of operations, and it uses the commander's guidance to establish the priorities of support to units for each phase of the operation. A commander's initial protection guidance may include protection priorities, civil considerations, protection task considerations, potential decision points, high-risk considerations, and acceptable risk.

3-32. Planners receive guidance as commanders describe their visualization of the operational concept and intent. This guidance generally focuses on the courses of action development by identifying main and supporting efforts, reserve massing effects, and stating priorities. Effective planning guidance provides a broad perspective of the commander's visualization, with the latitude to explore additional options.

3-33. The protection cell (supported by the protection working group) develops the scheme of protection after receiving guidance and considering the principles of protection in relation to mission variables and the systems requiring protection. The scheme of protection is based on the mission variables; thus, it includes protection priorities by area, unit, activity, or resource and should support the scheme of maneuver. It addresses how protection is applied and derived during all phases of an operation. For example, the security for routes, bases/base camps, and critical infrastructure is accomplished by applying protection assets in dedicated, fixed, or local security roles; or it may be derived from economy-of-force protection measures, such as area security techniques. It also identifies areas and conditions where forces may become fixed or static and unable to derive protection from their ability to maneuver. These conditions, areas, or situations are anticipated; and the associated risks are mitigated by describing and planning for the use of response forces (see FM 5-0 for additional information on the scheme of protection).

3-34. The protection cell develops the scheme of protection by considering the following items, at a minimum, to create a secure operational environment:

- Protection priorities (critical capabilities, areas, and information).
- Work priorities for survivability assets.
- Coordination of air and missile defense support.
- Specific terrain and weather factors.
- Information focus and limitations for security efforts.
- Areas or events where risk is acceptable.
- Friendly forces information requirements.
- CCIRs.
- Civilians and noncombatants in the area of operations.
- Vehicle and equipment safety or security constraints.
- Personnel recovery actions and control measures.
- Force protection condition (FPCON) status.
- Force health protection measures.
- Mission-oriented protective posture guidance.
- Environmental guidance.
- Scheme of information.
- Explosive ordnance and hazard guidance.
- Ordnance order of battle.
- OPSEC risk tolerance.
- Fratricide avoidance measures.
- Rules of engagement, standing rules for the use of force, and rules of interaction.
- Escalation of force and nonlethal weapons guidance.
- Operational scheme of maneuver.
- Military deception.
- Obscuration.
- Identified threats and hazards.

- Radiation exposure status or operational exposure guidance.
- Contractors in the area of operations.
- Electromagnetic spectrum status.
- Availability of personnel-recovery-capable assets, gaps in recovery coverage, preparation of individuals.

3-35. While each protection task and system has its own operational consideration, each must be synchronized and integrated within the scheme of protection to ensure reinforcing protection efforts. For example, air and missile defense tasks must include complementary survivability tasks to mitigate threat actions. Area security tasks must consider antiterrorism, OPSEC, and physical security to be effective. To ensure this synergy, the protection working group develops a scheme of protection around which MOPs and MOEs can be synchronized with the echelon decision support matrix, monitored, and evaluated.

SHIFTS IN PROTECTION PRIORITIES

3-36. Transitions mark a change of focus in an operation. Leaders plan transitions as part of the initial plan or parts of a branch or sequel. They can be unplanned and cause the protection cell and working group to react to unforeseen circumstances and reassess protection priorities. Changes to protection priorities should be anticipated and assets reassessed as transitions occur throughout an operation or as commanders shift their priorities (see figure 3-4, page 3-14). Common transitions that affect protection priorities are—

- Movement of forces into a theater of operations.
- Changes in the security environment that cause a reframe of the mission or change in the purpose of the operation
- Between crisis and armed conflict.
- Between branches and sequels of a campaign or major operation.
- Between operations dominated by offense, defense, and stability.
- Between phases of an operation.
- Shifts of the main effort, supporting effort, and reserve between units.
- Between command posts during emplacement, movement, and displacement of one or more nodes.
- Task organization changes.
- Transfer of area of operations responsibilities between units.
- Change in mission from combat operations to reconstitution.
- Transfer of responsibility for security and governance to legitimate authorities.
- Movement of forces out of theater.

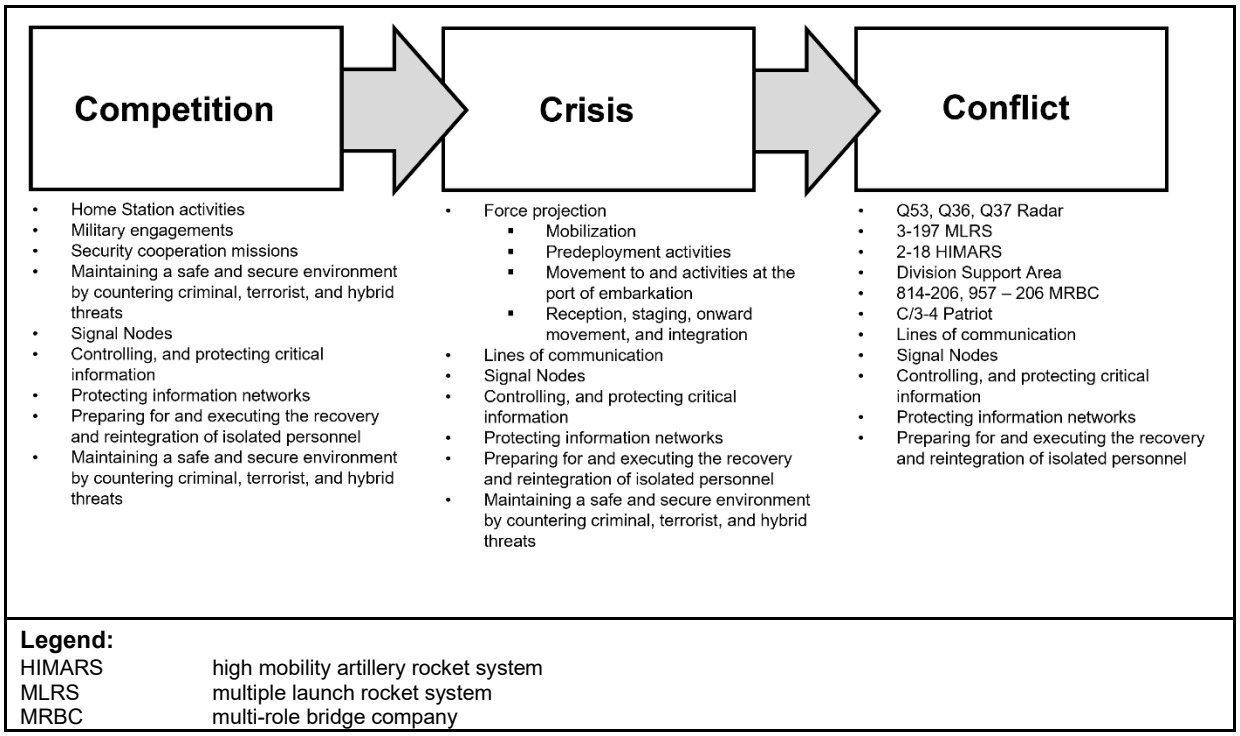


Figure 3-4. Example of shifts in protection priorities

3-37. Protection cells and working groups must account for the time required to plan, prepare, execute, and assess shifts in protection priorities in support of transitions. They must develop information requirements, including CCIR for decisions, to support shifts in protection priority and transitions They should also account for likely friction due to the environment, degraded communications, and enemy action. Effective transitions require protection cells and working groups to plan and prepare for changes in protection priorities well before their execution so the force can maintain the momentum and tempo of operations. Risk increases during transitions, so commanders and staffs establish protection requirements and priorities and direct, coordinate, and synchronize protection efforts and capabilities to support the transition.

INTEGRATING PROCESSES

3-38. Commanders and staffs integrate the protection warfighting functions and synchronize protection capabilities to adapt to changing circumstances throughout the operations process. They use several integrating processes to do this. An integrating process consists of a series of steps that incorporate multiple disciplines to achieve a specific end. For example, during planning, the MDMP integrates the commander and staff in a series of steps to produce a plan or order. Key integrating processes that occur throughout the operations process include—

- Intelligence preparation of the operational environment.
- Information collection.
- Targeting.
- Risk management.
- Knowledge management.

Intelligence Preparation of the Operational Environment

3-39. *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 (FM 2-0). Led by the intelligence officer and intelligence staff, the entire staff participates in intelligence preparation of the operational environment to develop and sustain an understanding of the enemy, terrain and weather, and civil considerations. It helps identify options available to friendly and threat forces.

3-40. Intelligence preparation of the operational environment consists of four steps. Each step is performed or assessed and refined to ensure that intelligence preparation of the operational environment products remain complete and relevant. The four steps are—

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine the threat COA.

3-41. Intelligence preparation of the operational environment begins in planning and continues throughout the operations process. This results in intelligence products used to aid in developing friendly COAs and decision points for the commander. Additionally, the conclusions reached and the products created during this process are critical to planning information collection and targeting. A key aspect is refinement in preparation and execution (see ATP 2-01.3).

3-42. The protection cell must assist the intelligence staff in producing and continuously refining all intelligence preparation of the operational environment products. Total staff integration ensures a holistic view of the operational environment, reduces the initial time required for development, and assists the commander in timely decision making. This coordination also improves the quality and accuracy of products. Below are examples of expertise that the protection cell may bring to intelligence preparation of the operational environment:

- Provides threat, hazard, and initial criticality and vulnerability analysis conducted by the protection working group.
- Provides input concerning threat mobility, countermobility, and survivability.
- Provides subject matter expertise and assists the assistant chief of staff, intelligence (G-2)/battalion or brigade intelligence staff officer (S-2) in determining the locations of enemy CBRN capabilities, the availability of systems to deliver CBRN materials, and the potential areas of CBRN employment.
- Provides inputs from the air and missile defense section on air and missile defense operations regarding the locations and projected areas of employment of threat air and missile defense artillery units.
- Provides subject matter expertise on criminal and irregular threats throughout the area of operations.
- Provides subject matter experts on environmental health threats and the disposition of captured enemy medical material.
- Provides intelligence requirements for personnel recovery operations and coordinates intelligence debriefing support for reintegration activities.

Information Collection

3-43. Commanders and staffs continuously plan, task, and employ collection assets and forces to collect information. They request information and resources through higher echelons. This information and intelligence helps commanders turn decisions into actions. Information collection planning is crucial to mission success. The four fundamentals to plan, synchronize, and integrate information collection activities include—

- An information collection effort driven by the commander.
- Full staff participation in effective information collection synchronization and integration.
- A collection capability, either organic or augmented by nonorganic resources, to conduct information collection.
- A capability to analyze and produce intelligence to conduct further information collection.

3-44. Commanders must quickly and clearly articulate their CCIR to the staff during the information collection planning process. This enables the staff to facilitate the commander's vision and decision making by focusing on the CCIRs. Protection cells support the collection planning process by recommending and coordinating information collection assets for protection, providing input into the information collection plan, and assisting in refining the information collection plan as required. Protection cells request information collection for protection priorities in the rear and close areas after they have situational understanding of threats against critical assets. See FM 3-55 for additional information on information collection.

Targeting

3-45. Targeting focuses on achieving the commander's objectives. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). The function of targeting is to efficiently achieve those objectives within the parameters set by the concept of operations, operational limitations in plans and orders, rules of engagement or rules for the use of force, the law of war, and other guidance given by the commander. It seeks to create specific desired effects through lethal and nonlethal actions. The art of targeting seeks to create desired effects with the least risk and expenditure of time and resources. See FM 3-60 for additional information on targeting.

3-46. The targeting process integrates commander guidance and priorities to determine which targets to engage and how, when, and where to engage them to assign friendly capabilities to create the desired effect. The staff then assigns friendly capabilities that are best suited to produce the desired effect on each target. An important part of targeting is identifying possibilities for fratricide and collateral damage. Commanders establish control measures, including the consideration for restraint, which are necessary to minimize the chance of these events.

3-47. The protection cell identifies the overall risk-to-mission and risk-to-force analysis (such as low, medium, high, or extremely high) during targeting working groups by enemy capability. This allows for the correct allocation of protection resources to address threats across the operational environment. The protection priorities must be integrated within the targeting process to achieve the desired objectives while ensuring the preservation of combat power. The protection cell supports targeting by—

- Identifying threat effects, critical capabilities, requirements, and vulnerabilities.
- Supporting intelligence staffs by providing the highest threat probability and risk in friendly forces area of operations.
- Conducting threat vulnerability assessments of threat capabilities and characteristics to determine their high-value targets.
- Nominating high-payoff targets and target area of interests to defeat or degrade threat capabilities such as CBRN, rotary- and fixed-wing aircraft, tactical ballistic missiles, and artillery.
- Developing target-sensing systems, attack guidance matrixes, and battle damage assessments for threat capabilities.
- Providing updates to the no-strike list (to include intelligence related to locations of isolated and captured personnel) and nominating targets to the restricted-target list.
- Conducting area analysis to identify potential medical and environmental hazards and threats.
- Developing target-sensing systems for criminal and irregular threats.

Risk Management

3-48. Commanders and staffs use risk management throughout the operations process to identify, prevent, and mitigate risks associated with detection or the effects of threats and hazards that have the potential to cause friendly and civilian casualties, damage or destroy equipment, or otherwise impact mission effectiveness. Like targeting, risk management begins in planning and continues through preparation and execution. The availability of relevant information directly impacts operational risk (see Appendix A and ATP 5-19 for additional discussion on risk management).

3-49. The protection cell provides technical risk management expertise to the commander and staff. The risk management responsibilities for the protection cell are to—

- Identify and assess hazards and propose controls for each COA during planning and preparation for operations.
- Understand, visualize, and identify protection priorities.
- Develop goals, objectives, and priorities for the command's force protection policy.
- Develop protection MOPs and MOEs related to risk management.
- Integrate and synchronize protection tasks and systems to increase the probability of mission success.
- Monitor the conduct of operations during execution, looking for variances from the protection plan or scheme of protection. They advise the commander when they detect that protection activities are not being met.
- Incorporate mitigation measures to reduce operational risk to the mission.
- Assess unit risk management and force protection performance during operations. Provide recommended changes to force protection guidance and controls.
- Capture lessons learned from risk management.

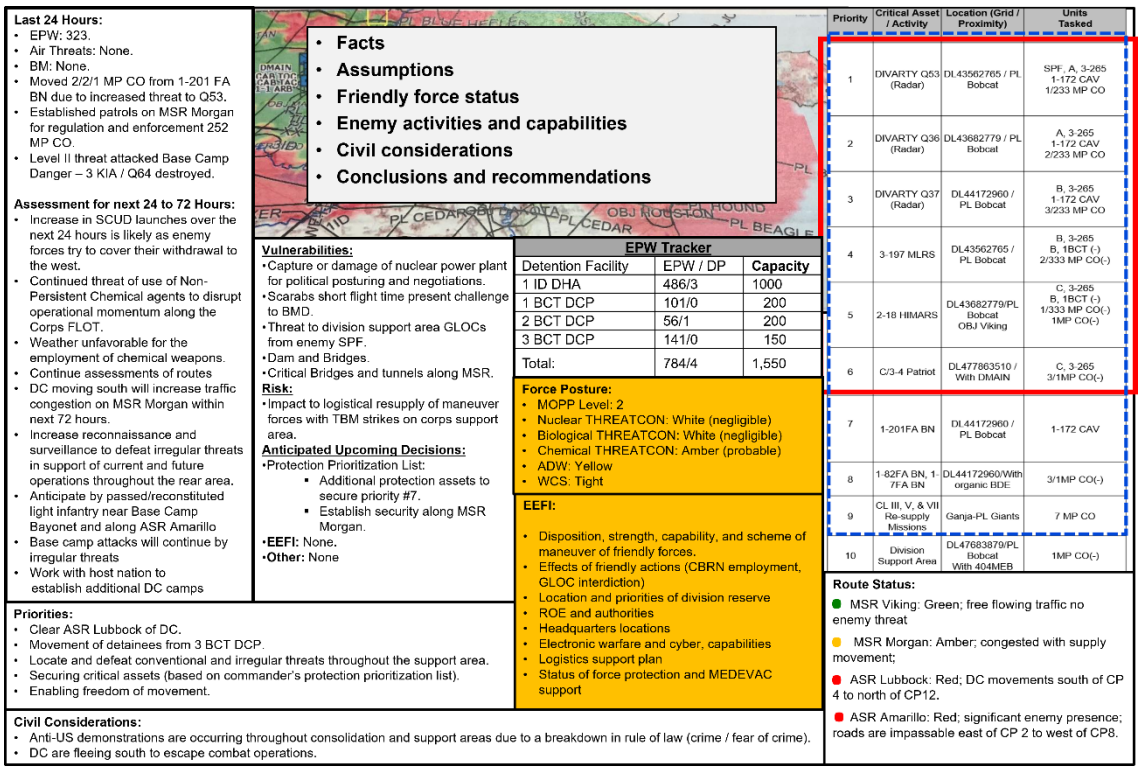
Knowledge Management

3-50. The purpose of knowledge management is to create shared understanding through the alignment of people, processes, and tools within the organizational structure and culture to increase collaboration and interaction between leaders and subordinates. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). Commanders and staffs employ knowledge management techniques to add clarity to information, speed its dissemination, and support situational understanding and protection related decision making. See ATP 6-01.1 for more information on knowledge management.

RUNNING ESTIMATE

3-51. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Failure to maintain accurate running estimates may lead to errors or omissions that result in flawed plans or bad decisions during execution. Running estimates include recommendations for anticipated decisions. During planning, commanders use these recommendations to select feasible, acceptable, and suitable COAs for further analysis. During preparation and execution, commanders use recommendations from running estimates in decision making. See ADP 5-0 for additional information on running estimates.

3-52. The protection working group develops and refines the protection running estimate (see figure 3-5, page 3-18). The protection estimate provides a picture to the command of the status of protection assets and activities, and a basis for reconsidering assumptions when new information arises. Information includes facts, assumptions, constraints, limitations, risks, and issues pertaining to the protection mission and the scheme of protection. It includes the essential tasks from a higher order.



Legend:

ADA	air defense artillery	EPW	enemy prisoner of war
ADW	air defense warning	FA	field artillery
ASR	alternate supply route	FLOT	forward line of troops
BCT	brigade combat team	GLOC	ground lines of communication
BDE	brigade	HIMARS	high mobility artillery rocket system
BM	ballistic missile	KIA	killed in action
BMD	ballistic missile defense	MEDEVAC	medical evacuation
BN	battalion	MLRS	multiple launch rocket system
CAV	cavalry	MOPP	mission oriented protective posture
CBRN	chemical, biological, radiological, and nuclear	MP	military police
		MRBC	multi-role bridge company
CO	company	MSR	main supply route
CP	check point	PL	phase line
DC	dislocated civilian	ROE	rules of engagement
DCP	detainee collection point	SCUD	surface-to-surface missile system
DHA	detainee holding area	THREATCON	threat condition
DIVARTY	division artillery	US	United States
DMAIN	division main command post	WCS	weapons control status
EEFI	essential element of friendly information		

Figure 3-5. Example protection running estimate

MILITARY DECISION-MAKING PROCESS

3-53. 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 MDMP integrates the activities of the commander, staff, subordinate headquarters, and unified action partners to understand the situation and mission, develop and compare COAs, decide on a COA that best accomplishes the mission, and produce an operation plan or order for execution. The MDMP helps leaders apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions. This process helps commanders, staffs, and others think

critically and creatively while planning. The MDMP results in an improved understanding of the situation and a plan or order that guides the force through preparation and execution.

3-54. Effective protection integration during operations depends on full integration into the MDMP and the overall operations process. The protection working group provides input to the commander's MDMP by integrating the threat and hazard assessment with the commander's essential elements of friendly information and the protection prioritization list. See table 3-4 for protection integration into MDMP.

Table 3-4. Protection integration into MDMP

Step 1: Receipt of Mission			
Key Input	***Protection Actions***	***Protection Output***	***Key Output***
• Higher HQ plan or order • New mission anticipated by the commander	• Identify hazards. • Consolidate protection-related running estimates from staffs. • Review consolidated protection array of assets. • Determine protection working group members. • Ensure protection planner integration within the unit planning team.	• Protection working group • Warning and reporting systems • Protection running estimate	• Commander's initial guidance • Initial allocation of time • Warning order
Step 2: Mission Analysis			
Key Input	***Protection Actions***	***Protection Output***	***Key Output***
• Commanders' initial guidance • Higher HQ plan or order • Higher HQ knowledge and intelligence products • Higher HQ assessments and estimates • Running estimates • Design concept (if developed)	• Conduct initial assessments. • Identify requests for information. • Determine available assets. • Conduct and consolidate initial assessments. • Conduct a protection working group. • Recommend and coordinate information collection assets for protection. • Identify CCIR. • Determine OPSEC indicators. • Develop essential tasks within each of the primary protection tasks. • Support analysis requirements for contributions to protection from other warfighting functions • Determine available unified action partner capabilities. • Determine funding sources, as required.	• Consolidated HVT list • RFIs • Threat and hazard assessment • Criticality assessment • Vulnerability assessment • Initial protection priorities • Identify protection priorities • Recommended EEFI and FFIR • Input into information collection plan and PIR	• Updated IPOE • Identified specified and implied tasks • Identified resource shortfalls • Approved constraints • Approved facts and assumptions • Approved CCIRs and EEFIs • Approved initial information collection plan • Updated timeline • Approved problem statement • Approved mission statement • Approved initial commander's intent

Table 3-4. Protection integration into MDMP (continued)

Step 2: Mission Analysis (continued)			
Key Input	***Protection Actions***	***Protection Output***	***Key Output***
			• Commanders initial planning guidance • Approved evaluation criteria Warning order
Step 3: COA Development			
Key Input	***Protection Actions***	***Protection Output***	***Key Output***
• Mission statement • Commander's planning guidance, CCIRs, and EEFIs • Updated IPOE products and running estimates • Evaluation criteria	• Determine array of protection assets. • Integrate protection tasks into COA. • Determine the initial scheme of protection. • Coordinate force health protection support requirements. • Determine priorities, focus, and key tasks and purposes for each protection primary task and activity. • Complete the criticality and vulnerability assessment. • Develop risk management and decision points for risk tolerance.	• Develop PPL. • Update and complete CCIR/IR. • Determine residual risk. • Develop initial OPSEC measures and countermeasures. • Develop an initial scheme of protection	• Commander's selected COAs with COA statements and sketches • Commander's refined planning guidance and evaluation criteria • Updated running estimates and IPOE • Updated assumptions
Step 4: COA Analysis (War Game)			
Key Input	***Protection Actions***	***Protection Output***	***Key Output***
• Updated running estimates • Commander's COA analysis guidance • COA statements and sketches • COA analysis specific assumptions	• Identify limitations and shortfalls of protection tasks for each COA. • Determine branches, sequels, decision points, unintended consequences, and second- and third-order effects. • Develop risk management and decision points for risk tolerance. • Develop MOE and MOP.	• Recommended updates to PPL • Refined CCIR/IR/EEFI • Refined information collection plan • Refine OPSEC measures and countermeasures • Initial risk management and risk tolerance decision point matrix • Refined scheme of protection	• Refined COAs • Draft DST and DSM • COA synchronization matrix or set of sketch notes • Refined task organization • Identification of potential branches and sequels • Updated running estimates • Updated assumptions

Table 3-4. Protection integration into MDMP (continued)

Step 5: COA Comparison			
Key Output	***Protection Actions***	***Protection Output***	***Key Output***
• Updated running estimates • Refined COAs • Evaluation criteria • War-game results • Updated assumptions	• Compare economy-of-force and risk reduction measures. • Develop risk decision criteria and weighting for COA.	• Refined protection priorities • Refined PPL • Refined EEFI • Refined scheme of protection	• Staff-recommended COA • Cost and benefits between COAs • COA selection rationale • Updated running estimates • Updated assumptions • Updated intelligence requirements • Updated IPOE
Step 6: COA Approval			
Key Output	***Protection Actions***	***Protection Output***	***Key Output***
• Updated running estimates • Evaluated COAs • Recommended COA • Updated assumptions	• Refine risk management and decision points for risk tolerance. • Brief scheme of protection. • Brief protection task specifics, as required.	• Refined protection priorities • Refined PPL • Refined EEFI • Refined scheme of protection	• Approved COA with any modifications • Refined commander's intent, CCIRs, and EEFIs • Warning order
Step 7: Orders Production, Dissemination, and Transition			
Key Output	***Protection Actions***	***Protection Output***	***Key Output***
• Approved COA with any modifications • Refined commander's intent, CCIRs, and EEFIs • Updated assumptions • Commanders' final planning guidance • Updated running estimates and IPOE	• Identify and assess hazards. • Monitor risk management and decision points. • Refine and develop protection annex and supporting appendixes. • Implement risk management controls, supervise, and assess.	• Protection annex and supporting appendixes	• Operation plan or order • Subordinates understand the plan or order

Legend:

CCIR	commander's critical information requirement	HVT	high-value target
COA	course of action	IPOE	intelligence preparation of the operational environment
DST	decision support template	IR	intelligence requirements
DSM	decision support matrix	MOE	measure of effectiveness
EEFI	essential element of friendly information	MOP	measure of performance
FFIR	friendly forces information requirements	OPSEC	operations security
HQ	headquarters	PIR	priority intelligence requirements
		PPL	protection priority list
		RFI	request for information

3-55. Staffs use a synchronization matrix as a tool to record the results of Step 4 courses of action analysis (war game) of the MDMP process to help synchronize a COA across time, space, and purpose in relationship to potential enemy and civil actions. The synchronization matrix typically identifies those pieces of critical information necessary to guide, record, and synchronize the war game, such as—

- Weather and light data.
- Area of influence critical information.
- Enemy actions.

- Population or civilian action when expected to impact operation.
- Decision points.
- Control measures.
- Friendly actions.
- Risk.
- Other organizations or partners potentially impacting a COA.

3-56. Table 3-5 provides an example of the protection cell inputs to the synchronization matrix tool. For additional information on the synchronization matrix tool, see FM 5-0.

Table 3-5. Protection cells input to a synchronization matrix tool example

Time/Event/Phase		*Initial Set*	*Turn 1*			*Turn 2*		
		H - hours (or event or phase)	***H- 24 hours (or event or phase)***			***H + 24 to H + 36 (or event or phase)***		
Step		**Initial Set**	**Action**	**Reaction**	**Counter-Action**	**Action**	**Reaction**	**Counter-Action**
Protection	**Priority 3**	No Change	No Change	No Change	No Change	Relocate to DL3980 2620; task-organize additional protection assets to secure and coordinate for AMD support	No Change	No Change
	Priority 11	Coordinate with HN for movement of DC on alternate route to clear ASR Lubbock	Coordinate with HN for movement of DC on alternate route to clear ASR Lubbock	No Change	No Change	Establish route security on MSR Viking	No Change	No Change
	Priority 13	Division main CP relocates with 1st ABCT Coordinate for AMD support	No Change	No Change	No Change	No Change	No Change	No Change

Legend:

ABCT	armored brigade combat team
AMD	air and missile defense
ASR	alternate supply route
CP	command post
DC	dislocated civilian
H	hour
HN	host nation
MSR	main supply route

TROOP LEADING PROCEDURES

3-57. Company-level and smaller units that lack formal staffs use troop leading procedures to plan and prepare for operations. *Troop leading procedures* are a dynamic process used by small-unit leaders to analyze a mission, develop a plan, and prepare for an operation (ADP 5-0). Leaders typically perform troop leading procedures while working alone or with a small group (such as executive officers, first sergeants, supply sergeants, and other specialists in the unit) to solve tactical problems.

- Step 1-Receive the mission.

- Step 2-Issue a warning order.
- Step 3-Make a tentative plan.
- Step 4-Initiate movement.
- Step 5-Conduct reconnaissance.
- Step 6-Complete the plan.
- Step 7-Issue the order.
- Step 8-Supervise and refine.

3-58. During step 3 of the troop leading procedures, leaders conduct mission analysis to better understand the problem, situation, and mission to drive subsequent planning. This form of mission analysis uses the mission variables of mission, enemy, terrain and weather, troops, and support available, time available, civil considerations, and informational considerations, represented by the mnemonic METT-TC (I) to determine protection requirements.

3-59. Company-level and smaller units use the information derived from the mission analysis to develop a course of action. During course of action development leaders will determine if their protection capabilities to prevent or mitigate detection and the effects of threats and hazards to enable mission accomplishment. These units employ individual Soldier common task and unit tactics, techniques, and procedures to enhance protection and survivability.

- Individual Soldier task include camouflage, cover, concealment, and the ability to properly wear their MOPP suit, don the protective mask, employ noise, and light discipline.
- Units employ tactics, techniques, and procedures to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission. To increase a unit's survivability, commanders can employ security operations, modify tempo, take evasive action, maneuver to gain positional advantages, decrease electromagnetic signatures, disperse, and establish local security.

3-60. Company-level and smaller units coordinate with their higher headquarters for additional protection resources needed to achieve mission success. See FM 5-0 for additional information on troop leading procedures.

PROTECTION PREPARATION

3-61. The force is often most vulnerable to an enemy or adversary surprise attack during preparation. Preparations during competition below armed conflict and crisis create conditions that improve friendly force opportunities for success during armed conflict. Preparation requires commander, staff, unit, and Soldier actions to ensure that the force is trained, equipped, and ready to execute operations. Preparation in support of protection is not a linear activity—protection preparation is a continuous and enduring activity.

3-62. Preparation activities help commanders, staffs, and Soldiers understand a situation and their roles in upcoming operations. Protection preparation requirements occur throughout all Army operations. They focus on deterring and preventing the enemy or adversaries from taking actions that would affect combat power during future operations. The execution of protection tasks with ongoing preparation activities helps prevent negative effects. Commanders ensure the integration of protection warfighting function tasks to safeguard friendly forces, civilians, and infrastructure while forces prepare for operations. Active defense measures help deny the initiative to the enemy or adversary, while the execution of passive defense measures prepares the force against threat and hazard effects and accelerates the mitigation of those effects.

PREPARATION CONSIDERATIONS

3-63. As the staff monitors and evaluates the performance or effectiveness of a friendly COA, information collection operations gather information that may confirm or deny forecasted threat COAs. As the threat changes, the risk to the force changes. Some changes may require a different protection posture or the implementation or cessation of specific protection measures, activities, or restraints. The protection cell analyzes changes or variances that may require modifications to protection priorities and obtains guidance when necessary. Threat assessments are a dynamic and continually changing process. Protection planners

stay alert for changing indicators and warnings within the operational environment that would signal new or fluctuating threats and hazards.

3-64. Detailed intelligence is used to develop threat assessments, and changes in the situation often dictate adjustments or changes to the plan when they exceed variance thresholds established during planning. During competition below armed conflict and crisis, the staff continues to monitor and evaluate the overall situation because variable threat assessment information may generate new priority intelligence requirements, while changes in asset criticality could lead to new friendly force information requirements. Updated information requirements could be required based on changes to asset vulnerability and criticality when combined with the threat assessment.

3-65. Commanders exercising command and control direct and lead throughout the operations process. Commanders' actions during preparation, competition below armed conflict, and crisis may include—

- Reconciling the threat assessment with professional military judgment and experience.
- Providing guidance on risk tolerance and making risk decisions.
- Emphasizing protection tasks during rehearsals.
- Minimizing unnecessary interference with subunits to allow maximum preparatory time.
- Circulating throughout the environment to observe precombat inspections.
- Directing control measures to reduce risks associated with preparatory movement.
- Expediting the procurement and availability of resources needed for protection implementation.
- Requesting higher headquarters support to reinforce logistical preparations and replenishment.

3-66. Depending on the situation and threat, some protection tasks may be conducted for short or long durations, covering the course of several missions or an entire operation. The staff coordinates the commander's protection priorities with vulnerability mitigation measures and clearly communicates them to higher headquarters, subordinate and adjacent units, civilian agencies, and personnel that are part of the force or those that may be impacted by the task or control.

3-67. Subordinate leaders also conduct integration processes and provide supervision to ensure that Soldiers understand their responsibilities and the significance of protection measures and tasks. This is normally accomplished through training, rehearsals, task organization, and resource allocation. Rehearsals, especially those using opposing force personnel, can provide a measure of protection plan effectiveness.

PROTECTION DURING PREPARATION ACTIVITIES

3-68. Commanders, units, and Soldiers conduct activities (as described in ADP 5-0) to help ensure that the force is protected and prepared for execution. Protection is incorporated throughout preparation activities during competition below armed conflict and crisis. Key protection activities include—

- Continuing to coordinate and conduct liaison with adjacent and protected units..
- Initiating information collection.
- Conducting rehearsals that focus on transitioning protection capabilities through the phases of the operation.
- Completing task organization.
- Conducting plans-to-operations transitions.
- Managing and preparing terrain
- Refining the scheme of protection.
- Implement vulnerability reduction measures.
- Direct OPSEC measures.
- Initiating security operations.
- Prepare and improve survivability positions.
- Initiating network preparations.
- Training with defended assets.
- Continuing to build partnerships and teams.
- Considering effects of protection activities in the information dimension.

- Analyzing terrain and weather.

Continue to Coordinate and Conduct Liaison

3-69. Continuous coordination and liaison between the command and unified action partners helps build a unity of effort and instill situational understanding of the scheme of protection and protection priorities established by higher, subordinate, and adjacent units and unified action partners. Unified action partners may also provide initial health care services for wounded U.S. troops engaged in multinational operations. The synchronization with unified action partners on all health care delivery to U.S. Soldiers and multinational forces is essential to ensure that the appropriate medical resources are available when needed.

Initiate Information Collection

3-70. Commanders and staffs continuously plan, task, and employ collection assets and forces to collect timely and accurate information that helps satisfy the CCIRs and other information requirements. For example, the protection working group uses staff analysis and coordination with higher headquarters to determine which critical assets or locations are likely to be attractive targets and might require protection assets.

3-71. The staff develops and refines the common operational picture of the area of interest. Relevant data obtained from information collection helps protection cells and working groups fill information gaps; refine potential threats and hazards data; and validate assumptions before, during, and after operations to improve protection efforts.

Initiate Security Operations

3-72. Commanders and staffs continuously plan and coordinate security operations throughout the operation. Security operations are those operations undertaken by a commander that provide an early and accurate warning of enemy or adversary operations. They also provide the force with the time and maneuver space necessary to react to the enemy or adversary, and to develop the situation so that commanders can effectively use the protected force.

3-73. One of the most common methods of providing protection for ground combat forces is the use of security operations. The ultimate goal of security operations is to protect main body forces from surprise and deny the enemy the freedom of action to collect on friendly forces. The protected force may not always be a military force; it can also be the civilian population, civil institutions, and civilian infrastructure in the unit's assigned area (see ADP 3-90).

3-74. Security operation types reflect differing levels of combat power that can be applied to protect an asset or force from a directed threat, and they are typically conducted by maneuver forces task organized for the degree of security required. The primary purpose of a screen operation is to provide early warning, thereby preventing surprise. Guard and cover operations involve fighting to gain time while also observing and reporting information with differing levels of capability and autonomy for independent action. Area security focuses on the protected force, installation, routes, or area.

Manage and Prepare Terrain

3-75. Terrain management is the process of allocating terrain by establishing areas of operations, designating assembly areas, and specifying locations for units and organizations to deconflict activities that might interfere with each other. Staffs deconflict operations, control movements, and deter the fratricide of units and unified action partners as they maneuver through the area of operations. The secure movement of theater resources is essential to ensure that commanders receive the forces, supplies, and equipment needed to support the operational plan and changing tactical situations, and it is an essential part of terrain management. Modifying the physical environment involves shaping the terrain to gain an advantage, such as improving cover, concealment, observation, fields of fire, obstacle effects through reinforcing obstacles, or mobility operations for the initial positioning of forces.

Analyze Weather and Terrain

3-76. Terrain and weather analysis are inseparable and directly influence each other's impact on military operations. Terrain includes natural features (such as rivers and mountains) and man-made features (such as cities, airfields, and bridges). Leaders analyze terrain using the five military aspects of terrain expressed in the memory aid observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment. The military aspects of weather include visibility, wind, precipitation, cloud cover, temperature, and humidity. Terrain and weather are neutral and impact both friendly and enemy operations, including impacts on communications, space-based support (including communication, navigation, and surveillance), military deception, and use of the electromagnetic spectrum. See FM 5-0 for additional information.

Integrate Information Advantage Activities

3-77. Information advantage is an operational benefit derived when friendly forces understand and exploit the informational considerations of the operational environment to achieve information objectives while denying the threat's ability to do the same. Most types of information advantage result from physical and human factors or activities intrinsic to the operations that Army forces conduct. A force that effectively communicates and protects its information while preventing the enemy from doing the same has an advantage. Defending networks, data, and systems; implementing OPSEC; and conducting security operations contribute to information advantages by protecting friendly information.

3-78. Commanders recognize that protection extends beyond the physical domains, to include the information dimension and cyberspace. The information dimension is the content, data, and processes that individuals, groups, and information systems use to communicate. They ensure close coordination between the protection cells/working group and the information and cyberspace electromagnetic activities elements/working groups. They visualize and understand how protection tasks and activities affect the information dimension and cyberspace and, in turn, how information advantage activities and cyberspace electromagnetic activities contribute to and support the protection warfighting function.

PROTECTION WORKING GROUP

3-79. The protection working group is led by the chief of protection and brings together representatives of all staff elements concerned with protection (see table 3-1, page 3-4). Preparation includes increased application and emphasis on protection measures. During preparation, the protection working group—

- Provides recommendations to refine the scheme of protection.
- Conducts analysis and makes recommendations for changes to the protection prioritization list based on the commander's priorities and changes during the phase of an operation.
- Identifies what harms friendly forces.
- Recommends systems to detect new threats to critical assets.
- Proposes the refinement of OPSEC measures.
- Monitors and receives feedback from tactical units on troop movements.
- Provides recommendations for improving survivability.
- Liaises and coordinates with adjacent and protected units.
- Determines protection indicators and warnings for information collection operations.
- Conducts information briefs.
- Analyzes and proposes vulnerability reduction measures.
- Provides recommended revisions to tactical standard operating procedures.
- Identifies personnel recovery assets and develops personnel recovery plans.

3-80. During preparation, the protection working group ensures that the controls and risk reduction measures developed during planning have been implemented and are reflected in plans, standard operating procedures, and running estimates, even as the threat assessment is continuously updated. New threats and hazards are identified or anticipated based on newly assessed threat capabilities or changes in environmental conditions as compared with known friendly vulnerabilities and weaknesses. Commanders conduct after action reviews and war-game to identify changes to the threat. The protection working group lead maintains a list of

prioritized threats, adverse conditions, and hazard causes. The challenge is to find the root cause or nature of a threat or hazard so that the most effective protection solution can be implemented and disseminated.

3-81. Protection specialty working groups (antiterrorism, explosive ordnance, CBRN, detainee operations) feed information to the protection working group and incorporate elements from other warfighting functions. Commanders augment the working groups with other unit specialties and unified action partners, depending on the operational environment and unit mission. The lead for each working group determines the agenda, meeting frequency, composition, input, and expected output. Ultimately, the output from the working groups helps refine protection priorities, protection running estimates, assessments, essential elements of friendly information, and the scheme of protection.

Antiterrorism Working Group

3-82. The antiterrorism working group is led by the antiterrorism officer and includes members from the protection working group, subordinate commands, host-nation agencies, and other unified action partners. It is normally conducted at echelons above brigade as required. It—

- Develops and refines antiterrorism plans.
- Oversees the implementation of the antiterrorism program.
- Addresses emergent and emergency antiterrorism program issues.
- Provides planning advice on the resolution of complex vulnerabilities, crisis management, and possible threats.

Explosive Ordnance Working Group

3-83. The explosive ordnance working group is led by the EOD officer and includes other members of the protection working group, subordinate commands, host-nation agencies, and other unified action partners. The explosive ordnance working group is normally conducted at echelons above brigade as required. It—

- Disseminates explosive ordnance information (including best practices), explosive ordnance trend analysis, and explosive ordnance defeat equipment and training issues.
- Determines operational tactics to analyze and defeat the area of operations explosive ordnance networks.
- Recommends to the commander explosive ordnance defeat initiatives relating to equipment, intelligence, and operations.
- Identifies explosive ordnance defeat requirements and issues throughout the unit, including separate and subordinate units.

Chemical, Biological, Radiological, and Nuclear Working Group

3-84. The CBRN working group is led by the CBRN officer and includes other members of the protection working group (see table 3-1, page 3-4), subordinate commands, host-nation agencies, and other unified action partners. It normally disseminates CBRN operations information, including trend analysis, defense best practices and mitigating measures, operations, the status of equipment and training issues, CBRN logistics and response, and remediation efforts. It also refines CBRN threat, hazard, and vulnerability assessments.

PROTECTION EXECUTION

3-85. The execution of protection is continuous. Commanders implement control measures and allocate resources that are sufficient to ensure protection, continuity, and restoration. Employed mitigation measures allow the force to quickly respond to and recover from the threat or hazard effects, ensuring a force that remains effective and continues the mission. Control measures may include restraint after careful and disciplined balancing decisions regarding the need for security and protection in the conduct of military operations.

3-86. As operations develop and progress, the commander interprets information that flows from systems for indicators and warnings that signal the need for the execution or adjustment of decisions. The continuous

and enduring character of protection makes the continuity of protection capabilities essential during execution.

3-87. The staff monitors the conduct of operations during execution, looking for variances from the scheme of maneuver and emerging vulnerabilities. When variances exceed a threshold value, adjustments are made to prevent a developing vulnerability or to mitigate the effects of the unforecasted threat or hazard. The status of protection assets is tracked and evaluated on the effectiveness of the protection systems as they are employed. Commanders maintain protection by applying comprehensive protection capabilities to the main and supporting efforts. Protection can be derived as a by-product or a complementary result of some combat operations (such as security operations), or it can be deliberately applied as commanders integrate and synchronize tasks that comprise the protection warfighting function.

3-88. The protection cell and working group monitor and evaluate several critical ongoing functions associated with execution for operational actions or change indicators that impact protection capabilities, which include—

- Changes to threat and hazard assessments.
- Changes in force vulnerabilities.
- Changes to unit capabilities.
- Relevancy of facts.
- Validity of assumptions.
- Reasons that new conditions affect the operation.
- Protection capabilities.
- Identification of what is harming friendly forces.
- System failures.
- Resource allocations.
- Increased risks.
- Support efforts.
- Force protection implementation measures, including site-specific antiterrorism measures.

ACTIVITIES OF EXECUTION

3-89. *Execution* is the act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation (ADP 5-0). During execution, commanders (supported by their staffs) focus their efforts on translating decisions into actions. Inherent in execution is deciding whether to execute planned actions, such as changing phases or executing a branch plan. Execution also includes adjusting the plan based on changes in the situation and an assessment of the operation's progress. Assessing, decision making, and directing action are major activities during execution. See FM 6-0 for additional information on decision making during execution.

RAPID DECISION MAKING AND SYNCHRONIZATION PROCESS

3-90. Operational and mission variables continually change throughout execution; therefore, commanders and staffs commonly use rapid decision making and synchronization processes to facilitate faster solutions. While the MDMP seeks the optimal solution, the rapid decision making and synchronization process seeks a timely and effective solution within the commander's intent, mission, and concept of operations. The protection cell participates in the rapid decision making and synchronization process to facilitate continuous integration and synchronization of protection capabilities within all warfighting functions to address ever-changing situations.

3-91. During execution, commanders and staffs monitor the situation to identify changes in conditions and then ask if these changes affect the overall conduct of operations or their part in them and if the changes are significant. Finally, they identify if the changed conditions represent variances from the order—especially opportunities and risks. Protection cells use running estimates to look for indicators of variances that affect their areas of expertise. See table 3-6 for examples of protection indicators. See FM 6-0 for additional information on the rapid decision making and synchronization process.

Table 3-6. Examples of change indicators

Type	*Indicators*	
General	• Answer to a commander's critical information requirement • Identification of an information requirement • Change in mission • Change in organization of unit	• Change in leaders • Signing or implementation of peace treaty or other key political arrangement • Change in capabilities of subordinate unit • Change in role of host-nation military force
Protection	• Transition to crisis, armed conflict, or competition below armed conflict • Chemical, biological, radiological, and nuclear report or other indicators of enemy chemical, biological, radiological, and nuclear use • Shift in boundaries • Report or other indicators of explosive hazard • Indicators of coordinated enemy actions against civilians or friendly forces	• Increase in organized protests or riots • Identification of threats to communications or computer systems • Reports of enemy targeting critical host-nation infrastructure • Identification of an increased threat • Escalation of force incidents • Task-organization changes • New phase of an operation • Increased criminal activity in each area of operations

PROTECTION ASSESSMENT

3-92. Protection assessment is an essential activity that continuously occurs throughout the operations process. It also involves comparing forecasted outcomes with events to determine the effectiveness of protection. Assessment helps the commander determine the progress toward attaining the desired end state, achieving objectives, and establishing the effectiveness of protection support in Army operations. While a failure in the execution of security and mobility support tasks is typically easy to detect, the successful application may be difficult to assess and quantify.

CONTINUOUS ASSESSMENT

3-93. *Assessment* is the determination of the progress toward accomplishing a task, creating a condition, or achieving an objective (JP 3-0). Commanders typically base assessments on their situational understanding, which is generally a composite of several informational sources and intuition. Assessments also involve continuously monitoring and evaluating the operational environment to determine what changes might affect the conduct of operations. The activities of assessment include monitoring the current situation to collect relevant information, evaluating progress toward attaining end-state conditions, achieving objectives, performing tasks, and recommending or directing actions for improvement.

3-94. Throughout the operations process, commanders integrate their assessments with those of the staffs, subordinate commanders, and other unified action partners. The primary tools for assessing the progress of the operation include the operation order, the common operational picture, personal observations, running estimates, and the assessment plan. Staff members develop running estimates that illustrate the significant aspects of a particular activity or function over time. Commanders maintain situational understanding and direct adjustments with the use of these estimates. Significant changes or variances among or within running estimates can signal a threat or an opportunity, alerting commanders to take action.

3-95. The assessment plan is enabled by monitoring and evaluating criteria derived from the protection warfighting function primary tasks. The criteria used to monitor and evaluate the situation or operation may be represented as an MOE or an MOP. These measures are discrete, relevant, and responsive benchmarks that are useful in all operations. They may contain the CCIRs and the essential element of friendly information and may generate information requirements. MOEs and MOPs can be significant decision support tools and may drive transition periods, resource allocations, and other critical decisions.

ASSESSMENT DURING PLANNING

3-96. The staff conducts analysis to assess threats, hazards, criticality, vulnerability, and capabilities to assist commanders in determining protection priorities, task-organization decisions, and protection task integration. Members of the protection cell evaluate COAs during MDMP against the evaluation criteria derived from the protection warfighting function to determine if each COA is feasible, acceptable, and suitable in relation to its ability to protect or preserve the force.

ASSESSMENT DURING PREPARATION

3-97. Assessment occurs during preparation and includes activities required to maintain situational understanding; monitor and evaluate running estimates, tasks, MOEs, and MOPs; and identify variances for decision support. These assessments generally provide commanders with a composite estimate of preoperational force readiness or status in time to make adjustments.

3-98. During preparation operations, the protection working group focuses on threats and hazards that can influence preparatory activities, including monitoring new Soldier integration programs and movement schedules and evaluating live-fire requirements for precombat checks and inspections. The protection working group may evaluate training and rehearsals or provide coordination and liaison to facilitate effectiveness in high-risk or complex preparatory activities, such as movement and sustainment preparation.

ASSESSMENT DURING EXECUTION

3-99. The protection working group monitors and evaluates the progress of current operations to validate assumptions made in planning and to continually update changes to the situation. The protection working group continually meets to monitor threats to protection priorities, and working group members recommend changes to the protection plan as required. They also monitor the conduct of operations, looking for variances from the operations order that affect their areas of expertise. When variances exceed a threshold value developed or directed during planning, the protection cell may recommend an adjustment to counter an unforecasted threat or hazard or to mitigate a developing vulnerability. It also tracks the status of protection assets and evaluates the effectiveness of the protection systems as they are employed. Additionally, the protection working group monitors the actions of other staff sections by periodically reviewing plans, orders, and risk assessments to determine if those areas require a change in protection priorities, posture, or resource allocation.

3-100. The protection working group monitors and evaluates—

- Changes to threat and hazard assessments.
- Changes in force vulnerabilities.
- Changes to unit capabilities.
- The relevancy of facts.
- The validity of assumptions.
- Reasons that new conditions affect the operation.
- Running estimates.
- Protection tasks.
- System failures.
- Resource allocations.
- Increased risks.
- Supporting efforts.

- Force protection implementation measures, including site-specific antiterrorism measures.
- OPSEC measures and countermeasures.

MEASURES OF EFFECTIVENESS AND PERFORMANCE

3-101. Criteria in the forms of MOEs and MOPs helps determine the progress toward attaining end-state conditions, achieving objectives, and performing tasks. An MOE helps determine if a task is achieving its intended results, and an MOP helps determine if a task is completed properly. MOEs and MOPs are simply criteria; they do not represent the assessment itself. MOEs and MOPs require relevant information in the form of indicators for evaluation. They are developed during planning, refined during preparation, and monitored during execution by the protection cell and working group.

MEASURE OF EFFECTIVENESS

3-102. A *measure of effectiveness* is an indicator used to measure a current system state, with change indicated by comparing multiple observations over time. (JP 5-0). An MOE helps measure changes in positive and negative conditions and is oriented to mission accomplishment, focuses on the results or consequences of an action, and is used to assess changes in the operational environment. This is more often a subjective assessment because it tends to measure long-term results. Thus, MOEs may consist of a series of indicators that are used to judge success or failure.

3-103. Significant changes to indicators can be subtle and may only occur over a long period of time. The enduring nature of protection can cause complacency requiring leaders to stay focused on, identifying, and assessing accurate protection indicators and warnings. Assessing these indicators and warning assist commanders and staffs in maintaining situational understanding and alert them to hazards and associated risk. If a protection measure appears to be failing in its desired effect, the result may be attributed to—

- Personnel or equipment system failure.
- Insufficient resource allocation at vulnerable points.
- Variances from the anticipated threat-combat power ratio, resulting in an increased risk equation.
- Ineffective supporting efforts, leading to a cumulative failure of more critical elements.
- Faulty planning assumptions.

3-104. Assessment identifies the magnitude and significance of variances in performance or conditions (from those that were expected through prior forecasting) to determine if an adjustment decision is needed. Commanders monitor the ongoing operation to determine if it is progressing satisfactorily according to the current plan, including fragmentary orders that have modified it. The staff assesses the situation in relation to established criteria that includes protection progress. This assessment ensures that facts and assumptions remain valid and identifies new facts and assumptions. Assessment decreases reaction time by anticipating future requirements and linking them to current plans.

MEASURE OF PERFORMANCE

3-105. A *measure of performance* is an indicator used to measure a friendly action that is tied to measuring task accomplishment (JP 3-0). An MOP helps answer questions such as, “Was the action taken?” or “Were the tasks completed to standard?” and confirms or denies that a task has been properly performed. An MOP is friendly-force-oriented, measures task accomplishment and, in its simplest form, answers the question of whether a task was performed successfully. See ADP 5-0 for additional information on MOPs.

LESSONS LEARNED INTEGRATION

3-106. The way in which organizations and Soldiers learn from mistakes is key in protecting the force. Although the evaluation process occurs throughout the operations process, it also occurs as part of the after action review and assessment following the mission. Leaders demonstrate their responsibility to the sound stewardship practices and risk management principles required to ensure minimal loss of resources and military assets due to hostile, nonhostile, and environmental threats and hazards. Key lessons learned are

immediately applied and shared with other commands. Commanders develop systems to ensure the rapid dissemination of lessons they have approved for implementation and the tactics, techniques, and procedures proven to save lives and protect equipment and information. The protection working group at each command echelon evaluates the integration of lessons learned and constantly coordinates protection lessons with other staff elements within and between the levels of command. Post operational evaluations typically—

- Identify threats that were not identified as part of the initial assessment or identify new threats that evolved during the operation or activity. For example, reevaluate when personnel, equipment, the environment, or the mission changes the initial assessments.
- Assess the effectiveness of supporting operational goals and objectives.
- Assess the implementation, execution, and communication of controls. For example, determine if the controls positively or negatively impacted training or mission accomplishment and determine if they supported existing doctrine and tactics, techniques, and procedures.
- Assess the accuracy of residual risk and the effectiveness of controls in eliminating hazards and controlling risks.
- Ensure coordination throughout the integration processes.
  - Was the process integrated throughout all phases of the operation?
  - Were risk controls effective?
  - Were risk decisions made at the appropriate level?
  - Did any unnecessary risks or benefits outweigh the cost in terms of expense, training benefits, or time?
- Ensure that the process is cyclic and continuous throughout the operation.

Chapter 4
Protection Cells

"The purpose of the staff is to serve the line."

Military Maxim

The protection warfighting function applies to all levels of command. Commands utilize a protection cell and protection working group to integrate and synchronize protection tasks and systems for each phase of an operation or major activity. The Army structure provides established protection cells at division level and above. Protection cells are found in main, tactical, and rear command posts at division and corps levels and in the main or contingency command posts at theater Army headquarters. At the brigade level, commanders designate a senior staff officer to serve as the chief of protection and as the lead for the protection working group. This chapter describes the roles and responsibilities of the protection cell at corps echelon and below, identifies the sections that make up the protection cell, describes the protection cell's relationship with other key staff sections, and identifies the working groups in which the protection cell must participate.

ROLES AND RESPONSIBILITIES

4-1. The protection cell advises, visualizes, and outlines protection requirements to the commander; prioritizes and synchronizes mitigating strategies, and coordinates protection. The protection cell recommends measures to deny enemy stand-off, reducing the degradation, disruption, and denial of friendly force operations. The protection cell advises commanders on the transition criteria required for advancing operations based on when the force is postured to best protect itself.

4-2. During the planning process, the protection cell provides input to the commander's MDMP by identifying tasks, systems, and methods that will prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action based on the developing courses of action. The protection cell ensures the integration of protection equities throughout the operations process via integrating processes, MDMP, working groups, planning sessions, and coordination between warfighting functions and echelons of command. This leads to the development and refinement of a scheme of protection and a protection plan that are comprehensive, integrated, layered, redundant, and enduring. All members of the protection cell and working group provide input and conduct actions that have beneficial output. The agenda, frequency, composition, input, and expected output for the working group are based on mission variables, MDMP integration, and commander's guidance.

4-3. The protection cell helps craft protection strategies reflected in the concept of protection and supports the maneuver concept included in the base order and appropriate annexes and appendixes. Some protection tasks, such as force health protection and coordinate air and missile defense support, may also have representation in other operational cells at higher-level organizations. Some significant, protection-related products produced in the planning process includes—

- A scheme of protection that supports and nests with the operational concept and scheme of maneuver.
- A running estimate that reflects protection tasks and systems.
- A quantifiable level of risk for specific events and activities.
- Protection MOE and MOP and threshold variances.
- Recommendations for the CCIRs that reflect decision criteria from protection tasks and systems.

- A protection prioritization list.
- Decision points based on the commander's risk tolerance level.
- Development of Annex E, Protection.

4-4. The protection cell identifies and recommends refinements to the courses of action necessary to reduce vulnerability, create windows of opportunity, and ensure mission success. The protection cell provides vulnerability mitigation measures to help reduce risks associated with a particular COA and conducts planning and oversight for multidomain operations. Representatives from the protection cell provide input to plans and future operations. Commanders tailor and augment the protection cell with functional expertise to form the protection working group as the mission requires.

4-5. A chief of protection is assigned to a division, corps, and theater Army headquarters staff. At brigade and below, the chief of protection is ad hoc, and the commander usually designates a senior leader to perform this role. The chief of protection participates in various forums to facilitate the continuous integration of protection tasks and systems throughout the operations process.

THEATER PROTECTION CELL

4-6. The theater Army requires a multifunctional capability to provide operational planning, synchronization, integration, and command and control of protection capabilities in support of the joint commander's requirements during competition below armed conflict, crisis, and armed conflict. A key factor in maintaining operational awareness and enabling unity of effort is theater sustainment command participation in and with combatant command, theater Army, and subordinate joint forces command boards, bureaus, centers, cells, and working groups. Established on an as-required basis, these events and elements set policies and priorities, provide for improved integration and synchronization, and enable the effective flow of resources in support of operational objectives. Protection cells may recommend the commander to tailor protective elements when required for the campaign or major operation. Tailoring includes the makeup of the force and the recommended sequence of its deployment. In addition to tailoring force packages, the theater Army protection cell—

- Examines other protection plans, concepts, and strategies for insights on survivability, security force employment, task organization, and economy-of-force options.
- Considers multinational and host-nation capabilities and determines how to integrate them into protection.
- Determines if other capabilities or disciplines (civil-military activities, information engagement tasks) from within the force can provide complementary or reinforcing capabilities to achieve protection and reduce the likelihood of successful adversarial attacks.

4-7. When the theater Army commander is designated as the joint force land component commander responsible for the joint security area, the theater Army protection cell (with augmented joint, interagency, and multinational personnel) provides the nucleus of the joint security coordination center. The protection cell—

- Integrates and synchronizes protection tasks and systems in the operations process.
- Advises commanders on the priorities for protection and coordinates the implementation and sustainment of measures to protect assets according to the commander's priorities.
- Provides input to the commander's plan by integrating the threat and hazard assessment to minimize vulnerability and provides vulnerability mitigation measures to help reduce risks.

Note. In support of the joint force commander's concept of operations, the joint force land component commander plans and conducts security operations to ensure the protection of U.S. and multinational mission-essential assets and the support areas required for sustainment of land operations. The joint force land component commander will typically assign an Army unit, potentially a maneuver enhancement brigade, for the security of defined operational areas to serve as its operational protection headquarters and assist the supported headquarters in retaining the freedom of action not assigned to maneuver units. See JP 3-10 for additional information on joint security operations. See JP 3-31 for additional information on joint land operations.

CORPS PROTECTION CELL

4-8. The corps requires a multifunctional capability to provide operational planning, synchronization, integration, and command and control of protection capabilities in support of theater Army requirements during competition below armed conflict, crisis, and armed conflict throughout the corps area of operations. The protection cell must focus on predictive and proactive measures that prevent and mitigate enemy threats from achieving their objectives. The protection cell does not require representatives from every primary task functional element of protection. However, dedicated members should coordinate with other personnel and special staff elements as required.

4-9. The corps protection cell coordinates with the other staff sections at different echelons of command to synchronize and converge multidomain protection capabilities that prevent or mitigate the enemy's freedom of action throughout the corps area of operations and integrates other corps protection capabilities to support operations at the division. The corps protection cell integrates with intelligence to see and understand the environment, coordinate counterintelligence to clearly recognize threat actors, and identify key enemy systems that present the greatest risk to friendly forces. The protection cell coordinates with the assistant chief of staff, signal (G-6) concerning information and cyber protection tasks, the surgeon concerning force health protection measures, and the fires cell for lethal and nonlethal targeting of enemy systems that present a protection challenge to the force.

4-10. The protection cell provides functional protection expertise and advises the commander in developing essential elements of friendly information and the corps protection-related products. The corps chief of protection must visualize and describe to the corps commander, staffs, and leaders the conditions and situations before transitioning, expanding operations, and moving forces when there is a protection risk. This chief of protection must think and act in a proactive and predictive manner against the threat, using tools to support the prevention or mitigation of projected threat actions.

DIVISION PROTECTION CELL

4-11. The division requires a multifunctional capability to provide operational planning, synchronization, integration, and command and control of protection capabilities in support of theater Army and corps requirements during competition below armed conflict, crisis, and armed conflict throughout the division's area of operations. The protection cell must focus on predictive and proactive measures that prevent and mitigate enemy threats from achieving their objectives.

4-12. The division protection cell coordinates with the other staff sections at division and different echelons to synchronize and integrate protection capabilities that prevent and mitigate the enemy's freedom of action throughout the division rear area. It also integrates other protection capabilities at the division echelon to enable operations for its brigade combat teams. The division protection cell integrates with intelligence to see and understand the environment, coordinate counterintelligence to clearly recognize threat actors, and identify key enemy systems that present the most significant risk to friendly forces. The protection cell coordinates with the G-6 concerning information and cyber protection tasks, the surgeon concerning force health protection measures, and the fires cell for lethal and nonlethal targeting of enemy systems that present a protection challenge to the force.

4-13. The protection cell provides functional protection expertise and advises the commander in developing essential elements of friendly information and the division's protection-related products. The division's chief of protection must visualize and describe to the division commander, staff, and leaders the conditions and situations before transitioning, expanding operations, and moving forces when there is a protection risk to the force. The protection cell coordinates for resources required to preserve essential capabilities either organically or by coordinating outside of the division for support.

4-14. The division protection cell coordinates with the division fires cell through the targeting working group to ensure that threats and hazards affecting the divisions and higher echelons critical assets are targeted to eliminate or mitigate in future air tasking orders. The protection team also ensures that the long-range fires assets and radars are maneuvered within the concept of protection to make certain that they are not vulnerable to enemy threats and hazards.

BRIGADE PROTECTION COORDINATOR

4-15. At the brigade echelon, the commanders designate a staff officer to serve as the protection coordinator and leader of the protection working group. Brigades are not authorized a designated protection cell. The brigade protection coordinator is critical in advising the commander and staff on vulnerabilities and risk and recommends measures that overcome enemy activity and preserve critical capabilities, areas, and information.

4-16. The protection coordinator works with the protection working group to integrate and synchronize protection tasks and systems for each phase of an operation or major activity. At a minimum, the protection working group should consist of a representative from CBRN, EOD, engineer, personnel recovery, brigade surgeon, and the provost marshal. The protection working group coordinates with the signal staff section to further facilitate the information protection task. The protection coordinator coordinates with higher headquarters for additional protection capabilities required for mission success and ensures that subordinate units can protect themselves.

ECHELONS ABOVE BRIGADE PROTECTION CELLS

4-17. The protection cell requires a section or representatives from every functional element of the protection warfighting function. The protection cell coordinates and synchronizes required protection capabilities through the protection working group and directly with other personnel and special staff elements as required. Primary members of the protection cell typically include the chief of protection and representatives from air and missile defense, personnel recovery, provost marshal, CBRN, EOD, engineer, medical, and antiterrorism/force protection sections.

CHIEF OF PROTECTION

4-18. The chief of protection may be designated by tables of organization and equipment or by the unit commander. The chief of protection is the principal advisor to the commander on all matters relating to the protection warfighting function and provides oversight and supervision of the protection cell. A chief of protection—

- Conducts criticality, vulnerability, and probability assessments to prioritize critical assets.
- Consolidates identified risk by staff and subordinate commands and graphically depicts them in time and space to enable the commander's situational understanding.
- Ensures that the staff identifies means to avoid, eliminate, or mitigate risk through various division working groups during the daily battle rhythm.
- Plans, coordinates, and integrates protection capabilities in support of main and supporting efforts.
- Builds and maintains a protection running estimate.
- Develops a comprehensive scheme of protection that integrates all complementary and reinforcing protection capabilities.
- Advises the commander on where to allocate and employ protection capabilities.
- Chairs protection working group meetings, coordinates input, and makes recommendations to the commander regarding protection priorities.
- Manages the writing of the protection annex and provides input to plans, orders, branches, and sequels.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups as required.
- Provides guidance on the execution of protection capabilities.
- Continually monitors and assesses the overall protection effort and risk to friendly forces.
- Plans and prepares for changes in protection priorities well before their execution so the force can maintain the momentum and tempo of operations.

AIR AND MISSILE DEFENSE SECTION

4-19. The air and missile defense section coordinates and synchronizes the air and missile defense capabilities throughout the area of operations. The air and missile defense section—

- Advises, monitors, and makes recommendations regarding the current enemy air and missile threat.
- Collaborates with higher headquarters to protect critical assets.
- Monitors current operations of subordinate air defense artillery forces.
- Monitors adjustments to sensor and engagement coverage based on changes in mission variables.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for air and missile defense requirements.

PERSONNEL RECOVERY SECTION

4-20. The personnel recovery section advises the commander on all aspects of personnel recovery operations. The personnel recovery section—

- Develops and maintains the organization's personnel recovery program.
- Recommends recovery courses of action to the commander.
- Coordinates personnel recovery issues, both vertically and horizontally.
- Develops personnel recovery standard operating procedures, plans, and annexes.
- Develops at echelon organic personnel-recovery-capable assets.
- Supports joint personnel recovery or establishes a joint personnel recovery center as required.
- Assists personnel recovery officers in developing subordinate recovery programs.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for personnel recovery requirements.

PROVOST MARSHAL SECTION

4-21. The provost marshal plans military police support for operations and provides advice on all military police capabilities. The provost marshal section—

- Provides organizational focus for task-organized military police assets.
- Synchronizes military police support (security and mobility support, detention operations, and police operations) across the supported echelon.
- Provides technical oversight of military police operations.
- Manages and provides technical oversight and guidance for all detention operations of the supported echelon.
- Coordinates and prioritizes military police capabilities in support of the main and supporting efforts.
- Makes recommendations on developing and allocating military police resources that protect critical capabilities, areas, and information .
- Coordinates and directs law enforcement operations, including liaison with local civilian law enforcement authorities.
- Provides technical oversight of military working dogs teams for the supported echelon.
- Coordinates and synchronizes forensics and criminal investigations support.
- Makes recommendations on assigning protective service details to high-risk personnel. These protective service details may be organic unit assets or an adjacent or higher unit passing through the division area of operations.
- Manages police intelligence operations related to the collection, assessment, development, and dissemination of police intelligence products. Ensures the fusion of police intelligence products with traditional intelligence to identify threats throughout the area of operations.
- Provides physical security guidance and support to the commander.

- Serves (possibly) as a member of a vulnerability assessment team.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for military police requirements.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR SECTION

4-22. The CBRN section conducts planning for, and advises the commander on, all CBRN operations. The CBRN section—

- Advises the commander on CBRN threats and hazards and CBRN defense measures.
- Assesses weather and terrain data to determine environmental effects on potential CBRN hazards and threats.
- Provides response analysis, written estimates and plans, and advice for future operations.
- Recommends courses of action to minimize friendly and civilian vulnerability.
- Recommends how to employ CBRN assets.
- Coordinates and prioritizes CBRN capabilities in support of main and supporting efforts.
- Implements and trains the staff on the CBRN warning and reporting system.
- Provides staff supervision for CBRN site assessments and CBRN response in the area of operations.
- Plans, coordinates, and provides technical oversight of CBRN decontamination (except patient decontamination) operations.
- Plans CBRN support with higher and adjacent units.
- Recommends facilities that should have requirements for CBRN collective protection systems.
- Recommends active and passive defense measures with higher and adjacent units.
- Conducts counter-weapons of mass destruction integration to deter or prevent weapons of mass destruction use.
- Monitors unit CBRN readiness and capability gaps.
- Coordinates and synchronizes CBRN requirements with other staff cells, nodes, and functional groups.
  - Monitors the status of, and coordinates for, the replenishment of resources expended in CBRN operations (such as individual protective equipment and decontaminants).
  - Advocates for the acquisition and management of medical CBRN defense material.
  - Coordinates CBRN support to EOD operations.
  - Coordinates and implements the theater CBRN sample management plan.

EXPLOSIVE ORDNANCE DISPOSAL SECTION

4-23. The EOD section conducts planning for, and advises the commander on, all EOD operations. The EOD section—

- Coordinates and provides technical oversight of detection, identification, recovery, evaluation, exploitation, render safe, and disposal of explosive hazards.
- Coordinates requirements for EOD support with requesting units, other Army commands, other Services, federal agencies, and multinational partners. Coordination may include administrative and logistic support for subordinate EOD units.
- Manages technical intelligence reporting procedures.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups concerning EOD requirements.

ENGINEER SECTION

4-24. The engineer section identifies requirements, prioritizes engineer capabilities and assets, and advises the commander on all engineer operations. The engineer section—

- Plans, coordinates, and provides technical oversight of engineer operations (combat engineering, general engineering, and geospatial engineering).
- Synchronizes engineer support across the supported echelon.
- Identifies and synchronizes requirements for the mobility of friendly forces.
- Identifies requirements for safeguarding bases.
- Advises on the aspects of survivability.
- Coordinates and prioritizes engineer capabilities in support of main and supporting efforts.
- Identifies general engineering requirements.
- Provides reachback to the Army Corps of Engineers.
- Serves (possibly) as a member of a vulnerability assessment team.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for engineer requirements.

ANTITERRORISM SECTION

4-25. The antiterrorism section identifies requirements, prioritizes antiterrorism measures, and advises the commander. The antiterrorism section—

- Establishes an antiterrorism program.
- Collects, analyzes, and disseminates threat information.
- Assesses and reduces critical vulnerabilities (conducts antiterrorism assessments).
- Increases antiterrorism awareness for Soldiers, DA Civilians, and family members.
- Maintains defense according to the force protection control measures.
- Establishes civil/military partnerships for terrorist incident crises.
- Conducts terrorism threat/incident response planning.
- Conducts exercises and evaluates/assesses antiterrorism plans.
- Serves as a member of the vulnerability assessment team as required.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for antiterrorism requirements.

STAFF COORDINATION

4-26. Protection cell effectiveness depends in part on its relationship with the other key staff sections responsible for protection capabilities. Although all staff sections have clearly defined functional responsibilities, none can operate effectively in isolation. Therefore, coordination is critical. Collaboration and dialogue aid in establishing a synchronized and integrated approach to protection. The protection working group brings together multiple staff representatives to provide analysis, coordination, and recommendations for protection; however, the protection cell must continuously synchronize and integrate protection capabilities with OPSEC, the safety section (risk management, surgeon force health protection), the signal section (cyberspace security and defense, electromagnetic protection), and public affairs (misinformation/ disinformation).

G-3, Assistant Chief of Staff, Operations

4-27. The G-3 is the chief of the movement and maneuver warfighting function and the commander's principal staff officer for coordinating and synchronizing all operations in their entirety. The G-3 is responsible for all matters concerning training, operations, and plans, and, at division and higher echelons. The G-3—

- Integrates, coordinates, and task the protection cell for protection requirements.
- Ensures the protection warfighting function is integrated and synchronized across the planning horizons in current operations, future operations, and plans integrating cells.
- Authenticates the protection plan and annex to ensure synchronization of protection in time, space, and purpose in accordance with the commander's intent and planning guidance.
- Participates in the protection cell working group and meetings.

Operations Security Section

4-28. The OPSEC section identifies and recommends critical information requirements. The OPSEC section—

- Analyzes adversaries, vulnerabilities, and indicators as part of the intelligence preparation of the operational environment process.
- Assesses OPSEC risk.
- Develops, coordinates, and applies OPSEC measures across the staff.
- Writes the OPSEC estimate and tab for the protection appendix.
- Monitors, assesses, and adjusts OPSEC measures in terms of the MOE and MOP.
- Reviews internal staff documents, information system logs, and news releases for sensitive information, unauthorized disclosures, and compromised essential elements of friendly information.
- Searches news sources, web logs, and other websites for sensitive information and compromised essential elements of friendly information.
- Serves as a member of the vulnerability assessment team as required.
- Participates in protection cell workgroups and meetings.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for OPSEC requirements.

Surgeon Section

4-29. The surgeon section coordinates and synchronizes health assets and operations within the command. The surgeon section—

- Provides and oversees medical care, to include CBRN.
- Manages unit acquisition and managements of medical CBRN defense material.
- Advises the commander on the health of the command.
- Provides health education and training.
- Coordinates combat operational stress control.
- Coordinates dental services.
- Coordinates for veterinary services, to include animal medicine, food and bottled water, sanitary audits, and zoonotic disease consultation.
- Assesses the medical effects of CBRN hazards on Soldier health, rations, and water.
- Provides oversight of medical laboratory services and the blood program.
- Serves as a member of the vulnerability assessment team as required.
- Coordinates operational public health to accomplish occupational and environmental health surveillance and risk assessment.
- Conducts disease and nonbattle injury tracking and reporting.

- Resources, trains, and certifies units to ensure that they are ready to execute patient decontamination, mass casualty decontamination, and contaminated casualty retrograde operations.
- Supervises and prepares health-related reports and statistics.
- Advises on the effects of the medical threat on personnel, rations, and water.
- Advises how operations affect the public health of personnel and the indigenous populations.
- Participates in protection cell workgroups and meetings.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for force health protection requirements.

SIGNAL SECTION

4-30. The signal section is responsible for all matters concerning network operations (jointly consisting of Department of Defense Information Network Operations and applicable portions of the Defensive Cyber Operations), network transport, information services, and spectrum management operations. The signal section—

- Prepares and maintains network operations estimates, plans, and orders.
- Oversees Department of Defense Information Network Operations related functions that engineer and install the network to support operational requirements.
- Directs and manages the operation of the network to ensure network and information system availability and information delivery.
- Manages the execution of Defensive Cyber Operations for the network in coordination with other staff sections.
- Oversees or participates in the development of plans and orders for cyberspace electromagnetic activities in conjunction with other staff sections.
- Oversees or participates in the development and maintenance of the cyberspace common operational picture with assistance from the G-2 (S-2) and other staff sections.
- Coordinates and manages electromagnetic spectrum operations and communications security within the area of operations.
- Recommends command post locations based on operational requirements and the information environment.
- Recommends network-related essential elements of friendly information.
- Coordinates contractor and maintenance support for all network operations, information services, and electromagnetic spectrum management operations.
- Serves as a member of the vulnerability assessment team as required.
- Participates in protection cell workgroups and meetings.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for cybersecurity and defense and electromagnetic protection requirements.

SAFETY SECTION

4-31. The safety section is responsible for coordinating safety activities throughout the command and advises the commander on matters relating to the Army safety program, including its implementation and effectiveness (see AR 385-10 and ATP 5-19 for additional information on safety). The safety section—

- Conducts safety inspections and assessments in support of the protection cell.
- Works with engineers providing safety considerations for building designs. Assesses other construction projects regarding explosives safety arcs. Provides safety expertise for construction on airfields, heliports, and base camps.
- Provides input for the design and development of ranges, surface danger zones, and safety procedures in coordination with engineers and the assistant chief of staff, operations (G-3).
- Works with G-3 to provide safety inputs to operations plans and orders as required and for the distribution of safety-related messages.

- Works with the G-3 air for aviation operations safety functions. Participates in aviation safety councils.
- Attends, and provides input during, planning in joint facilities utilization boards (engineers).
- Coordinates with quality assurance specialist's ammunition surveillance/assistant chief of staff, logistics (G-4), and the ammunition manager for ammunition inspections, transportation safety, and malfunction reporting.
- Coordinates with the public affairs officer for command messaging about mishaps and investigations.
- Coordinates with the staff judge advocate for legal issues pertaining to mishaps.
- Participates in protection cell workgroups and meetings.
- Provides guidance on the establishment, maintenance, and construction of all ammunition holding areas and ammunition supply points.
- Assists with licensing and citing all ammunition/explosive storage locations.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups to meet safety requirements, including support for Army reportable accidents.

CIVIL AFFAIRS SECTION

4-32. The Civil Affairs Operations staff section is responsible for coordinating the planning and execution of governance, populace and resources control measures, and civil knowledge integration into the Army's integrating processes and operations process. The Civil Affairs Operations section ensures civil-military integration and civil network development and engagement throughout the command's area of operations. The Civil Affairs Operations staff—

- Plans and coordinates populace and resources control measures to protect the populace from the effects of military operations and control access to areas and resources that enhance operational and civil security.
- Provides input for the protection of critical infrastructure and civil networks to be added to the protection prioritization list.
- Coordinates with interagency and interorganizational entities for force protection measures and resources.
- Plans and coordinates for the integration of civil networks in governance and civil security.
- Uses civil networks to increase sensor range for early threat warning capability.
- Coordinates and synchronizes with other staff cells, nodes, and functional groups for civil-military operations support.

G-2, INTELLIGENCE SECTION

4-33. The intelligence section is responsible for providing intelligence to support current and future operations and plans. The primary role of the intelligence section is to provide the commander the most timely, relevant, accurate, and predictive intelligence available (see AR 381-10). The intelligence staff has roles and responsibilities that support the conduct of operations across all echelons. The G-2—

- Oversees the intelligence cell (specifically situation development and target development) support to lethal and nonlethal targeting, warning intelligence, assessment, and protection.
- Provides the commander and staff assessments of key groups and populations, including capabilities, intentions, and potential courses of action.
- Identifies gaps in intelligence and developing collection strategies.
- Disseminates intelligence products throughout the unit and to higher echelon, subordinate, and adjacent unit headquarters.
- Recommends changes to the information collection plan based on changes in the situation and weather.
- Leads the staff in intelligence preparation of the operational environment and in consolidating the staff's products into a coherent and holistic product.

- Ensures that ongoing intelligence operations are collecting information needed for anticipated decisions or other priority intelligence requirements.
- Coordinates and provides counterintelligence threat assessments.
- Serves as part of a vulnerability assessment team when needed.

PUBLIC AFFAIRS SECTION

4-34. The public affairs section understands and coordinates the flow of information to Soldiers, the Army community, and the public. The public affairs section develops and employs public affairs activities for the command to ensure the trust and confidence of the U.S. population, friends, and allies; deter and dissuade adversaries; and counter misinformation and disinformation. The public affairs section—

- Assesses the information requirements of Army forces and the expectations of the public.
- Advises the commander about communication strategies.
- Leads the commander's communication synchronization.
- Corrects misinformation and counters disinformation.
- Monitors media and public opinion and evaluates the effectiveness of communication.

PROTECTION CELL PARTICIPATION

4-35. A protection cell representative must participate in daily, weekly, monthly, or intermittent working groups across the supported echelon to present and exchange protection information, coordinate protection activities, integrate protection capabilities, and enhance planning and decision making. The number of meetings or working groups and the subjects the working group participates in depend on the situation and echelon. Typical working groups in which protection cell participation is required include the following:

- Assessment working group (plans or future operations cell).
- Operations and intelligence working group (intelligence cell).
- Command post organization and operations.
- Targeting working group (fires cell).
- Protection working group (protection cell).
- Civil affairs operations working group (civil affairs operations staff section).
- Information activities working group (movement and maneuver cell).
- Cyberspace electromagnetic activities working group (electromagnetic warfare element).

.

This page intentionally left blank.

Appendix A

Protection Warfighting Function Primary Tasks

Military operations are inherently complex. Army operations and missions are executed through tactical tasks. The protection warfighting function enables the commander to maintain force integrity and combat power through the integration of protection capabilities during competition below armed conflict, crisis, and armed conflict. This appendix defines and examines the protection warfighting function and the primary tasks associated with it.

CONDUCT RISK MANAGEMENT

A-1. Risk, uncertainty, and chance are inherent in all military operations. Army organizations at every level must understand and apply risk management throughout competition below armed conflict, crisis, and during armed conflict. Risk management during competition below armed conflict and crisis enables commanders to maintain combat power while ensuring mission accomplishment during current and future operations. During armed conflict, it assists commanders and staffs in making informed decisions to reduce or offset risk, which increases the organization's operational effectiveness and its probability of mission success. To assist in risk management, commanders and their staffs must develop or institute a risk management process tailored to their mission or area of operations (see ATP 5-19). Commanders determine the level of risk that is acceptable and identify it in the commander's intent.

A-2. Risk management is an invaluable tool for commanders and staffs that provides a systematic and standardized process to identify hazards and react to changes within an operational environment. It focuses on designing, implementing, and monitoring risk decisions. Commanders may choose to avoid, eliminate, mitigate, or accept risk. Acceptance and avoidance are risk decisions made as a matter of strategy, policy, operations, or tactics. Mitigating and eliminating risk are key to risk management.

- **Avoid.** Forego the activity that would produce unacceptable risk.
- **Eliminate.** Take action to remove the risk or transfer the risk when and where it is incurred to a unit better postured to manage the threat.
- **Mitigate.** Implement measures that decrease the probability or consequence of harm.
- **Accept.** Make an informed decision to act without further mitigating the risk.

A-3. Risk management must be integrated throughout each warfighting function. All staff sections integrate risk management for hazards within their functional areas throughout the first four steps of the MDMP and should consider it throughout the entire MDMP process. Risk should first be avoided and then eliminated if possible, and the remaining risk should be mitigated before the commander chooses to accept the residual risk. Below are examples of warfighting function integration and the roles they play in risk management:

- The movement and maneuver warfighting function avoids, mitigates, or eliminates risk through movement and maneuver by dispersing and displacing the force; exploiting positions of relative advantage; and achieving surprise, shock, and momentum.
- The intelligence warfighting function assists the commander in avoiding risk. It informs them of where enemy forces are strong and weak or of where critical battlefield systems are arrayed.
- The fires warfighting function eliminates enemy systems that threaten friendly combat power with indirect fires.
- The sustainment warfighting function mitigates risk by identifying and resourcing logistics and personnel shortfalls; eliminating or reducing the effects of explosive hazards; and promoting, improving, or conserving the behavioral and physical wellbeing of Soldiers.

- The protection warfighting function synchronizes and integrates protection capabilities to mitigate or prevent risk and assist in survivability.
- The command and control warfighting function enables the commander to determine the level of risk that is acceptable to achieve their operational end state. The command ensures that tasks and responsibilities are issued, acknowledged, and understood.

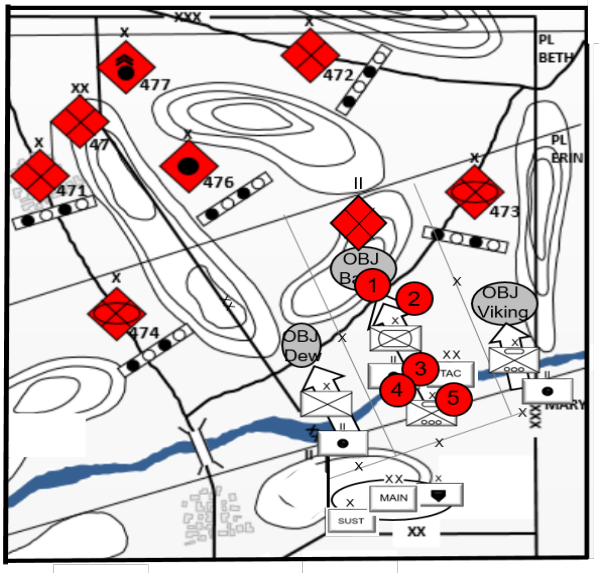
A-4. During mission analysis, the commander and staff focus on identifying and assessing hazards as they relate to risk to force (increased probability of the degradation of an organization's combat power) and risk to mission (increased probability of failure to achieve a desired end state). The assessment of risk to mission and risk to force should include an overall risk-to-mission and risk-to-force analysis (such as low, medium, high, or extremely high). Course-of-action development focuses on avoiding, eliminating, mitigating, or accepting risk. It identifies how control measures affect the risk and where the organization may incur risk during the operation. Some risk cannot be avoided; however, all risk should be identified to the greatest extent possible. Controls reduce or eliminate risk. Controls generally fall into one of three categories:

- **Educational.** These controls are based on knowledge and skills and are implemented through training.
- **Physical.** These controls are barriers, guards, or signs which warn that a hazard exists. Special oversight personnel are included in this category.
- **Hazard elimination.** These controls include positive actions to prevent exposure, substantial reduction, or elimination of the hazard.

A-5. The risk management process during course-of-action analysis (war game) helps identify protection limitations and shortfalls for each COA and for unintended consequences, branches, sequels, second- and third-order effects, and decision points for risk tolerance. It also provides facts to help inform the war game. Following course-of-action development, staff sections continue monitoring risk as part of their running estimate. The chief of protection (in coordination with the safety officer) consolidates staff risk assessments and develops the risk matrix to inform the commander of risk and the required controls to mitigate the risk to an acceptable level.

A-6. The risk matrix should be detailed and under continuous refinement. It should assist the commander to visualize, describe, and direct the operation. The chief of protection should develop a risk matrix that enables the commander to see risk in time, space, and purpose. Figure A-1, page A-3, provides one simplified example of a matrix that addresses critical information for the management of risk during an operation. Risk management considerations include—

- Risk decision points.
- Risk that the organization can directly influence.
- Risk that the organization cannot directly influence.
- Risk that can cause culmination.
- Risk that can result in failing to achieve a desired end state.
- Risk with political consequences.
- Approaches to risk management.
    - **Deliberate risk management.** Deliberate risk management refers to situations in which ample time is available to apply the five-step process as part of the detailed planning for an operation.
    - **Real-time risk management.** Real-time risk management refers to the immediate management of threats and hazards as they occur, usually during execution of an operation of the performance of a task.



	Hazard	Method			Offensive Operation			
		Avoid	Eliminate	Mitigate	Supporting Task Required	Asset Assigned	Risk to Mission	Risk to force
1	7th ID reduced to 65% combat power for wet gap crossing		X	X	NAI #1 - ENY strength on OBJ Baker; NAI #2 - ENY Tank Brigade movement			
2	7th ID mass casualty			X	CASEVAC	44th Medical Brigade		
3	Persistent chemical used near wet gap crossing site #2 ENY forces mass on OBJ Baker			X	CBRN route recon; CBRN decon	12th Hazard Response Company		
4	ENY forces massing on 7th ID wet gap crossing	X	X	X	Integrate Joint fires; Maintain tempo at crossing sites	Coordinate Joint fires with III Corps; 502nd Engineer Company (MRBC)		
5	2/7 FAB cannot range FSCL	X		X	2/7 FAB moves up in the order of march; Establish position areas for artillery	2/7 Field Artillery Battalion		

Legend:

CASEVAC	casualty evacuation
CBRN	chemical, biological, radiological, and nuclear
ENY	enemy
FAB	field artillery brigade
FSCL	fire support coordination line
ID	infantry division
MRBC	multi-role bridge company
NAI	named area of interest
OBJ	objective
PL	phase line
SUST	sustainment
TAC	tactical

Figure A-1. Risk matrix example during large-scale combat operations

CONDUCT SURVIVABILITY

A-7. Leaders assess survivability as the ability of a friendly force to withstand enemy effects while remaining mission-capable. It represents the degree to which a formation is hard to destroy. *Survivability* is a quality or capability of military forces which permits them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission (ATP 3-37.34). Personnel and physical assets have inherent survivability qualities or capabilities that are enhanced through various means and methods. For example, the body armor or mission-oriented protective posture gear enhances survivability when worn correctly in the corresponding threat environments. These qualities are especially important when elements are targeted by threats and protection capabilities are limited.

A-8. *Survivability operations* are those military activities that alter the physical environment to provide or improve cover, camouflage, and concealment (ATP 3-37.34). Survivability operations enhance the ability to avoid or withstand hostile actions by altering the physical environment. Units accomplish this by providing or improving camouflage, cover, and concealment by—

- Constructing fighting positions.
- Constructing protective positions.
- Hardening infrastructure.
- Employing camouflage and concealment.

A-9. Survivability and survivability operations are not interchangeable. Survivability refers to a quality or capability, while survivability operations refer to tasks that enhance survivability. Survivability and survivability operations employ active and passive measures to enable freedom of action when synchronized and integrated with the other protection capabilities. Survivability operations are the responsibility of every unit at all echelons. Some units, such as engineer and CBRN, possess capabilities that enable survivability operations. Survivability focuses on providing camouflage, cover, and concealment. Some of the means and methods that enhance survivability become a part of the protected personnel or physical assets, which safeguard assets even while mobile. In addition to activities that alter the physical environment, other capabilities and activities are used to conduct or support survivability by—

- Establishing local security.
- Conducting military deception.
- Employing protective obstacles.
- Mitigating the emission of electromagnetic radiation.
- Countering unmanned aircraft systems.
- Maintaining dispersion.
- Using obscuration.
- Remaining mobile.
- Modifying the tempo.
- Taking evasive actions.
- Maintaining noise and light discipline.
- Implementing CBRN defensive measures.

A-10. Survivability operations are ongoing activities throughout the Army's strategic context and are not limited to crisis and armed conflict. Commanders include survivability and survivability operations into training during competition below armed conflict to validate their unit's individual and collective proficiency. Proficiency is an inherent form of passive protection. Organizations may also employ hardening measures, such as emplacing bollards to provide standoff and prevent threat effects from damaging critical deployment-related infrastructure or command and control facilities. Army forces, especially those stationed in forward locations or tasked with protecting critical capabilities, areas, and information, never stop improving the survivability of their positions. Plans and orders should specify dispersion and survivability requirements.

A-11. During crisis and armed conflict, units improve survivability within the limits of their capabilities. Competing demands and limited resources for conducting survivability operations are predominant factors throughout an operational environment and are considered during planning. Commanders identify those critical capabilities, areas, and information requiring additional protection because their loss or degradation would have a significant and/or debilitating effect on operations. When existing terrain features offer insufficient cover, concealment, and dispersion, altering the physical environment provides or improves cover and concealment, which enhances survivability. Similarly, using natural or artificial materials such as camouflage may confuse or mislead the enemy. See ATP 3-37.34 for additional information on survivability.

COORDINATE AIR AND MISSILE DEFENSE SUPPORT

A-12. Air and missile defense constitutes the defensive counterair portion of the joint counterair framework. Air defense artillery units protect friendly forces from ballistic missiles, large-caliber rockets, cruise missiles, air-to-surface missiles, hypersonic weapons, unmanned aircraft systems, manned fixed- and rotary-wing aircraft, rockets, artillery, and mortars using active and passive defensive actions and measures. These are used to destroy, nullify, or reduce the effectiveness of hostile air and ballistic missile threats. Active and passive air and missile defense are—

- **Active air and missile defense.** Direct defensive actions taken to destroy, nullify, or reduce the effectiveness of air and missile threats against friendly forces and assets (see JP 3-01). Active air and missile defense includes air defense; ballistic missile defense; and counter-rocket, artillery, and mortar defensive measures using surface-to-air missiles and guns. These are supported by sensors and command and control elements to engage aerial threats inside and outside the atmosphere.
- **Passive air and missile defense.** All measures, other than active air and missile defense, taken to minimize the effectiveness of hostile air and ballistic missile threats against friendly forces and critical assets (see JP 3-01). These measures include detection, warning, camouflage, concealment, deception, dispersion, hardening, and the use of protective construction.

A-13. Air and missile defense tasks fall under both the protection and fires warfighting functions. *Fires warfighting function* is the related tasks and systems that create and converge effects in all domains against the adversary or enemy to enable operations across the range of military operations (ADP 3-0). Coordinating air and missile defense support is a protection task, while the employment of and engagements by air defense artillery forces are fires tasks.. All tasks, whether protection or fires, address the defense of critical assets against ballistic missile, air, rocket artillery, and mortar threats. See FM 3-01 for more information on the air and missile defense tasks in the fire's warfighting function.

A-14. Air and missile defense is a critical consideration in competition below armed conflict, crisis, and armed conflict The right mix of capabilities and the correct amount of air defense artillery forces are required to counter aerial threats in various air environments. During competition below armed conflict, theater strategic level ballistic missile defense units provide commanders a secure environment in which to generate, project, and preserve combat power. As competition transitions into crisis, air defense artillery units are added or repositioned to create a defense in depth. With the transition into armed conflict and the beginning of large-scale combat operations, short-range air defense units are deployed to defend friendly forces and defeat hostile air threats in the rear and close fight.

A-15. All members of the combined arms team perform air and missile defense tasks; however, air defense artillery is the Army's primary contributor to air and missile defense. Air defense artillery officers, from theater to maneuver brigade level, synchronize their actions with other Service air and missile defense elements and with supported land-based forces. At theater level, the Army Air and Missile Defense Command provides active air and missile defense protection of critical assets designated by the joint force commander. In joint operations, the Army Air and Missile Defense Command integrates subordinate air defense artillery units into theater defensive counterair operations. The Army Air and Missile Defense Command advises the designated engagement authority of the air and missile defense designs, consistent with the joint force commander's desired levels of protection. In support of Army operations, air defense artillery commanders establish support relationships with Army maneuver formations and keep those formations informed of their actions and activities.

A-16. Engagements of air and missile threats are conducted at all echelons according to air and missile defense directives and under the direction of a designated engagement authority. Engagement authority may vary by type of air or missile threat, time, situation (intensity of the aerial threat), or location. Typically, engagement authority for fixed-wing aircraft is held at the air defense artillery commander or regional/sector air defense commander level. Authority for ballistic missile engagements may be delegated to an air defense artillery battalion commander, and engagements of small-unmanned aircraft systems and rockets, artillery, and mortars may be delegated down to air defense artillery crews, squads, or individual Soldiers. Engagement authority for air threats engaged by nonair defense artillery elements will be executed based on rules of engagement, rules for use of force, unit standing operating procedures, and command policy. Nonair defense units may be equipped with counter-small, unmanned aircraft system capabilities to protect critical assets against small-unmanned aircraft. These capabilities may include electronic and/or direct fire capabilities.

A-17. An air defense artillery unit collaborates with a supported echelon's protection cell, through the echelon's air and missile defense section, to ensure that protection cell members understand its capabilities and capacity. The protection cell identifies the most critical assets within the formation requiring defense against air and ballistic missile threats and creates or updates a protection prioritization list for the echelon's commander for approval. Following approval, the protection cell coordinates with the air and missile defense section and supporting air defense artillery unit for air and missile defense support. The air defense artillery commander and staff identify those assets that can be defended with available forces to the protection levels specified by the echelon commander. These are coordinated with the protection cell and briefed to the echelon commander for approval. Adjustments are made as required. The air and missile defense section officer, as a member of the protection working group, keeps all working group members advised of pertinent air and missile defense directives, actions (to include the status of units and engagements), and the overall air and missile defense picture. See FM 3-01 and JP 3-01 for additional information on air and missile defense.

CONDUCT CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR OPERATIONS

A-18. During military operations, CBRN environments create added risk to an already hazardous environment by adding immediate or delayed effects that could be nonpersistent or persistent. The *chemical, biological, radiological, and nuclear environment* is an operational environment that includes chemical, biological, radiological, and nuclear threats and hazards and their potential resulting effects (JP 3-11).

A-19. Commanders and protection cells synchronize, integrate, and organize CBRN operations and employ capabilities with other protection activities to prevent or mitigate the effects of CBRN threats and hazards to preserve combat power and enable freedom of action. *Chemical, biological, radiological, and nuclear operations* include the employment of capabilities that assess, protect against, and mitigate the entire range of chemical, biological, radiological, and nuclear incidents to enable freedom of action (FM 3-11). The CBRN core functions (assess, protect, mitigate) have a role in preserving combat power in CBRN environments, and the CBRN integrating activity (hazard awareness) enables the commander's understanding of the operational environment.

- **Assess.** Collection assets gather CBRN information on threat capabilities. CBRN staffs advise commanders using CBRN warning, reporting, and modeling to inform the commander's decision making. Assessments should identify CBRN threats and hazards, to include industrial sites containing toxic industrial material that could present a hazard to the force. Threat analysis should also include an analysis of friendly vulnerability to CBRN hazards. Reconnaissance and surveillance provide capabilities to locate, detect, identify, quantify, sample, survey, observe, monitor, report, and mark contaminated areas.
- **Protect.** All units employ measures to reduce the likelihood of CBRN threats and hazards having an adverse effect on mission, personnel, equipment, and installations/facilities. These measures are integrated into operations to balance increasing protection while retaining freedom of action.

- **Mitigate.** CBRN units and staffs provide the subject matter expertise and equipment to reduce or neutralize the hazard to protect forces and allow freedom of action. *Contamination mitigation* is the planning and actions taken to prepare for, respond to, and recover from contamination associated with all chemical, biological, radiological, and nuclear threats and hazards in order to continue military operations (JP 3-11).
- **CBRN hazard awareness and understanding.** This is an integrating activity of CBRN operations that enables the three core functions and provides commanders the information needed to make risk-based decisions in CBRN environments. CBRN staffs conduct risk and vulnerability assessments to capture information about hazards within the operational area and provide recommendations for protection planning. The ability to protect the force begins with the ability to recognize vulnerabilities, identify and understand CBRN hazards and their consequences, and plan and respond appropriately to protect the force. See FM 3-11 for additional information on CBRN hazard awareness and understanding.

A-20. The CBRN core functions support the tasks of active and passive CBRN defense. CBRN defense is the measures taken to minimize or negate the vulnerabilities to, and/or the effects of, a CBRN hazard or incident (see JP 3-11). The CBRN defense tasks that support protection include—

- Preform CBRN (including toxic industrial materials) vulnerability analysis.
- Develop a CBRN defense plan.
- Declare CBRN alarm conditions, which trigger the initiation of protection measures.
- Coordinate and synchronize CBRN protection for personnel, equipment, and infrastructure.
- Implement the CBRN warning and reporting system. This is the system for the exchange of information on CBRN incidents and includes predictive modeling, hazard predictions, and CBRN reports.
- Establish operational exposure guidance and military exposure guidelines.
- Plan and synchronize the CBRN reconnaissance and surveillance plan.

A-21. CBRN operations during competition below armed conflict provide military forces time to prepare for armed conflict, opportunities to assure allies and partners of the United States' resolve and commitment, and time to set the necessary conditions to prevent crisis or conflict through deterrence. Through military engagements with allies and partner nations, CBRN operations build partner capacity and demonstrate the readiness and capability of U.S. forces to operate in a CBRN contaminated environment. In competition below armed conflict, CBRN capabilities provide support to civil authorities or foreign humanitarian assistance in response to natural and man-made disasters. Integrated training exercises that incorporate live-agent scenarios signal the U.S. capacity to conduct large-scale combat operations in a CBRN environment. See ADP 3-28 for more information on defense support of civil authorities. See JP 3-29 regarding more information on foreign humanitarian assistance.

A-22. Peer adversaries will likely have knowledge of U.S. force intent and operations to project forces in response to a crisis. In this phase, CBRN operations aim to protect critical assets and activities facilitating the flow of forces from fort to seaport/airport, theater reception, staging, onward movement, and integration. CBRN assets deploy to designated homeland and theater nodes to deter CBRN threats and must be prepared to conduct CBRN operations if deterrence is unsuccessful.

A-23. During armed conflict, some adversaries will have the ability to employ traditional and novel CBRN agents to produce mass casualties and/or as a key element of their antiaccess/area denial plan. CBRN operations during armed conflict focus on achieving early warning, detection, and avoidance of contaminated areas and on mitigating the effects of hazards by CBRN decontamination operations. CBRN reconnaissance and surveillance units integrate with maneuver forces to employ standoff hazard detection and identification to avoid contamination if it supports the scheme of maneuver. Decontamination operations provide commanders the ability to restore combat power degraded by CBRN contamination, reconstitute critical force providers, and avoid or mitigate ground contamination (obstacles) to ensure freedom of movement and action.

A-24. As weapons of mass destruction material and technology proliferate across the globe, it is likely that U.S. forces will encounter them in military operations throughout all phases, to include competition below armed conflict, crisis, and armed conflict. Countering weapons of mass destruction are efforts against actors of concern to curtail the conceptualization, development, possession, proliferation, use, and effects of these weapons of mass destruction, related expertise, materials, technologies, and means of delivery (see JP 3-40). CBRN operations support operational and theater strategic objectives to counter weapons of mass destruction and protect the force in a CBRN environment by preventing the acquisition of weapons of mass destruction, which is the best deterrent. See FM 3-11 for additional information on CBRN operations.

CONDUCT ELECTROMAGNETIC PROTECTION

A-25. Many Army capabilities, including communications, cyberspace operations, information collection, space capabilities, target detection, and precision guided munitions, depend on assured access to, and the use of, the electromagnetic spectrum. Electromagnetic protection helps to ensure access to the electromagnetic spectrum for these capabilities. Electromagnetic protection remains constant during competition below armed conflict, crisis, and during armed conflict. Electromagnetic protection is a command responsibility but is only effective when everyone in an organization understands its importance and can readily identify opportunities to implement protection activities. The actions to protect Army access to, and the use of, the electromagnetic spectrum are—

- Conduct electromagnetic protection actions.
- Conduct spectrum operations.

CONDUCT ELECTROMAGNETIC PROTECTION ACTIONS

A-26. *Electromagnetic protection* is the division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). Electromagnetic protection measures eliminate or mitigate negative influences of intentional and unintentional electromagnetic interference. Electromagnetic protection measures include—

- Electromagnetic compatibility.
- Electromagnetic hardening.
- Electromagnetic masking.
- Electromagnetic spectrum operations.
- Emission control.
- Wartime reserve modes.

Electromagnetic Compatibility

A-27. *Electromagnetic compatibility* is the ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response (JP 3-85). Before units acquire electromagnetic warfare equipment, they conduct electromagnetic compatibility analysis. Spectrum managers implement electromagnetic compatibility to mitigate electromagnetic vulnerabilities by applying sound spectrum planning, coordination, and management of the electromagnetic spectrum.

Electromagnetic Hardening

A-28. *Electromagnetic hardening* is action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 3-85). Multiple actions can be taken to protect friendly communications and noncommunications resources from threat identification, lethal and nonlethal attack, and exploitation. These actions include inspecting the configuration of unit equipment, such as the proper grounding of communications assemblages, serviceability of cable shielding, and adequate cable connectivity. An example of electromagnetic hardening includes installing electromagnetic conduit consisting of conductive or magnetic materials to shield against undesirable effects of electromagnetic energy.

Electromagnetic Masking

A-29. *Electromagnetic masking* is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-85). Electromagnetic masking disguises, distorts, or manipulates friendly electromagnetic radiation to conceal military operations information or present false perceptions to adversary commanders.

Electromagnetic Spectrum Management

A-30. Electromagnetic spectrum operations enable cyberspace electromagnetic activities by ensuring access and deconfliction for the Army's use of the electromagnetic spectrum. Cyberspace electromagnetic activities' execution of cyberspace and electronic warfare operations enables the Army to secure and defend friendly force networks and to protect personnel, facilities, and equipment. Planning, integration, and synchronization of the interrelated actions support the overall mission (see JP 3-85 for additional information).

Emission Control

A-31. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan (JP 3-85). Emission control protocols provide guidance on which emitters can be used for certain missions and in various situations. Effective emission control practices greatly reduce the ability of the threat to detect, identify, locate, and attack friendly forces.

Wartime Reserve Modes

A-32. *Wartime reserve modes* are characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to, or misunderstood by, opposing commanders before they are used but could be exploited or neutralized if known in advance (JP 3-85). Potential adversaries search for information that reveals friendly electromagnetic warfare vulnerabilities in the information environment, such as technical articles, magazines, news programs, and web pages that are available on the internet. The Army prevents public access to wartime reserve modes.

Conduct Electromagnetic Spectrum Management

A-33. *Electromagnetic spectrum management* is the operational, engineering, and administrative procedures to plan and coordinate operations within the electromagnetic operational environment (JP 3-85). To conduct electromagnetic protection in an environment, units must know the types and quantity of friendly transmitters in the area of operations. When units use frequencies employed by other friendly forces in the same area of operations, it may cause undesirable electromagnetic interference. Conducting spectrum management enables electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. As a result, this mitigates and avoids most electromagnetic environmental effects, such as electromagnetic interference, electromagnetic pulse, electromagnetic radiation hazards, and various natural phenomena effects.

CONDUCT AREA SECURITY

A-34. Security operations prevent surprise, reduce uncertainty, and provide early warning of enemy activities. Security is a dynamic effort that anticipates and thwarts enemy efforts. When successful, security operations allow the force to maintain the initiative. The synchronization and integration of area and local security are essential to protecting the force. All units are responsible for their own local security and responding to Level I threats. Forces assigned an area security focus on and protect a force, installation, route, area, or asset.

A-35. Local security is not an operation of its own; it includes any local measure taken by units that protects against enemy actions. It involves avoiding enemy detection or deceiving the enemy about friendly positions and intention.

A-36. Area security operations support a higher echelon's overall operation and require them to take advantage of local security measures performed by all units in the area, regardless of their command and control relationships. Although vital to the success of military operations, area security is normally an economy-of-force mission, often designed to ensure the continued conduct of sustainment operations that generate and maintain combat power. Area security operations occur regardless of what type of operation the higher echelon is conducting.

A-37. Typically, units assigned an area security mission operate in a division or higher echelon's rear area and facilitate the positioning, employment, and protection of resources required to sustain, enable, and control forces. The task organization of the unit assigned the area security mission should correspond with the level of threat. For example, if the threat in the rear area is a Level II threat, a military police company should be sufficient. If the threat is a Level III threat, a combined arms team from a brigade combat team is a more appropriate unit.

A-38. Sometimes area security forces must retain readiness over long periods of time without contact with the enemy. This occurs most often during area security operations, when the enemy commander knows that enemy special purpose forces or insurgents are seriously overmatched in available combat power. In this case, the enemy commander normally tries to avoid engaging friendly forces unless it is on terms favorable to the enemy. These favorable terms include the use of indirect fires, improvised explosive devices, mines, or booby traps. Forces conducting area security should not develop a false sense of security, even if the enemy appears to have ceased operations in the secured area. Security units must assume that the enemy is observing friendly operations and is seeking to identify routines, weak points, and lax security for the opportunity to strike with minimum risks. This requires small-unit leaders to maintain vigilance and discipline in their Soldiers to prevent that opportunity from developing.

A-39. All commanders apportion combat power and dedicate assets based on an analysis of the operational environment, the likelihood of threat action, the relative value of friendly resources, and the risk to civilian populations. Although all friendly resources have value, the mission variables of METT-TC (I) make some resources, assets, or key terrain more essential to successful mission accomplishment from enemy or adversary and friendly perspectives. Commanders create and use a decision support matrix and template to facilitate decision making, issue guidance, and allocate resources. Criticality, vulnerability, and recoverability are some of the most significant considerations in determining protection priorities that become the focus of area security. Area security is conducted through the following five variations:

- **Site Security.** Area security forces provide protection through area security techniques that involve the employment of protection and security assets in a layered, integrated, and redundant manner. A unit conducting site security may protect locations, such as—
  - Base/base camps.
  - Tactical assembly areas.
  - Critical assets.
  - Port areas and piers.
- **Line of communication and route security.** The security and protection of lines of communications and supply routes are critical to military operations because most support traffic moves along these routes. A route security force prevents an enemy or adversary force from impeding, harassing, or destroying traffic along a route or portions of a route.
- **Convoy security.** A convoy security operation is a specialized type of line of communication or route security operation. Units conduct convoy security operations when there are insufficient friendly forces to continuously secure routes in an area of operations and there is a significant danger of enemy or adversary ground action directed against the convoy. Commanders may also conduct convoy security operations in conjunction with route security operations.

- **Response force operations.** Response forces take active measures to prevent enemy attacks. If enemy attacks happen, they quickly respond by providing additional capabilities when the threat exceeds the current local and area security capabilities.
  - **Mobile security force.** A *mobile security force* is a highly mobile and dedicated security force with the capability to defeat Level I and II threats in a joint security area (JP 3-10). Typically, a mobile security force is a military police element.
  - **Tactical combat force.** A *tactical combat force* is a rapidly deployable, air-ground, mobile combat unit with appropriate combat support and combat service support assets assigned to, and capable of, defeating Level III threats, including combined arms (JP 3-10). Typically, a tactical combat force is either a combined arms battalion, Stryker infantry battalion, or a cavalry squadron.
- **Area damage control.** *Area damage control* consists of measures taken before, during, and/or after a hostile action or natural or man-made disasters to reduce the probability of damage and minimize its effects (JP 3-10).

IMPLEMENT OPERATIONS SECURITY

A-40. *Operations security* is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3). Effective and disciplined OPSEC is employed during all military operations. Units routinely employ OPSEC to protect essential elements of friendly information. An essential element of friendly information is a critical aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to the failure of, or limit the success of the operation and therefore should be protected from enemy detection. Traditional security programs protect classified information but are not necessarily designed to protect essential elements of friendly information, which can be revealed by indicators discovered in unclassified information. Identifying and mitigating indicators helps to prevent enemy or adversary reconnaissance and other information collection capabilities from gaining an advantage because the threat has knowledge of identifiable or observable unit-specific information. The OPSEC process may be used to—

- Identify actions that can be observed not only by enemy or adversary intelligence systems, but also by the casual observer.
- Determine friendly indicators that systems might obtain and which could be interpreted or pieced together to derive critical information in time to be useful to adversaries or enemies.
- Select measures and countermeasures that eliminate or reduce vulnerability or are indicators of observation and exploitation:
  - Avoid drastic changes as OPSEC measures and countermeasures are implemented. Changes in procedures alone may alert the adversary that an operation or exercise is starting.
  - Prevent the display or collection of critical information, especially during the preparation for, and the execution of, actual operations.
  - Avoid patterns of behavior, when feasible, to preclude the possibility of adversary intelligence constructing an accurate model.
- Preserve a commander's decision cycle and allow options for military actions.

A-41. OPSEC applies to all operations and must be considered throughout competition below armed conflict, crisis, and during armed conflict. OPSEC is a force multiplier that can maximize operational effectiveness by saving lives and resources when integrated into operations, activities, plans, exercises, training, and capabilities. Good field craft and the disciplined enforcement of camouflage and concealment are essential to OPSEC. The unit OPSEC officer coordinates additional OPSEC measures with other staff and command elements and synchronizes with adjacent units. The OPSEC officer develops potential OPSEC measures during MDMP. The G-2 assists the OPSEC process by comparing friendly OPSEC indicators with enemy or adversary intelligence collection capabilities.

A-42. OPSEC, integrated and synchronized in combination with other protection measures, may be employed with deception to ensure that only desired events reach the enemy and that supported operations are concealed. At times, unit commanders employ deception in support of OPSEC to create multiple false indicators and countermeasures that confuse enemy or adversary forces operating in the unit's area of operations, making unit intentions harder to interpret. Deception in support of OPSEC uses controlled information about friendly force capabilities, activities, and intentions to shape perceptions. It targets and counters threat intelligence, surveillance, and reconnaissance capabilities to distract the threat away from, or provide cover for, unit operations. Deception in support of OPSEC is a relatively easy countermeasure to use and is appropriate for use at battalion level and below. To be successful, OPSEC and deception requirements must achieve balance (see ATP 3-13.3 for additional information).

CONDUCT CYBERSPACE SECURITY AND DEFENSE

A-43. The Army portion of cyberspace is the Department of Defense information network–Army (DODIN-A). The *Department of Defense information network–Army* is an Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide (ATP 6-02.71). Cybersecurity and defense remain constant during competition below armed conflict, crisis, and during armed conflict.

A-44. The DODIN-A enables command and control and facilitates all military operations and business functions. The network allows commanders to leverage information to gain understanding of the operational environment, influence behavior, support decision making, and synchronize warfighting functions. The Army secures and defends the network through a defense-in-depth approach, incorporating layered security and defenses. The tasks to secure and defend cyberspace are—

- Perform cybersecurity activities.
- Conduct defensive cyberspace operations–internal defensive measures.

PERFORM CYBERSECURITY ACTIVITIES

A-45. Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (see DODI 8500.01 for additional information on cybersecurity). Cybersecurity activities take place throughout the system life cycle. Cybersecurity measures apply to general threats and known vulnerabilities, not specific attacks. Through cybersecurity, DODIN-A operations providers protect, monitor, analyze, detect, respond to, and report unauthorized activity within DOD information systems and computer networks. Robust cybersecurity measures prevent adversaries from accessing the DODIN-A through known vulnerabilities. Effective cybersecurity is achieved through a continuous cycle of planning cybersecurity measures, applying cybersecurity controls, and assessing effectiveness. See ATP 6-02.71 and FM 6-02 for more information about cybersecurity.

CONDUCT DEFENSIVE CYBERSPACE OPERATIONS–INTERNAL DEFENSIVE MEASURES

A-46. Defensive cyberspace operations may be a response to attacks, exploitations, intrusions, or effects of malware on the DODIN-A or other assets that the DOD is directed to defend. *Defensive cyberspace operations–internal defensive measures* is a defensive cyberspace operations mission in which defense actions occur within the defended portion of cyberspace (JP 3-12). Defensive cyberspace operations–internal defensive measures may involve reconnaissance measures within the DODIN-A to locate internal threats and may respond to unauthorized activity, alerts, and threat information. Army units plan, integrate, and synchronize defensive cyberspace operations–internal defensive measures to preserve freedom of action to support the commander's objectives as part of the operations process. See FM 3-12 for additional information on defensive cyberspace operations.

IMPLEMENT PHYSICAL SECURITY MEASURES AND PROCEDURES

A-47. Physical security is the part of security concerned with physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and safeguard them against espionage, sabotage, damage, and theft. Commanders employ physical security measures in depth to protect personnel, information, and critical resources in all locations and situations against various threats through effective physical security programs, policies, and procedures.

A-48. The physical security program is the interrelationship of various components that complement each other to produce a comprehensive approach to security matters. A physical security program is built on the foundation that baseline security and protection posture are established—the local threat, site-specific vulnerabilities, the number and type of critical assets, and the employment of available resources. To successfully counter threats, physical security systems must be scalable and proportional to increases in the local threat and designed to employ layered defense in depth. Physical security measures are a combination of active and passive systems, devices, and security forces that are used to protect an asset or facility from possible threats. These systems and measures include—

- Barrier systems.
- Security lighting.
- Integrated electronic security systems.
- Access control systems.
- Key and locking systems.
- Security and guard forces.

A-49. The goal of physical security systems is to employ security in depth to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage, or other criminal activity. To achieve this goal, each security system component has a function and related measures that provide an integrated capability for—

- **Deterrence.** A potential aggressor who perceives a risk of being caught may be deterred from attacking an asset. The effectiveness of deterrence varies with the aggressor's sophistication, the value of the asset, and the aggressor's objective. Although deterrence is not considered a direct design objective, it may be a result of the design.
- **Detection.** A detection measure senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a response force. A detection system must provide all three of these capabilities to be effective. Detection measures may detect aggressor movement via intrusion detection systems, weapons, and tools via X-ray machines or metal or explosive detectors. Detection measures may also include access control elements that assess the validity of identification credentials. These control elements may provide a programmed response (admission or denial), or they may relay information to a response force. Guards also serve as detection elements, detecting intrusions and controlling access.
- **Assessment.** Assessment—through the use of video surveillance systems, other types of detection systems, patrols, or fixed posts—assists in localizing and determining the size and intent of an unauthorized intrusion or activity.

- **Delay.** Delay measures protect an asset from aggression by delaying or preventing aggressor movement toward the asset or by shielding the asset from weapons systems and explosive hazards. Delay measures may be active or passive. Active delay measures are manually or automatically activated in response to acts of aggression. Passive delay measures (such as blast-resistant building components and fences) do not depend on detection or a response. Guards may also be considered delay measures.
  - Delay aggressors from gaining access by forced entry using tools (barriers, response force).
  - Prevent aggressor movement toward assets. These measures provide barriers to movement and obscure the line of sight to assets.
  - Protect the asset from the effects of tools, weapons, and explosives.
- **Response.** Most protective measures depend on response personnel to assess unauthorized acts, report detailed information, and defeat an aggressor. Although defeat is not a design objective, defensive and detection systems must be designed to accommodate (or at least not interfere with) response force activities.

A-50. Both at home station and while deployed, physical security measures provide a secure environment for commanders to generate, project, and preserve combat power throughout competition below armed conflict, crisis, and armed conflict. In both environments, implementing physical security measures can be a challenge. Adversaries can observe operational patterns and determine existing defensive measures. Such vulnerabilities can be reduced by developing proper standoff distances, installing early-detection sensors and countersurveillance devices, aggressively patrolling, and implementing random antiterrorism measures.

A-51. During crisis and armed conflict and war, Army forces should expect deployments to be contested by the enemy in all domains and theaters of war. During deployment, equipment and personnel can be particularly vulnerable while in transit between home stations and ports of embarkation/debarkation because threats will attempt to contest or take advantage of U.S. military force projection. Expeditionary forces can protect combat power by establishing a system of complementary, overlapping physical security measures to control access to critical resources and personnel. As conditions improve and resources become available, other security measures (remotely monitored electronic sensors, forward-looking infrared systems, unmanned aircraft systems) may be used to improve protection.

A-52. Establishing access control measures; installing concrete barriers, fences, exterior security lighting, concertina wire, and guard towers; and conducting aggressive security patrols can deny enemy access to the area immediately surrounding friendly forces. Whether establishing a base camp or occupying an existing one, military leaders should focus on establishing or reassessing protective measures at the perimeter of the base camp. Once these measures are adequate, leaders can then direct attention to the measures used to protect personnel or assets located at the interior of the base camp. See ATP 3-39.32 for additional information on physical security.

APPLY ANTITERRORISM MEASURES

A-53. Throughout the world, terrorists threaten U.S. military operations in competition below armed conflict, crisis, and armed conflict. Terrorist networks benefit from even the smallest attacks against accessible U.S. forces that are forward deployed, creating symbolic value and persuasive recruiting material. The primary purpose of antiterrorism is to maintain mission capabilities by safeguarding personnel, property, and resources during Army operations. It is also designed to detect and deter a terrorist threat, enhance security and awareness, and assign antiterrorism responsibilities for Army installations and stand-alone facility personnel. (See ATP 3-37.2 for additional information on antiterrorism.) The following five antiterrorism principles represent the characteristics of successful antiterrorism integration and synchronization within the Army and the joint functional concept of protection:

- **Assess.** Assessment is the method of monitoring and evaluating the current situation and progress of an operation, task, or mission. Assessing includes the analysis of the security environment, threat information, and effectiveness of planning and execution measures to mitigate risk.
- **Detect.** Detection identifies an act of aggression and analyzes its validity. It also supports the principles of defend and warn by providing appropriate information to units, response forces, and

command and control elements. A detection system must provide all three (identify, analyze, and support) of these capabilities to be effective.

- **Warn.** Warning includes the knowledge and communication of a broad range of dangers, from general to specific and imminent threats, due to the wide spectrum of potential enemy activities. Examples of warning tasks are training, education, and awareness of the terrorist threat; use of local area networks, electronics, and communication devices to disseminate threat warnings and indications; and imminent threat warning systems (command information networks).
- **Defend.** Defense protects an asset from aggression by delaying or preventing enemy movement toward the asset or by shielding the asset from threat tactics, tools, weapons, and explosive hazards. Defensive measures may be active (reaction forces, activation of an entry control barrier) or passive (blast-resistant building components, perimeter fencing, Jersey barriers).
- **Recover.** Recovery deals with the need to recover after a terrorist incident. In an almost seamless evolution, the emphasis on response changes to recovery operations. Within recovery, actions are taken to help military personnel, installations, facilities, and operating units return to a preincident operating status. Short-term recovery (hours to weeks) includes immediate measures that support crisis response activities.

A-54. Antiterrorism must be integrated into all Army operations and always considered during competition below armed conflict, crisis, and armed conflict. Awareness must be built into every mission, every Soldier, and every leader. Typical Army antiterrorism programs are composed of several adjunct and information programs, including tasks for specialized, nonprotection military occupational specialties. At a minimum, antiterrorism includes—

- Risk management (threat, critical, vulnerability, and antiterrorism risk assessments of units, installations, facilities, and base camps).
- Antiterrorism planning (units, installations, facilities, and bases).
- Antiterrorism awareness training and command information programs.
- Antiterrorism exercises that validate defensive plans, incident response, consequence management, and continuity of essential military operations.
- Antiterrorism protection measures to protect individual personnel, high-risk personnel, physical assets (physical security), designated critical assets, and information. This includes providing isolated personnel guidance and equipment to personnel at risk of isolation.
- Antiterrorism resource application to apply risk management to vulnerabilities and mitigate against known and postulated threats.
- Civil and military partnerships, including response and protective posture agreements.
- FPCON systems to support terrorist threat and incident response plans.
- Comprehensive antiterrorism program reviews.

PROVIDE EXPLOSIVE ORDNANCE DISPOSAL SUPPORT

A-55. Explosive hazards are an ever-present danger in all areas of the battlefield. Explosive hazards include mines, unexploded ordnance, and improvised explosive devices, which limit maneuver and mobility, deny the use of critical assets, and cause military and civilian casualties. Ordnance capable of dispersing improved conventional munitions submunitions (which can be dispersed by rockets, projectiles, and bombs) impedes access across a wide area and increases the volume of unexploded ordnance on the battlefield. EOD forces enable access to areas denied by explosive ordnance, explosive hazards related to CBRN, and weapons of mass destruction threats. EOD forces perform render-safe procedures and exploitation disposal of explosive hazards, and they are specially trained in CBRN munitions and weapons of mass destruction capabilities. EOD operations enable freedom of action. While other forces may have the ability to destroy limited explosive ordnance by detonation, they are not properly equipped, trained, or authorized to perform render-safe procedures, exploitation, or other disposal procedures that preserve critical infrastructure. EOD is a critical capability that enhances force protection of military and civilian personnel, critical assets, infrastructure, and public safety.

A-56. EOD missions and primary tasks vary based on the mission, operational environment, and echelon of the supported force. In the theater and corps areas, EOD missions and tasks are focused on protecting and sustaining force generation activities; enabling movement of forces along lines of communications; deliberate exploitation of captured enemy materiel; and cooperation with joint, interorganization, and multinational EOD and related forces. Conversely, EOD support to divisions, brigade combat teams, and other units in the division area of operations focuses on enabling maneuver through the identification, render safe, and disposal of explosive ordnance threatening key terrain, routes, critical infrastructure (such as bridges), populations, activities within the assigned area, and reduction of the immediate operational risk unexploded ordnance creates during military operations. EOD forces enable lethal operations through the direct integration of EOD teams into maneuver squads, platoons, and other elements conducting kinetic operations; multiechelon participation in special access programs; and other activities that involve integration with forces conducting lethal operations in support of Army operations.

A-57. EOD operations occur during competition below armed conflict, crisis, and armed conflict. In order to manage and mitigate risk at the lowest possible level, commanders must ensure that EOD capabilities are integrated throughout the operations process. EOD operations during competition below armed conflict include explosive ordnance mitigation, training and ranges, physical security, stockpile management, humanitarian mine action, defense support to civil authorities, and security cooperation. These operations are designed to improve partner nation EOD capabilities. EOD support to security cooperation enhances protection by developing partner nation EOD, class V safety, and related capabilities. As operations transition to crisis, EOD operations may include initial clearance of explosive hazards at aerial ports of debarkation and seaports of debarkation, explosive ordnance mitigation to enable freedom of movement as personnel and equipment proceed with onward movement, and support to special operations forces.

A-58. During armed conflict, EOD support varies based on mission requirements of the supported unit. In the theater and corps areas, EOD missions may include missions more commonly associated with EOD tasks during competition below armed conflict and crisis. EOD support to divisions and subordinate units focuses on reducing the immediate operational risk that unexploded ordnance creates during military operations. Examples include, but are not limited to, protecting critical infrastructure and key terrain necessary to maneuver and sustain forces; processing, rendering safe, and disposing of captured enemy ammunition, enemy weapons systems, and explosive ordnance; and conducting improvised explosive device response, technical intelligence, and battle damage assessments and analysis of affected civilian and military equipment and infrastructure. Following armed conflict, EOD core competencies assist the United States in returning to competition below armed conflict by enabling limited local governance and by integrating other supporting and contributing joint, intergovernmental, and multinational organizations, nongovernmental organizations, or U.S. government agency participants until legitimate local entities are functioning. See ATP 4-32, ATP 4-32.1, ATP 4-32.3, and JP 3-42 for additional information on EOD.

CONDUCT PERSONNEL RECOVERY

A-59. *Army personnel recovery* is the military efforts taken to prepare for and execute the recovery and reintegration of isolated personnel (FM 3-50). This includes U.S. military, DOD civilian, and DOD contractor personnel or other personnel (as directed by the President or Secretary of Defense) who are isolated in an operational environment. It integrates a whole-of-government effort backed by holistic and cross-functional planning, preparation, execution, and assessment that is doctrinally aligned under the protection warfighting function, where isolation management enables the preservation of combat power through proactive measures to—

- Recover isolated forces before capture/captivity.
- Deny adversary the ability to influence diplomatic and military efforts through exploitation of isolated forces.
- Account for all Soldiers and evidence of the unaccounted. See FM 3-50 for additional information on personnel recovery.

A-60. Personnel recovery directly supports the protection framework, enabling commanders to apply maximum combat power at the appropriate place and time to accomplish the mission. It is consistent with federal statute, DOD, and Army policy and is nested with the Department of Defense Personnel Recovery Program. Personnel recovery includes three main areas:

- **Operate in isolation.** Army forces execute their strategic roles across the competition continuum. An Army element becomes isolated when it is no longer under the command and control of its tactical leader, has met the commander's issued isolation criteria, and is executing its isolated Soldier guidance across the spectrum of violence. It occurs because of actions by friendly forces, the threat, or hazards in the operational environment. It exists within every operational environment and forms a logical extension of the battlefield that may extend beyond that of the unit's area of operation, influence, or interest. There are two forms of isolation:
  - **Evasion.** Evasion is a form of isolation where the tactical situation dictates a change of mission requiring an isolated element to avoid capture while executing independent recovery or enabling other recovery methods.
  - **Captivity.** Captivity is a form of isolation where the isolated element has been captured and is under the direct control of an adversary or foreign government. Captivity occurs during peace and war and by nonstate hostage takers. Variations between each must be understood and applied by each captive through the Code of Conduct as an internee, hostage, prisoner of war, or retained person.
- **Isolation management.** Isolation management is the systematic process used to recover isolated forces. The process integrates the isolation management tasks of report, locate, support, recover, and screen.
  - Report includes the recognition, proper notification, and validation that personnel have or may have become isolated. The report task is generated by an accountability mechanism; visual sightings; intelligence, surveillance, and reconnaissance operations; or communications with the isolated element reporting the event.
  - Locate includes the actions taken to precisely locate the isolated element. Location efforts, using all necessary means, begin with the initial report and continue until recovery of the isolated element.
  - Support includes the actions taken to sustain the isolated element mentally, physically, and emotionally, as well as their next of kin. It includes actions such as establishing communications, conducting resupply, maintaining their morale, and protecting them (such as emplacing no-fire areas on isolated element locations). Support to families includes preparing them for potential media interaction and providing other support to reduce their anxiety and possible frustration during isolation and recovery activities.
  - Recover includes the use of three tactical recovery methods to regain command and control of an isolated element. Recovery ends with the transfer of the previously isolated element to the medical authority conducting postisolation screening and/or reintegration activities. The three tactical recovery methods include independent recovery, hasty recovery, and deliberate recovery. A final method of recovery (external recovery) includes those activities that the Army takes to either lead or support a joint recovery effort or provide support to either diplomatic or civil activities, or the recovery activities employed by Army special operations forces.
  - Screening is performed at echelons brigade and higher to collect operational and isolation information from a previously isolated element; assess their physical, mental, and spiritual condition; and inform the commander's decision to reconstitute or reintegrate commensurate with mission requirements and available resources.
- **Postisolation reintegration.** Postisolation reintegration is the joint process that allows DOD to provide medical care and protect the wellbeing of recovered personnel through decompression while conducting debriefings to gather necessary intelligence and survival, evasion, resistance, and escape information. During their planning, commanders establish a reintegration process, to include locations, teams, and responsibilities. Phase I and Phase II of reintegration are a joint responsibility of the combatant commander.

CONDUCT POLICE OPERATIONS

A-61. Police operations are an integral part of the protection warfighting function, and commanders rely on military police to assist them in understanding how crime, disorder, and the fear of crime are persistent and debilitating factors that contribute to instability across an operational environment. Military police maintain order and discipline by preventing and mitigating crime through proactive crime prevention efforts and investigating major crimes that impact unit readiness and the commander's ability to preserve combat power. Commanders can visualize potential solutions to prevent criminal acts through an understanding of how police operations are integrated within the protection warfighting function and how it applies to the protection of forces and populations within their area of operations.

A-62. Police operations encompass two tasks—law enforcement and policing. These two tasks are complementary and interdependent but are conducted with a different intent. As the term suggests, law enforcement is conducted for the purpose of enforcing laws, investigating crimes, and apprehending (when warranted) persons for adjudication within the appropriate judicial system. *Policing* is the application of control measures within an area of operations to maintain law and order, safety, and other matters affecting the general welfare of the population (FM 3-39). Policing focus on maintaining order and establishing security, not on enforcing laws on the population or compelling compliance at the risk of legal penalties. The relative emphasis given to policing and law enforcement tasks specifically depends on the operational environment, the level of violence, and the presence of the applicable Rule of Law. An operational environment characterized by general war requires police operations heavily weighted toward policing tasks, with minimal emphasis on law enforcement. Operational environments characterized by relative stability and governance under the Rule of Law require much more law enforcement activity and less focus on policing tasks.

A-63. During competition below armed conflict, police operations support various long-term military engagements; security cooperation; and deterrence missions, tasks, and actions intended to assure allies, build partner capacity and capability, and promote regional stability. Police operations can help support the geographic combatant commander's theater campaign plan or the theater security cooperation plan. These operations help counter actions by adversaries that challenge the stability of a nation or region that is contrary to U.S. interests. Commanders, provost marshals, and military police planners must synchronize, integrate, and organize military police capabilities and resources throughout operations to protect U.S. interests and build partner capacity and partnerships.

A-64. Police operations during competition below armed conflict also include unit home station activities (maintaining operational readiness, training, contingency planning). Combined exercises and training, military exchange programs, and foreign military member attendance at Army schools are examples of activities during competition below armed conflict. At home stations, military police conduct law enforcement, criminal investigations, police engagement, corrections, physical security procedures, antiterrorism, and protective services tasks to maintain safe and secure environments. This enables commanders to generate, project, and preserve combat power during training and deployment tasks that are associated with Army Sustainable Readiness requirements in support of multidomain operations.

A-65. Police operations during crisis helps deter adversary actions that are contrary to U.S. interests. They are conducted in response to activities that threaten unified action partners and require the deployment or repositioning of credible forces in a theater to demonstrate the willingness to fight if deterrence fails. Police operations support mobilization and the transit of Army forces and cargo along movement routes, at initial staging areas, and at subsequent assembly areas where uncertain threat conditions require a delicate balance between protection and building combat power. Police operations also help set conditions for a stable environment during the consolidation of gains. These activities include populace and resources control, security cooperation, law and order reestablishment, humanitarian assistance, and critical infrastructure protection and restoration.

A-66. During armed conflict, military police continue to protect forces, populations, and critical infrastructure and assets. Police operations are conducted to conduct reconnaissance and surveillance of bases, routes, facilities, and storage sites to detect, deter, and defeat criminals and irregular threats. Many of the information and operational requirements that police operations support at home stations are generally the same requirements they support throughout the operational framework during large-scale combat operations.

A-67. Current assessments of peer competitors indicate that criminals, irregular threats, and proxies will likely operate throughout the operational framework. Military police conducting police operations counter these threats from home-station installations through the close area. Police operations conducted at home station in the strategic support areas should be considered an extension of police operations conducted throughout the operational framework. Only by treating them as interdependent and interrelated missions will the Army generate the synergies and achieve the desired security effects and outcomes required to prevail during periods of competition below armed conflict, crisis, and armed conflict. See ATP 3-39.10 for additional information on police operations.

CONDUCT DETENTION OPERATIONS

A-68. Detention operations are significant to the protection warfighting function and across the range of military operations. Detention involves the detainment of a population or group that poses some level of threat to military operations. These operations are conducted to shelter, sustain, guard, protect, and account for populations (detainees or U.S. military prisoners) as a result of military or civil conflict or to facilitate criminal prosecution. The Army is the DOD executive agent for detainee operations and for the long-term confinement of U.S. military prisoners. Detention operations include—

- Interning U.S. military prisoners. See FM 3-39 for additional information on the battlefield confinement of U.S. military prisoners.
- Conducting detainee operations. See FM 3-63 for additional information on detainee operations.
- Supporting host-nation corrections reform. See FM 3-39 and FM 3-63 for additional information on host-nation corrections reform.

A-69. During competition below armed conflict, detention operations support various long-term military engagements; security cooperation; and deterrence missions, tasks, and actions intended to assure allies, build partner capacity and capability, and promote regional stability. Detention operations help support the geographic combatant commander's theater campaign plan or the theater security cooperation plan. These operations help counter actions by adversaries that challenge the stability of a nation or region that is contrary to U.S. interests. Commanders and staffs must synchronize, integrate, and organize detention capabilities and resources throughout operations to protect U.S. interests and build partner capacity and partnerships.

A-70. Detention operations during competition below armed conflict also includes the incarceration of U.S. military prisoners at home stations. The incarceration of U.S. military prisoners protects society by incarcerating U.S. military prisoners and prepares U.S. military prisoners for their release (regardless of whether they are returning to duty or civilian status), with the prospect of becoming productive Soldiers/citizens by conforming to U.S. military or civilian environments. Detention operations at home stations provide a safe and secure environment for commanders to generate, project, and preserve combat power during training and deployment tasks that are associated with Army Sustainable Readiness requirements in support of multidomain operations.

A-71. During a crisis, U.S. forces may be deployed to areas of operation with a limited or failed corrections system. This includes host-nation capability and capacity for the detention of detained personnel and the subsequent incarceration of convicted criminals. U.S forces may be required to initially perform corrections duties to establish or maintain a secure environment. If required, U.S. forces conduct the battlefield detention and confinement of U.S forces to help maintain discipline, law, and order. Battlefield detention and confinement facilities can provide the necessary pretrial and posttrial confinement for U.S. military prisoners and other persons subject to the Uniform Code of Military Justice. During a crisis, commanders and staffs must also plan and prepare for the transition to armed conflict and the capture, initial detention and screening, transportation, protection, and housing of detainees.

A-72. The primary focus of detention operations during armed conflict is the conduct of detainee operations. Detainee operations is a broad term that encompasses the capture, initial detention, screening, transportation, treatment, protection, housing, transfer, and release of the wide range of persons who could be categorized as detainees. The term detainee includes any person captured, detained, or otherwise under the control of DOD personnel. Detainee categories include—

- Enemy prisoners of war.
- Retained personnel.
- Civilian internees.
- Detained personnel.

A-73. Detainee operations during an armed conflict are the range of actions taken by U.S. Armed Forces, beginning at the point of capture; through movement to a detention facility (detainee collection point, detainee holding area, or theater detention facility); and until detainee transfer, release, repatriation, death, or escape. All commanders and Soldiers participating in military operations must be prepared to process and safeguard detainees. Detainee operations begin at the point of capture (the point at which a Soldier has the custody of, and is responsible for, safeguarding a detainee). They can directly affect mission success and have a lasting impact on U.S. tactical, operational, and strategic military objectives.

A-74. The number of detainees captured by U.S. Armed Forces at any given point can range from one to thousands, depending on the scope of the armed conflict and the elements involved. While one or two detainees may not create a major logistic or accountability challenge, a large number of detainees require a larger number of guards and significantly more resources. The larger the number of detainees, the higher the security risks to Soldiers and detainees.

A-75. Detainees must be safeguarded, to include provisions for adequate space, food, and waste disposal. Force health protection measures must be implemented in detainee operations to prevent outbreaks of infectious diseases. Field-expedient measures may be needed to sustain field sanitation practices of detainees. Commanders provide personal hygiene and field sanitation facilities commensurate with those they would provide for their Soldiers based on available resources. (See ATP 4-02.46 for further guidance on medical considerations to detainee operations.) These tasks are manpower-intensive, can cause significant delays in onward movement, and can divert unit assets from the primary mission.

CONDUCT POPULACE AND RESOURCES CONTROL

A-76. Military forces base the extent of populace and resources control functions on their current operational environment. Populace and resources control is an extension of the function of local civil administration and is more effective when led and executed locally. In the absence of a sovereign government, the implementation of a populace and resources control policy begins with the establishment of a military government or a transitional military authority. Populace and resources control measures implemented at the operational and tactical levels result from policy developed at national and theater strategic levels during competition below armed conflict (see ATP 3-39.30, ATP 3-57.10, FM 3-57, and JP 3-57 for additional information on populace and resources control.). Commanders must consider the impact of military operations on the civilian population and the affects the civilian population has on military operations.

A-77. During competition below armed conflict, U.S. forces must plan and prepare for conducting populace and resources control to uphold policy and strengthen the sovereignty of a legitimate government to govern the people and resources within its borders. Populace and resources control in support of crisis helps deter adversary actions that are contrary to U.S. interests. They are conducted in response to activities that threaten host-nation civilian populations and resources and demonstrate the willingness of U.S. forces to fight if deterrence fails. During crisis, populace and resources control activities may include providing support to dislocated civilian operations, providing security cooperation, maintaining/reestablishing law and order, providing humanitarian assistance, and protecting critical resources.

A-78. As operations transition to armed conflict, U.S. forces continue to conduct populace and resources control to protect civilian populations by maintaining curfews, restricting movement, and resettling dislocated civilians. The implementation of resources control measures during armed conflict regulates the consumption of resources, controls the movement of resources, denies the enemy the use of resources, detects and mitigates the effectiveness of criminal activity, and minimizes negative impacts on maneuver forces.

A-79. Populace and resources control functions consist of two distinct—yet linked—components: populace control and resources control. Normally the responsibility of civilian governments, combatant commanders define and enforce these controls during large-scale ground combat, consolidation of gains, and times of crisis (civil or military emergency).

POPULACE CONTROL

A-80. Populace control provides security for the indigenous populace, mobilizes civilian resources, denies enemy access to the population, and detects and reduces the effectiveness of enemy agents. Populace control measures are a key element in the consolidation of gains and the execution of primary stability tasks of civil security and civil control. Commanders and leaders set the conditions for the operation by gaining the cooperation and support of the populace by building mutual trust. This involves establishing public order and safety, securing borders, protecting population centers and people, holding individuals accountable for criminal activities, controlling the activities of individuals or groups that pose a security risk, reestablishing essential civil services, and setting operational area conditions that support stability through unity of effort. Populace control may become necessary as a result of military operations or man-made or natural disasters.

A-81. Populace control measures can be used to protect civilians by keeping them away from military operations, which safeguards them from becoming a collateral damage casualty and protects the OPSEC of the mission by limiting access to information and locations. The use of curfews and movement restrictions, instituting policies regarding the regulation of air and overland movement and relocating the population may be necessary for successful military operations.

A-82. International law may require a military force to consider some essential tasks that establish a safe, secure environment and address the humanitarian needs of the local population (see FM 6-27 for additional information). Determining which populace control measures to employ requires a framework that applies across the range of military operations, from stable peace to general war. Dislocated civilian operations and noncombatant evacuation operations are two special categories of populace control that require extensive planning and coordination among various military and nonmilitary organizations.

RESOURCES CONTROL

A-83. Resources control provides security for the indigenous natural and man-made materiel resources of a nation-state, mobilizes economic resources, denies the enemy access to resources that protract a conflict, and detects and reduces the effectiveness of enemy and criminal activity. It also includes protection of U.S. assets to deny or defeat enemy and criminal activities against them.

A-84. Resources control directly impacts the economic system of a host nation or territory governed by U.S. forces and includes property control, which is the control of movable and immovable private and public property. Resources control measures regulate public and private property and the production, movement, or consumption of materiel resources. Controlling a nation’s resources is normally the responsibility of indigenous civil governments. During a civil or military emergency, proper authorities define, enact, and enforce resources control measures to maintain public order and enable the execution of the primary stability tasks of civil security, civil control, restoration of essential services, and support to economic and infrastructure development. Enforcement of resources control must be consistent and impartial so that the government or military establishes and maintains legitimacy among the populace. A well-crafted personnel recovery plan limits control measures to the least restrictive measures necessary to achieve the desired effect.

PROVIDE FORCE HEALTH PROTECTION

A-85. Force health protection is a mission component of the Army Health System and is a continual process with measures that enable a healthy and fit force, prevent injury and illness, and protect the force from health hazards. *Force health protection* are measures that promote, improve, or conserve the behavioral and physical well-being of Soldiers comprised of preventive and treatment aspects of medical functions that include: combat and operational stress control, dental services, veterinary services, operational public health, and laboratory services (FM 4-02). Medical mobilization and predeployment support ensures that Soldiers are prepared for deployment, including immunizations; predeployment health assessments; dental, vision, and hearing readiness testing and treatment; and health risk communications on health hazards in the operational environment. Force health protection measures include—

- Establishing and sustaining a healthy and fit force.
- Preventing and controlling diseases and injuries.
- Assessing occupational and environmental health.
- Identifying health threats in all settings (both deployed and garrison).
- Determining force health protection activities.
- Employing preventive medicine toxicology and laboratory services.
- Developing and implementing personal protective measures to reduce exposure to health hazards.
- Performing health risk assessments.
- Disseminating health information.
- Mitigating the adverse effects of the impact of health threats.

A-86. During competition below armed conflict, Army force health protection efforts are a continuous process that begins with the Soldier's entry into the military and is continuous throughout the Soldier's military career. At home station, commanders ensure that Soldiers receive training and education on preventive measures (including dental care and actions taken to prevent disease) that promote, improve, and conserve behavioral and physical well-being through illness and injury prevention, nutrition, physical fitness, and health improvement to sustain a healthy and fit force.

A-87. Force health protection during crisis and armed conflict enables commanders to increase return-to-duty rates and maintain combat power spanning the operational area, from point of injury/illness to definitive care, with an overall goal of treating all potentially survivable injuries. Commanders and unit leaders must remain informed and proactively engaged to ensure that health threats are reduced. They must promote measures to reduce stressors and risks and enforce countermeasures to prevent diseases, operational and health hazards, poisonous or toxic flora and fauna, physical effects of weapons, and physiological and psychological stressors.

A-88. The medical functions that make up Army force health protection efforts have corresponding preventive tasks that reduce hazards to preserve combat power and increase return-to-duty rates. Key preventive tasks by function are outlined in table A-1. See FM 4-02 for a more detailed description of each task purpose.

Table A-1. Force health protection primary preventive tasks by function

Medical Function	*Primary Tasks*
Operational public health	• Conduct health surveillance and epidemiology. • Conduct occupational health. • Monitor environmental health. • Provide occupational and environmental medicine. • Conduct operational public health. • Conduct a health risk assessment. • Provide clinical public health. • Provide community-based prevention and health promotion. • Provide public health toxicology. • Perform public health laboratory services. • Deliver public health communication. • Provide public health emergency management.
Veterinary Services	• Provide animal medical care. • Conduct food protection activities. • Execute veterinary public health activities.
Dental Services	• Conduct periodic examinations of Soldiers' teeth, gums, and jaw. • Classify Soldiers' dental conditions in the dental classification system and determine Soldiers' dental readiness status. • Provide training to Soldiers and units on how to mitigate the adverse impact of dental threats.
Combat and Operational Stress Control	• Implement a combat and operational stress control plan/program. • Perform a combat and operational stress control unit needs assessment. • Conduct traumatic event management for potentially traumatic events. • Screen and evaluate Soldiers with maladaptive behaviors to rule out neuropsychiatric/behavioral health conditions. • Conduct combat and operational stress restoration and reconditioning programs, to include warrior resiliency training. • Perform command-directed evaluation for Soldier's behavioral health status. • Screen patients with potential behavioral health issues for signs/symptoms of mild traumatic brain injuries.
Laboratory Services	• Provide analytical, investigational, and consultative capabilities. • Provide special environmental control and containment. • Provide data and data analysis. • Conduct medical laboratory analysis. • Deploy modular sections or sectional teams.

A-89. Methods to prevent disease are best applied through the synchronization of multiple efforts. Effective field hygiene and sanitation practices, waste management, and pest and vector control are crucial to disease prevention. Conducting vector surveillance and proper use of the DOD arthropod repellent system (wearing permethrin-treated uniforms, using insect repellent on skin, and using bed nets) are good examples of mosquito/tick/sandfly disease prevention. Prophylactic measures can also include human and animal immunizations, dental chemoprophylaxis and examinations, epidemiology, optometry exams, medical intelligence on specific health threats, and personal protective clothing and equipment.

A-90. The key to disease and injury prevention is timely hazard identification and risk communication. Derived from robust health surveillance and medical intelligence, this information addresses occupational, local environmental, and medical threats from industrial hazards, air and water pollution, endemic or epidemic disease, CBRN, and directed-energy device weapons (high-powered microwaves, particle beams, lasers). Health service support must be capable of acquiring, analyzing, and disseminating information that is timely and accurate for Soldiers. This information capability is crucial to force health protection. See FM 4-02 for additional information on force health protection.

Note. Commanders and staffs should be informed and aware of any application host-nation laws, nongovernmental organizations, and international agreements that may affect the execution of force health protection during this phase outside of the United States.

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. All websites accessed on 4 June 2023.

1-1 “It is a doctrine of war not to assume the enemy …”. Sun Tzu

Quoted in Dictionary of Military and Naval Quotations, compiled by Robert Debs Heinl, Jr. (Annapolis, MD: United States Naval Institute, 1966).

2-1 “Nine times out of ten an Army has been destroyed …”. General Douglas MacArthur, 1950. Quoted in Dictionary of Military and Naval Quotations, compiled by Robert Debs Heinl, Jr. (Annapolis, MD: United States Naval Institute, 1966).

3-1 “It is always necessary to shape operations plans…”. Fredrick the Great. Quoted in Dictionary of Military and Naval Quotations, compiled by Robert Debs Heinl, Jr. (Annapolis, MD: United States Naval Institute, 1966).

4-1 “The purpose of the staff is to serve the line…”. Military Maxim. Quoted in Dictionary of Military and Naval Quotations, compiled by Robert Debs Heinl, Jr. (Annapolis, MD: United States Naval Institute, 1966).

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. Terms for which ADP 3-37 is the proponent (authority) manual are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
AFTTP	Air Force tactics, techniques, and procedures
AJP	Allied joint publication
AR	Army regulation
AT	antiterrorism
ATP	Army techniques publication
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirement
CGTTP	Coast Guard tactics, techniques, and procedures
COA	course of action
DA	Department of the Army
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense instruction
DODIN-A	Department of Defense information network–Army
DSCA	defense support of civil authorities
EM	emergency management
EOD	explosive ordnance disposal
FPCON	force protection condition
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-6	assistant chief of staff, signal
JP	joint publication
MCRP	Marine Corps reference publication
MCTP	Marine Corps tactical publication
MCWP	Marine Corps warfighting publication
MDMP	military decision-making process
METT-TC(I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations

MOE	measure of effectiveness
MOP	measure of performance
NTTP	Navy tactics, techniques, and procedures
OPSEC	operations security
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
S-2	battalion or brigade intelligence staff officer
TC	training circular
TM	technical manual
U.S.	United States
USC	United States Code

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)

air and missile defense

Direct [active and passive] defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile air and ballistic missile threats against friendly forces and assets. (JP 3-01)

air defense artillery

Weapons and equipment for actively combating air targets from the ground. (JP 3-01)

area damage control

Measures taken before, during, and/or after a hostile action or natural or manmade disasters to reduce the probability of damage and minimize its effects. (JP 3-10)

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)

Army personnel recovery

The military efforts taken to prepare for and execute the recovery and reintegration of isolated personnel. (FM 3-50)

assessment

Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. (JP 3-0)

chemical, biological, radiological, and nuclear environment

An operational environment that includes chemical, biological, radiological, and nuclear threats and hazards and their potential resulting effects. (JP 3-11)

chemical, biological, radiological, and nuclear operations

Chemical, biological, radiological, and nuclear operations include the employment of capabilities that assess, protect against, and mitigate the entire range of chemical, biological, radiological, and nuclear incidents to enable freedom of action. (FM 3-11)

combat identification

The process of attaining an accurate characterization of detected objects in the operational environment sufficient to support an engagement decision. (JP 3-09)

combat power

The total means of destructive and disruptive force that a military unit/formation can apply against an enemy at a given time. (JP 3-0)

contamination mitigation

The planning and actions taken to prepare for, respond to, and recover from contamination associated with all chemical, biological, radiological, and nuclear threats and hazards in order to continue military operations. (JP 3-11)

counterintelligence

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (JP 2-0)

countermobility

A set of combined arms activities that use or enhance the effects of natural and man-made obstacles to prevent the enemy freedom of movement and maneuver. (ATP 3-90.8)

cover

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

crisis

An emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives. (JP 3-0)

critical asset

A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP 3-26)

defensive cyberspace operations-internal defensive measures

A defensive cyberspace operations mission in which defense actions occur within the defended portion of cyberspace. (JP 3-12)

defensive operation

An operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations. (ADP 3-0)

Department of Defense information network-Army

An Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide. (ATP 6-02.71)

domain

A physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills. (FM 3-0)

electromagnetic compatibility

The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. (JP 3-85)

electromagnetic hardening

Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (JP 3-85)

electromagnetic masking

The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-85)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

electromagnetic spectrum management

The operational, engineering, and administrative procedures to plan and coordinate operations within the electromagnetic operational environment. (JP 3-85)

emission control

The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan. (JP 3-85)

enemy

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

execution

The act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation. (ADP 5-0)

explosive hazard

Any material posing a potential threat that contains an explosive component. (JP 3-15)

explosive ordnance

All munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. (JP 3-34)

fires warfighting function

The related tasks and systems that create and converge effects in all domains against the adversary or enemy to enable operations across the range of military operations. (ADP 3-0)

force health protection

Measures to promote, improve, or conserve the behavioral and physical well-being of Soldiers to enable a healthy and fit force, prevent injury and illness, and protect the force from health hazards. (FM 4-02)

force projection

The ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations. (JP 3-0)

force protection

Preventive measures taken to mitigate hostile actions against Department of Defense personnel (including family members), resources, facilities, and critical information. (JP 3-0)

***fratricide**

The unintentional killing or wounding of friendly or neutral personnel by friendly firepower.

general engineering

Those engineering capabilities and activities, other than combat engineering, that provide infrastructure and modify, maintain, or protect the physical environment. (JP 3-34)

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)

hazard

A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. (JP 3-33)

homeland defense

The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. (JP 3-27)

information collection

An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of 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)

intelligence preparation of the operational environment

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. (FM 2-0)

knowledge management

The process of enabling knowledge flow to enhance shared understanding, learning, and decision making. (ADP 6-0)

local security

The low-level security activities conducted near a unit to prevent surprise by the enemy. (ADP 3-90)

main effort

A designated subordinate unit whose mission at a given point in time is most critical to overall mission success. (ADP 3-0)

measure of effectiveness

An indicator used to measure a current system state, with change indicated by comparing multiple observations over time. (JP 5-0)

measure of performance

An indicator used to measure a friendly action that is tied to measuring task accomplishment. (JP 3-0)

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)

mobile security force

A highly motivated and dedicated security force with the capability to defeat Level I and Level II threats in a joint security area. (JP 3-10)

mobilization

The process by which the Armed Forces of the United States, or part of them, are brought to a state of readiness for war or other national emergency. (JP 4-05)

multidomain operations

The combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders. (FM 3-0)

offensive operation

An operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers. (ADP 3-0)

operation

A sequence of tactical actions with a common purpose or unifying theme. (JP 1, Volume 1)

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)

operational framework

A cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations. (ADP 1-01)

operations process

The major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation. (ADP 5-0)

operations security

A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. (JP 3-13.3)

policing

The application of control measures within an area of operations to maintain law and order, safety, and other matters affecting the general welfare of the population. (FM 3-39)

principle

A comprehensive and fundamental rule or an assumption of central importance that guides how an organization approaches and thinks about the conduct of operations. (ADP 1-01)

protection

Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 3-0)

protection warfighting function

The related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action. (FM 3-0)

risk management

The process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

rules of engagement

Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 3-84)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander’s intent and if planned future operations are supportable. (ADP 5-0)

screen

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

security operations

Those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy, and to develop the situation to allow commanders to effectively use their protected forces. (ADP 3-90)

stability operation

An operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADP 3-0)

survivability

A quality or capability of military forces which permits them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission. (ATP 3-37.34)

survivability operations

Those military activities that alter the physical environment to provide or improve cover, camouflage, and concealment. (ATP 3-37.34)

tactical combat force

A rapidly deployable, air-ground, mobile combat unit with appropriate combat support and combat service support assets assigned to, and capable of, defeating Level III threats, including combined arms. (JP 3-10)

tactical deception

A friendly activity that causes enemy commanders to take action or cause inaction detrimental to their objectives. (FM 3-90)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

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)

wartime reserve modes

Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to, or misunderstood by, opposing commanders before they are used but could be exploited or neutralized if known in advance. (JP 3-85)

working group

A grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. (FM 6-0)

This page intentionally left blank.

References

All websites accessed on 4 June 2023.

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. September 2023.

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

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

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online at https://www.jcs.mil/doctrine/. Most Department of Defense publications are available online at https://www.esd.whs.mil/DD/.

DODD 4500.09. *Transportation and Traffic Management.* 27 Dec 2019.

DODI 8500.01. *Cybersecurity.* 14 March 2014.

JP 1, Volume 1. *Joint Warfighting.*27 August 2023

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

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

JP 3-01. *Countering Air and Missile Threats*. 06 April 2023.

JP 3-09. *Joint Fire Support.*10 April 2019.

JP 3-10. *Joint Security Operations in Theater*. 25 July 2019.

JP 3-11. *Operations in Chemical, Biological, Radiological, and Nuclear Environments.* 29 October 2018.

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

JP 3-13.3. *Operations Security.* 6 January 2016.

JP 3-15. *Barriers, Obstacles, and Mines in Joint Operations.* 26 May 2022.

JP 3-26. *Joint Combating Terrorism*. 30 July 2020.

JP 3-27. *Homeland Defense*. 10 April 2018.

JP 3-29. *Foreign Humanitarian Assistance.* 14 May 2019.

JP 3-31. *Joint Land Operations.* 3 October 2019.

JP 3-33. *Joint Force Headquarters.* 9 June 2022.

JP 3-34. *Joint Engineer Operations.* 6 January 2016.

JP 3-35. *Joint Deployment and Redeployment Operations.* 31 March 2022.

JP 3-40. *Joint Countering Weapons of Mass Destruction*. 27 November 2019.

JP 3-42. *Joint Explosive Ordnance Disposal*. 14 September 2022.

JP 3-57. *Civil-Military Operations.* 9 July 2018.

JP 3-84. *Legal Support.* 2 August 2016.

JP 3-85. *Joint Electromagnetic Spectrum Operations.* 22 May 2020.

JP 4-05. *Joint Mobilization Planning.* 23 October 2018.

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

ARMY PUBLICATIONS

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

ADP 1. *The Army.* 31 July 2019.

ADP 1-01. *Doctrine Primer.* 31 July 2019.

ADP 2-0. *Intelligence*. 31 July 2019.

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

ADP 3-05. *Army Special Operations.* 31 July 2019.

ADP 3-07. *Stability.* 31 July 2019.

ADP 3-28. *Defense Support of Civil Authorities.* 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 381-10. *The Conduct and Oversight of U.S. Army Intelligence Activities.* 27 January 2023.

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

AR 385-10. *The Army Safety and Occupational Health Program.* 24 July 2023.

AR 525-2. *The Army Protection Program.* 9 June 2023.

ATP 2-01.3. *Intelligence Preparation of the Battlefield.* 1 March 2019.

ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities.* 11 December 2015.

ATP 3-01.8. *Techniques for Combined Arms for Air Defense.* 29 July 2016.

ATP 3-01.81. *Counter-Unmanned Aircraft System.* 11 August 2023.

ATP 3-05.1. *Unconventional Warfare at the Combined Joint Special Operations Task Force Level.* 9 April 2021.

ATP 3-05.20. *Special Operations Intelligence.* 3 May 2013.

ATP 3-12.3. *Electromagnetic Warfare Techniques.* 30 January 2023.

ATP 3-13.3. *Army Operations Security for Division and Below.* 16 July 2019.

ATP 3-35. *Army Deployment and Redeployment.* 9 March 2023.

ATP 3-37.2. *Antiterrorism.* 19 July 2021.

ATP 3-39.10. *Police Operations.* 24 August 2021.

ATP 3-39.30. *Security and Mobility Support.* 21 May 2020.

ATP 3-39.32. *Physical Security.* 8 March 2022.

ATP 3-57.10. *Civil Affairs Support to Populace and Resources Control.* 6 August 2013.

ATP 4-02.46. *Army Health System Support to Detainee Operations.* 24 August 2021.

ATP 4-32. *Explosive Ordnance Disposal (EOD) Operations.* 12 May 2022.

ATP 4-32.1. *Explosive Ordnance Disposal (EOD) Group and Battalion Headquarters Operations.* 24 January 2017.

ATP 4-32.3. *Explosive Ordnance Disposal (EOD) Company, Platoon, and Team Operations.* 1 February 2017.

ATP 5-19. *Risk Management.* 9 November 2021.

ATP 6-01.1. *Techniques for Effective Knowledge Management.* 6 March 2015.

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

FM 2-0. *Intelligence.* 1 October 2023.

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

FM 3-01. *U.S. Army Air and Missile Defense Operations.* 22 December 2020.

FM 3-07. *Stability.* 2 June 2014.

FM 3-11. *Chemical, Biological, Radiological, and Nuclear Operations.* 23 May 2019.

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

FM 3-13. *Information Operations.* 6 December 2016.

FM 3-13.4. *Army Support to Military Deception.* 26 February 2019.

FM 3-14. *Army Space Operations.* 30 October 2019.

FM 3-16. *The Army in Multinational Operations.* 8 April 2014.

FM 3-39. *Military Police Operations.* 9 April 2019.

FM 3-50. *Army Personnel Recovery*. 2 September 2014.

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

FM 3-57. *Civil Affairs Operations.* 28 July 2021.

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

FM 3-63. *Detainee Operations.* 2 January 2020.

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

FM 3-94. *Armies, Corps, and Division Operations.* 23 July 2021.

FM 4-02. *Army Health System.* 17 November 2020.

FM 5-0. *Planning and Orders Production*. 16 May 22.

FM 6-0. *Commander and Staff Organization and Operations.* 16 May 2022.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

TM 3-11.91. *Chemical, Biological, Radiological, and Nuclear Threats and Hazards.* 13 December 2017.

MULTI-SERVICE PUBLICATIONS

ATP 3-28.1/MCRP 3-30.6/NTTP 3-57.2/AFTTP 3-2.67/CGTTP 3-57.1. *Multi-Service Tactics, Techniques, and Procedures for Defense Support of Civil Authorities (DSCA)*. 11 February 2021.

ATP 3-34.20/MCRP 3-17.2D. *Countering Explosive Hazards.* 21 January 2016.

ATP 3-34.40. *General Engineering.* 14 April 2023.

ATP 3-37.34/MCTP 3-34C. *Survivability Operations.* 16 April 2018.

ATP 3-90.8/MCTP 3-34B. *Combined Arms Countermobility.* 30 November 2021.

FM 3-24/MCWP 3-33.5. *Insurgencies and Countering Insurgencies.* 13 May 2014.

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

OTHER PUBLICATIONS

Most Allied Joint publications are available online at: https://nso.nato.int/protected/nsdd/main/standards.

AJP-01. *Allied Joint Doctrine*. 1 December 2022.

AJP 3.14. *Force Protection*. 19 August 2015.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website at https://armypubs.army.mil.

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

RECOMMENDED READINGS

AR 5-12. *Army Use of the Electromagnetic Spectrum*. 8 February 2020.

DODD 3150.08. *DOD Response to U.S. Nuclear Weapon and Radiological Material Incidents.* 27 Nov 2020.

DODI O-2000.16, Volume 2. *DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System*. 17 November 2016.

DODI 6055.17. *DOD Emergency Management (EM) Program.* 13 February 2017.

FM 3-52. *Airspace Control.* 20 October 2016.

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

JP 3-08. *Interorganizational Cooperation.* 12 October 2016.

JP 3-28. *Defense Support of Civil Authorities.* 29 October 2018.

JP 3-50. *Personnel Recovery.* 14 August 2023.

JP 3-52. *Joint Airspace Control*. 22 October 2022.

JP 6-0. *Joint Communications System*. 10 June 2015.

TC 3-04.9. *Commander's Aviation Mission Survivability Program.* 11 August 2023.

18 USC 1385. *Use of Army, Navy, Marine, Air Force, and Space Force as Posse Comitatus*. 5 June 2023.

Index

Entries are by paragraph number.

A

air and missile defense. 3-36, 4-5
Air and missile defense. A-5
antiterrorism. 2-159, 2-160, 3-8, 3-78, 3-96, 4-17
area of operations. 2-16, 4-6
area security. 1-28, 2-110, 2-132, 3-22, 3-33, A-36, A-37, A-39

C

CBRN. 2-107, 3-80, 4-22, 4-23, A-19
chemical, biological, radiological, nuclear, and high-yield explosives
  element. 4-6
combat identification
  definition. 2-84
combat power. 2-22, A-64, A-70
combined arms. 2-73
complementary protection
  capabilities. 1-29
consolidate gains. 3-10
continuing activity. 3-1
course of action. 4-1
critical asset. 4-5
critical asset list. 3-8, 3-26, 4-4
  4-5
critical asset security. A-39
critical information requirements. 4-8
cyberspace. 3-8, 3-74

D

defended asset list. 3-26, 4-4, 4-5
defense. 1-18, 2-102, 2-104, 2-106, 2-107, 2-122
detention
  host nation. A-71
detention operations. A-68

E

EOD. 3-79, 4-17

F

force health protection. 3-36
fratricide. 2-16
full spectrum. 2-70, 4-2

I

intelligence preparation of the battlefield. 4-8

L

large-scale ground combat. 2-64
Level I threat. 1-15
Level II threat. 1-15
Level III threat. 1-15
local security. 2-88, 3-35, 3-100

O

offense. 2-100, 2-102, 2-122, 2-121, 2-124
operations security. A-40
operations to prevent. 2-32, 2-33, 2-36, 3-10, 3-60, 3-61, 3-94
operations to shape. 2-20, 2-22, 3-60, 3-61, 3-64, 3-94

P

peer threat. 1-12
personnel recovery. 3-36, 4-5
primary protection tasks. 1-22
principles. 1-24, 2-122, 3-35, 3-104
protection cell. 4-1, 4-4
  composition. 4-4
protection prioritization list. 3-27, 3-75, 4-3
protection strategy. 4-1
protection warfighting function. 1-10, 3-92
protection working group. 4-4
provost marshal. 4-17, 4-21

R

reachback. 4-7
reinforcing capabilities. 1-29
rule of law. 2-152
rules of engagement
  definition. 2-84

S

stability. 2-160
stability operations. 2-152
survivability. 2-104, A-7, A-8

T

tactics, techniques, and procedures. 2-84
theater army. 4-2

V

vulnerability assessment. 3-19, 3-21, 4-21, 4-24

W

warfighting function. 4-1, 4-4
  maneuver. 2-71

This page intentionally left blank.

ADP 3-37
10 January 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
2400301

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. To be distributed in accordance with the initial distribution number (IDN) 110502, requirements for ADP 3-37.

This page intentionally left blank.

PIN: 102965-000