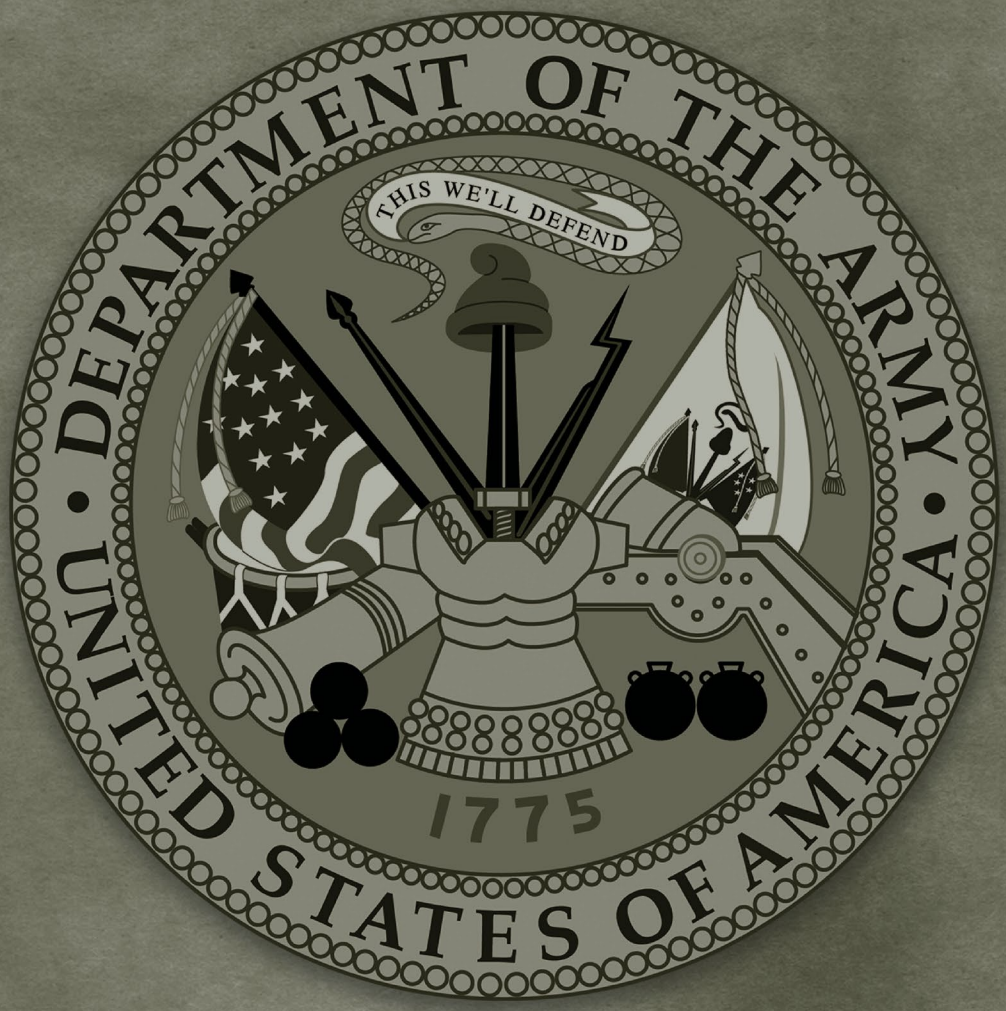
ADP 3-37
Protection



JULY 2019

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes ADP 3-37, dated 11 December 2018.

HEADQUARTERS, DEPARTMENT OF THE ARMY

*ADP 3-37

Army Doctrine Publication
No. 3-37

Headquarters
Department of the Army
Washington, DC, 31 July 2019

Protection

Contents

*This publication supersedes ADP 3-37, dated 11 December 2018.

Figures

Tables

Preface

ADP 3-37 provides guidance on protection and the protection warfighting function. It establishes the protection principles for commanders and staffs who are responsible for planning and executing protection in support of unified land operations. The synchronization and integration of protection tasks enable commanders to safeguard bases, secure routes, and protect forces. ADP 3-37 corresponds with the Army operations doctrine introduced in ADP 3-0, ADP 5-0, ADP 6-0 and the staff organization discussed in FM 6-0.

The principal audience for ADP 3-37 is commanders and staffs. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. In addition, trainers and educators throughout the Army will use this manual as a doctrinal reference for protection.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States, international, and in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the rules of engagement (see FM 27-10).

ADP 3-37 uses joint terms where applicable. For joint and Army definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. Terms for which ADP 3-37 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary; their definitions are boldfaced in the text. These terms and their definitions will be included in the next revision of ADP 1-02.

ADP 3-37 applies to the Active Army, Army National Guard/Army National Guard of the United States and United States Army Reserve unless otherwise stated.

The proponent of ADP 3-37 is the Maneuver Support Center of Excellence (MSCoE). The preparing agency is the Assistant Chief of Staff (G-3)/Directorate of Training and Doctrine (DOTD). Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, MSCoE, ATTN: ATZT-OPD-D, 14000 MSCoE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929; by e-mail to usarmy.leonardwood.mscoe.mbx.mpdoc@mail.mil; or submit an electronic DA Form 2028.

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 serves as an Army warfighting function. A shared understanding of the joint protection function (see JP 3-0) enables Army leaders to integrate the Army's protection warfighter function with unified action partners. Army leaders must anticipate that joint support will be limited in larger-scale ground combat operations and must protect the force 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

Protection is not linear – planning, preparing, executing, and assessing protection is continuous and enduring. The protection warfighting function tasks are incorporated into the operations process in a comprehensive, layered, and redundant approach to achieve enduring force protection. Protection preserves capability, momentum, and tempo which are important contributors to operational reach. Synchronizing, integrating, and organizing protection capabilities and resources throughout the operations process preserves combat power and mitigates the effects of threats and hazards to enable freedom of action.

The prioritization of protection assets is situationally dependent and resource informed. The goal of protection capabilities integration is to balance protection with the freedom of action throughout the duration of military operations. This is achieved by integrating reinforcing or complementary protection capabilities in order to mitigate or assume risk for all identified and prioritized vulnerabilities. The collaboration, integration, and synchronization between the warfighting functions assist in identifying threats and hazards and mitigating their effects. Not all assets listed on the protection prioritization list receive continuous protection. Some critical assets only receive protection assets based on available resources. Determining and directing protection priorities may involve the most important decisions commanders make and their staffs support.

Overall, ADP 3-37 remains consistent with previous protection doctrine. The protection warfighting function establishes the protection tasks and systems that are synchronized and integrated throughout the operations process and, with the other elements of combat power, preserves the force so that commanders can apply maximum combat power to accomplish the mission. The doctrine described in this publication is nested with FM 3-0.

This manual 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. The following are brief chapter summaries and changes to ADP 3-37:

- **Chapter 1** defines and examines the role of protection and establishes protection as a warfighting function. This chapter also includes a discussion on the levels of threat and eliminates the use of protection as a continuing activity, but highlights protection as a continuous and enduring activity throughout the entire operations process.
- **Chapter 2** expands on the discussion of all 16 primary protection tasks and systems in support of the protection warfighting function. Protection tasks enable commanders to preserve the force, safeguard critical sites, and secure routes. Each task and its associated systems are associated with a staff or staff proponent that performs specific duties.

- **Chapter 3** describes how planning is the first step toward effective protection. Through planning, commanders and staffs identify what the command must accomplish, when and where it must be done and, most importantly, why it must be accomplished—the purpose for the operation. Chapter 3 describes how protection planning is a continuous process that must include an understanding of the threats and hazards that may impact operations from the deep area back to the strategic support area. It also establishes a protection prioritization list—a key protection product that is developed during initial assessments (which ranks orders protection for friendly forces first, then civilians, and then infrastructure) and continuously assessed and revised throughout each phase of an operation.
- **Chapter 4** discusses how protection during preparation activities is a continuous and enduring activity. During preparation activities, the protection focus is on deterring enemy or adversary actions that would affect combat power and on how the integration of protection tasks safeguards friendly forces, civilians, and infrastructure.
- **Chapter 5** discusses how the execution of protection is continuous and must occur throughout all operations to shape, operations to prevent, large-scale ground combat operations, and operations to consolidate gains, with a focus on deterring and preventing the enemy, adversaries, or hazards from actions that affect the force. Effective execution is aided by seizing the initiative through action and accepting prudent risk to exploit opportunities to gain positions of relative advantage. The continuous and enduring character of protection activities makes the continuity of protection actions essential during execution. Commanders implement control measures and allocate resources that are sufficient to ensure protection continuity and restoration.
- **Chapter 6** discusses the continuous assessment of protection throughout planning, preparation, operations to shape, operations to prevent, large-scale ground combat operations, and operations to consolidate gains. Continuous assessment allows commanders and staffs to evaluate the progress of achieving desired effects and to adapt protection measures, as necessary.

Based on current doctrinal changes, certain terms for which ADP 3-37 is proponent have been added, rescinded, or modified for purposes of this publication. The glossary contains acronyms and defined terms. See introductory table-1 and introductory table-2 for specific term changes.

Introductory table-1. Rescinded Army terms

Term	*Remarks*
operational area security	Rescinded.

Introductory table-2. Modified Army terms

Term	*Remarks*
critical asset security	Proponent changed from ADRP 3-37 to ADP 3-37.
fratricide	Proponent changed from ADRP 3-37 to ADP 3-37.
movement corridor	Proponent changed from FM 3-81 to ADP 3-37.

This page intentionally left blank.

Chapter 1
Protection Framework

Protection safeguards friendly forces, civilians, and infrastructure and is inherent to command. The protection warfighting function enables the commander to maintain the force's integrity and combat power through the integration of protection capabilities throughout operational preparation, operations to shape, operations to prevent, large-scale ground combat operations, and operations to consolidate gains. This chapter defines and examines the role of protection as a warfighting function, establishes guidance for the integration of protection capabilities into operations, and identifies the tasks of protection.

PROTECTION WARFIGHTING FUNCTION

1-1. The *protection warfighting function* is the related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission (ADP 3-0). Preserving the force includes protecting personnel (combatants and noncombatants) and physical assets of the United States, unified action partners, and host nations. Protection is not a linear activity—planning, preparing, executing, and assessing protection is a continuous and enduring activity. Commanders plan, prepare, execute, and assess protection capability requirements throughout operations to shape, operations to prevent, large-scale ground combat operations, and operations to consolidate gains. Protection efforts must consider and account for threats and hazards in all directions, at all times, and in all environments. The protection warfighting function enables the commander to maintain the force's integrity and combat power.

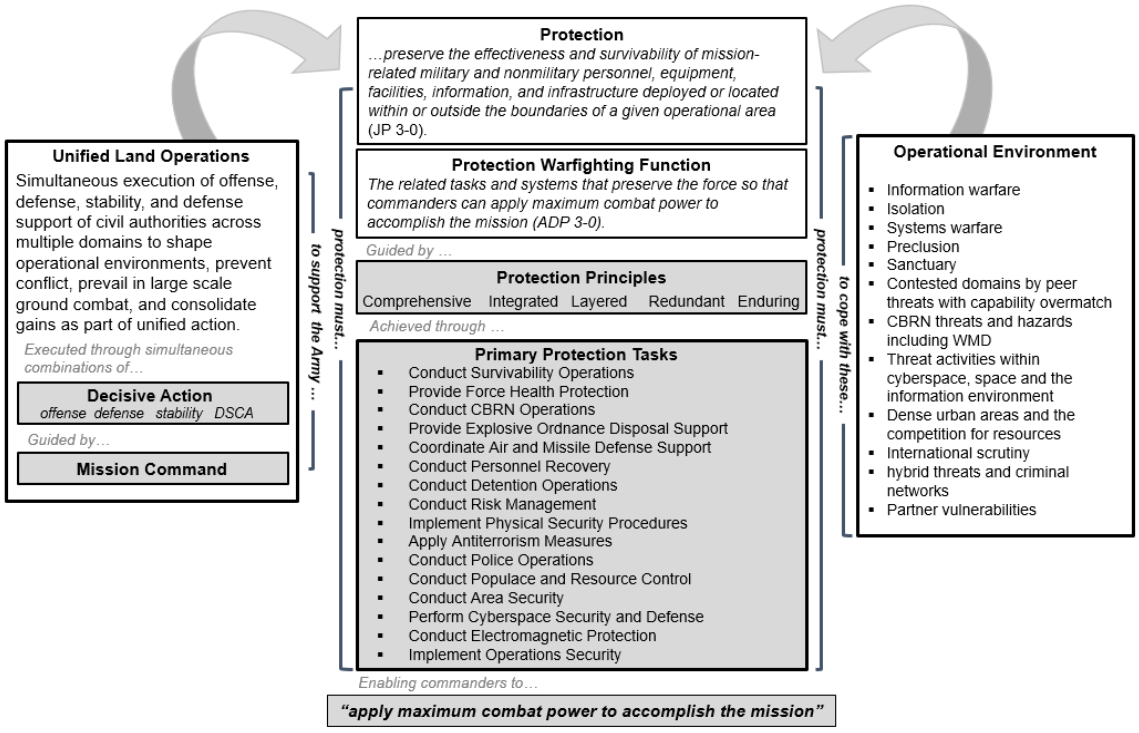
1-2. Protection is an enduring quality that differentiates it from defense and specific security operations. While a tactical force defends only until it can resume the offense and a formation provides security in a manner that maintains freedom of action, protection has a persistent character that serves one dominate purpose—the preservation of the protected asset. Commanders incorporate protection when they understand and visualize threats and hazards in the operational environment (OE), evaluate available protection capabilities, and apply the elements of combat power to deter or mitigate these threats or hazards from negatively impacting friendly operations. Prioritization of protection capabilities is situationally dependent and resource-informed (see figure 1-1, page 1-2).

1-3. The following are the eight elements of combat power:

- Leadership.
- Information.
- Command and control.
- Movement and maneuver.
- Intelligence.
- Fires.
- Sustainment.
- Protection.

1-4. Combat power includes all capabilities provided by unified action partners that are integrated and synchronized with the commander's objectives to achieve a unity of effort in sustained operations. Warfighting functions are the physical means that tactical commanders use to execute operations and accomplish missions. The purpose of warfighting functions is to provide an intellectual organization for common critical capabilities available to commanders and staffs at all echelons and levels of warfare.

Protection closely relates to endurance and momentum. It also contributes to the commander's ability to extend operations in time and space.



Legend:

ADP	Army doctrine publication	JP	joint publication
CBRN and	chemical, biological, radiological, nuclear	WMD	weapons of mass destruction
DSCA	defense support of civil authorities		

Figure 1-1. Protection logic map

1-5. A primary planning assumption for commanders and staffs is that government organizations and Department of Defense (DOD) affiliates are currently under observation by adversaries and will be under observation by threats and enemies across one or more domains within OEs. Operational and functional concepts are translated through warfighting functions into tasks for the development of plans, orders and, ultimately, unit missions. Commanders develop protection priorities for each phase of an operation or major activity. They integrate and synchronize primary protection tasks and additional protection tasks to reduce risk, mitigate identified vulnerabilities, and act on opportunity. When properly integrated and synchronized, the tasks and systems that comprise the protection warfighting function effectively preserve the force.

THE ROLE OF PROTECTION

1-6. Army forces gain, sustain, and exploit control over land to deny its use to an enemy. They do this with combined arms formations, possessing the mobility, firepower, and protection to defeat an enemy and establish control of areas, resources, and populations. Military activities and operations are inherently hazardous. Commanders and leaders conducting unified land operations must accept prudent risks every day based on the significance of the mission, the demand of the operation, and opportunity. In warfare, this reality defines the sacred trust that must exist between leaders and Soldiers regarding mission accomplishment and force protection. *Force protection* is preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include 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 must balance these competing responsibilities and make risk decisions based on experience, ethical and analytical reasoning, knowledge of the unit, and the situation.

Note. In an environment where terrorism persists, additional protection tasks must be considered in garrison and in preparatory phases to operations.

1-7. Commanders and staffs synchronize, integrate, and organize capabilities and resources to preserve combat power and identify and prevent or mitigate the effects of threats and hazards. Protection integrates all protection capabilities to safeguard the force, personnel (combatants and noncombatants), systems, and physical assets of the United States and its mission partners. In addition to the primary protection task, commanders and staffs must coordinate, synchronize, and integrate additional protection capabilities and resources of unified action partners.

1-8. The goal of protection integration is to balance protection with the freedom of action throughout the duration of military operations. This is achieved by integrating reinforcing or complementary protection capabilities to mitigate or assume risk for identified and prioritized vulnerabilities.

1-9. All military activities have some inherent or organic protection capability (survivability, antiterrorism [AT] measures, local and area security). Protection capabilities are identified as one of the following:

- **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.

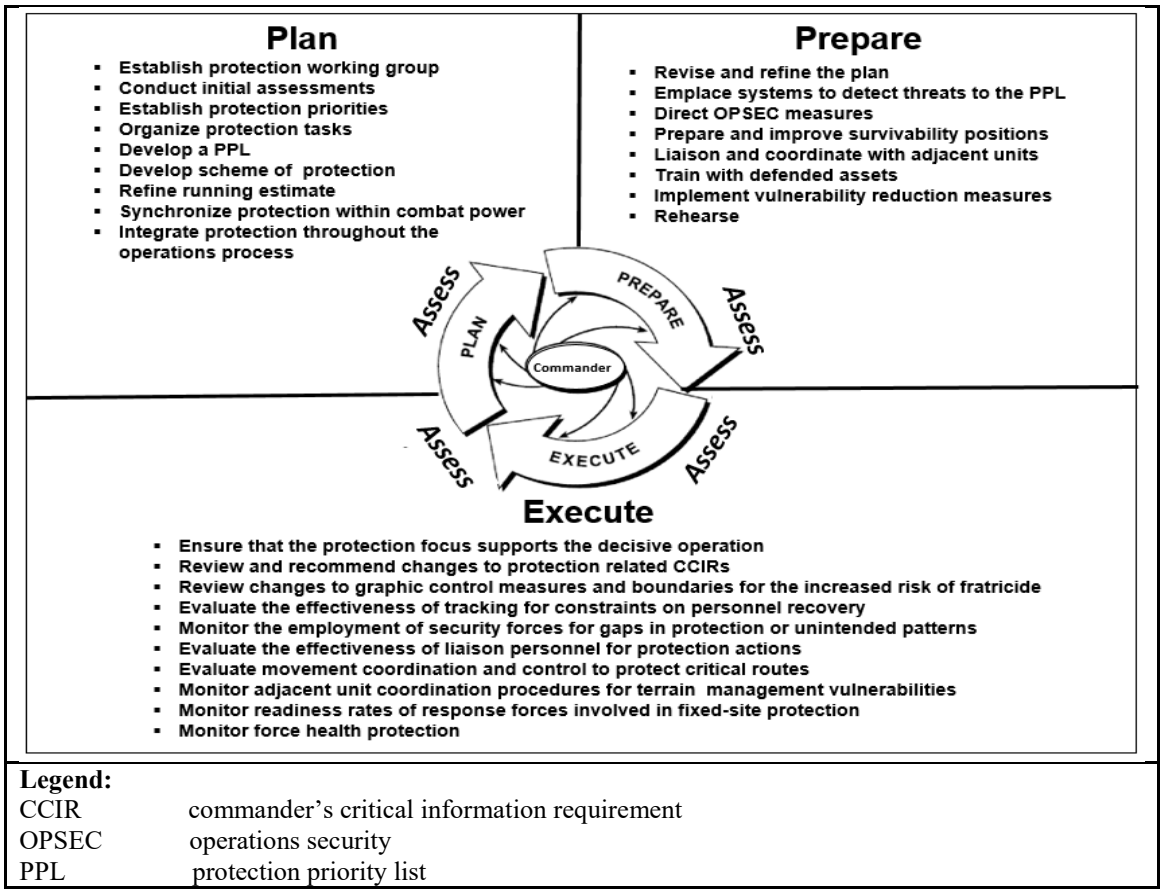
1-10. Army leaders are responsible for clearly articulating their visualization of operations in time, space, purpose, and resources. The commander's inherent responsibility to protect and preserve the force and secure the area of operations (AO) is vital in seizing, retaining, and exploiting the initiative (see figure 1-2, page 1-4). Protection must be considered continuously throughout the operations process to—

- Identify threats and hazards.
- Implement control measures to prevent or mitigate enemy or adversary actions.
- Manage capabilities to mitigate the effects and preserve time to react or maneuver against the enemy to gain superiority and retain the initiative.

PROTECTION PRINCIPLES

1-11. The five principles of protection—comprehensive, integrated, layered, redundant, and enduring—summarize the characteristics of successful protection integration and practice. These principles provide Army professionals with a context for implementing protection tasks, developing schemes of protection, and allocating resources:

- **Comprehensive.** Protection is an all-inclusive utilization of complementary and reinforcing protection tasks and systems available to commanders and incorporated into the plan to preserve the force.
- **Integrated.** Protection is unified with other activities, systems, efforts, and capabilities associated with the conduct land operations to shape security environments, prevent conflict, prevail in ground combat, and consolidate gains across the range of military operations. Integration must occur vertically and horizontally with unified action partners throughout the operations process.
- **Layered.** Protection capabilities are deliberately sequenced across multiple domains to eliminate, mitigate, or assume the risk of threat effects.
- **Redundant.** Protection efforts for identified critical vulnerabilities require dedicated primary and alternate protection capabilities.
- **Enduring.** Protection is a continuous activity. Commanders and leaders preserve combat power and reduce the risk of loss, damage, or injury to their formations.



Legend:

CCIR	commander's critical information requirement
OPSEC	operations security
PPL	protection priority list

Figure 1-2. Integration of protection throughout the operations process

PROTECTION IN SUPPORT OF ARMY OPERATIONS

1-12. The Army accomplishes its mission by supporting the joint force in four strategic roles: shape OEs, prevent conflict, conduct large-scale ground combat, and consolidate gains. The strategic roles clarify the enduring reasons for which the United States (U.S.) Army is organized, trained, and equipped. The Army conducts operations across multiple domains and the information environment. All Army operations are multi-domain operations, and all battles are multi-domain battles. Multi-domain operations include airborne and air assault operations, air and missile defense, fire support, aviation, cyberspace electromagnetic activities, information operations, space operations, military deception, and information collection. Large-scale ground combat operations such as these entail significant operational risk, synchronization and capabilities convergence, and high operational tempo. (See FM 3-0 for additional information on multi-domain battle and large-scale ground combat operations.) Protection is a key consideration for operating in multiple domains.

1-13. Protection emphasizes the importance of planning and expanding protection priorities, to include protecting mission partners, civilian populations, equipment, resources, infrastructure, and cultural landmarks across the range of military operations. The synchronization, integration, and organization of protection capabilities and resources to preserve combat power from the effects of threats and hazards are essential. When properly integrated and synchronized, the tasks and systems that relate to protection effectively protect the force, preserve combat power, and increase the probability of mission success. (See table 1-1 for a complete list of primary protection tasks.)

Table 1-1. Primary protection tasks

Primary Protection Task	*Tasks*
Conduct Survivability Operations (ATP 3-37.34, ATP 3-34.20, ATP 3-90.4)	• Employ camouflage, cover, and concealment • Establish fighting positions • Harden facilities • Construct protective works for explosive hazards • Clear routes and areas of explosive hazards
Provide Force Health Protection (ATP 4-02.8)	• Provide preventive medicine • Provide veterinary service • Provide combat and operational stress control • Provide preventive dentistry • Conduct area medical laboratory support
Conduct CBRN Operations (FM 3-11, ATP 3-11.32, ATP 3-11.36)	• Conduct CBRN information collection • Provide hazard awareness and understanding • Conduct CBRN defense • Respond to CBRN events
Provide EOD Support (ATP 4-32.1, ATP 4-32.3)	• Identify and collect information on explosive ordnance and hazards • Render-safe and dispose of explosive ordnance and hazards • Post blast investigations
Coordinate Air and Missile Defense Support (FM 3-01, FM 3-27)	• Plan ballistic missile defense • Conduct ballistic missile defense • Manage system configuration • Perform asset management • Provide global missile defense capabilities
Conduct Personnel Recovery (FM 3-50)	• Apply the fundamentals of Army personnel recovery • Support the Commander and Staff Organization and Operations • Coordinate Knowledge Management • Manage the Unit Personnel Recovery Program
Conduct Detention Operations (FM 3-63)	• Conduct detainee operations • Confine U.S. military prisoners • Conduct host nation corrections training and support
Conduct Risk Management (ATP 5-19)	• Identify hazards • Assess hazards • Develop controls • Implement controls • Supervise and evaluate
Implement Physical Security Procedures (ATP 3-39.32)	• Deter • Detect • Assess • Delay • Respond
Apply Antiterrorism Measures (ATP 3-37.2)	• Establish an antiterrorism program • Collect, analyze, and disseminate threat information • Assess and reduce critical vulnerabilities • Increase antiterrorism awareness • Maintain defenses • Establish civil-military partnerships • Conduct terrorist threat/incident response planning • Conduct exercises, and evaluate/assess the plan

Table 1-1. Primary protection tasks (continued)

Primary Protection Task	*Tasks*
Conduct Police Operations (ATP 3-39.10)	• Perform law enforcement • Conduct criminal investigations • Conduct traffic management and enforcement • Employ forensics capabilities • Conduct police engagement • Conduct customs operations • Support host nation police development • Conduct civil law enforcement support • Conduct border control and boundary security support
Conduct Populace and Resources Control (ATP 3-39.30, ATP 3-57.10, ATP 3-07.6)	• Support dislocated civilian operations • Support noncombatant evacuation operations • Protect and maintain critical infrastructure • Enforce resource control measures
Conduct Area Security (JP 3-10, ADP 3-90)	• Conduct area and base security operations • Conduct critical installation and facilities security • Provide protective services for selected individuals • Conduct response force operations • Secure supply routes and convoys • Conduct support area operations • Establish local security
Perform Cyberspace Security and Defense (JP 3-12, FM 3-12, FM 6-02, ATP 6-02.71)	• Perform cybersecurity activities • Conduct defensive cyberspace operations-internal defensive measures
Conduct Electromagnetic Protection (JP 6-01, FM 3-12, ATP 6-02.70)	• Conduct electronic protection actions • Conduct defensive electronic attack • Conduct electromagnetic spectrum management
Implement Operations Security (JP 3-13.3, ATP 3-13.3)	• Conduct operations security • Analyze threat • Implement measures and counter measures
Legend: ATP Army techniques publication CBRN chemical, biological, radiological, and nuclear FM field manual JP joint publication	

1-14. Protection is achieved through commanders and their units by changing tempo, taking evasive action, or maneuvering to gain positional advantage in relation to a threat. Formations often derive protection by exploiting terrain and weather conditions, or by using the cover of darkness to mask movement. The use of key physical terrain features supports protection measures and complements the positioning of forces during planning. The ability to protect and preserve the force and secure the AO is vital in seizing, retaining, and exploiting the initiative to shape the OE, prevent conflict, consolidate gains, and win wars as a part of unified action.

OPERATIONS TO SHAPE

1-15. Army operations to shape bring together all of the activities intended to promote regional stability and to set conditions for a favorable outcome of a military confrontation. Army operations to shape help dissuade adversary activities designed to achieve regional goals. Shaping activities include security cooperation and forward presence to promote U.S. interests, develop allied and friendly military capabilities for self-defense and multinational operations, and provide U.S. forces with peacetime and contingency access to a host nation.

Regionally aligned and engaged Army forces are essential to achieving objectives to strengthen the global network of multinational partners and prevent conflict.

1-16. Operations to shape 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, protection tasks maintain safe and secure environments that 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 unified land operations.

1-17. The Army Protection Program complements, reinforces, and overlaps the protection warfighting function during operations to shape. The Army Protection 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 management program for synchronizing, integrating, coordinating, and prioritizing policies, decisions, and resources of the 12 nonwarfighting Army protection program functional elements and the three enabling functions (see figure 1-3). The Army Protection Program unifies the protection effort to support the execution of Army missions and DOD mission essential functions in an all threats and hazards environment by integrating, coordinating, synchronizing, and effectively prioritizing the efforts and resources of the Army Protection Program functional elements and enabling functions. See AR 525-2 for additional information on the Army Protection Program.

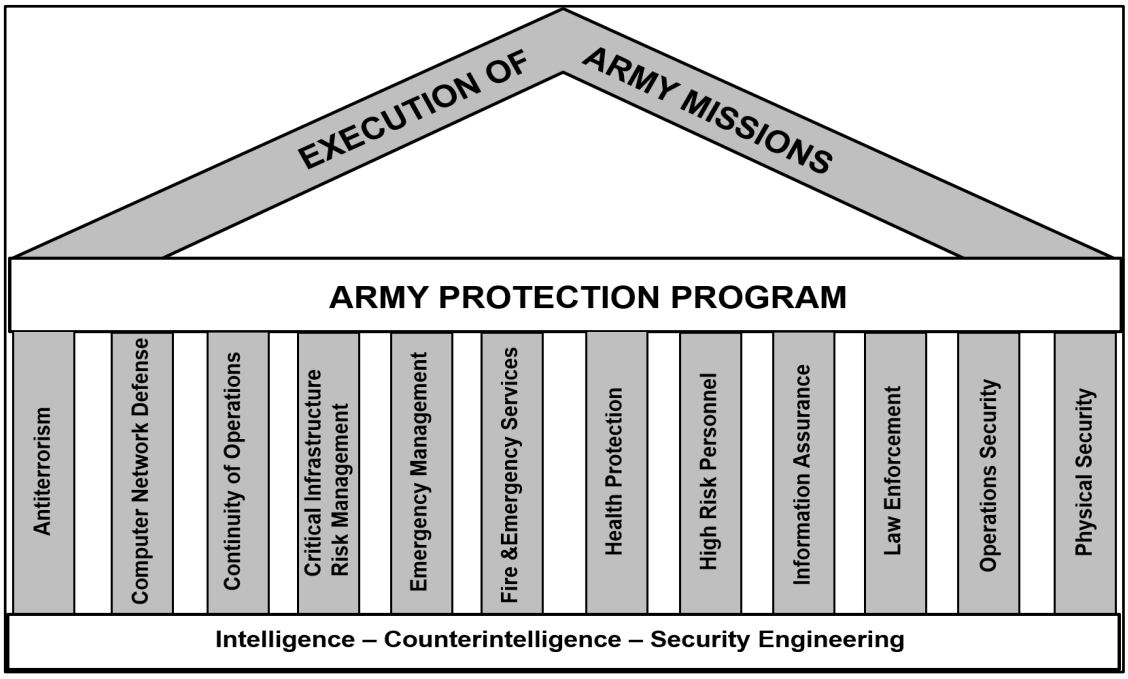


Figure 1-3. Army Protection Program's functional elements and enabling functions

OPERATIONS TO PREVENT

1-18. Army operations to prevent include all activities to deter an adversary's undesirable actions. These operations are an extension of operations to shape. They are designed to prevent opportunities for the adversary to further exploit positions of relative advantage by raising the potential costs of continuing activities. Prevent activities are generally focused toward actions to protect friendly forces, assets, and partners and to indicate U.S. intent to execute subsequent phases of a planned operation.

1-19. Army protection capabilities support operations to prevent 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.

CONDUCT LARGE-SCALE GROUND COMBAT OPERATIONS

1-20. *Large-scale ground combat operations* is sustained combat operations involving multiple corps and divisions (ADP 3-0). Army forces focus on the defeat and destruction of enemy ground forces as part of the joint team during large-scale ground combat operations. Army leaders must anticipate that joint support will be limited in large-scale ground combat operations and must use a combination of measures to protect the force. Army forces close with and destroy enemy forces in any terrain, exploiting success and breaking their opponent's will to resist. Army forces conduct offense, defense, and stability operations and consolidate gains to attain national objectives. Divisions and corps are the formations that are central to the conduct of large-scale ground combat operations. They are organized, trained, and equipped to enable subordinate organizations. The ability to prevail in the land domain is a decisive factor in breaking an enemy's will to continue a conflict. Conflict resolution requires the Army to conduct sustained operations with unified action partners as long as necessary to achieve national objectives. Conducting large-scale ground combat operations corresponds to seize the initiative and dominate phases of a joint operations.

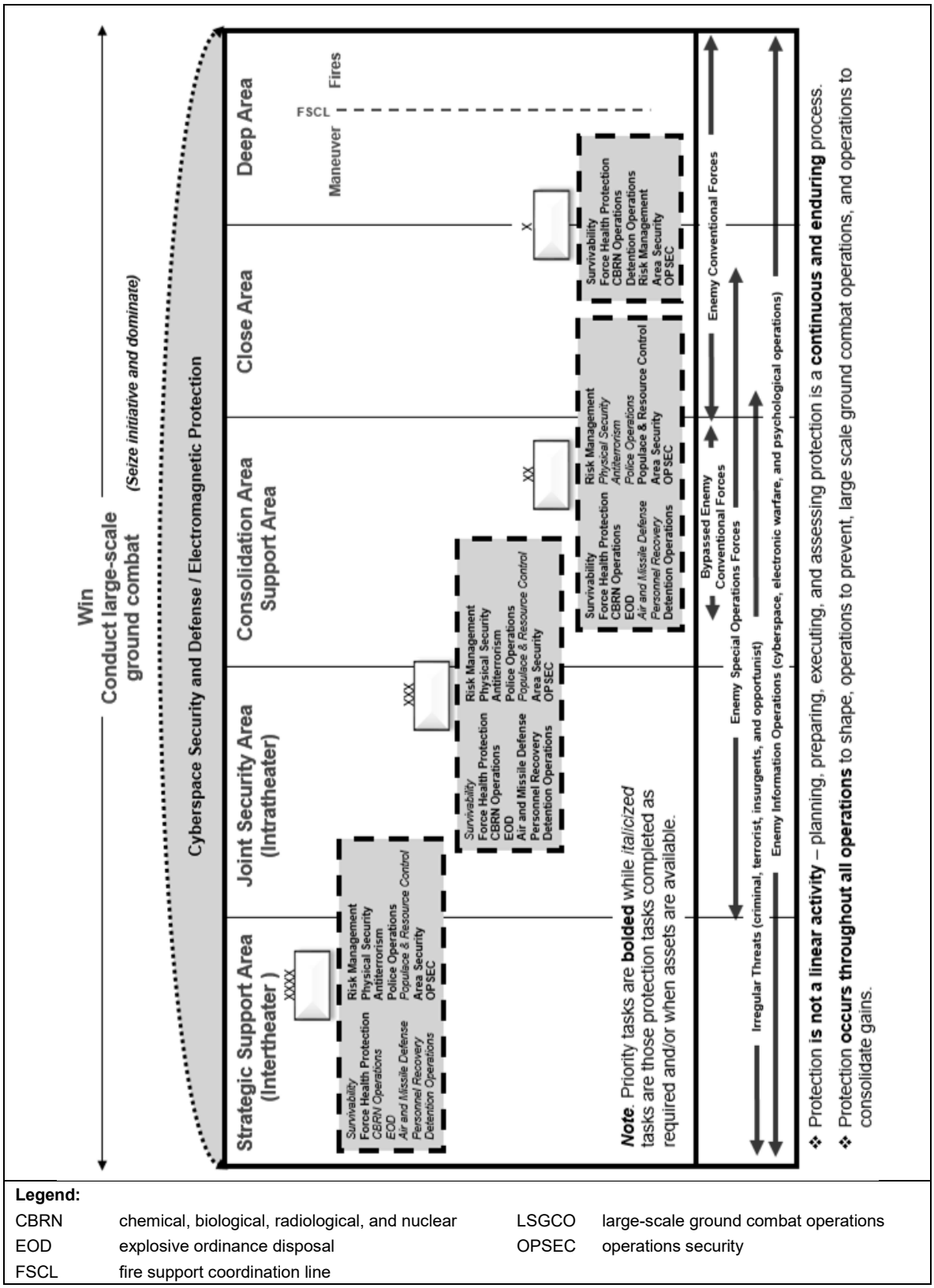
1-21. During large-scale ground combat operations, commanders and staffs deliberately plan and integrate protection capabilities to protect the force, preserve combat power, reduce risk, mitigate identified vulnerabilities, and act on opportunity. Commanders also develop a scheme of protection for the 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 the transition and follow-on operations.

1-22. Protection support within a theater of operations during large-scale ground combat operations is executed throughout the operational framework from the deep area through the strategic support area. During execution phase, the protection priorities are not the same at every echelon or in every area of operations. While some multidomain protection considerations such as cyberspace and electromagnetic protection are executed at a strategic level throughout the breadth and depth of the area of operations or area of influence, protection priorities diverge based on time and proximity to different threats. Changes to protection prioritization should be anticipated and assets reassessed as transitions occur throughout operations or changes to the commander's priorities (see figure 1-4).

CONSOLIDATE GAINS

1-23. Army operations to consolidate gains include activities to make temporary operational success enduring and to set the conditions for a stable environment, allowing for a transition of control to legitimate civil authorities. Consolidation of gains is an integral and continuous part of armed conflict, and it is necessary for achieving success across the range of military operations. Army forces deliberately plan to consolidate gains during all phases of an operation. Early and effective consolidation activities are a form of exploitation conducted while other operations are ongoing, and they enable the achievement of lasting favorable outcomes in the shortest time span. Army forces conduct these activities with unified action partners. In some instances, Army forces are in charge of integrating forces and synchronizing activities to consolidate gains. In other situations, Army forces are in support of activities to consolidate gains. Army forces may conduct stability tasks for a sustained period of time over large land areas.

1-24. While Army forces consolidate gains throughout an operation, consolidating gains becomes the focus of Army forces after large-scale ground combat operations have concluded. Army operations to consolidate gains correspond with, stabilize, and enable the civil authority phases of a joint operation. Commanders continuously consider the synchronization, integration, and organization of protection capabilities necessary to consolidate gains and achieve the desired end state. Consolidate gains activities include displaced civilian relocations, detainee operations, law and order reestablishment, humanitarian assistance, and critical infrastructure protection and restoration.



Legend:

CBRN	chemical, biological, radiological, and nuclear	LSGCO	large-scale ground combat operations
EOD	explosive ordinance disposal	OPSEC	operations security
FSCL	fire support coordination line		

Figure 1-4. Protection support within a theater of operations during large-scale ground combat operations

OPERATIONAL ENVIRONMENT

1-25. The nature and outcome of military operations are shaped by complex and dynamic environmental factors. Peer threats can contest positions of relative advantage across all domains. The *operational environment* is defined as a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An OE includes physical areas (air, land, maritime, and space domains) and the information environment (including cyberspace). Modern information technology makes the information environment, which includes cyberspace and the electromagnetic spectrum, indispensable to military operations. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13).

1-26. An OE for any specific operation does not consist of just isolated conditions of interacting variables that exist within a specific AO; it also involves interconnected influences from the global or regional perspective (for example, politics and economics) that impact conditions and operations. To be successful in the conduct of military operations, commanders must thoroughly understand and appreciate the changing nature of an OE.

1-27. Emerging OEs are uncertain. They can be marked by rapid change and a wide range of threats and hazards that significantly challenge military forces. The insider threat poses a significant risk to protection. Commanders must be aware of personnel within their own force who have authorized access to DOD facilities, systems, equipment, information, or infrastructure and who may want to maliciously cause damage, disrupt operations, commit espionage, or support a criminal or terrorist organization. Protection preserves the combat power potential and survivability of the force by providing capabilities to identify and prevent threats and hazards or mitigate their effects.

1-28. Commanders and leaders charged with providing or ensuring protection must begin with a thorough understanding of the OE, the risks and opportunities resident there, and the ways and means available for preserving combat power through protection. Army doctrine recognizes the eight operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) for analyzing and understanding any OE. To support military plans, missions, and orders, relevant information from these operational variables can be filtered into the categories of the six Army mission variables of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). Using the METT-TC factors, leaders examine the environment as it relates to their mission and begin the process of identifying threats and hazards. Joint and Army doctrine recognizes the need to understand sociocultural factors, which are key to understanding populations proximate to friendly forces. It can be easy to focus on known enemy capabilities or adversaries and heavily concentrate analytical efforts in that direction. However, applying due diligence in operational variable and sociocultural analyses can help identify potential threats from previously unknown hostile groups, neutral groups, and isolated groups within a larger, friendly population. These analyses provide an understanding of the OE that helps to identify current, developing, and potential hazards and threats and enable the protection tasks to be taken to mitigate or eliminate them. (See ATP 2-01.3, ATP 3-05.20, and JP 2-01.3 for additional information.)

THREATS AND HAZARDS

1-29. The protection warfighting function preserves the combat power potential 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. Commanders and staffs analyze the following potential threats and hazards:

- **Hostile actions.** Threats from hostile actions include any capability that forces or criminal elements have to inflict damage on personnel, physical assets, or information. These threats may include improvised explosive devices; suicide bombings; network attacks; mortars; asset theft; air attacks; cyber network and electronic attack; or chemical, biological, radiological, and nuclear (CBRN) weapons.
- **Nonhostile activities.** Nonhostile activities include hazards associated with Soldier duties within their occupational specialty, Soldier activity while off duty, and unintentional actions that cause

harm. Examples include on- and off-duty accidents, operations security violations, network compromises, equipment malfunctions, or accidental CBRN incidents.

- **Environmental conditions.** Environmental hazards associated with the surrounding environment could degrade readiness or mission accomplishment. Common examples include weather, natural disasters, 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. This proves especially advantageous as global and regional weather forecasting models continue their evolution to ever-increasing levels of spatial resolution (for example, to support operations within dense urban environments). The staff also considers how military operations may affect noncombatants in the AO. Such considerations prevent unnecessary collateral damage and take into account how civilians may affect the mission. Heavy civilian vehicle or pedestrian traffic adversely affects convoys and other operations.

1-30. Commanders use the METT-TC mission variables to describe the OE, including threats that may impact protection. In most cases, they can draw the relevant information from an ongoing analysis of the OE by using the PMESII-PT operational variables.

Threats

1-31. 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 AO can qualify as a threat, an enemy, an adversary, a neutral, or a friendly:

- A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). Threats may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, nation-states, or national alliances. When threats execute their capability to do harm to the United States, they become enemies.
- 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 *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).
- 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 during combat and combat support operations is an identity applied to a track whose characteristics, behavior, origin, or nationality indicate that it is neither supporting nor opposing friendly forces.
- A *friendly* is a contact positively identified as a friend using identification, friend or foe and other techniques (JP 3-01).

1-32. The term hybrid threat has evolved to capture the increased complexity of operations, the multiplicity of actors involved, and the blurring between traditional elements of conflict. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting threat effects (ADP 3-0). Hybrid threats combine regular forces (governed by international law and military traditions and customs) with unregulated forces that act with no restrictions on violence or their targets. These may involve nation-state actors who employ protracted forms of warfare (possibly using proxy forces to coerce and intimidate) or nonstate actors using operational concepts and high-

end capabilities traditionally associated with states. Such varied forces and capabilities enable hybrid threats to capitalize on perceived vulnerabilities, making them particularly effective.

Hazards

1-33. 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, while synchronizing those efforts in space and time. However, hazards can be enabled by the tempo or friction or by the complacency that sometimes develops during extended military operations.

LEVELS OF THREAT

1-34. There are three levels of threat. 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 and prevent or mitigate the effects of threats and hazards. Table 1-2, page 1-12, provides examples of each of these levels of threat. Each level or any combination of levels may exist throughout the OE. (See JP 3-10 for additional information on the levels of threat.)

Table 1-2. Levels of threat

Threat Level	*Examples*
Level I	Squad size unit of enemy forces, agents, saboteurs, sympathizers, terrorists, civil disturbances, criminals
Level II	Small tactical units, enemy special operations teams, long-range reconnaissance units, mounted or dismounted combat reconnaissance teams, and partially attrite small combat units; irregular forces may include significant stand-off weapons threats
Level III	Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations

1-35. 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 base camp security forces and have a negligible impact on the mission, or a Level I threat may have a catastrophic impact. An example of this is the attack on the USS Cole by two suicide bombers. According to the chart, it was a Level I threat; however, the attack was catastrophic, killing 17 U.S. Servicemen and rendering the ship inoperable. 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.** Typical 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 conducting irregular warfare 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.
- **Level III threats.** Level III threats may be encountered when a threat force has the capability of projecting combat power by air, land, or sea or anywhere into the AO. 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 base and base cluster security forces and can only be effectively defeated by a tactical combat force or other significant forces.

Chapter 2
Protection Tasks

Army operations and missions are executed through tactical tasks. Commanders incorporate protection tasks when they understand and visualize available protection capabilities. Protection tasks enable commanders to maintain their force's integrity and combat power by preserving the force, safeguarding critical assets and information, and securing routes. This chapter examines the primary protection warfighting function tasks that commanders and staffs must synchronize, integrate, and organize throughout the operations process.

PRIMARY PROTECTION WARFIGHTING FUNCTION TASKS

2-1. Military operations are inherently complex. Commanders incorporate protection when they understand and visualize threats and hazards in the OE. Protection determines the degree to which potential threats can disrupt operations in order to counter or mitigate those threats before they can act. Protection is not a linear activity─planning, preparing, executing, and assessing protection is a continuous and enduring activity. Commanders synchronize and integrate all protection capabilities throughout the entire operation to safeguard bases, secure routes, and protect forces. Prioritization of protection capabilities are situationally dependent and resource-informed.

2-2. Commanders must deliberately plan and integrate the ethical application of military force against an enemy while protecting the force and preserving combat power. Commanders develop protection strategies for each phase of an operation or major activity. They integrate and synchronize protection tasks and systems to reduce risk, mitigate identified vulnerabilities, and act on opportunity. When properly integrated and synchronized, the tasks and systems that comprise the protection warfighting function increase the probability of mission success. Units must consider all protection tasks and systems and apply them as appropriate. Each task and its associated system are typically associated with a staff or staff proponent that performs specific duties.

CONDUCT SURVIVABILITY OPERATIONS

2-3. *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 can be enhanced through various means and methods. These qualities are especially important where elements that are targeted by threats and other protection capabilities are in limited supply. Survivability and survivability operations are not interchangeable. Survivability refers to a quality or capability, while survivability operations are a specific group of tasks that enhance survivability.

2-4. Units conduct survivability within the limits of their capabilities. When existing terrain features offer insufficient cover and concealment, altering the physical environment to provide or improve cover and concealment enhances survivability. Similarly, using natural or artificial materials such as camouflage may confuse or mislead the enemy or adversary. Together, these are called survivability operations—those protection activities that alter the physical environment by providing or improving camouflage, cover, and concealment. (See ATP 3-37.34 for additional information on survivability.) While such activities often have the added benefit of providing shelter from the elements, survivability focuses on providing camouflage, cover, and concealment. Movement, such as rapid dispersal, is used with cover and concealment to enhance protection.

2-5. Survivability operations enhance the ability to avoid or withstand hostile actions by altering the physical environment. They accomplish this by providing or improving camouflage, cover, and concealment via the following four tasks:

- Employing camouflage, cover, concealment, and movement.
- Constructing fighting positions.
- Hardening facilities.
- Constructing protective positions.

2-6. Constructing survivability positions against threats from indirect and direct fire may also require actions to protect forces and equipment from other explosive hazards. Enemy forces employ moving or mobile improvised explosive devices (vehicle borne, personnel-borne, airborne, and waterborne) against stationary targets in a unit's area of operation. Units harden structures against the effects of mobile improvised explosive devices by creating standoff distance between a vehicle-borne improvised explosive device attack against a high occupancy structure such as a living area or headquarters. A condition also exists where there is captured enemy ammunition and bulk explosives located in the area of operations and under friendly force control. They are not impeding movement or maneuver, but may require protective barriers constructed around them or they require manpower to assist in proper disposal using demolitions. These actions to construct barriers, walls, shields, or berms enhance a unit's protection. See ATP 3-34.20 for more information on countering explosive hazards.

PROVIDE FORCE HEALTH PROTECTION

2-7. Force health protection is defined as the measures to promote, improve, or conserve the behavioral and physical well-being of Soldiers. Its mission is under the protection warfighting function. Force health protection measures enable a healthy and fit force, prevent injury and illness, and protect the force from health hazards. (See FM 4-02 for additional information.) It includes the prevention aspects of the following Army Medical Department functions:

- Preventive medicine (medical surveillance, occupational and environmental health surveillance).
- Veterinary services (food inspection, animal care missions, prevention of zoonotic disease transmissible to Soldiers).
- Combat and operational stress control.
- Dental services (preventive dentistry).
- Laboratory services (area medical laboratory support).

2-8. Major force health protection measures include—

- Preventing and controlling diseases.
- Assessing occupational and environmental health.
- Determining force health protection activities.
- Employing preventive medicine toxicology and laboratory services.
- Performing health risk assessments.
- Disseminating health information.

2-9. The Army Medical Department is transforming its focus from a health care system to a system of health that emphasizes wellness and health preservation. More specifically, it is designed to promote a healthy lifestyle that prevents casualties from preventable illness and injury through physical fitness, medical treatment, and health improvement. This initiative, directed by the Army Surgeon General, is known as the Performance Triad Program. Its major components consist of—

- Sleep.
- Activity.
- Nutrition.

2-10. Methods to prevent disease are best applied synergistically. Effective field hygiene and sanitation practices, waste management, and pest and vector control are crucial to disease prevention. The regional spraying and application of insect repellent is an example of a good prevention method. 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.

2-11. The key to preventive and protective care is information—which provides the capacity to assess the current health environment and properly deliver information to the affected human population. 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.

CONDUCT CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR OPERATIONS

2-12. The c*hemical, 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). It consists of conditions that resulted from immediate or persistent effects of CBRN attacks or unintentional releases. CBRN operations include the employment of tactical capabilities that anticipate and counter the entire range of CBRN threats and hazards.

2-13. The prevention of the catastrophic consequences of CBRN threats and hazards on personnel and the environment by prevention of the acquisition of weapons of mass destruction (WMD) is perhaps the most effective means of protection. CBRN defense measures include the protection of personnel, equipment, and facilities from CBRN hazards through protective equipment, exposure guidance, and alarm conditions. Contamination mitigation is the planning and actions taken to prepare for, respond to, and recover from contamination. When requested, CBRN protection extends into defense support of civil authorities.

2-14. CBRN protection measures are taken to keep CBRN threats and hazards from having an adverse effect on military and nonmilitary personnel, equipment, and facilities. CBRN threats and hazards include WMD, improvised weapons and devices, and toxic industrial material. All of these can potentially cause mass casualties and large-scale destruction. Many state and nonstate actors (including terrorists and criminals) possess or have the capability to possess, develop, or proliferate WMD. The most likely adversaries during large-scale ground combat have significant WMD capabilities and the doctrine to employ them during conventional operations. The training to conduct operations in a WMD environment is critical to operational success.

2-15. The activities to implement protection include the following:

- Understand the environment. 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 when they appear, and respond appropriately to protect the force.
- Conduct CBRN information collection through reconnaissance and surveillance. Collecting CBRN information before an event enables an accurate and timely understanding of the CBRN environment. Reconnaissance and surveillance elements provide capabilities to locate, detect, identify, quantify, sample, survey, observe, monitor, report, and mark contaminated areas.
- Conduct CBRN defense. CBRN defense employs the assessment of the risk and identification of mitigation effects that encompass tactical tasks to counter the entire range of CBRN threats and hazards before and during a CBRN event. These measures minimize or negate the vulnerability to and the effects of CBRN incidents. Protection is a principle of CBRN passive defense, which focuses on maintaining the force ability to continue military operations in a CBRN environment. (See FM 3-11 for additional information.) The ability of the force to survive and continue operations in a CBRN environment hinges on its ability to effectively employ CBRN protection measures.

- Cooperate with and support partners. Through cooperation, partners assist during the execution of CBRN operations. Close cooperation with partners includes sharing vital information about detection and methods of employment. It is also vital in coordinated strategic communications.
- Establish CBRN response efforts to minimize the effects of a CBRN incident. This includes having the plans, policies, procedures, training, and equipment necessary to effectively respond to CBRN incidents. (See JP 3-41 for additional information.)

PROVIDE EXPLOSIVE ORDNANCE DISPOSAL SUPPORT

2-16. Explosive ordnance disposal (EOD) is a key asset in the protection of military and civilian personnel, critical assets, infrastructure, and public safety. EOD personnel provide support across the range of military operations by detecting, locating, identifying, diagnosing, rendering safe, exploiting, and disposing of all explosive ordnance, improvised explosive devices, and WMD. (See ATP 4-32.1 and ATP 4-32.3 for additional information.)

2-17. Explosive ordnance are ever-present dangers in most AOs. They limit mobility, deny the use of critical assets, and cause friendly force and civilian casualties. Munitions that disperse submunitions across a wide area have led to increased amounts of unexploded ordnance on the battlefield. EOD forces are specifically trained in render-safe procedures and the disposal of explosive ordnance. 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 or other disposal procedures. EOD elements—

- Identify and collect information on explosive ordnance.
  - Perform an assessment of found munitions, including single munitions discovered or captured during military operations (patrols, raids, maneuvers) and those obtained through buyback or amnesty programs.
  - Assist commanders with AT, including intelligence support, electronic-warfare defense plans, bomb threat and search procedures, facility site surveys, and the development and implementation of EOD emergency response and AT plans.
  - Collect information on explosive ordnance, including first-seen items of interest.
- Render-safe and dispose of explosive ordnance.
  - Assist commanders with the implementation of protective works and consequence management.
  - Provide technical advice and assistance to combat engineers during route, area, and minefield clearance operations.
  - Provide support responses to nuclear and chemical accidents and incidents, including technical advice and procedures to mitigate hazards.
  - Provide EOD forces in support of humanitarian assistance efforts that involve explosive ordnance.
- Support exploitation.
  - Provide capabilities to support counter-improvised explosive device exploitation.
  - Conduct site exploitation of captured material.
  - Support captured enemy ammunition supply points (exploitation and disposal of enemy ordnance).

COORDINATE AIR AND MISSILE DEFENSE SUPPORT

2-18. Air and missile defense constitutes the defensive counterair portion of the joint counterair framework. It includes 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. Air threats include manned fixed- and rotary-wing aircraft, unmanned aircraft systems, cruise missiles, tactical air-to-surface missiles, and, in Army air and missile defense doctrine, rockets, artillery, and mortars. Ballistic missiles encompass close-range (ranges up to 300 kilometers) through intercontinental variants (ranges greater than 5,500 kilometers). Active air and missile defense is the direct measures taken to defeat the aerial threats. Active measures include the

use of surface-to-air missiles and guns, supported by sensors and command and control elements, to engage aerial threats inside and outside the atmosphere. Passive air and missile defense measures are all others (other than active measures) taken to minimize the effectiveness of aerial threats. Passive measures include detection, warning, camouflage, concealment, deception, dispersion, hardening, and the use of protective construction. For more information on air and missile defense, see FM 3-01 and JP 3-01.

2-19. 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 operations in theater. Air defense artillery officers at echelons ranging from theater to brigade levels synchronize their actions with other service air and missile defense elements and with supported land-based forces. In joint operations, air defense artillery forces are linked to the engagement authority designated by the joint force commander for active defense. Air defense artillery officers coordinate defense designs and levels of protection of the joint force commander's critical assets with that authority, normally the area air defense commander. In support of Army operations, commanders of allocated air defense artillery units establish support relationships with designated Army maneuver formations and keep those formations informed of their actions and activities through the protection cell.

2-20. The protection cell planners coordinate air and missile defense support for their respective echelon with the air and missile defense section. The protection cell identifies the most critical assets within the formation requiring defense against aerial threats, and works with the air and missile defense section to develop the echelon's protected asset list. This list is briefed to the echelon commander to ensure that the identified assets are defended to the degree the commander desires. If additional air defense artillery units are deemed necessary to achieve the desired protection, the protection cell will work with the air and missile defense section to request them. If additional units are not available, the protection cell will inform the commander and, according to the commander's direction, adjust the priority of the assets or the levels of protection. Any modifications to the list or levels of protection are recoordinated with the air and missile defense section for implementation. Continuous coordination is conducted to refine the list of critical assets and those to be defended throughout operations, ensuring the protection of critical assets and forces from air and missile attack and surveillance. 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 status of units and engagements), and the overall air and missile defense picture.

CONDUCT PERSONNEL RECOVERY

2-21. *Army personnel recovery* refers to the military efforts taken to prepare for and execute the recovery and reintegration of isolated personnel (FM 3-50). Personnel recovery is the overarching term for operations that focus on recovering isolated personnel before detention or capture by the enemy. These personnel consist of U.S. forces, Department of the Army (DA) Civilians, or other personnel (as designated by the President or the Secretary of Defense) who are in an OE beyond the Army's positive or procedural control, requiring them to survive, evade, resist, or escape. Every unit must have procedures in place to recover personnel.

2-22. The commander and staff use the operational variables (PMESII-PT) and the mission variables (METT-TC) to assess the OE to refine their understanding of the situation and its relationship to personnel recovery. Threats to isolated personnel vary based on the OE and include peacetime captivity, hostage and prisoner of war. Threats to isolated personnel vary based on the OE. During large-scale ground combat, the scale and scope of operations will likely create situations during which personnel recovery must address isolated units as big as companies, battalions, or even brigades.

2-23. Commanders must integrate personnel recovery throughout operations. This requires an understanding of the complex, dynamic relationships between friendly forces and enemies and of the other aspects of the OE (including the populace). This understanding helps commanders visualize and describe their intent for personnel recovery and assists them in developing focused planning guidance. Personnel recovery guidance is contained in various parts of the order, including the base order, appropriate annexes, appendixes, tabs, and exhibits. Commanders translate the personnel recovery guidance into recommendations known as isolated Soldier guidance. The commander gives guidance for developing isolated Soldier guidance during initial planning. Effective isolated Soldier guidance addresses the challenges of isolation within the unit AO and mission.

2-24. Isolated Soldier guidance provides a framework for how the unit and subordinates synchronize the actions of the commander and staff, isolated personnel, and recovery force. Personnel recovery guidance provides a framework for how the unit and subordinates synchronize the actions of isolated personnel and the recovery force. Isolated Soldier guidance applies to the entire command because the uncertainty and complexity of military operations expose everyone to the risk of isolation. Isolated Soldier guidance provides proactive measures to enable the rapid recovery of isolated personnel. (See FM 3-50 for additional information on personnel recovery.)

CONDUCT DETENTION OPERATIONS

2-25. Detention involves the detainment of a population or group that poses some level of threat to military operations. Detention operations are conducted by military police to shelter, sustain, guard, protect, and account for populations (detainees or U.S. military prisoners [U.S. military personnel ordered to confinement]) as a result of military or civil conflict or to facilitate criminal prosecution. Detention operations are essential to setting the conditions for the consolidation of gains during large-scale ground combat.

2-26. Detention operations inherently control the movement and activities of a specific population for imperative reasons of security and safety. The Army is the DOD executive agent for detainee operations and for the long-term confinement of U.S. military prisoners.

2-27. 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 (including privileged belligerents [enemy prisoners of war], unprivileged belligerents, retained personnel, and civilian internees). (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.)

CONDUCT RISK MANAGEMENT

2-28. Commanders and their staffs use intellectual tools to help understand the operational environment and visualize and describe their approach for conducting an operation. Collectively, these tools make up the elements of operational art and include risk (see ADP 3-0). Risk is the probability and severity of loss linked to hazards. Risk, uncertainty, and chance are inherent in all military operations. *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 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. Commanders must understand, visualize, and describe their protection priorities clearly within their intent and guidance to ensure that proper integration and synchronization of protection assets are considered throughout the entire operation.

2-29. The Army uses risk management to help maintain combat power while ensuring mission accomplishment during current and future operations. It is the Army process for helping organizations and individuals make informed decisions to reduce or offset risk. Risk management applies to operations and to nonoperational activities. Using this process increases operational effectiveness and the probability of mission accomplishment. The process applies to all types of operations, tasks, and activities and is incorporated by all staff elements through their running estimates. Staffs also provide recommendations for controls to mitigate risk within their areas of expertise during the entire operations process. The commander has overall responsibility for risk management and is the risk acceptance authority.

2-30. ***Fratricide* is the unintentional killing or wounding of friendly or neutral personnel by friendly firepower.** Due to the destructive power and range of modern weapons, coupled with the high intensity and rapid tempo of combat, the increased risk or potential for fratricide exists. Tactical maneuvers, terrain, and weather conditions may also increase the danger of fratricide. Commanders, leaders, and Soldiers must know the range and blast characteristics of their weapons systems and munitions to prevent ricochet, penetration, and other unintended effects. Accurate information about locations and activities of friendly and hostile

forces and an aggressive airspace management plan help commanders avoid fratricide and enable commanders to preserve the force.

2-31. The five steps of the risk management process follows a logical sequence that correlates with the operations process (see table 2-1). Steps 1 and 2 of risk management normally have the greater emphasis in the planning activity. Step 3 normally begins in planning and continues through the preparing activity. The majority of step 4 normally occurs within the preparing and executing activities, with some continuing emphasis in planning. Step 5 normally occurs during the executing activity with some continuing emphasis in planning. The assessment activity for risk management coincides with the protection assessment process and is continuous. (See ATP 5-19 for more information on risk management.)

Table 2-1. Risk management in the operations process

Risk Management Steps	*Operations Process Activities*	
Step 1 – Identify the hazards	Planning	*Assessing*
Step 2 – Assess the hazards	Planning	
Step3 – Develop controls and make risk decisions	Planning and preparing	
Step 4 – implement controls	Planning, preparing, and executing	
Step 5 –Supervise and evaluate	Planning and executing	

IMPLEMENT PHYSICAL SECURITY PROCEDURES

2-32. Physical security consists of physical measures that are designed to safeguard personnel and to prevent unauthorized access to equipment, installations, material, and documents and safeguard them against espionage, sabotage, damage, theft, and terrorism. The Army employs physical security measures in depth to protect personnel, information, and critical resources in all locations and situations against various threats through effective security policies and procedures. This total system approach is based on the continuing analysis and employment of protective measures, including physical barriers, clear zones, lighting, access and key control, intrusion detection devices, biometrically-enabled base access systems, defensive positions, and nonlethal capabilities. (See ATP 3-39.32 for additional information on physical security.)

2-33. 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 attractiveness of the asset, and the aggressor's objective.
- **Detection.** A detection measure senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a response force.
- **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 actual or perceived intrusion by delaying or preventing an aggressor's movement toward the asset or by shielding the asset from weapons and explosives.
- **Response.** Most protective measures depend on response personnel to assess unauthorized acts, report detailed information, and defeat an aggressor.

APPLY ANTITERRORISM MEASURES

2-34. AT consists of proactive defensive measures used to deter, detect, delay, deny, and defend individuals and property against terrorist acts. These measures include limited response and containment by security forces. AT measures are required to be incorporated into all military operations. (See ATP 3-37.2 for additional information on AT.)

2-35. AT is an integral part of Army efforts to defeat terrorism. Terrorists may target Army elements at any time and in any location. AT must be integrated into all Army operations and considered at all times. AT should be an integral part of military operations, from inception and planning phases to recovery and after-action phases. Awareness must be built into every mission, every Soldier, and every leader. Integrating AT is crucial for Army success. Typical Army AT programs are composed of several adjunct and information programs, including tasks for specialized, nonprotection military occupational specialties. At a minimum, AT includes—

- Risk management (threat, critical, vulnerability, and AT risk assessments of units, installations, facilities, and base camps).
- AT planning (units, installations, facilities, and bases).
- AT awareness training and command information programs.
- AT exercises that validate defensive plans, incident response, consequence management, and continuity of essential military operations.
- AT protection measures to protect individual personnel, high-risk personnel, physical assets (physical security), designated critical assets, and information.
- AT 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.
- Force protection condition (FPCON) systems to support terrorist threat and incident response plans.
- Comprehensive AT program review.

CONDUCT POLICE OPERATIONS

2-36. Police operations encompass policing and the associated law enforcement activities to control and protect populations and resources and to facilitate the existence of a lawful and orderly environment. Police operations and the associated skills and capabilities inherent in that function provide the fundamental basis on which all other military police disciplines are framed and conducted. (See ATP 3-39.10 for additional information on police operations.)

2-37. Police operations are conducted across the range of military operations and are fundamental to the consolidation of gains in large-scale ground combat. As the operation transitions and the OE stabilizes, civil control efforts are implemented and the rule of law is established. The closer the OE moves toward stability and full implementation of host nation governance under the rule of law, the more general policing activities transition to law enforcement activities.

2-38. Military police attempt to maintain order and security when conducting police operations. They share a common, general understanding of the OE while adding a degree of focus on those aspects that are necessary to maintain order and enforce laws. The ultimate goal is to maintain order while protecting personnel and assets. Care should be taken to eliminate jurisdictional overlap and under lap. Police operations include—

- Performing law enforcement.
- Conducting criminal investigations.
- Conducting traffic management and enforcement.
- Employing forensics capabilities.
- Conducting police engagement.
- Providing customs support.
- Providing host nation police development.
- Supporting civil law enforcement.
- Supporting border control, boundary security, and the freedom of movement.
- Conducting police intelligence operations.

CONDUCT POPULACE AND RESOURCES CONTROL

2-39. The function of populace and resources control is conducted in conjunction with, and as an integral part of, all military operations. Populace and resources control functions consist of two distinct, yet linked, components: populace control and resources control. These controls are normally the responsibility of indigenous civil governments. Combatant commanders define and enforce these controls during large-scale ground combat, consolidation of gains, and times of civil or military emergency.

2-40. Military forces base the extent of populace and resources control functions on their current OE. When forces deploy in support of a host nation, the U.S. populace and resources control policy upholds and strengthens the sovereignty of the legitimate government to govern the people and resources within its borders. 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. (See ATP 3-39.30 and ATP 3-57.10 for additional information on populace and resources control.)

POPULACE CONTROL

2-41. Populace control provides security for the indigenous populace, mobilizes human 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 execution of primary stability tasks in the areas 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.

2-42. International law requires the military force to focus on essential tasks that establish a safe, secure environment and address the immediate humanitarian needs of the local population. Populace control measures include curfews, movement restrictions, travel permits, registration cards, and resettlements of civilians. 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.

RESOURCE CONTROL

2-43. Resource 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.

2-44. Resource control directly impacts the economic system of a host nation or territory governed by U.S. forces. Resource 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 resource 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.

CONDUCT AREA SECURITY

2-45. Security operations prevent surprise, reduce uncertainty, and provide early warning of enemy activities. Security is a dynamic effort that anticipates and thwarts enemy collection efforts. When successful, security operations allow the force to maintain the initiative. The synchronization and integration of area and local security tasks are essential to protecting the force. Forces engaged in area security protect the force,

installation, route, area, or asset. 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 and to support decisive and shaping operations by generating and maintaining combat power.

AREA SECURITY

2-46. *Area security* is a security task conducted to protect friendly forces, installations, routes, and actions within a specific area (ADP 3-90). Area security may be the predominant method of protecting the support areas and consolidation areas that are necessary to facilitate the positioning, employment, and protection of resources required to sustain, enable, and control forces. When designated, a consolidation area refers to an AO assigned to an organization that extends from its higher headquarters boundary to the boundary of forces in close operations. It requires a purposefully task-organized, combined-arms unit to conduct area security and stability tasks and to employ and clear fires. (See FM 3-0 for additional information on consolidation areas.)

2-47. Area security is often an effective method of providing civil security and control during the consolidation of gains. Forces engaged in area security can saturate an area or position on key terrain to provide protection through early warning, reconnaissance, or surveillance and to guard against unexpected enemy or adversary attack with an active response. This early warning, reconnaissance, or surveillance may come from ground- and space-based sensors. Area security may focus on named areas of interest in an effort to answer commander's critical information requirements, aiding in tactical decision making and confirming or denying threat intentions. Area security preserves the commander's freedom to move reserves, position fire support means, provide for command and control, conduct sustaining operations, and contribute to other consolidation of gains activities. Forces engaged in area security are typically organized in a manner that emphasizes their mobility, lethality, and communications capabilities. However, area security takes advantage of the local security measures performed by all units, regardless of their location in the AO.

2-48. All commanders apportion combat power and dedicate assets to protection tasks and systems based on an analysis of the OE, the likelihood of threat action, and the relative value of friendly resources and populations. Based on their assessments, joint force commanders may designate the Army to provide a joint security coordinator to be responsible for designated joint security areas. Although all resources have value, the mission variables of METT-TC make some resources, assets, or locations more essential to successful mission accomplishment from enemy or adversary and friendly perspectives. Commanders rely on the risk management process and other specific assessment methods 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 subject of commander guidance and the focus of area security. Area security often focuses on the following activities:

- **Tactical assembly area security.** In large-scale ground combat operations, protection is critical for forces that are arrayed in tactical assembly areas and do not possess comprehensive, organic protection capabilities or are focused on other mission objectives.
- **Base/base camp defense.** *Base defense* consists of the local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base, to ensure that the maximum capacity of its facilities is available to United States forces (JP 3-10). A division or corps may be required to protect multiple support areas, bases, or base camps. Units may be assigned base defense operations within the support area on a permanent or rotating basis, depending on the mission variables.
- Critical asset security. *Critical asset security* is the protection and security of personnel and physical assets or information that is analyzed and deemed essential to the operation and success of the mission and to resources required for protection.
- **Node protection.** Command posts and operations centers are often protected through area security techniques that involve the employment of protection and security assets in a layered, integrated, and redundant manner. This can often keep hostile threats at a distance by maximizing the standoff distance from explosive effects, while keeping the protected asset outside the range of enemy or adversary direct-fire weapons and observation.

- **High-risk personnel security.** *High-risk personnel* are personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets (JP 3-07.2). Special precautions are taken to ensure the safety and security of these individuals and their family members. When units identify a significant risk to selected personnel, the local commander normally organizes security details from internal resources. However, under certain circumstances, designated personnel may require protective service details by specially trained units. (See ATP 3-39.35 for more information on high-risk personnel security.)
- **Movement corridor. A *movement corridor* is a designated area established to protect and enable ground movement along a route.** The establishment of a movement corridor is, by necessity, a combined arms technique that could be listed as a mobility operation and a security operation because it extracts multiple supporting tasks and activities from both. It many ways, this is simply a special area security mission. Units establish a movement corridor to set the conditions to protect and enable the movement of traffic along a designated surface route. Units conduct synchronized operations (reconnaissance, security, mobility, information collection) within the movement corridor for forces that require additional command and control, protection, and support to enable their movement. A movement corridor may be established to facilitate the movement of a single element, or it may be established for a longer period of time to facilitate the movement of a number of elements along a given route. The owner of an AO may establish a movement corridor within the AO along an established main supply route or a route designated for unit movement. The movement corridor typically includes the airspace above to allow the establishing unit to conduct aerial reconnaissance and fires.
- **Response force operations.** Response force operations expediently reinforce unit organic protection capabilities or complement that protection with maneuver capabilities based on the threat. Response force operations include planning for the defeat of Level I and II threats and the shaping of Level III threats until a designated tactical combat force arrives for decisive operations. Response force operations use a quick-reaction force with appropriate fire support (usually designated by the area commander) to deal with Level II threats in the AO. (See FM 3-39 for more information on response force operations.)
- **Lines of communications 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. The security of lines of communications and supply routes (rail, pipeline, highway, and waterway) presents one of the greatest security challenges in an AO. Route security operations are defensive in nature and are terrain-oriented. A route security force may prevent an enemy or adversary force from impeding, harassing, or destroying traffic along a route or portions of a route by establishing a movement corridor (see FM 3-81). Units conduct synchronized operations (mobility and information collection) within the movement corridor. A movement corridor may be established in a high-risk area to facilitate the movement of a single element or to accommodate an enduring operation.
- **Checkpoints and combat outposts.** It is often necessary to control the freedom of movement in an AO for a specific period of time or as a long-term operation. This may be accomplished by placing checkpoints and combat outposts along designated avenues and roadways or on key terrain identified through METT-TC. Checkpoints are used for controlling, regulating, and verifying movement; combat outposts are used for sanctuary, support, information collection, or area denial. (See ATP 3-90.4 for more information on combat outposts.)
- **Convoy security.** A convoy security operation is a specialized type of area security operation conducted to protect convoys. Units conduct convoy security operations when there are insufficient friendly forces to continuously secure routes in an AO 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. Planning includes designating units for convoy security; providing guidance on tactics, techniques, and procedures (TTP) for units to provide for their own security during convoys; or establishing protection and security requirements for convoys carrying critical assets. Local or theater policy typically dictates when and which convoys receive security and protection. (See ATP 4-01.45 for more information on convoy security training requirements and TTP.)

- **Port area and pier security.** Ground forces may typically provide area security for port and pier areas. The joint force commander and subordinate joint force commanders ensure that port security plans and responsibilities are clearly delineated and assigned. Area commanders who are assigned a port area as part of their AO must develop and organize plans to ensure that forces are trained, led, and equipped to concentrate the necessary combat power at the decisive time and place to protect or secure port areas and cargo, as necessary. The patrol of harbors and anchorages is generally the mission of a dedicated port security unit and may include waterfront security operations. (See JP 3-10 for additional information on port security units.)
- **Area damage control.** Area damage control consists of measures taken before, during, or after hostile actions or natural or man-made disasters to reduce the probability of damage and minimize its effects. Commanders utilize elements of combat power to establish area damage control measures as part of decisive action tasks. Protection working groups assist the commander in considering area damage control measures in planning and operations (see JP 3-10).

LOCAL SECURITY

2-49. Area security activities take advantage of the local security measures performed by all units (regardless of their location) in an AO, and all local security activities should be linked to the broader area security activities. *Local security* is a security task that includes low-level security activities conducted near a unit to prevent surprise by the enemy (ADP 3-90). Local security provides immediate protection to friendly forces 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. Local security may include countermobility and survivability activities.

2-50. Local security includes any local measure taken by units that protect against enemy 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. Units use active and passive measures to provide local security.

2-51. Active local security measures include but are not limited to—

- Observation posts.
- Patrols.
- Unmanned aircraft systems.
- The establishment of specific levels of alert within the unit. The commander adjusts those levels based on the factors of METT-TC.
- The establishment of stand-to times. The unit standard operating procedure details the unit activities during the conduct of stand-to.

2-52. Passive local security measures include but are not limited to—

- Camouflage and concealment.
- Movement control.
- Noise and light discipline.
- Proper communications procedures.
- The employment of available ground sensors.
- The use of night vision devices and daylight sights to maintain surveillance over the area immediately around the unit.
- The incorporation of emission control to prevent the enemy from detecting, identifying, and locating friendly forces.

CONDUCT CYBERSPACE SECURITY AND DEFENSE

2-53. The Army's 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). The DODIN-A enables command and control and facilitates all warfighting and business functions. The network allows commanders to leverage information to gain understanding of the operational environment, influence behavior, support decision making, and synchronize and integrate the elements of combat power.

2-54. 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

2-55. *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 (DODI 8500.01). Cybersecurity activities take place throughout the system life cycle. Cybersecurity measures apply to general threats and known vulnerabilities as opposed to specific attacks. Through cybersecurity, DODIN 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 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

2-56. 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* are operations in which authorized 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.

CONDUCT ELECTROMAGNETIC PROTECTION

2-57. Many Army capabilities, including communications, cyberspace operations, information collection, space capabilities, target detection, and precision guided munitions depend on assured access to the electromagnetic spectrum. The tasks to protect Army access to the electromagnetic spectrum are—

- Conduct electronic protection actions.
- Conduct defensive electronic attack.
- Conduct electromagnetic spectrum management.

CONDUCT ELECTRONIC PROTECTION ACTIONS

2-58. Electronic protection includes actions taken to ensure friendly use of the electromagnetic spectrum, such as frequency agility in a radio or variable pulse repetition frequency in radar. Electronic protection protects U.S. and allied systems from the effects of friendly and enemy electronic attack and electromagnetic interference.

2-59. Electronic protection actions include—

- Electromagnetic compatibility.
- Electromagnetic hardening.
- Electronic masking.
- Emission control.
- Wartime reserve modes.

CONDUCT DEFENSIVE ELECTRONIC ATTACK

2-60. Defensive electronic attack primarily protects friendly personnel and equipment or platforms against lethal attacks by denying enemy use of the electromagnetic spectrum to guide or trigger weapons. Defensive electronic attack uses the electromagnetic spectrum to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as the use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasures, and counter radio-controlled improvised explosive device systems.

CONDUCT ELECTROMAGNETIC SPECTRUM MANAGEMENT

2-61. *Electromagnetic spectrum management* is planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures (JP 6-01). Spectrum management enables electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

IMPLEMENT OPERATIONS SECURITY

2-62. *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 operations security (OPSEC) is employed during decisive action. Units routinely employ OPSEC to protect essential elements of friendly information (EEFI). This 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. OPSEC may also be used to—

- Identify actions that can be observed by enemy or adversary intelligence systems.
- Determine indicators of hostile intelligence 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 countermeasures that eliminate or reduce vulnerability or indicators to observation and exploitation:
  - Avoid drastic changes as OPSEC 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.

2-63. OPSEC applies to all operations. 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 OPSEC measures during the military decisionmaking process (MDMP). The assistant chief of staff, intelligence, assists the OPSEC process by comparing friendly OPSEC indicators with enemy or adversary intelligence collection capabilities.

2-64. 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 supported operations are concealed. At times, unit commanders employ deception in support of OPSEC to create multiple false indicators 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 intelligence, surveillance, and reconnaissance capabilities to distract intelligence collection 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).

This page intentionally left blank.

Chapter 3

Protection Planning

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. An effective scheme of protection and risk decisions is developed based on the information that flows from mission analysis. Mission analysis provides commanders with a better understanding of the situation and problem. Commanders and staffs identify what the command must accomplish, when and where it must be 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. The keys to protection planning are: identifying threats and hazards, assessing the threats and hazards to determine the risks, developing preventive measures, and integrating protection tasks into a comprehensive scheme of protection that includes mitigating measures. The warfighting functions are synchronized throughout the operations process to assist in the development of an enduring scheme of protection.

INITIAL ASSESSMENTS

3-1. Initial protection planning requires various assessments to establish protection priorities. Assessments include threats, hazards, vulnerability, and criticality. These assessments are used to determine which assets can be protected given no constraints and which assets can be protected with available resources. There are seldom sufficient resources to simultaneously provide all assets the same level of protection. For this reason, commanders make decisions on acceptable risks and provide guidance to the staff so that they can employ protection capabilities based on the protection priorities.

3-2. Protection planning is a continuous process that must include an understanding of the threats and hazards that may impact operations from the deep area back to the strategic support area. Protection capabilities are aligned to protect critical assets and mitigate effects from threats and hazards. The protection cell and protection working group must prioritize the protection of critical assets during operations to shape, operations to prevent, large-scale ground combat, and during the consolidation of gains that best supports the commander's end state.

3-3. During shaping operations, the focus is on cooperation, prevention, and deterrence. Within planning, the protection staff 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 and training and exercises.

3-4. During operations to prevent, the main purpose is to deter adversary actions. The staff estimates the protection assets necessary for future operations and the increased threat according to the commander's priorities, forces availability, and the adversary's perceived intent. Units prioritize protection capabilities and align them to defend critical assets. It is imperative to conduct information operations to deny adversaries the ability to obtain information.

3-5. Planning prioritization considerations for large-scale ground combat operations includes efforts to conserve and increase combat power; protect nodes that are critical to force projection and sustainment; counter enemy fires and maneuver by making personnel, systems, and units difficult to locate, strike, and

destroy; gain air, space, and electromagnetic spectrum superiority; use defensive information operations; and protect airports, seaports, lines of communication networks, and base camps.

3-6. Success in consolidating gains is obtained through setting the conditions for a stable environment. Staffs should weigh the prioritization of protection capabilities required to support large-scale and stability operations with the simultaneous protection of consolidation areas. During operations to consolidate gains, prioritization considerations are focused on security tasks to stabilize the area and protect the force, bases, routes, areas, and critical infrastructure.

3-7. An important aspect of protection planning for corps and divisions involves the support and consolidation areas. If conditions in the support area degrade, it is detrimental to the success of operations. A degraded support area also 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. When the support area is located inside a division consolidation area, the unit that is assigned responsibility for the consolidation area provides significant protection for support area units.

THREAT AND HAZARD ASSESSMENT

3-8. Personnel from all staff sections and warfighting functions help conduct threat and hazard analysis. This analysis comprises a thorough, in-depth compilation and examination of information and intelligence that address potential threats and hazards in the AO. The integrating processes (intelligence preparation of the battlefield, targeting, and risk management) provide an avenue to obtain the threats and hazards that are reviewed and refined. Threat and hazard assessments are continuously reviewed and updated as the OE changes.

3-9. Considerations for the threat and hazard assessment include—

- Enemy and adversary threats.
  - Operational capabilities.
  - Intentions.
  - Activities.
- Foreign intelligence entities (see ATP 2-22.2-1).
- Criminal activities.
- Civil disturbances.
- Health and safety hazards.
- CBRN weapons and toxic industrial materials.
- Cyberspace threats.
- Other relevant aspects of the OE.
- Incident reporting and feedback points of contact.

3-10. 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. Table 3-1 shows examples of potential threats and hazards in an AO. In the context of assessing risk, the higher the probability or likelihood of a threat or hazard occurring, the higher the risk of asset loss.

Table 3-1. Potential threats and hazards

Area of Concern	*Potential Threats and Hazards*
Survivability	• Hostile actions (lethal and nonlethal capabilities) • Weather effects or environmental conditions
Force health protection	• Endemic and epidemic diseases • Environmental factors • Diseases from animal bites, poisonous plants, animals, or insects • Risks associated with the health, sanitation, or behavior of the local populace
CBRN	• CBRN weapons • Toxic industrial materials

Table 3-1. Potential threats and hazards (continued)

Area of Concern	*Potential Threats and Hazards*
EOD	• Explosive ordnance and hazards (friendly and enemy) • Adversary attacks on personnel, vehicles, or infrastructure
Air and missile defense	• Artillery • Mortars • Rockets • Ballistic and cruise missiles • Fixed- and rotary-wing aircraft • Unmanned aircraft systems
Personnel recovery	• Events that separate or isolate individuals or small groups of friendly forces from the main force • Weather effects or environmental conditions
Detention operations	• U.S. military prisoners • Detainees
Risk management	• Hazards associated with enemy or adversary activity • Accident potential • Weather or environmental conditions • Equipment
Physical security	• Adversary attacks on personnel, vehicles, or infrastructure • Insider threats • Weather or environmental conditions • Criminals
AT	• Improvised explosive devices • Suicide/mail bombs • Snipers • Standoff weapons • Active shooters • Insider threats
Police operations	• Criminals • Active shooters • Insider threats • Bombs
Populace and resources control	• Criminals • Dislocated civilians • Insider threats
Area Security	• Adversary attacks on personnel, vehicles, or infrastructure • Explosive ordnance and hazards (friendly and enemy) • Criminals • Dislocated civilians • Unmanned aircraft systems

Table 3-1. Potential threats and hazards (continued)

Area of Concern	*Potential Threats and Hazards*
Cyberspace Security and Defense	• Network attacks, exploitations, intrusions or effects of malware • Known system vulnerabilities • Insider threats
Electromagnetic Protection	• Electromagnetic energy, directed energy, and antiradiation weapons • Electromagnetic interference, jamming • Electromagnetic deception
Operations Security	• Enemy collection plans • Friendly vulnerabilities • Indicators
Legend:	
AT	antiterrorism
CBRN	chemical, biological, radiological, and nuclear
EOD	explosive ordnance disposal
U.S.	United States

CRITICALITY ASSESSMENT

3-11. A criticality assessment identifies key assets that are required to accomplish a mission. It addresses the impact of a temporary or permanent loss of key assets or the unit ability to conduct a mission. A criticality assessment should also include high-population facilities (recreational centers, theaters, sports venues) that may not be mission-essential. It examines 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 an accurate status 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.

3-12. The protection cell staff and working group continuously update criticality assessments during the operations process. As the staff develops or modifies a friendly course of action (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 OE.

VULNERABILITY ASSESSMENT

3-13. A vulnerability assessment is an evaluation (assessment) to determine the magnitude of a threat or hazards effect on an installation, personnel, a unit, an exercise, a port, a ship, a residence, a facility, or other site. It identifies the areas of improvement required to withstand, mitigate, or deter acts of violence or terrorism or attacks against threats. The staff addresses who or what is vulnerable and how it is vulnerable against threats. The vulnerability assessment identifies physical characteristics or procedures that render critical assets, areas, infrastructures, or special events vulnerable to known or potential threats and hazards. 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.

3-14. 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.

3-15. 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 (MSHARPP).** MSHARPP is a targeting analysis tool that is geared toward assessing personnel vulnerabilities, but it can also be applied in conducting a broader analysis. The purpose of the MSHARPP matrix is to analyze likely terrorist targets and to assess their vulnerabilities from the inside out. Consideration is given to local threats, the probable means of attacks, and variables that affect dispositions of potential targets. After developing a list of potential targets, MSHARPP selection factors are used to assist in further refining the assessment by associating a weapon or tactic with a potential target to determine the efficiency, effectiveness, and plausibility of the attack method and to identify vulnerabilities related to the target.
- **Criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER).** The CARVER matrix is a valuable tool in determining criticality and vulnerability. For criticality purposes, CARVER helps assessment teams and commanders (and the assets that they are responsible for) to determine assets that are more critical to the success of the mission. This also helps determine which resources should be allocated to protect critical assets (personnel, infrastructure, and information). The CARVER targeting matrix assesses a potential target from a terrorist perspective to identify what the enemy might perceive as a good (soft or valuable) target. (See ATP 3-37.2 for more information on MSHARPP and CARVER.)

PROTECTION PRIORITIES

3-16. Criticality, vulnerability, and recoverability are some of the most significant considerations in determining protection priorities that become the subject of commander guidance and the focus of area security operations. The scheme of protection is based on the mission variables and should include protection priorities by area, unit, activity, or resource.

3-17. Although all military assets are important and all resources have value, the capabilities they represent are not equal in their contribution to decisive operations or overall mission accomplishment. Determining and directing protection priorities may involve the most important decisions that commanders make and their staffs support. There are seldom sufficient resources to simultaneously provide the same level of protection to all assets.

3-18. Most prioritization methodologies assist in differentiating what is important from what is urgent. In protection planning, the challenge is to differentiate between critical assets and important assets and to further determine what protection is possible with available protection capabilities. Figure 3-1, page 3-6, provides examples of possible protection priorities at the theater, corps, and division level. 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 and sustainable scheme of protection. In either situation, commanders must provide guidance on prioritizing protection capabilities and categorizing important assets.

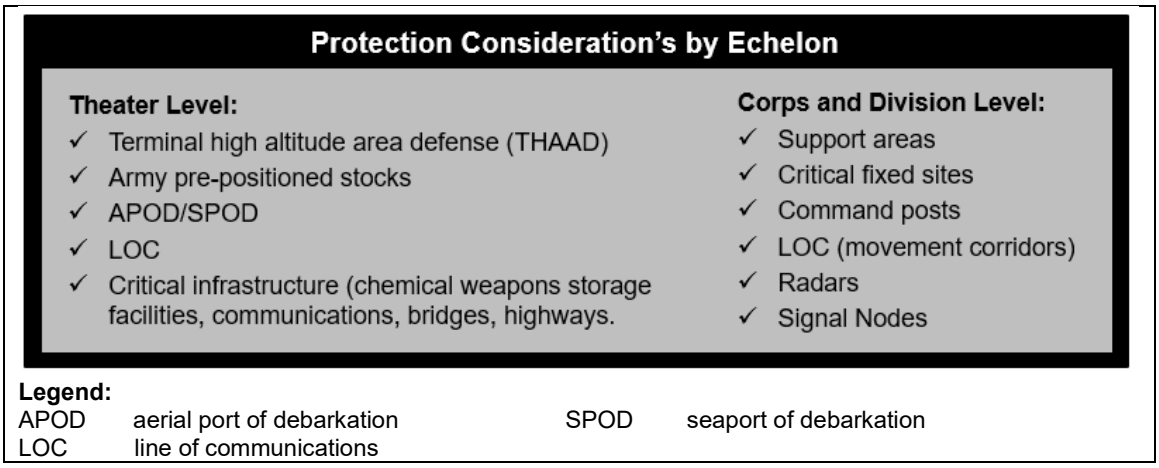


Figure 3-1. Example of protection considerations by echelon

PROTECTION PRIORITIZATION LIST

3-19. Protection prioritization lists are organized through the proper alignment of critical assets. The commander's priorities and intent and the impacts on mission planning determine critical assets. 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 3-07.2). Critical assets can be people, property, equipment, activities, operations, information, facilities, or materials. For example, important communications facilities and utilities, analyzed through criticality assessments, provide information to prioritize resources while reducing the potential application of resources on lower-priority assets. Stationary weapons systems 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.

3-20. The protection cell and working group use information derived from the commander's guidance, the intelligence preparation of the battlefield, targeting, risk management, warning orders, the critical asset list (CAL) and defended asset list (DAL), and the mission analysis to identify critical assets. Critical assets at each command echelon must be determined and prioritized.

3-21. The protection prioritization list is a key protection product developed during initial assessments. The protection cell and working group must use criticality, threat vulnerability, and threat probability 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 is essential to accomplish the mission. It is determined by assessing the impact that damage to, or destruction of, the asset will have on the success of the operation. Damage to an asset may prevent, delay, or have no impact on the success of the plan.
  - **Catastrophic.** Complete mission failure or the inability to accomplish the mission, death or total disability, 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; total disability, partial disability, or temporary disability; extensive damage to equipment or systems; significant damage environment; security failure; or significant collateral damage.
  - **Marginal.** Degraded mission capability or unit readiness; minor damage to equipment or systems, property, or the environment; lost days due to injury or illness; or minor damage to property or the environment.

- **Negligible.** Little or no adverse impact on mission capability, first aid or minor medical treatment, slight equipment or systems damage (remaining fully functional or serviceable), or little or no property or environmental damage.

- Threat vulnerability measures the ability for a threat to damage the target (asset) using available systems (people and material). An asset's 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 may not require additional protection assets, 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 recoverability (which measures the time required for the asset to be restored, considering the availability of resources, parts, expertise, manpower, and redundancies).
  - **Level I threat.** Agents, saboteurs, sympathizers, terrorists, civil disturbances.
  - **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.
- Threat probability assesses the probability that an asset will be targeted for surveillance or attack by a credible/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. Examples are surveillance, criminal activities, cyberspace attacks, indirect fire, and small-arms fire.
  - **Likely**. Occurs several times; a common occurrence. Examples are explosive booby traps/improvised explosive devices, ambushes, and bombings.
  - **Occasional.** Occurs sporadically, but is not uncommon. Examples are air-to-surface attacks or insider threats, which may result in injury or death.
  - **Seldom.** Remotely possible; could occur at some time. Examples are the release of CBRN hazards or the employment of WMD.
  - **Unlikely.** Presumably, the action will not occur, but it is not impossible. Examples are the detonation of containerized ammunition during transport or the use of a dirty bomb.

3-22. 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 to provide the assessment and recommended protection prioritization list to the commander for approval (see table 3-2, page 3-8).

Table 3-2. Sample protection prioritization list

Rec Priority	Asset	Location	Notes	Requirement	Threat	Mitigation	Unit Tasks
1	DIVARTY Q53 (Radar)	PL Bobcat	Critical for Counterfire missions, 4x	1 x MP CO	ENY Air, IDF(G-6, 9A51, 9A52, 2S19), SPF, EW Jamming	Survivability Position; Passive Air Defense; CAV SQDN & MP CO securing	SPF, A, 3-265 1-172 CAV 233 MP CO
2	DIVARTY Q36 (Radar)	PL Bobcat	Critical for Counterfire missions, 3x	1 x MP CO	ENY Air, IDF(G-6, 9A51, 9A52, 2S19), SPF, EW Jamming	Survivability Position; Passive Air Defense; CAV SQDN & MP CO securing	A, 3-265 1-172 CAV 233 MP CO
3	DIVARTY Q37 (Radar)	PL Bobcat	Critical for Counterfire missions, 3x	1 x MP CO	ENY Air, IDF(G-6, 9A51, 9A52, 2S19), SPF, EW Jamming	Survivability Position; Passive Air Defense; CAV SQDN & MP CO securing	A, 3-265 1-172 CAV 233 MP CO
4	3-197 MLRS	PL Bobcat	BN assigned to DIVARTY, 16x	1 x Avenger PLT	IDF(G-6, 9A51, 9A52, 2S19), Chemical Attack	Survivability Position; Passive Air Defense; CAV SQDN & MP CO securing	A, 3-265 1-172 CAV 233 MP CO
5	2-18 HIMARS	OBJ Viking	BN assigned to DIVARTY, 16x	1 x Avenger PLT (VIC FLOT)	IDF(G-6, 9A51, 9A52, 2S19), Chemical Attack	Survivability Position; Passive Air Defense; CAV SQDN & MP CO securing	A, 3-265 1-172 CAV 233 MP CO
6	814-206, 957-206 MRBC	In place on river	Maintain GLOCs	1 x Avenger PLT; Secure by ABCTs	SPF, IDF(G-6, 9A51, 9A52, 2S19)	Passive Air Defense; defended in echelon	B, 3-265(-)
7	Division Support Area	With 404MEB	Open additional GLOC	1 x Avenger PLT; Secure by MEB	SPF, IDF(G-6, 9A51, 9A52, 2S19)	Passive Air Defense; defended in echelon	B, 3-265(-)
8	C/3-4 Patriot	Vicinity DMAIN	Theater Asset	1 x MP PLT	SPF, IDF(G-6, 9A51, 9A52, 2S19), Chemical Attack	1 x MP PLT Organic Avenger System	3/333 MP CO(-)
9	1-35 EN BN	OBJ Riverrun	Mobility Support Asset	1 x Avenger PLT (VIC FLOT)	Enemy Air, UAS, IDF, DF, Chemical Attack	Passive Air Defense, Area Security	A, 3-265
10	Airfield	SACP	Resupply Hub for 1 SBDE	1 x MP CO; Secure by MEB	Enemy Air, Rotary Wing, UAS, SPF	Neutralize ENY Rotary, UAS, AS to Destroy SPF	404 MEB, 233 MP CO
11	CL III, V, & VII Re-supply Missions	Ganja-PL Giants	TACON for Convoy Security	2 x MP CO	SPF, IDF(G-6, 9A51, 9A52, 2S19)	MP Convoy Security	252 MP CO 253 MP CO
12	265 ADA BN (Avengers)	Various	Necessary for Protection Plan of other PPL	1 x PLT per Battery (3 x PLT total)	Chemical Attack, SPF		Secure by supported units

Defended Asset List (DAL) – those critical assets with air defense units assigned for AMD.

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

Legend:

ABCT	armored brigade combat team	HIMARS	high mobility artillery rocket system
ADA	air defense artillery	IDF	indigenous forces
AMD	air and missile defense	MEB	maneuver enhancement brigade
BDE	brigade	MLRS	multiple launch rocket system
BN	battalion	MP	military police
BTY	battery	MRBC	multi-role bridge company
CAV	cavalry	OBJ	objective
CO	company	PL	phase line
CL	class	PLT	platoon
DIVARTY	division artillery	PPL	protection prioritization list
DMAIN	division main command post	REC	recommended
EN	engineer	SBDE	sustainment brigade
ENY	enemy	SPF	special purpose forces
EW	electronic warfare	SQDN	squadron
FA	field artillery	TACON	tactical control
FLOT	forward line of troops	UAS	unmanned aircraft system
GLOC	ground lines of communication	VIC	vicinity

3-23. Changes to protection prioritization should be anticipated and assets reassessed as transitions occur with the operation or with changes to the commander's priorities (see figure 3-2).

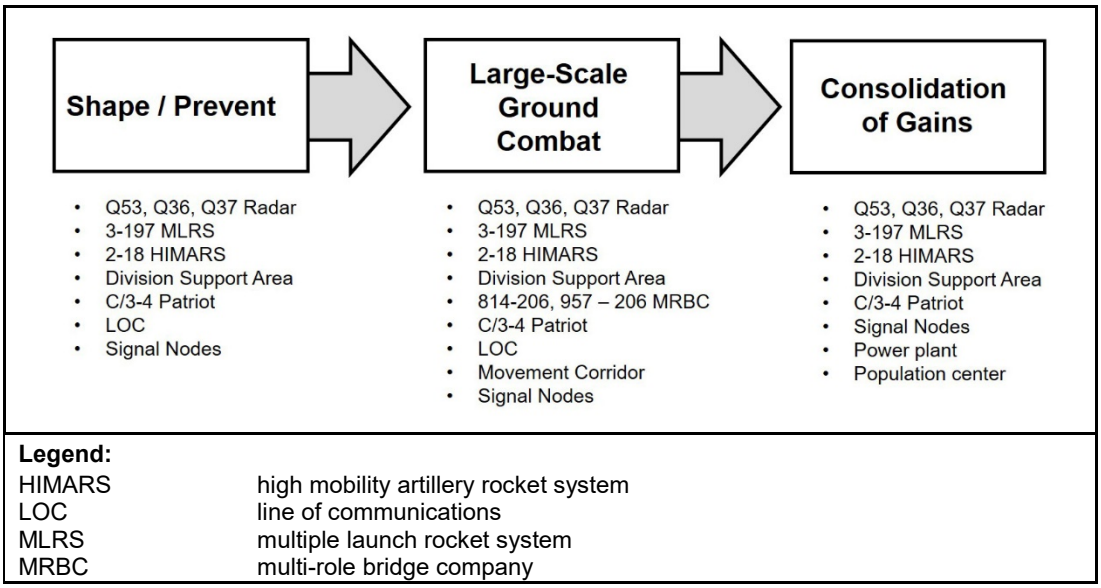


Figure 3-2. Example of protection prioritization by Army strategic roles

SCHEME OF PROTECTION DEVELOPMENT

3-24. The scheme of protection describes how protection tasks 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 protection decisive points, high-risk considerations, and prudent risk. Figure 3-3 provides an example of a scheme of protection.

(U) References: Refer to base OPORD.

(U) Time Zone Used Throughout the OPORD: ZULU

1. (U) Situation. Refer to base OPORD.

2. (U) Mission. Refer to base OPORD.

3. (U) Execution.

(1) (U) Scheme of Protection. During division operations priority of protection support is focused on the protection prioritization list: Division Level - division fires, division support area, bridging assets, division mission command nodes and lines of communication. Air missile defense assets will be arrayed to support division artillery and protect critical assets throughout division's area of operations. Priority for military police forces is to conduct area security throughout the division support area, main supply route security and traffic control in support of gap-crossing, provide convoy security for high value convoys in support of sustainment, and establish a division holding area to conduct detainee operations. Chemical, biological, radiological, and nuclear (CBRN) forces will provide CBRN defense, establish CBRN response, and conduct information collection to identify chemical warehouses/plants, hydrocarbon/oil pipelines, and contaminated areas throughout the divisional area of operations. Key risks to mission throughout this phase include CBRN attacks focused on obstacles and key terrain such as WILSON gap-crossing (wet) efforts and terrain that naturally canalizes maneuver efforts. Engineer's priority of effort will focus on survivability efforts to avoid and withstand hostile actions by constructing protective positions and hardening facilities. Engineers will provide support to explosive ordnance assets during route clearance activities. All division units will - incorporate survivability tasks; apply antiterrorism measures; implement physical security procedures; plan for the recovery and reintegration of isolated personnel; establish force health protection measures to enable a healthy, fit force and prevent injury and illness; and incorporate risk management throughout all operations. Additional risks include enemy Special Forces efforts to disrupt sustainment in the division support area.

Figure 3-3. Scheme of protection example

3-25. Planners receive guidance as commanders describe their visualization of the operational concept and intent. This guidance generally focuses on the COA development by identifying decisive and supporting efforts, massing effects, and stating priorities. Effective planning guidance provides a broad perspective of the commander's visualization, with the latitude to explore additional options.

3-26. 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, the incorporation of efforts, and the protection required. The scheme of protection is based on the mission variables, thus it includes protection priorities by area, unit, activity, or resource. 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.

3-27. The protection cell considers the following items, at a minimum, as it develops the scheme of protection:

- Protection priorities.
- Work priorities for survivability assets.
- Air and missile defense positioning guidance.
- Specific terrain and weather factors.
- Information focus and limitations for security efforts.
- Areas or events where risk is acceptable.
- Protected targets and areas.
- Civilians and noncombatants in the AO.
- Vehicle and equipment safety or security constraints.
- Personnel recovery actions and control measures.
- FPCON status.
- Force health protection measures.
- Mission-oriented protective posture guidance.
- Environmental guidance.
- Scheme of information operations.
- 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.
- Radiation exposure status.
- Contractors in the AO.

TASKS AND SYSTEMS INTEGRATION

3-28. To achieve protection and preserve combat power across the range of military operations, the scheme of protection must be comprehensive, integrated, layered, redundant, and enduring.

3-29. Protection tasks 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 their

available capabilities to defend the protection priorities, and a layering of capabilities reduces the destructive effect of threats and hazards.

3-30. 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 AT 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 protected priorities throughout the range of military operations in any OE.

RUNNING ESTIMATE

3-31. 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.)

3-32. The protection working group develops and refines the protection running estimate. The protection running estimate provides a picture to the command on how protection is comprehensive, integrated, layered, redundant, and enduring. It is developed from information (including the 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. Integrating process data and continuing activities (assets available, civil considerations, threat and hazard assessments, criticality assessments, vulnerability assessments, capability assessments, MOEs, MOPs, EEFI, protection priorities, risk decision points, supporting tasks) feed updates to the running estimate.

PROTECTION CELL AND WORKING GROUP

3-33. 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.

PROTECTION CELL MEMBERS

3-34. The protection cell membership does not require representatives from every functional element of protection. However, dedicated members should coordinate with other personnel and special staff elements as required, Primary members of the protection cell typically include the chief of protection, an air and missile defense officer, a personnel recovery officer, a provost marshal, a CBRN officer, an EOD officer, an engineer officer, and an AT officer.

Chief of Protection

3-35. The chief of protection may be designated by tables of organization and equipment or by the unit commander. He is the principal advisor to the commander on all matters relating to the protection warfighting function. A chief of protection—

- Plans and coordinates protection functions and missions.
- 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.
- Synchronizes with other staff cells, nodes, and functional groups.

- Provides guidance on the execution of protection tasks and systems.
- Continually monitors and assesses the overall protection effort.

Air and Missile Defense Officer

3-36. The air and missile defense officer coordinates and synchronizes the air and missile defense tasks in the AO. The air and missile defense officer—

- Advises, monitors, and makes recommendations regarding the current enemy air and missile threat.
- Collaborates with higher headquarters to protect critical and defended assets.
- Coordinates current operations of subordinate air defense artillery forces.
- Coordinates adjustments of sensor and engagement coverage based on changes in the mission variables.
- Leads or augments other protection components when operating in a low-threat air environment.

Personnel Recovery Officer

3-37. The PR officer advises the commander on all aspects of PR operations. He plans and coordinates the operations necessary to obtain the release or recovery of captured, missing, or isolated personnel from uncertain or hostile environments and denied areas.

Provost Marshal

3-38. The provost marshal plans military police support for operations and provides advice on military police capabilities. The provost marshal—

- Makes recommendations on developing and allocating military police resources that protect priorities.
- Synchronizes military police operations and law enforcement guidance between main and tactical command posts and among subordinate, adjacent, and higher units.
- Provides military police and physical security planning expertise, including—
  - Police operations.
  - Detention operations.
  - Security and mobility 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 AO.
- May serve as a member of a vulnerability assessment team.
- Coordinates with the engineer officer to plan for the support and protection of river-crossing operations and main supply route security and protection.

Chemical, Biological, Radiological, and Nuclear Officer

3-39. The CBRN officer conducts planning for and oversees all CBRN operations. The CBRN officer—

- Provides response analysis, written estimates and plans, and advice.
- Provides staff supervision for CBRN site assessments and consequence management operations in the AO.
- Plans CBRN support with higher and adjacent units.
- Supports the CBRN warning and reporting system.
- Recommends how to employ CBRN assets.
- Coordinates with the engineer officer for explosive hazard operations by identifying the appropriate mix of complementary and reinforcing capabilities.

Explosive Ordnance Disposal Officer

3-40. The EOD officer incorporates EOD requirements into plans and orders. The EOD officer—

- Recommends how to implement EOD-unique skills.
- Tracks UXO, IED, and WMD incident support.
- Recommends reinforcing support.

3-41. If assigned to the headquarters, the explosive hazards coordination cell can assist the protection cell through the collection, analysis, and dissemination of explosive hazard information. This cell is a specialized Army engineer force pool unit assigned to corps, division, or brigade staffs. Within the theater, it can predict, track, distribute information on, and mitigate explosive hazards that affect force application, focused logistics, survivability, and situational awareness.

Engineer Officer

3-42. The engineer officer identifies requirements and prioritizes engineer capabilities and assets. The engineer officer—

- Identifies current and future operations that require force packaging to meet operational requirements.
- Identifies and synchronizes requirements for the mobility of friendly forces.
- Identifies requirements for safeguarding bases.
- Advises on the aspects of survivability, as defined in chapter 2.
- Facilitates the sustainment of friendly forces.
- Identifies general engineering operations.
- Synchronizes with the CBRN officer to apply battlefield obscuration and decontamination support, as appropriate.
- Provides reachback to the Army Corps of Engineers.
- Contributes to a clear understanding of the physical environment.
- Provides support to noncombatants, other nations, and civilian authorities and agencies.

Antiterrorism Officer

3-43. The AT officer—

- Establishes an AT program.
- Collects, analyzes, and disseminates threat information.
- Assesses and reduces critical vulnerabilities (conducts AT assessments).
- Increases AT awareness in Soldiers, Civilians, and Family members.
- Maintains defense according to the FPCON.
- Establishes civil/military partnerships for terrorist incident crises.
- Conducts terrorism threat/incident response planning.
- Conducts exercises and evaluates/assesses AT plans.

Operations Security Officer

3-44. The OPSEC officer identifies and recommends critical information requirements. The OPSEC officer—

- Analyzes adversaries and vulnerabilities as part of the intelligence preparation of the battlefield 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 and compromised EEFI.
- Searches news sources, Web logs, and other Web sites for sensitive information and compromised EEFI.

PROTECTION WORKING GROUP

3-45. *Working groups* address various subjects depending on the situation and echelon. A *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 working groups to 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 synchronizes the contributions of all staff elements with the work of the protection cell. It also synchronizes protection with future operations and current operations integration cells.

3-46. 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 assessments, vulnerability assessments, and protection priority recommendations. The protection working group calls upon existing resources from the staff.

3-47. The protection working group is led by the chief of protection and normally consists of the following:

- An air and missile defense officer.
- An AT officer.
- A CBRN officer.
- An engineer officer.
- An electronic warfare element representative.
- An EOD officer.
- A fire support representative.
- An OPSEC officer.
- A provost marshal.
- A safety officer.
- An intelligence representative.
- A civil affairs officer.
- A personnel recovery officer.
- A public affairs officer.
- A staff judge advocate.
- A chaplain.
- A surgeon.
- A medical representative.
- A veterinary representative.
- Subordinate unit liaison officers.
- An operations representative.
- An area contracting officer.
- A cyberspace representative.
- An information officer.
- Logisticians.

3-48. Protection working group meetings have the same purpose, 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. The protection working group—

- Determines likely threats and hazards from updated enemy tactics, the environment, and accidents.
- Determines vulnerabilities as assessed by the vulnerability assessment team.

- Establishes and recommends protection priorities, such as the CAL.
- Provides recommendations for the CAL and DAL.
- Reviews and coordinates unit protection measures.
- Recommends FPCONs and random AT measures.
- Determines required resources and makes recommendations for funding and equipment fielding.
- Provides input and recommendations on protection-related training.
- 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 according to Department of Defense Instruction (DODI) 2000.16.
- Accesses assets and infrastructure that are designated as critical by higher headquarters.

3-49. Commanders augment the team with other unit specialties and unified action partners, depending on the operational environment and the unit mission. The chief of protection determines the working group agenda, meeting frequency, composition, input, and expected output. Table 3-3 shows a sample purpose, agenda, and composition of a protection working group with staff inputs and outputs.

Table 3-3. Sample protection working group activities

Purpose and Frequency	**Purpose:** ● Determines likely threats and hazards ● Determines vulnerabilities ● Establishes and recommends protection priorities ● Provides recommendations for the critical asset list and defended asset list ● Reviews and coordinates 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 ● 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 ● Develops personnel recovery guidance and isolated Soldier guidance. ● Provides input and recommendations for cyberspace network protection. ● Identifies risks to the mission **Frequency**: Every other day
Composition	**Chair:** Chief of protection Attendees: ● Air and missile defense officer ● Antiterrorism officer ● Chemical, biological, radiological, and nuclear officer ● Engineer officer ● Electronic warfare element representative ● Explosive ordnance disposal officer ● Fire support representative ● Operations security officer ● Provost marshal ● Safety officer ● Intelligence representative ● Civil affairs officer ● Public affairs officer. ● Staff judge advocate. ● Chaplain. ● Surgeon. ● Medical representative. ● Veterinary representative ● Subordinate unit liaison officers ● Operations representative ● An area contracting officer ● Cyberspace representative ● Information officer ● Logisticians ● Personnel recovery officer

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

Inputs and outputs	**Inputs:** ● Commanders guidance and intent ● Operations and warning orders ● Current scheme of protection ● Threat and hazard assessment ● Vulnerability assessment ● Criticality assessment ● Risk management ● Critical asset list ● Defended asset list	**Outputs:** ● Update protection assessment ● Scheme of protection ● Protection Running estimate ● Protection prioritization list ● Recommended force protection condition ● Recommended protection guidance and mitigation measures ● Recommended changes to essential element of friendly information ● Recommended changes to critical asset list and defended asset list
Agenda	● Roll call ● Operations/intelligence update (assistant chief of staff, operations [G-3]/ assistant chief of staff, intelligence [G-2]) ● 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)	

ROLES AND RESPONSIBILITIES

3-50. The protection cell and working group are responsible for integrating, coordinating, and synchronizing protection tasks and activities. The protection cell advises commanders on the priorities for protection and coordinates the implementation and sustainment of protective measures to protect assets according to the commander's priorities. The protection cell and working group help develop a concept of protection tailored to the type of operation the unit is conducting.

3-51. During the planning process, the protection cell provides input to the commander's MDMP by integrating the threat and hazard assessment with the commander's EEFI and the protection prioritization list. While the planning cell develops plans, the protection cell and working group attempt to minimize vulnerability based on the developing COA. The intent is to identify and recommend refinements to the COA that are necessary to reduce vulnerability and ensure mission success. The protection cell and working group provide vulnerability mitigation measures to help reduce risks associated with a particular COA and conduct planning and oversight for unified land operations.

3-52. The protection working group—

- Determines likely threats and hazards from updated enemy or adversary tactics, the environment, and accidents.
- Determines vulnerabilities as assessed by the vulnerability assessment team.
- Establishes and recommends protection priorities.
- Provides recommendations for the CAL/DAL and protection prioritization list.
- Reviews and coordinates unit protection measures.
- Recommends FPCONs and random AT measures.
- Determines required resources and makes recommendations for funding and equipment fielding.
- Provides input and recommendations on protection-related training.
- 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 according to DODI O-2000.16, Volume 1.

- Assesses assets and infrastructure that are designated as critical by higher headquarters.
- Analyzes and provides recommendations for the protection of civilians in the AO.
- Develops and refines the running estimate.
- Develops a scheme of protection, ensuring that it nests with the operational concept.
- Establishes the personnel recovery coordination center.
- Develops personnel recovery guidance and isolated Soldier guidance.
- Provides input and recommendations for cyberspace network protection.
- Identifies risks to the mission.

3-53. The approved vulnerability reduction mitigation measures, commander's decisions for acceptable risks, and protection prioritization list represent running estimates that are incorporated into appropriate plans and orders. Based on these estimates, the protection cell develops the scheme of protection in the base order and appropriate annexes.

3-54. Planners integrate protection actions and information throughout specific plans and orders. Some significant, protection-related products that are often produced in the planning process include the—

- Scheme of protection that supports and nests with the operational concept.
- Running estimate that reflects protection tasks and systems.
- Quantifiable level of risk for specific events and activities.
- Protection MOE and MOP and threshold variances.
- Recommendations for the commander's critical information requirements that reflect decision criteria from protection tasks and systems.
- Protection prioritization list.
- Decision points based on the commander's risk tolerance level.

COORDINATION AND RELATIONSHIPS

3-55. The protection cell ensures the integration of protection equities throughout the operations process via integrating processes, continuing activities, the MDMP, working groups, planning sessions, and coordination between warfighting functions. This develops and refines 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 (see table 3-3) that have beneficial output, which develops the scheme of protection and enhances the overall protection plan. The agenda, frequency, composition, input, and expected output for the working group are determined by the lead protection working group officer and are based on mission variables and MDMP integration.

INTEGRATING PROCESSES

3-56. The integrating processes of intelligence preparation of the battlefield, targeting, risk management, and OPSEC are essential in providing assessments or key information to assessments. They are a vital part of integrating protection within the other warfighting functions and throughout the operations process.

3-57. Intelligence preparation of the battlefield is a systematic process of analyzing the mission variables of threat, terrain, weather, and civil considerations in a specific area of interest to determine their effects on operations. By conducting the intelligence preparation of the battlefield, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space.

3-58. 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 likelihood of these events. The protection priorities must be integrated within the targeting process to achieve the desired effects and ensure the preservation of combat power.

3-59. Risk management is the process of identifying, assessing, and controlling risks that arise from operational factors and of making decisions that balance risk cost with mission benefits. Threat, hazard, capability, vulnerability, and criticality assessments are used to evaluate the risk to the force, determine critical assets, ascertain available resources, and apply security or defensive measures to achieve protection. Risk management helps commanders to preserve lives and resources, avoid or mitigate unnecessary risk, identify and implement feasible and effective control measures where specific standards do not exist, and develop valid COAs. Risk management integration during operations process activities is the primary responsibility of the unit protection officer or operations officer.

3-60. OPSEC is the properly implemented measures and countermeasure that protect EEFI from enemy or adversary observation and collection. OPSEC is fully integrated into all plans and orders, and begins during receipt of the mission. The OPSEC planner begins to identify EEFI by analyzing the enemy's capabilities, with special emphasis on the enemy's ability to conduct reconnaissance, surveillance, intelligence gathering, and information collection directed at the unit. Once the EEFI are initially developed, the OPSEC planner focuses on protecting this information during the remaining steps of the MDMP and refining the process. OPSEC measures and countermeasures are developed using the risk assessment matrix to determine OPSEC vulnerabilities and residual risk associated with each measure or countermeasure.

3-61. The Army's portion of cyberspace, the DODIN-A, is a single, secure, standards-based, versatile infrastructure nested within the DODIN. It is linked by networked, redundant transport systems, sensors, warfighting and business applications, and services. The DODIN-A provides Soldiers and civilians timely and accurate information in any environment to enable decisive action with our unified action partners. The DODIN-A provides all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide and provides a powerful tool for leaders to use in synchronizing their efforts. The primary signal operations planner is an active member of the operations process to ensure supportability and feasibility of the signal plan being considered throughout the MDMP. Refer to table 3-4.

Table 3-4. Protection integration to MDMP

Key Input	*Protection Actions*	*Steps*	*Protection Output*	*Key Output*
• Higher HQ plan or order • New mission anticipated by the commander	• 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	Step 1: Receipt of Mission Warning Order	• Protection working group • Warning and reporting systems • Protection running estimate	• Commander's initial guidance • Initial allocation of time
• Higher HQ plan or order • Higher HQ knowledge and intelligence products • Knowledge products from other organizations • Design concept (if developed)	• Provide input on critical networks or nodes that can be influenced • Identify requests for information • Determine available assets • Conduct and consolidate initial assessments • Conduct protection working group • Recommend and coordinate information collection assets for protection • Develop OPSEC indicators • Identify EEFI, and establish how long it should be protected • Develop essential survivability and other engineering tasks • Identify available information on routes and key facilities • Analyze protection considerations of civilians in the AO • Determine available unified action partner capabilities • Determine funding sources, as required • Determine availability of construction and other engineering materials	Step 2: Mission Analysis Warning Order	• Consolidated HVT list • RFIs • Initial assessments • Recommended PPL • Recommended EEFI • Initial protection priorities • Input into information collection plan	• Problem statement • Mission statement • Initial commander's intent • Initial planning guidance • Initial CCIRs and EEFIs • Initial OPSEC planning guidance • Updated IPB and running estimates • Assumptions

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

Key Input	*Protection Actions*	*Steps*	*Protection Output*	*Key Output*
• Mission statement • Initial commander's intent, planning guidance, CCIRs, and EEFIs • Updated IPB and running estimates • Assumptions	• Determine array of protection assets • Integrate protection tasks into COA • Determine initial scheme of protection • Coordinate health support requirements • Ensure that link architecture meets requirements and has been allocated from respective agents • Recommend appropriate level of survivability effort for each COA based on the expected threat • Determine alternate construction location, methods, means, materials, and timelines to give the commander options • Determine real-property and real estate requirements • Identify indicators and vulnerabilities	Step 3: COA Development	• Recommended updates to PPL • Recommended updates to EEFIs • Determine residual risk • Develop initial OPSEC measures and countermeasures • Initial scheme of protection	• COA statements and sketches • Tentative task organization • Broad concept of operations • Revised planning guidance • Updated assumptions
• Updated running estimates • Revised planning guidance • COA statements and sketches • Updated 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	Step 4: COA Analysis (War Game)	• Initial DAL • Refined 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 • Potential decision points • War-game results • Initial assessment measures • Updated assumptions
• Updated running estimates • Refined COAs • Evaluation criteria • War-game results • Updated assumptions	• Compare economy-of-force and risk reduction measures	Step 5: COA Comparison	• Refined protection priorities • Refined PPL • Refined EEFI • Refined scheme of protection	• Evaluated COAs • Recommended COAs • Updated running estimates • Updated assumptions

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

Key Output	*Protection Actions*	*Steps*	*Protection Output*	*Key Output*
• Updated running estimates • Evaluated COAs • Recommended COA • Updated assumptions	• Brief scheme of protection • Brief protection task specifics, as required	Step 6: COA Approval Warning Order	• Refined protection priorities • Refined EEFI • Refined • Refined scheme of protection	• Commander-selected COA and modifications • Refined commander's intent, CCIRs, and EEFIs • Updated assumptions
• Commander-selected COA with any modifications • Refined commander's intent, CCIRs, and EEFIs • Updated assumptions	• Refine and develop protection annex and supporting appendixes	Step 7: Orders Production, Dissemination, and Transition	• Protection annex and supporting appendixes	• Approved operation plan or order • Subordinate understanding of plan or order • Update EEFIs as needed

Legend:

AO	area of operations
CCIR	commander's critical information requirement
COA	course of action
DAL	defended asset list
EEFI	essential element of friendly information
HQ	headquarters
HVT	high-value target
IPB	intelligence preparation of the battlefield
MOE	measure of effectiveness
MOP	measure of performance
OPSEC	operations security
PPL	protection priority list
RFI	request for information

This page intentionally left blank.

Chapter 4
Protection Preparation

The force is often most vulnerable to an enemy or adversary surprise attack during preparation. Preparation, operations to shape, and operations to prevent create conditions that improve friendly force opportunities for success. 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. Preparation activities help commanders, staffs, and Soldiers to understand a situation and their roles in upcoming operations. Protection preparation requirements occur throughout operations to shape, operations to prevent, large-scale ground combat operations, and operations to consolidate gains. 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.

CONSIDERATIONS

4-1. As the staff monitors and evaluates the performance or effectiveness of a friendly COA, ground- and space-based information collection operations are used to collect 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 assessment is a dynamic and continually changing process. Protection planners stay alert for changing OE indicators and warnings that would signal new or fluctuating threats and hazards.

4-2. 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 preparation, operations to shape, and operations to prevent, 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.

4-3. Commanders exercising mission command direct and lead throughout the operations process. Commanders' actions during preparation, operations to shape and operations to prevent, 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.

4-4. Depending on the situation and the 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 and 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.

4-5. 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

4-6. 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 the following preparation activities, operations to shape, and operations to prevent, some of which are further discussed below:

- Continue to coordinate and conduct liaison.
- Conduct rehearsals.
- Initiate information collection.
- Conduct plans-to-operations transitions.
- Initiate security operations.
- Refine the plan.
- Initiate troop movement.
- Integrate new Soldiers and units.
- Initiate sustainment preparations.
- Complete task organization.
- Initiate network preparations.
- Train.
- Manage terrain.
- Perform pre-operation checks and inspections.
- Prepare terrain.
- Continue to build partnerships and teams.
- Conduct confirmation briefs.
- Consider effects of protection activities in the information environment.

CONTINUE TO COORDINATE AND CONDUCT LIAISON

4-7. Coordination and liaison help ensure that leaders who are internal or external to the headquarters understand the unit role in upcoming operations and ensure that they are prepared to perform that role. Continuous coordination and liaison between the command and unified action partners help 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.

INITIATE INFORMATION COLLECTION

4-8. Throughout the operations process, commanders take every opportunity to improve their situational understanding. This requires aggressive and continuous information collection. Commanders and staffs continuously plan, task, and employ collection assets and forces to collect timely and accurate information that helps satisfy the commander's critical information requirements 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 require surveillance.

4-9. 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

4-10. Commanders and staffs continuously plan and coordinate security operations throughout the operation. Security operations are those operations undertaken by a commander to—

- Provide an early and accurate warning of enemy or adversary operations.
- Provide the force with the time and maneuver space necessary to react to the enemy or adversary.
- Develop the situation so that commanders can effectively use the protected force.

4-11. One of the most common methods of providing protection for ground combat forces during unified land operations is through the use of security operations. The ultimate goal of security operations is to protect the force from surprise and to reduce the unknown in any situation (see ADP 3-90).

4-12. Security operations reflect increasing levels of combat power that can be applied to protect an asset or force from a directed threat, and they are typically conducted by operating forces designed to gain and exploit the initiative. 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, route, or area. Local security protection ranges from echelon headquarters to reserves and sustainment forces.

MANAGE AND PREPARE TERRAIN

4-13. Terrain management is the process of allocating terrain by establishing AOs, 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 AO. 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. It can make the difference between operation success and failure.

INTEGRATE INFORMATION OPERATIONS

4-14. *Information operations* is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). By definition, information operations has an inherent protection requirement—to safeguard friendly decision making while degrading the enemy's or adversary's decision making. One means to degrade the enemy's decision making is to deny the enemy access to friendly information.

4-15. Commanders recognize that protection extends beyond the physical domains to include the information environment and cyberspace. They ensure close coordination between the protection cell/working group and the information operations and cyberspace electromagnetic activities elements/working groups. They visualize and understand how protection tasks and activities affect the information environment and cyberspace and, in turn, how information operations and cyberspace electromagnetic activities contribute to and support the protection warfighting function. (See FM 3-13 for additional information on information operations.)

PROTECTION WORKING GROUP

4-16. Preparation includes increased application and emphasis on protection measures. During preparation, operations to shape, and operations to prevent, the protection working group—

- Provides recommendations to refine the scheme of protection.
- Makes changes to the protection prioritization list based on the commander's priorities and changes during the phase of an operation.
- Recommends systems to detect threats to the critical assets.
- Proposes the refinement of OPSEC measures.
- Monitors quick-reaction force or tactical and troop movements.
- Provides recommendations for improving survivability.
- Liaisons and coordinates with adjacent and protected units.
- Determines protection indicators and warnings for information collection operations.
- Confirms backbriefs.
- Analyzes and proposes vulnerability reduction measures.
- Provides recommended revisions to tactical standard operating procedures.
- Conducts personnel recovery rehearsals.

4-17. During preparation, operations to shape, and operations to prevent, 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.

4-18. Subworking groups 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 OE and the 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, EEFI, and the scheme of protection.

ANTITERRORISM WORKING GROUP

4-19. The AT working group is led by the AT officer and includes members from the protection working group, subordinate commands, host nation agencies, and other unified action partners. It—

- Develops and refines AT plans.
- Oversees the implementation of the AT program.
- Addresses emergent and emergency AT program issues.

COUNTER IMPROVISED EXPLOSIVE DEVICE WORKING GROUP

4-20. The counter improvised explosive device 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. It—

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

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR WORKING GROUP

4-21. The CBRN working group is led by the CBRN officer and includes other members of the protection working group, subordinate commands, host nation agencies, and other unified action partners. It—

- 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.
- Refines the CBRN threat, hazard, and vulnerability assessments.

This page intentionally left blank.

Chapter 5

Protection Execution

The execution of protection is continuous and must occur throughout operations to shape, operations to prevent, large-scale ground combat operations, and operations to consolidate gains, with a focus on deterring and preventing the enemy, adversaries, or hazards from actions that effect the force. Commanders implement control measures and allocate resources that are sufficient to ensure protection continuity and restoration. Employed mitigation measures that have been planned and prepared for allow the force to quickly respond 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.

EXECUTION

5-1. Commanders who exercise mission command decide, direct, lead, access, and provide leadership to organizations and Soldiers during execution. 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. Commanders may direct and redirect the way that combat power is applied or preserved, and they may adjust the tempo of operations through synchronization. The continuous and enduring character of protection makes the continuity of protection capabilities essential during execution. Commanders implement control measures and allocate resources that are sufficient to ensure protection continuity and restoration.

5-2. The staff monitors the conduct of operations during execution, looking for variances from the scheme of maneuver and protection. 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, from main and supporting efforts to decisive and shaping operations. 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.

5-3. The protection cell and working group monitor and evaluate several critical ongoing functions associated with execution for operational actions or changes that impact protection cell proponents, 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.
- Running estimates.
- Protection tasks.
- System failures.
- Resource allocations.
- Increased risks.

- Supporting efforts.
- Force protection implementation measures, including site-specific antiterrorism measures.

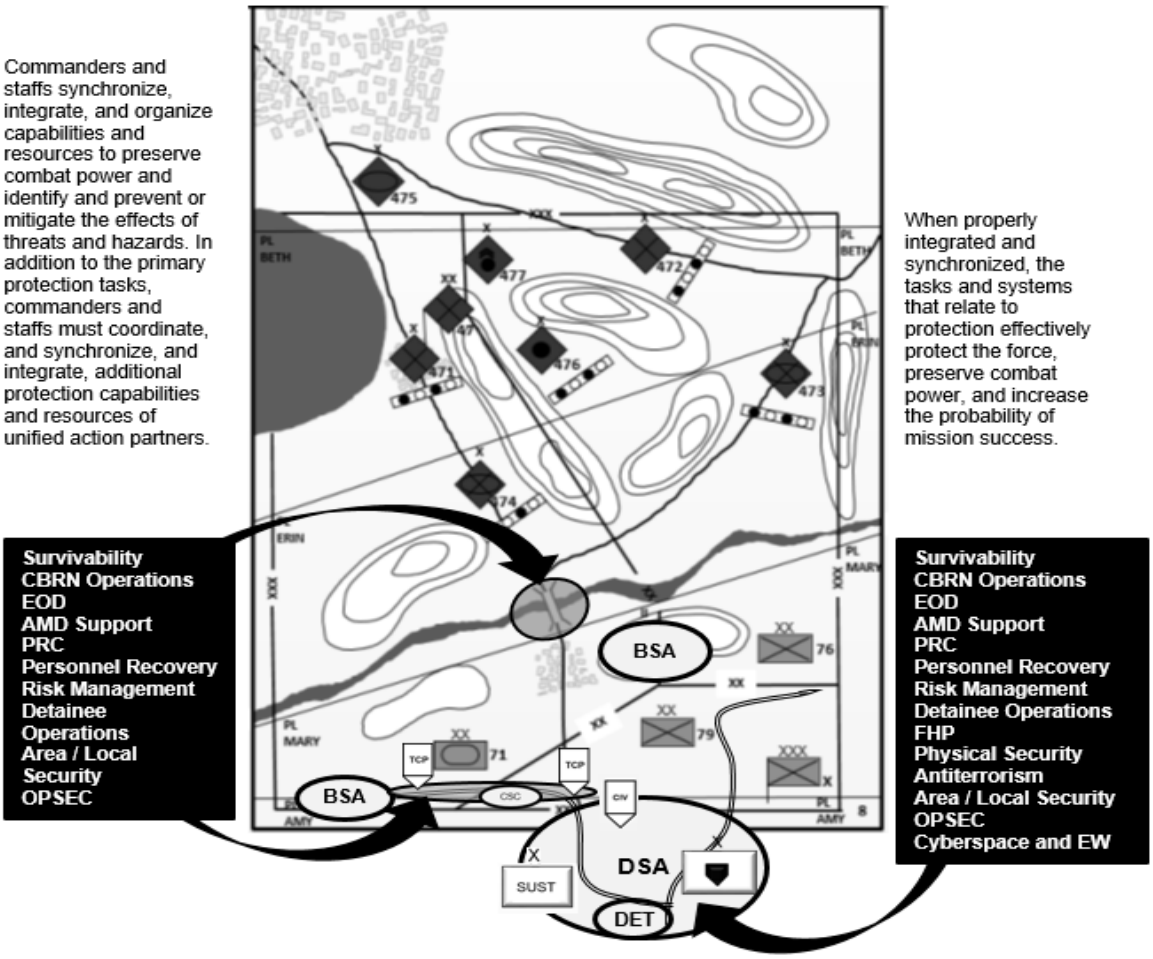
PROTECTION IN SUPPORT OF DECISIVE ACTION

5-4. In large-scale ground combat operations against a peer threat, commanders conduct decisive action to seize, retain, and exploit the initiative. *Decisive action* is the continuous, simultaneous execution of offensive, defensive, and stability operations or defense support of civil authority tasks (ADP 3-0). Operations conducted outside the United States and its territories simultaneously combine three elements—offense, defense, and stability. Within the United States and its territories, decisive action combines the elements of defense support of civil authorities and offense and defense to support homeland defense, when required.

5-5. Decisive action begins with the commander's intent and concept of operations. As a single, unifying idea, decisive action provides direction for the entire operation. Based on a specific idea of how to accomplish the mission, commanders and staffs refine the concept of operations during planning and determine the proper allocation of resources and tasks. Leaders must have a situational understanding in simultaneous operations due to the diversity of threats, the proximity to civilians, and the impact of information during operations. The changing nature of operations may require a surge of certain capabilities, such as protection, to effectively link decisive operations to shaping or stabilizing activities in the AO. In other operations, the threat may be less discernible, unlikely to mass, and immune to the center of gravity analysis, which requires a constant and continuous protection effort or presence.

5-6. Commanders must accept risk when exploiting time-sensitive opportunities by acting before adversaries discover vulnerabilities, take evasive or defensive action, and implement countermeasures. Commanders and leaders can continue to act on operational and individual initiative if they make better risk decisions faster than the enemy or adversary, ultimately breaking enemy or adversary will and morale through relentless pressure. Commanders can leverage information collection capabilities, such as geospatial intelligence products or processes, to minimize fratricide and increase the probability of mission accomplishment.

5-7. Accurate assessment is essential for effective decision making and the apportionment of combat power to protection tasks. Commanders fulfill protection requirements by applying comprehensive protection capabilities from main and supporting efforts to decisive and shaping operations. Protection can be derived inherently from combat operations (such as security operations), or it can be deliberately applied as commanders integrate and synchronize tasks and systems that comprise of the protection warfighting function in order to apply maximum combat power (see figure 5-1).



Legend:

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

Figure 5-1. Protection in support of large-scale ground combat

OFFENSE

5-8. An *offensive operations* is an operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers (ADP 3-0). Offensive operations impose the commander's will on the enemy or adversary. 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. In the offense, the decisive operation is a sudden, shattering action against an enemy or adversary weakness that capitalizes on speed, surprise, and shock. 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.

5-9. Characteristics of the offense include audacity, concentration, surprise, and rapid tempo. Effective offensive actions capitalize on accurate, predictive, and timely 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). Protection can be derived through audacity, concentration, surprise, or increased operating tempo. 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.

5-10. In offense, protection is applied carefully and selectively to ensure that it does not have a debilitating effect on a commander's freedom of action. This is accomplished through protection integration and synchronization. Protection tasks are integrated with other combat power elements and synchronized simultaneously or sequentially where and when significant threats and hazards are projected in the offensive plan.

5-11. 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, environmental factors including climatic injuries, infectious diseases, disease vectors and their control, education, mental health assessment, and dental hygiene. 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.

5-12. An enemy force may resort to the use of CBRN capabilities or scorched-earth techniques to delay, divert, or culminate an operation against it. Friendly CBRN reconnaissance and surveillance assets must be positioned and synchronized to allow commanders an early CBRN detection, identification, and avoidance capability that enables rapid and decisive movement and maneuver and the adjustment of mission-oriented protective posture levels while preparing for decontamination. Force health practitioners monitor offensive running estimates for the evidence of a deliberate or incidental epidemic.

5-13. Offensive operations are executed with an audacity, concentration, surprise, and operating tempo that 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 forces and supporters 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

5-14. Offensive operations, as well as protection posture, are further enabled through information operations 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 operations.) Measures taken to protect networks and computers from disruption and degradation can support and sustain the operating 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.

5-15. Increased operating tempo can result in combat identification errors and fratricide. Risk management must be integrated into every operation. Deliberate precautions are taken to prevent friendly fire incidents through positive and procedural control mechanisms, standard unit marking schemes and patterns, and sound navigation and reporting procedures.

5-16. Offensive operations conducted during large-scale ground combat operations will result in large numbers of detainees, categorized as EPWs. Entire enemy units separated and disorganized from shock and intense combat maybe captured. These large numbers of detainees will 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.

5-17. The protection of critical combat power systems requires survivability assets that alter the physical environment to provide or improve camouflage, cover, and concealment. Such terrain modifications may require significant amounts of time, making them infeasible for the protection of assets that must frequently

move to keep pace with operations. The protection of such assets can be enhanced by such measures as survivability moves, the maximum use of existing terrain, obscuration, and military deception. EOD focus on the elimination or reduction of the effects of explosive hazards in order to preserve combat power.

5-18. Air missile defense assets during offensive task can provide vital protection from air threats and contribute to the freedom of maneuver by friendly forces. Commanders coordinate and synchronize air missile defense assets for coverage over maneuver forces and their critical assets, to include denying surveillance by threat aerial platforms. Air missile defense assets also protect forward based infrastructure such as lines of communications and command nodes from aerial attack, determine, and predict and reporting ballistic missile launch points and impact points, and providing early warning and surveillance.

5-19. Area security operations support offensive operations by providing a response capability to base clusters 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. Bases/base camps employ local security measures (including EOD, assessments and recommendations, random AT measures, and increased FPCONs), but may be vulnerable to enemy or adversary remnant forces requiring a response that is beyond base camp capabilities. In support areas, commanders conduct area damage control to prevent and respond to the negative effects of enemy or adversary action that can diminish combat power.

DEFENSE

5-20. 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). Commanders can use the defense to gain time and economize forces so that offensive operations can be executed elsewhere. Defensive operations—

- Set conditions for a counteroffensive or counterattack that enables Army forces to regain the initiative.
- Serve as a counter to enemy offense operations.
- Defeat attacks, destroying as much of the attacking enemy as possible.
- Preserve and maintain control over land, resources, and populations.
- Retain terrain and guard populations and protect critical capabilities against enemy attacks.

5-21. No matter which defensive task is performed (area or 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 AT 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. In mature theaters or base camps, commanders plan and prepare for enemy attacks by predicting where the next attack will occur and then apply measures to mitigate the effectiveness of the attack. These attacks may be from conventional, irregular, or terrorist forces; and they drive changes in local FPCONs or individual protective measures. Incident management plans and area damage control in execution are key components to a successful protection plan. These plans cover all threat capabilities and environmental considerations, and they integrate protection tasks and systems. EOD assets and personnel support AT efforts on bases/base camps and in base clusters during defensive operations by providing vulnerability assessments, conducting postblast analysis/battle damage assessments, conducting render-safe procedures, and disposing of unexploded ordnance.

5-22. 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.

5-23. 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. Protection measures and tasks are applied within the principles of protection in the defense.

5-24. 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.

5-25. In the defense air missile defense assets optimize the protection of Soldiers by providing coverage over defended forces and other designated critical assets. Other air missile defense task in the defense include providing and disseminating early, situational awareness of airspace, contributing to targeting information determining/predicting and reporting enemy missile and launch points and impact points, and proactively engaging threat aerial platforms before they attack or surveil.

5-26. 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 indirect fire, even if exposure is for a short duration. Systems for combat stress identification and treatment are deliberately emplaced to reduce the return-to-duty time of affected personnel.

5-27. Defensive operations typically demand the most effort and resources for survivability. Activities in the defense include constructing survivability positions for command post, artillery, air and missile defense, and critical 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 unconventional threats (suicide bombings, vehicle-borne improvised explosive devices [VBIEDs], CBRN hazards). The relative amount of survivability effort placed against these threats depends on the threat analysis and the available resources.

5-28. Commanders integrate air defense 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 the hostile aerial targets and protecting friendly aerial assets. The deployed air defense systems defend friendly forces and critical assets from aerial attacks and bombardments. Commanders enforce the employment of passive air defense measures.

5-29. Units develop, train, and rehearse a CBRN defense plan to protect personnel and equipment from an attack or incident involving CBRN threats or hazards. CBRN threat and hazard assessments help determine initial, individual protective equipment levels and the positioning of decontaminants. Force health personnel maintain the medical surveillance of personnel strength information for indications of force contamination, epidemic, or other anomalies apparent in force health trend data.

5-30. 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 within the limits of their capabilities. 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.

5-31. Effective and disciplined OPSEC protects EEFI, preventing 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 preventing surprise during defensive operations. OPSEC and cyberspace and electronic warfare activities deny the enemy access to information systems and prevent network intrusion, degradation, or destruction through computer network defensive TTP. Electronic protection capabilities prevent an attacking enemy from using the electromagnetic spectrum to degrade, neutralize, or destroy friendly combat capabilities.

5-32. Personnel rest and recovery plans, leader experience, and skill levels are safety considerations that influence risk management decisions during large-scale ground 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 accidents and events.

STABILITY

5-33. 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, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADP 3-0). While *stability tasks* are tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADP 3-07).

5-34. Stability operations are used to support a host nation or interim government or a transitional military authority when no government exists. They involve coercive and constructive actions, help establish or maintain a safe and secure environment, and facilitate reconciliation among local or regional adversaries. Stability operations can also help establish political, legal, social, and economic institutions while supporting the transition to legitimate host nation governance. Stability operations cannot be successful if they are only used to react to enemy or adversary initiatives; they must also be used to maintain the initiative through the pursuit of objectives that resolve the causes of instability.

5-35. Military forces must quickly seize and retain the initiative when conducting stability operations by engaging civil mechanisms to prevent local conditions from destabilizing or deteriorating. Acting boldly can prevent organized resistance from developing while creating opportunities to reduce suffering, strengthen institutions, and begin the transition to civil authority. Bold initiatives during stability operations involve risk. The close proximity to civilians with immediate access to global information conduits can magnify the consequences of action, inaction, accidents, collateral damage, and casualties. Leaders must carefully balance lethal and nonlethal actions. Overcautious prevention activities or procedures can limit the freedom of action.

5-36. Fragile states suffer from institutional weaknesses that threaten the survival of their central government. (See FM 3-07 for additional information.) Stability strategies are developed to achieve conflict resolution by enhancing host nation legitimacy; developing civil institutions through capacity-building activities; addressing legitimate grievances; and progressing toward, or returning to, an equitable justice system and the rule of law. They support and reflect overarching national security, defense, and military strategies and policies and are eventually articulated within the framework of the campaign plan at the operational level. At this level, stability strategies often require the integration of operational and tactical tasks along the lines of effort that lead to the following end-state conditions:

- A safe and secure environment.
- Established rule of law.
- Social well-being.
- A stable government.
- A sustainable economy.

5-37. When conducting stability operations, protection is essential for success at all operating levels, from tactical to strategic. Like offensive and defensive operations, stability operations can derive some protection from the concept of operations alone, but the most sustainable protection success for the force is achieved by integrating the protection tasks that comprise the protection warfighting function. 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.

5-38. 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 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 minimum force necessary, which is consistent with the approved rules of engagement. The escalation of force TTP must also be rehearsed and be flexible enough to change with the local threat conditions. Collateral damage caused by military operations can negatively impact the mission and can support enemy or adversary

provocation tactics. Conversely, overly restrictive rules of engagement can limit the freedom of action and the ability to protect the force.

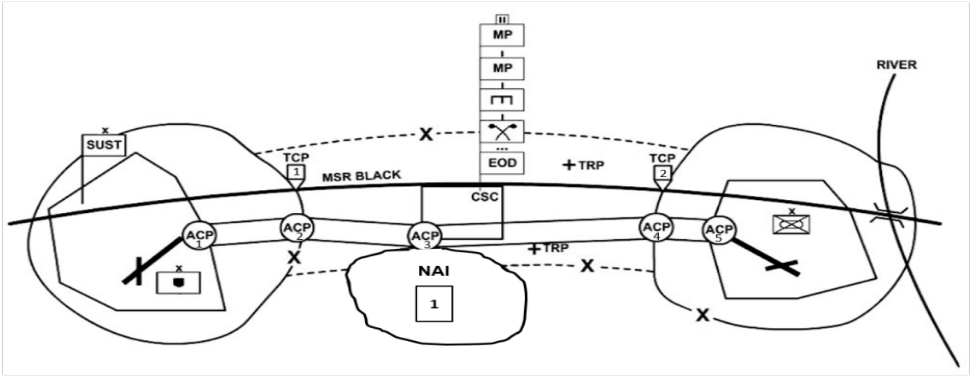
5-39. Army units should account for the protection of civilians from other hazards, in addition to their own direct and indirect fires. Particularly in counterinsurgency and when executing stability task situations, population support may be the center of gravity; and it is unlikely that support can be achieved if the population is not protected. Army units may be expected to take measures that protect civilians from enemy or adversary actions. AT measures should also account for the protection of civilians, as they are likely to become incidental casualties by deliberate attacks against soft and populated targets.

5-40. Civilian casualty mitigation is similar to fratricide avoidance, as both are intended to avoid casualties upon 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 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 mind-set regarding the avoidance of civilian casualties.

5-41. Stability operations and irregular warfare often involve 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 AT based on METT-TC.

5-42. 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 after participating in various atrocities.

5-43. Civil 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 contemplated by the enemy or adversary. Commanders may gradually apply protection to protect movement, or they may establish a movement corridor (see figure 5-2).



Legend:	
ACP	airspace control point
CSC	convoy support center
EOD	explosive ordnance disposal
MP	military police
MSR	main supply route
NAI	named area of interest
SUST	sustainment
TCP	traffic control post
TRP	target reference point

Figure 5-2. Sample movement corridor

5-44. Information operations is a key protection enabler. Information operations assists 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 improvised explosive device, 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.

5-45. The close proximity of civilians and Soldiers can also promote force health protection issues (such as communicable disease) through close contact with local civilians, detainees, 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.

5-46. The protection of civil institutions, processes, and systems that are required to reach the end-state conditions of the stability framework can often be the most decisive factor in operations because its accomplishment is essential for long-term success. For that reason, stability operations require a whole-of-government approach that sets the conditions necessary to enable the elements of national power (diplomatic, information, military, and economic). Stability operations tasks include—

- Establishing civil security.
- Establishing civil control.
- Restoring essential services.
- Providing support to governance.
- Providing support to economic and infrastructure development.
- Conducting security cooperation.

5-47. Information operations are also essential to the success of stability operations. Unified action and interagency participation are achieved by nesting the six stability tasks with the five stability sectors identified by the Department of State. To support stability operations, the scheme of protection is developed and refined to link stability and protection tasks to operational goals and end states. Stability operations and security sectors are integrated within the stability framework to help define and measure progress and to provide a context for conducting operations. The stability framework defines the environment according to two quantifiable, complementary scales—decreasing violence and increasing normalization of the state.

5-48. Protection schemes for stability operations often begin 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.

Civil Security

5-49. An initial response to operations conducted in an occupied territory or failing state may emphasize the establishment of civil security as a primary stability task. Establishing civil security is a means of protecting civilian resources, infrastructure, population facilities, and key personnel. When supporting a partner nation, border or boundary control operations protect the integrity and sovereignty of the host nation while providing protection against illegal entrants, contraband, disease, and the enemy or adversary. Border operations can be conducted to complement area defense operations or through area security tasks and TTP integrating checkpoints, mobile patrols, and designated fixed sites.

5-50. Civil security focuses on establishing a stable security environment and developing legitimate institutions and infrastructure to maintain that environment. While protecting the lives of local civilians from the violence of conflict and restoring the territorial integrity of the state, intervening forces stabilize the security environment. This stability allows for comprehensive reform efforts that are best accomplished by civilian personnel from other stakeholder agencies and organizations.

5-51. Stability operations in decisive action are often characterized by retaining the initiative. Tactical and nontactical movement occurs throughout the AO as a matter of military necessity and as a component of a normalized society. Controlling and maintaining the freedom of movement in the AO—

- Are essential for efficiency and for the protection of friendly military forces and the population.
- Can include various methods (curfews, routine restrictions, travel authorizations) that are enforced and monitored throughout checkpoints or technologies.
- May be accomplished through movement and maneuver enhancement, area security operations, or in conjunction with police operations as a function of traffic regulation enforcement.

5-52. Commanders should employ pattern analysis to identify patterns of activities, associations, and events within the AO. The basic premise of pattern analysis uses activities, associations, and events to identify irregularities to normal patterns (such as a market closing early for no observable reason) and to identify trends in the components of threat activities (such as similarities of time, geography, personnel, victims, techniques, and tactics). Information operations are often essential when implementing movement or traffic controls and restrictions on a given population in an AO. Through Soldier and leader engagement, the civil military operations center, or other outreach efforts, commanders can leverage host nation security, police, and civic organizations through security cooperation and partner activities to assist with the implementation of movement controls and traffic enforcement for the safety and security of the force and the local population. Response force operations that support troops engaged in controlling or limiting movement take deliberate precautions to prevent fratricide.

5-53. Establishing civil security involves providing for the safety of the host nation and its population, including protection from internal and external threats; it is essential to provide a safe and secure environment and gain the cooperation and support of the populace by building mutual trust. Until an interim authority can assume responsibility for governance, military forces perform the tasks associated with civil security. At the same time, they help develop host nation security forces (including police) capabilities and capacities related to security tasks. This type of assistance spans from individual training and education to unit exercises that involve training assistance to develop and train institutions and staffs. Building host nation capacity for civil security is paramount to establishing the foundation for lasting civil order. Community-oriented police services that are under civilian control and clearly separate the roles of the police and military are essential to success. As with host nation security forces, the development of police forces proves integral to providing a safe, secure environment for the local populace.

5-54. The protection of key personnel and facilities may be an essential task anywhere in the fragile-state spectrum or stability framework where there is a directed threat. Key civil leaders may require protective service details or police protection, and their work areas and homes may require the employment of additional physical security measures to ensure personal safety. Facilities that have national, cultural, religious, or military significance may need dedicated security to reduce civil tension. Police stations, armories, and hospitals may require immediate protection. Records and documentation for verifying identity and authority, deviant behavior, key governmental actions, and other important historical events and information may need to be protected from destruction and misuse. Explosive and CBRN threats and hazards may exist in the OE at the cessation of hostilities or may be introduced deliberately or accidentally. These threats and/or hazards may require an integrated EOD, demining, or foreign consequence management response.

Civil Control

5-55. Civil control regulates behavior in an AO and builds the foundation for order, justice, and the rule of law. There are a host of enforcement mechanisms in a given society to maintain normalcy and civil behavior, including law enforcement officials, local political and civic leaders, educators, clergy, and others who reflect and maintain local law, customs, norms, and values. Most civil societies follow some form of predictable social activity cycle, which often includes seasonal, ethnic, religious, or cultural events (holidays, school or academic periods, days of specific observance). The chief of protection examines the significance of each event for potential hazards, risks, and opportunities and applies the requisite protection capability. For example, religious holidays or pilgrimages may increase the number of third-world nationals entering the AO, while a national event could lead to the massing of civilians at key governmental locations. The end of the academic school period may mark an increase in the number of adolescents in the streets of certain regions.

5-56. Military forces may be initially engaged in conducting policing and penal operations to prevent criminal activity or to reduce crime-conducive conditions in a particular area. These activities protect communities from criminal predators who can have a chilling effect on populations and can destabilize specific areas. In these operations, military forces must be proficient in the escalation of force before resorting to lethal action within the rules of engagement. Nonlethal TTP and capabilities provide commanders with the ability to implement or initiate a scalable force response, which can contribute to the protection of the force and the civilian populace. The presence of well-trained, -equipped, and -disciplined Soldiers with lethal capability can often be sufficient to deter violence, confrontation, or conflict while conducting stability operations. However, the rules of engagement are tested by adversaries and the capability to respond first with nonlethal means and to escalate only as required serves the long-term objectives well. Law enforcement activities transition from military personnel to civilian police who are supplied by the host nation or as part of another nation or international policing effort. Police training, development, and mentoring may continue until normalization is achieved. (See ATP 3-39.10 for additional information on host nation police development.) Commanders may authorize, develop, and train civilian volunteers to augment civil control efforts or to serve as a police auxiliary.

5-57. To successfully provide for the safety and security of the populace, an effective judiciary branch and a functioning corrections system must complement state security institutions. (See ATP 3-07.6 for additional information on the protection of populations.) Together with governance and civil security, civil control is a core element of security sector reform. This reform establishes the foundation to enable the rule of law, government and economic reform, successful humanitarian relief, and social development.

5-58. As with other elements of the civil security and governance sectors, an appropriate authority assists the judiciary, police, and corrections staffs and oversees their activities as part of the security sector reform program. Conducted in parallel with other reform processes, near-term efforts focus on building host nation capacity by restoring the components of the justice system. Long-term development aims to institutionalize a rule-of-law culture within the government and society.

Essential Services

5-59. Areas that have been neglected or damaged as a result of conflict may require the protection of essential infrastructure. Power generation, water treatment, and medical and transportation facilities and systems may require protection from pilferage, sabotage, or neglect—which may be accomplished through physical security, survivability operations, or area security. Broadcast news, journalists, media outlets, and other information sources often adhere to a predictable media or news cycle. The chief of protection works with public affairs personnel to restore local media outlets and to anticipate the impact of negative or sensational broadcast media or other information releases to the force or in the OE. Inform activities involve significant Soldier and leader engagement with the local population as a means of informing the public while gathering information on the environment.

5-60. By integrating military and indigenous police forces while asserting transitional military authority, commanders obtain police- or street-level information on local criminal elements, including organized crime. When assisting an interim government or partner nation in foreign internal defense, commanders help establish a safe and secure environment for U.S. forces, partner nation forces, and civilians. Such multinational operations help build mutual trust between U.S. and partner nation forces and the populace while improving the perception of host nation government legitimacy. When no insurgent or terrorist threat exists, the integration of protection actions may be limited to safety and force health protection activities.

5-61. Efforts to restore essential services ultimately contribute to achieving stability, sustainable economic growth, and the social well-being of the population. This gives a sense of normalcy back to the population.

Governance Support

5-62. When U.S. forces are committed to a military intervention and as a result occupy territory, they may be required to assert transitional military authority and take a direct role in establishing military government until an interim civilian authority is established. Asserting transitional military authority includes conducting civic functions that are normally the responsibility of a civil government according to international law or mandate. Upon transition to interim civilian authority, military forces must be capable of providing support

to civil administrations. In either scenario, military forces may be required to protect the integrity of specific governmental processes. Elections normally follow a predictable cycle of activity that can be examined for evidence of corruption, election fraud, organized criminal involvement, or threat interference. Election events, voting sites, and ballots require protection and safe access to ensure the legitimacy of election results. International-election monitors or support personnel may also require some level of personnel protection. High-risk personnel, AT, and OPSEC plans and procedures should include considerations for the protection of key civil leaders.

Economic and Infrastructure Development

5-63. Protection capabilities are often applied to support economic and infrastructure developmental efforts to foster sustainability during stability operations. Building capacity within the economic sector often requires the protection of specific activities and conditions for local economies to thrive and develop. Business and economic activities typically follow a cycle. Agricultural economy cycles are often seasonal, coinciding with events such as agricultural harvests or conditions that make commodity gathering or production optimal. Industrial-based economy or market cycles may also be impacted by seasons when the change of seasons impacts the ability to transport resources. They may also be founded on a specific calendar, such as a fiscal calendar, which may dictate when investment and production occur. Each market has its own factors that influence its cycles—for example, clothing manufacturers, restaurants, and fish mongers. Each should be looked at separately and holistically from an economic perspective of the OE. These predictable events often telegraph other corresponding or supporting activities that may require protection from interference. Commodity markets can be influenced and manipulated, or commodity producers may be denied access to markets. Manufacturing facilities may be susceptible to illicit labor practices. Black markets can create shortages, while human trafficking may thrive due to underdeveloped economic conditions. Banks and other monetary institutions may require deliberate fixed-site or area security during periods of unrest and shortage or during a shoring-up of their digital security infrastructure.

5-64. Infrastructure development complements and reinforces efforts to stabilize the economy. It focuses on the physical aspects of the society that enable state economic viability. These physical aspects include construction services, engineering, and physical infrastructure in the following sectors:

- Transportation (roads, railways, airports, ports, waterways).
- Telecommunications.
- Energy (natural resources, electrical power).
- Municipal and other public services.

Security Cooperation

5-65. *Security cooperation* is all Department of Defense interactions with foreign security establishments to build security relationships that promote specific United States security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide United States forces with peacetime and contingency access to allied and partner nations (JP 3-22). The capacities and capabilities of partners directly correlate to the type of activities undertaken. Goals range from creating a positive relationship that allows freedom of movement to creating global security interoperability with core partners to addressing regional security organizations and alliance organizations. A broad range of interconnected and integrated security cooperation activities accomplishes security cooperation. (See ADP 3-0 and FM 3-22 for additional information.)

5-66. Security cooperation primarily focuses on interoperability programs with unified action partners and the security forces of a host nation or partner nation. The Army supports security cooperation through security assistance, security force assistance, foreign internal defense, and security sector reform.

5-67. Commanders must fully understand the threat environment in the operational area and employ measures to safeguard personnel and facilities that support security cooperation activities. Protection planning considerations should address additional support requirements for quick-reaction forces and personnel recovery and the requirement to integrate security force assistance personnel into the host nation protection plan. Insider threats during security cooperation activities are a major concern. Commanders should ensure that personnel are trained to identify behavioral indicators of possible insider threats and the

means to apply prevention tools to mitigate this threat. Cultural awareness yields situational awareness and leads to increased force protection for security force assistance personnel.

5-68. Another significant challenge during security cooperation activities is the need to deny critical information about friendly intentions, capabilities, and activities to hostile elements. The nature of security cooperation activities implies that many host nation officials and the populace will know of certain activities as they occur. Criminal and insurgent groups may have members or sympathizers within host institutions who act as formal informants, or there may be individuals within host institutions who are disinterested in protecting information for a cause they do not support. U.S. military and foreign personnel involved in security cooperation activities and programs should be provided extensive OPSEC training to ensure the effectiveness of their operations.

DEFENSE SUPPORT OF CIVIL AUTHORITIES

5-69. Defense support of civil authorities refers to support provided by U.S. military forces and DOD civilians, contractors, and component assets in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities or from qualifying entities for special events. Defense support of civil authorities includes tasks that address the consequences of natural or man-made disasters, accidents, terrorist attacks, and incidents in the United States and its territories. Army forces conduct defense support of civil authority tasks in support of homeland operations when the size and scope of events exceed the capabilities or capacities of domestic civilian agencies.

5-70. Leaders must understand the unique operational and mission variables associated with this complex OE and be able to rapidly transition—from conventional wartime terrain to the constraints inherent to the homeland—to contribute to prevention, protection, mitigation, response, and initial recovery from an assortment of threats and hazards. Commanders must operationally adapt to the characteristic blend of legal and policy challenges that have a distinctive effect on their freedom of action while operating in the homeland. In particular, leaders need to have a good understanding of the Posse Comitatus, information collection activities, and the standing rules for the use of force. The integration of Army capabilities into the guidance and parameters set forth by national policy requires the innovative integration of command and control and other warfighting functions to achieve a unity of effort. Commanders must be able to integrate and synchronize protection efforts with the lead federal agency or other governmental agencies. This results in protecting Soldiers in various duty statuses and civilian personnel from hostile actions while conducting defense support of civil authority tasks. The requirement to deploy into a constrained OE and operate with joint and interagency elements requires a unity of command and flexible Soldiers who are able to improvise and adapt systems originally intended for combat into robust, civilian disaster response systems that are based on the National Incident Management System.

5-71. Soldiers who are engaged in the defense support of civil authorities may face threats or hazards from criminals, outraged citizens, protestors, extremist groups, disease, the weather, structural instability, explosive ordnance hazards, or CBRN incidents. The tasks of safety, force health protection (preventive medicine), AT, and CBRN passive defense and consequence management are critical considerations for protecting deployed personnel and assets. The continual integration of the risk management process is vital in determining whether and how the commander provides defense support of civil authorities.

5-72. The CBRN response conducted by DOD in the U.S. homeland (with the exception of response conducted on federal installations) is a specialized type of defense support of civil authorities. DOD support is tailored to the scope and magnitude of the incident. DOD assets are employed, with a focus on response requirements beyond the resources of state and federal civil authorities. The purpose is to save lives; prevent injury; and provide temporary, critical life support. CBRN response consists of tiered response packages that support state and federal authorities.

5-73. Force health protection capabilities may support the preservation of life within the framework of the National Disaster Medical System. The National Disaster Medical System combines federal and nonfederal medical resources into a unified medical response system for incidents involving public health and medical emergencies. Under the auspices of the Department of Health and Human Services, the National Disaster Medical System facilitates the deployment of various medical response teams to an incident area. The Army response to this effort may include the formation of a medical task force or the deployment of specialized

expertise. The Army medical response to disasters is coordinated by U.S. Army North in conjunction with DOD medical commands. Larger events might require a functional task force, such as a medical task force, to conduct medical evacuation, triage, treatment, and public health and medical surveillance.

5-74. It may be necessary for DOD to augment civil air space management assets and capabilities when their effectiveness has been so significantly degraded that the probability of a catastrophic aviation event is high. The Air Component Command to the U.S. Northern Command has the capabilities to provide support to civil aviation and to deconflict the complexities of operations involving air assets from multiple organizations.

Chapter 6
Protection Assessment

Protection assessment is an essential activity that continuously occurs throughout the operations process. While a failure in protection is typically easy to detect, the successful application of protection may be difficult to assess and quantify.

CONTINUOUS ASSESSMENT

6-1. *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 help commanders determine progress toward attaining the desired end state, achieving objectives, and performing tasks. It also involves continuously monitoring and evaluating the OE to determine what changes might affect the conduct of operations.

6-2. Throughout the operations process, commanders integrate their assessments with those of the staff, 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. These estimates are used by commanders to maintain situational understanding and direct adjustments. Significant changes or variances among or within running estimates can signal a threat or an opportunity, alerting commanders to take action.

6-3. The assessment plan is enabled by monitoring and evaluating criteria derived from the warfighting function protection 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 commander's critical information requirements and the EEFI 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

6-4. The staff conducts analyses to assess threats, hazards, criticality, vulnerability, and capability to assist commanders in determining protection priorities, task organization decisions, and protection task integration.

6-5. Members of the protection cell evaluate COAs during the 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 ACTIVITIES

6-6. Assessment occurs during preparation, operations to shape, and operations to prevent 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.

6-7. During preparation, operations to shape, and operations to prevent, 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

6-8. 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 they 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 in 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.

6-9. 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 AT measures.
- OPSEC measures and countermeasures.

MEASURES OF EFFECTIVENESS AND PERFORMANCE

6-10. Criteria in the forms of MOEs and MOPs help 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

6-11. A *measure of effectiveness* is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (JP 3-0). 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 OE. 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.

6-12. Significant changes in some conditions of the OE are subtle and only occur over a long period of time; however, protection activities must be continual. The enduring nature of protection can cause complacency or inattentiveness, requiring leaders to stay focused on determining, monitoring, and evaluating accurate protection indicators and warnings that maintain situational understanding and alert them to hazards and associated risk.

6-13. Commanders monitor MOEs and evaluate variances and change indicators for cause and effect to forecast failure or to identify a critical point of failure in an activity or operation. Based on this assessment, resources can be reassigned to mitigate the overall risk to the mission or to support or reinforce specific local security efforts. The goal is to anticipate the need for action before failure occurs, rather than react to an unplanned loss. Thorough staff planning during the MDMP allows commanders to accelerate decision making by preplanning responses to anticipated events through the use of battle drills, branches, and sequels. War-gaming critical events also allows commanders to focus their critical information requirements and the supporting information collection effort. Information developed during this process can be used to develop EEFI and indicators or warnings that relate to the development of protection priorities.

6-14. If an action 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 in the anticipated threat-combat power ratio, resulting in an increased risk equation.
- Ineffective supporting efforts, leading to a cumulative failure of more critical elements.

6-15. 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 protection criteria. This assessment ensures that facts and assumptions remain valid and also identifies new facts and assumptions. Assessment decreases reaction time by anticipating future requirements and linking them to current plans.

Measure of Performance

6-16. A *measure of performance* is a criterion used to assess friendly actions 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. A 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

6-17. The manner 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 at all levels ensure that Soldiers and equipment are combat-ready. 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 approved lessons learned and TTP 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. Postoperational 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. For example, determine if the controls positively or negatively impacted training or mission accomplishment and determine if they supported existing doctrine and TTP.

- Assess the implementation, execution, and communication of controls.
- 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 benefit, or time?
  - Was the process cyclic and continuous throughout the operation?

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
AR	Army regulation
AFTTP	Air Force tactics, techniques, and procedures
AO	area of operations
AT	antiterrorism
ATP	Army techniques publication
attn	attention
CAL	critical asset list
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CBRN	chemical, biological, radiological, and nuclear
COA	course of action
DA	Department of the Army
DAL	defended asset list
DC	District of Columbia
DOD	Department of Defense
DODI	Department of Defense instruction
DODIN-A	Department of Defense information network–Army
DOTD	Directorate of Training and Doctrine
EEFI	essential elements of friendly information
EOD	explosive ordnance disposal
FM	field manual
FPCON	force protection condition
G-3	Assistant Chief of Staff
JP	joint publication
MCRP	Marine Corps reference publication
MCWP	Marine Corps warfighting publication
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MO	Missouri
MOE	measure of effectiveness
MOP	measure of performance
MSCOE	Maneuver Support Center of Excellence

MSHARPP	mission, symbolism, history, accessibility, recognizability, population, and proximity
NTTP	Navy tactics, techniques, and procedures
OE	operational environment
OPSEC	operations security
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
TTP	tactics, techniques, and procedures
U.S.	United States
USC	United States Code
WMD	weapons of mass destruction

SECTION II—TERMS

adversary

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

area security

A security task conducted to protect friendly forces, installations, routes, and actions within a specific area. (ADP 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)

base defense

The local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base, to ensure that the maximum capacity of its facilities is available to United States forces. (JP 3-10)

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)

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 3-07.2)

***critical asset security**

The protection and security of personnel and physical assets or information that is analyzed and deemed essential to the operation and success of the mission and to resources required for protection.

cyberspace

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12[R])

cyberspace electromagnetic activities

The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. (ADP 3-0)

decisive action

The continuous, simultaneous execution of offensive, defensive, and stability operations or defense support of civil authorities tasks. (ADP 3-0)

defensive cyberspace operations

Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. (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)

electronic attack

Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-13.1)

electronic protection

Division of electronic 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 3-13.1)

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

enemy

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

force protection

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

***fratricide**

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

friendly

A contact positively identified as a friend using identification, friend or foe and other techniques. (JP 3-01)

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)

high-risk personnel

Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. (JP 3-07.2)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting threat effects. (ADP 3-0)

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

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)

large-scale ground combat operations

The sustained combat operations involving multiple corps and divisions (ADP 3-0).

local security

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

measure of effectiveness

A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 3-0)

measure of performance

A criterion used to assess friendly actions that is tied to measuring task accomplishment. (JP 3-0)

***movement corridor**

A designated area established to protect and enable ground movement along a route.

offensive operation

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

operational environment

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

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)

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 and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission. (ADP 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)

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)

security cooperation

All Department of Defense interactions with foreign security establishments to build security relationships that promote specific United States security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide United States forces with peacetime and contingency access to allied and partner nations. (JP 3-20)

stability operation

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

stability tasks

Tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADP 3-07)

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/MCTP 3-34C)

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)

This page intentionally left blank.

References

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. June 2019.

ADP 1-02. *Terms and Military Symbols.* 14 August 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT

Most joint publications are available online at <http://www.jcs.mil/doctrine/>.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment.* 21 May 2014.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-01. *Countering Air and Missile Threats*. 21 April 2017.

JP 3-07.2. *Antiterrorism.* 14 March 2014.

JP 3-10. *Joint Security Operations in Theater*. 13 November 2014.

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

JP 3-12. *Cyberspace Operations.*8 June 2018.

JP 3-13. *Information Operations.* 27 November 2012.

JP 3-13.1. *Electronic Warfare.* 8 February 2012.

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

JP 3-20. *Security Cooperation.* 23 May 2017.

JP 3-22. *Foreign Internal Defense.* 17 August 2018.

JP 3-33. *Joint Task Force Headquarters.* 31 January 2018.

JP 3-41. *Chemical, Biological, Radiological, and Nuclear Response.* 9 September 2016.

JP 6-01. *Joint Electromagnetic Spectrum Management Operations.* 20 March 2012.

ARMY

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

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

ADP 3-07. *Stability.* 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.

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

AR 525-2. *The Army Protection Program.* 8 December 2014.

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 (U).* 11 December 2015.

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

ATP 3-07.6. *Protection of Civilians.* 29 October 2015.

ATP 3-13.3. *Army Operations Security for Division and Below.* 17 June 2019.

ATP 3-37.2. *Antiterrorism.* 3 June 2014.

ATP 3-39.10. *Police Operations.* 26 January 2015.

ATP 3-39.30. *Security and Mobility Support.* 30 October 2014.

ATP 3-39.32. *Physical Security.* 30 April 2014.

ATP 3-39.35. *Protective Services.* 31 May 2013.

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

ATP 4-02.8. *Force Health Protection.* 9 March 2016.

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.* 14 April 2014.

ATP 6-02.70. *Techniques for Spectrum Management Operations*. 31 December 2015.

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

FM 3-0. *Operations.* 6 October 2017

FM 3-01. *U.S. Army Air and Missile Defense Operations.* 2 November 2015.

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

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

FM 3-12. *Cyberspace and Electronic Warfare Operations.* 11 April 2017.

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

FM 3-22. *Army Support to Security Cooperation.* 22 January 2013.

FM 3-27. *Army Global Ballistic Missile Defense Operations.* 31 March 2014.

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

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

FM 3-63. *Detainee Operations.* 28 April 2014.

FM 3-81. *Maneuver Enhancement Brigade.* 21 April 2014.

FM 4-02. *Army Health System.* 26 August 2013.

FM 6-0. *Commander and Staff Organization and Operations.* 5 May 2014.

FM 6-02. *Signal Support to Operations*. 22 January 2014.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

MULTI-SERVICE

ATP 3-11.32/MCWP 10-10E.8/NTTP 3-11.37/AFTTP 3-2.46. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Passive Defense.* 13 May 2016.

ATP 3-11.36/MCRP 10-10E.1/NTTP 3-11.34/AFTTP 3-2.70. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Planning.* 24 September 2018.

ATP 3-34.20/MCRP 3-17.2D. *Countering Explosive Hazards.* 21 January 2016.

ATP 3-37.34/MCTP 3-34C. *Survivability Operations.* 16 April 2018.

ATP 3-90.4/MCWP 3-17.8. *Combined Arms Mobility.* 8 March 2016.

ATP 4-01.45/MCRP 3-40F.7 [MCRP 4-11.3H]/AFTTP 3-2.58. *TCO Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations*. 22 February 2017.

OTHER

DODI O-2000.16, Volume 1. *DOD Antiterrorism (AT) Program Implementation: DOD AT Standards.* 17 November 2016. <https://www.esd.whs.mil/Directives/issuances/dodi>, accessed on 17 June 2019.

DODI 8500.01. *Cybersecurity.* 14 March 2014. <https://www.esd.whs.mil/Directives/issuances/dodi>, accessed 17 June 2019.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Web site at <https://armypubs.army.mil.>

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

RECOMMENDED READINGS

ATP 3-11.41/MCRP 3-37.2C/NTTP 3-11.24/AFTTP 3-2.37. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Consequence Management Operations.* 30 July 2015.

ATP 3-36. *Electronic Warfare Techniques.* 16 December 2014.

DODI O-2000.16, Volume 2. *DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System*. 17 November 2016. <https://directives.whs.mil/issuances/O200016v2_dodi_2016.pdf,> accessed on 17 June 2019.

DODI 6055.17. *DOD Emergency Management (EM) Program.* 13 February 2017. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/605517p.pdf?ver=2018-11-21-081404-563,> accessed on 17 June 2019.

FM 2-0. *Intelligence*. 6 July 2018.

FM 3-52. *Airspace Control.* 20 October 2016.

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

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

JP 2-0. *Joint Intelligence.* 22 October 2013.

JP 3-08. *Interorganizational Cooperation.* 12 October 2016.

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

JP 3-28. *Defense Support of Civil Authorities.* 29 October 2018.

JP 3-50. *Personnel Recovery.* 2 October 2015.

JP 3-52. *Joint Airspace Control*. 13 November 2014.

JP 6-0. *Joint Communications System*. 10 June 2015.

18 USC 1385. *Use of Army and Air Force as Posse Comitatus*.

http://uscode.house.gov/view.xhtml?req=(title:18 section:1385 edition:prelim), accessed on 17 June 2019.

This page intentionally left blank.

Index

Entries are by paragraph number.

This page intentionally left blank.

ADP 3-37

31 July 2019

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1919103

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: To be distributed in accordance with the initial distrubution number (IDN) 110502, requirements for ADP 3-37.

This page intentionally left blank.

PIN: 102965-000