



# ADRP 3-37 PROTECTION



**AUGUST 2012**

**DISTRIBUTION RESTRICTION:**

Approved for public release; distribution is unlimited.

**HEADQUARTERS, DEPARTMENT OF THE ARMY**

This publication is available at Army Knowledge Online  
(<https://armypubs.us.army.mil/doctrine/index.html>).

Army Doctrine Reference Publication  
No. 3-37

Headquarters  
Department of the Army  
Washington, DC, 31 August 2012

# Protection

## Contents

	<b>Page</b>
<b>PREFACE.....</b>	iii
<b>INTRODUCTION .....</b>	iv
<b>Chapter 1 PROTECTION FRAMEWORK.....</b>	<b>1-1</b>
Protection Principles.....	1-1
Protection in Support of Unified Land Operations.....	1-1
Operational Environment.....	1-2
Protection Warfighting Function .....	1-2
Supporting Tasks.....	1-3
Tasks and Systems Integration .....	1-14
<b>Chapter 2 PROTECTION PLANNING .....</b>	<b>2-1</b>
Initial Assessments.....	2-1
Integrating Processes.....	2-1
Threats and Hazards .....	2-2
Critical and Defended Asset Lists .....	2-6
Scheme of Protection Development.....	2-7
Protection Priorities .....	2-8
Running Estimate .....	2-8
Protection Cell and Working Group.....	2-9
<b>Chapter 3 PROTECTION IN PREPARATION .....</b>	<b>3-1</b>
Considerations.....	3-1
Protection Within Preparation Activities .....	3-2
Protection Cell and Working Group.....	3-3
<b>Chapter 4 PROTECTION IN EXECUTION .....</b>	<b>4-1</b>
Protection in Unified Land Operations.....	4-1
Protection Cell and Working Group.....	4-13
<b>Chapter 5 PROTECTION ASSESSMENT .....</b>	<b>5-1</b>
Continuous Assessment.....	5-1
Assessment During Planning .....	5-1
Assessment During Preparation.....	5-2

---

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

\*This publication supersedes FM 3-37, dated 30 September 2009.

## **Contents**

---

Assessment During Execution .....	5-2
Measures of Effectiveness and Performance .....	5-2
Lessons Learned Integration .....	5-3
<b>GLOSSARY .....</b>	<b>Glossary-1</b>
<b>REFERENCES.....</b>	<b>References-1</b>
<b>INDEX .....</b>	<b>Index-1</b>

## **Figures**

Introductory Figure-1. Protection within the operations process .....	vi
Figure 2-1. Risk management process .....	2-2
Figure 2-2. Sample protection running estimate .....	2-9
Figure 4-1. Sample movement corridor .....	4-6
Figure 4-2. Whole-government, integrated approach to stability .....	4-7
Figure 4-3. Stability framework .....	4-8
Figure 4-4. Freedom-of-movement control .....	4-9

## **Tables**

Introductory Table-1. New Army terms .....	v
Introductory Table-2. Modified Army terms .....	v
Table 2-1. Potential threats and hazards .....	2-4
Table 2-2. Protection working group actions .....	2-12

## Preface

Army Doctrine Reference Publication (ADRP) 3-37 provides guidance on protection and the protection warfighting function. It also provides the guiding protection principles for commanders and staffs who are responsible for planning and executing protection in support of unified land operations. ADRP 3-37 corresponds with the Army operations doctrine introduced in ADP 3-0 and the protection principles in ADP 3-37.

The principal audience for ADRP 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. Trainers and educators throughout the Army will also use this manual.

ADRP 3-37 outlines how protection is synchronized and integrated to preserve combat power, populations, partners, essential equipment, resources, and critical infrastructure from the effects of threats and hazards. The protection warfighting function enables commanders to preserve force combat power by integrating protection capabilities within operations. It explains how protection can be achieved and applied through the combination and integration of reinforcement and complementary capabilities.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable U.S., international and, in some cases, host nation laws and regulations. All commanders ensure that Soldiers operate according to the law of war and the rules of engagement (see FM 27-10).

ADRP 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 ADRP 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 in the next revision of ADRP 1-02.

---

**Note.** For the purposes of this publication, the terms *threat* and *range of threats* include enemies and adversaries.

---

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

The proponent and preparing agency for ADRP 3-37 is Headquarters, U.S. Army Maneuver Support Center of Excellence. Send comments and recommendations on Department of the Army (DA) Form 2028 (*Recommended Changes to Publications and Blank Forms*) directly to Commander, U.S. Army Maneuver Support Center of Excellence, ATTN: ATSN-Z, 464 MSCOE Loop, Suite 2617, Fort Leonard Wood, MO 65473. Submit an electronic DA Form 2028 or comments and recommendations in the DA Form 2028 format by e-mail to <[usarmy.leonardwood.mscOE.mbx.cdidcodddcbrndoc@mail.mil](mailto:usarmy.leonardwood.mscOE.mbx.cdidcodddcbrndoc@mail.mil)>.

## Introduction

ADRP 3-37 is a new publication that expands on the protection principles found in ADP 3-37. The doctrine described in this publication is nested within ADRP 3-0 and describes protection as a continuing activity and a warfighting function. It presents overarching doctrinal guidance and direction for conducting protection within unified land operations. ADRP 3-37 provides emphasis to Soldiers, leaders, and organizations on integrating protection capabilities into the operations process in order to identify, prevent, or mitigate the effects of threats and hazards. Overall, ADRP 3-37 remains consistent with previous doctrine. This manual modifies the current protection definition by aligning it with the joint definition of *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 (Joint Publication [JP] 3-0). The protection principle of “full dimension” is replaced with “comprehensive,” which expands on the definition of an all-inclusive utilization of complementary and reinforcing protection tasks and systems available to commanders, incorporated into the plan, to preserve the force. The protection warfighting function is updated to exemplify the tasks and systems that are synchronized and integrated throughout the operations process and with the other elements of combat power to preserve the force so that the commander can apply maximum combat power to accomplish the mission (introductory tables 1 through 3):

- “Air and missile defense” was modified. “Coordinate air and missile defense” is within the protection warfighting function, and “conduct air and missile defense” is within the fires warfighting function. Coordinating air and missile defense protects the force from missile attack, air attack, and aerial surveillance.
- The definition of fire support now includes air missile defense (see ADP 3-09 and ADRP 3-09).
- “Information protection” is now within the mission command warfighting function (see ADP 6-0 and ADRP 6-0).
- “Conduct operational area security,” “implement physical security procedures,” “conduct law and order,” and “conduct internment and resettlement” were added to the protection warfighting function. “Conduct internment and resettlement” moved from the sustainment warfighting function.
- “Fratricide avoidance” was incorporated into “employ safety techniques (including fratricide avoidance)” within the protection warfighting function.

The joint protection function tasks and key considerations in JP 3-0 are not directly aligned, one for one, with the Army protection warfighting function tasks, but they are integrated in how the Army operates. A shared understanding and purpose of the joint protection function allows Army leaders to integrate their actions within the unified action and to synchronize operations. The joint protection function focuses on preserving the joint force fighting potential in four primary ways:

- Active defensive measures to protect the joint force, its information, its bases/base camps, critical infrastructure, and lines of communications from an enemy or adversary attack.
- Passive defensive measures to make friendly forces, systems, and facilities difficult to locate, strike, and destroy.
- 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.

---

**Note.** See JP 3-0 for additional information on the joint protection function, its tasks, and key considerations.

---

The protection warfighting function, the Army Protection Program, and force protection are important aspects of protection that reinforce each other:

- 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 (ADRP 3-0).
- The Army Protection Program is a management framework to synchronize, prioritize, and coordinate protection policies and resources (see Army Directive 2011-04). It includes the twelve non-warfighting functional elements:
  - Emergency management.
  - Computer network defense.
  - Continuity of operations.
  - Critical infrastructure risk management.
  - Operations security (OPSEC).
  - Antiterrorism (AT).
  - Fire and emergency services.
  - Force health protection.
  - High-risk personnel.
  - Law enforcement.
  - Information assurance.
  - Physical security.
- *Force protection* is preventative measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information (JP 3-0).

The protection warfighting function supports unified action and unified land operations, whereas the Army Protection Program manages and executes the programs within the non-warfighting functional elements. Additionally, the protection warfighting function focuses on preserving the force and protecting personnel (friendly combatants and noncombatants) and physical assets of the United States and unified action partners. The complementary capabilities within the non-warfighting elements and the protection warfighting function assist in reinforcing protection throughout.

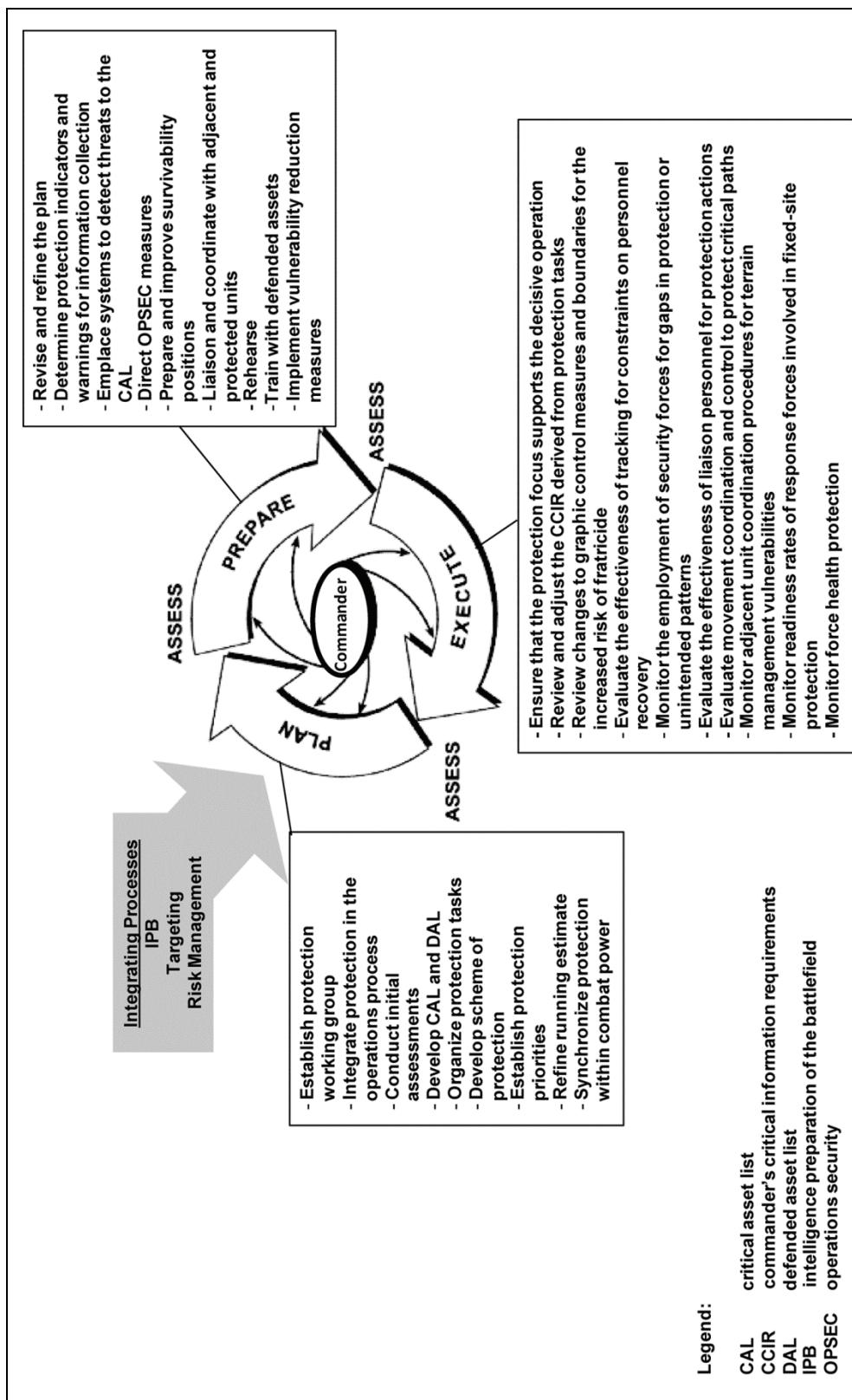
The chapters within this manual expound on the protection framework (chapter 1) and protection integration and synchronization throughout the operations process (chapters 2 through 5). Chapter 1 provides a common understanding of protection principles, protection nesting within unified land operations, the protection warfighting function, and the integration of the protection warfighting function tasks and systems. Chapters 2 through 5 elaborate on protection within the operations process—plan, prepare, execute, and assess (introductory tables 1 and 2) (introductory figure 1, page vi).

**Introductory Table-1. New Army terms**

<b>Term</b>	<b>Remarks</b>
critical asset security	New term and definition.
fratricide	New term and definition.

**Introductory Table-2. Modified Army terms**

<b>Term</b>	<b>Remarks</b>
protection	Adopts the joint definition.



Introductory Figure-1. Protection within the operations process

## Chapter 1

# Protection Framework

Commanders and staffs synchronize, integrate, and organize capabilities and resources throughout the operations process to preserve combat power and the freedom of action and to mitigate the effects of threats and hazards. Protection safeguards the force, personnel (combatants and noncombatants), systems, and physical assets of the United States and unified action partners. Survivability refers to the capacity, fitness, or tendency to remain alive or in existence. For the military, survivability is about much more than mere survival—it is also about remaining effective. Military forces are composed of personnel and physical assets, each having their own inherent survivability qualities or capabilities that permit them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission. These inherent qualities or capabilities are affected by various factors (dispersion, redundancy, morale, leadership, discipline, mobility, situational understanding, terrain and weather conditions) and can be enhanced by tasks within the protection warfighting function.

## PROTECTION PRINCIPLES

1-1. The following principles of protection provide military professionals with a context for implementing protection efforts, 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, incorporated into the plan, to preserve the force.
- **Integrated.** Protection is integrated with other activities, systems, efforts, and capabilities associated with unified land operations to provide strength and structure to the overall effort. Integration must occur vertically and horizontally with unified action partners throughout the operations process.
- **Layered.** Protection capabilities are arranged using a layered approach to provide strength and depth. Layering reduces the destructive effect of a threat or hazard through the dispersion of energy or the culmination of the force.
- **Redundant.** Protection efforts are often redundant anywhere that a vulnerability or a critical point of failure is identified. Redundancy ensures that specific activities, systems, efforts, and capabilities that are critical for the success of the overall protection effort have a secondary or auxiliary effort of equal or greater capability.
- **Enduring.** Protection capabilities are ongoing activities for maintaining the objectives of preserving combat power, populations, partners, essential equipment, resources, and critical infrastructure in every phase of an operation.

## PROTECTION IN SUPPORT OF UNIFIED LAND OPERATIONS

1-2. The synchronization, integration, and organization of capabilities and resources to preserve combat power from the effects of threats and hazards are essential. The ability to protect and preserve the force and secure the area of operations is vital in seizing, retaining, and exploiting the initiative. Protection emphasizes the importance of planning and expanding our protection priorities, to include protecting unified action partners, civilian populations, equipment, resources, infrastructure, and cultural landmarks across the range of military operations. It focuses on adapting our force to better leverage, integrate, and

synchronize unified action capabilities and better understand operational environments. It emphasizes the need for Soldiers, leaders, and organizations to identify, prevent, or mitigate threats and hazards. Mutually supporting and overlapping protection capabilities through operational and tactical level actions better position forces to defend, respond, and recover from threat and hazard effects and to deter, counterattack, neutralize, and defeat the threats.

## **OPERATIONAL ENVIRONMENT**

1-3. An operational environment includes physical areas (air, land, maritime, and space domains) and the information environment (including cyberspace). An operational environment for any specific operation is not only isolated conditions of interacting variables that exist within a specific area of operations, but 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 operational environment.

1-4. Emerging operational environments are uncertain. They are marked by rapid change and a wide range of threats and hazards that will provide significant challenges for military forces. Commanders must also be aware of personnel within their own force who are authorized access to Department of Defense (DOD) facilities, systems, equipment, information, or infrastructure and who may want to maliciously cause damage, disrupt operations, commit espionage, or support a terrorist organization. This threat poses a significant risk to protection. Protection preserves the combat power potential and survivability of the force by providing capabilities to identify and prevent the threats and hazards or mitigate their effects.

1-5. Commanders and leaders charged with providing or ensuring protection must begin with a thorough understanding of the operational environment, 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 operational environment. To support military operations, 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 doctrine recognizes the need to understand sociocultural factors, which are key to understanding populations proximate to friendly forces (see JP 2-01.3).

## **PROTECTION WARFIGHTING FUNCTION**

1-6. 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. Preserving the force includes protecting personnel (combatants and noncombatants) and physical assets of the United States and unified action partners. The protection warfighting function enables commanders to preserve force integrity and combat power by integrating protection capabilities to safeguard bases, secure routes, and protect forces.

1-7. Combat power has eight elements:

- Leadership.
- Information.
- Mission command.
- Movement and maneuver.
- Intelligence.
- Fires.
- Sustainment.
- Protection.

1-8. Commanders incorporate protection when they understand and visualize capabilities available for protection. Some of these actions or effects may be achieved through the combined integration of the

elements of combat power, resulting in an increasingly effective and efficient scheme of protection. They may also be achieved through the integration of specialized capabilities, such as space-based capabilities that help commanders visualize the operational environment.

1-9. Commanders must deliberately plan and integrate the application of military force against an enemy or adversary while protecting the force and preserving combat power. Operational and functional concepts are translated through the warfighting functions into tasks for the development of plans, orders and, ultimately, unit missions. Commanders develop protection systems for each phase of an operation or major activity. They integrate and synchronize 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 protect the force, enhance the preservation of combat power, and increase the probability of mission success.

## SUPPORTING TASKS

1-10. Supporting tasks of the protection warfighting function include—

- Conduct operational area security.
- Employ safety techniques (including fratricide avoidance).
- Implement OPSEC.
- Provide intelligence support to protection.
- Implement physical security procedures.
- Apply AT measures.
- Conduct law and order.
- Conduct survivability operations.
- Provide force health protection.
- Conduct chemical, biological, radiological, and nuclear (CBRN) operations.
- Provide explosive ordnance disposal (EOD) and protection support.
- Coordinate air and missile defense.
- Conduct personnel recovery.
- Conduct internment and resettlement.

## CONDUCT OPERATIONAL AREA SECURITY

1-11. The task of conducting operational area security is a form of security operations conducted to protect friendly forces, installations, routes, and actions within an area of operations. Forces engaged in operational area security protect the force, installation, route, area, or asset. Although vital to the success of military operations, operational 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.

1-12. Operational area security may be the predominant method of protecting support areas that are necessary to facilitate the positioning, employment, and protection of resources required to sustain, enable, and control forces. Operational area security is often an effective method of providing civil security and control during some stability operations. Forces engaged in operational 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. Operational area security often focuses on named areas of interest in an effort to answer commander's critical information requirements, aiding in tactical decisionmaking and confirming or denying threat intentions. Forces engaged in operational area security are typically organized in a manner that emphasizes their mobility, lethality, and communications capabilities. The maneuver enhancement brigade and some military police units are specifically equipped and trained to conduct operational area security and may constitute the only available force during some phases of an operation. However, operational area security takes advantage of the local security measures performed by all units, regardless of their location in the area of operations.

1-13. All commanders apportion combat power and dedicate assets to protection tasks and systems based on an analysis of the operational environment, 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 significant 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 decisionmaking, 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 operational area security. Operational area security often focuses on the following activities:

- **Base/base camp defense.** *Base defense* is 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 U.S. forces (JP 3-10). A division or corps may be required to protect multiple bases or base camps. Units may be assigned base defense operations 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 Army doctrine pertaining to protective services for more information.)
- **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 combined arms 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 area of operations. (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 since 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 area of operations. 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 3-90). 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 it may be an enduring operation.
- **Checkpoints and combat outposts.** It is often necessary to control the freedom of movement in an area of operations 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 Army Tactics, Techniques, and Procedures [ATTP] 3-90.4 for more information on combat outposts.)

- **Convoy security.** A *convoy security operation* is a specialized kind of area security operations conducted to protect convoys (FM 3-90). Units conduct convoy security operations anytime there are insufficient friendly forces to continuously secure routes in an area of operations and there is a significant danger of enemy or adversary ground action directed against the convoy. Commanders may also conduct convoy security operations in conjunction with route security operations. 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 or which convoys receive security and protection. (See FM 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 area of operations 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 more information on port security units.)
- **Area damage control.** Commanders conduct area damage control when the damage and scope of the attack are limited and they can respond and recover with local assets and resources. Optimally, commanders aim to recover immediately. This involves resuming operations; maintaining or restoring order; administering first aid; searching and rescuing entrapped, sick, and injured personnel; evacuating casualties; isolating danger or hazard areas; and mitigating personnel and materiel losses. Some attacks may rise to the level of national significance and require additional resources for mitigation, recovery, and investigation. (See Army doctrine pertaining to area damage control for more information.)

## EMPLOY SAFETY TECHNIQUES (INCLUDING FRATRICIDE AVOIDANCE)

1-14. Safety techniques are used to identify and assess hazards to the force and make recommendations on ways to prevent or mitigate the effects of those hazards. Commanders have the inherent responsibility to analyze the risks and implement control measures to mitigate them. All staffs understand and factor into their analysis how their execution recommendations could adversely affect Soldiers. Incorporating protection within the risk management integrating process is key. It ensures a thorough analysis of risks and implements controls to mitigate their effects. Risk management integration during operations process activities is the primary responsibility of the unit protection officer or operations officer. All commands develop and implement a command safety program that includes fratricide avoidance, occupational health, risk management, fire prevention and suppression, and accident prevention programs focused on minimizing safety risks.

1-15. **Fratricide is the unintentional killing or wounding of friendly or neutral personnel by friendly firepower.** The destructive power and range of modern weapons, coupled with the high intensity and rapid tempo of combat, increase the potential for fratricide. Tactical maneuvers, terrain, and weather conditions may also increase the danger of fratricide.

1-16. Fratricide is accidental and is usually the end product of an error by a leader or Soldier. Accurate information about locations and activities of friendly and hostile forces and an aggressive airspace management plan help commanders avoid fratricide. The U.S. Army Space and Missile Defense Command Mission Management Center provides joint friendly force tracking for all Services, which improves the situational awareness and helps prevent fratricide. Liaison officers increase situational understanding and enhance interoperability. 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.

1-17. Commanders, leaders and Soldiers are responsible for preventing fratricide. They must lower the probability of fratricide without discouraging boldness and audacity. Good leadership that results in positive weapons control, the control of troop movements, and disciplined operational procedures contribute to achieving this goal. Situational understanding, friendly personnel identification methods, and combat identification methods also help. Soldiers must be confident that the probability of misdirected friendly fire is low. Contractors authorized to accompany the force; local, national day laborers; and nongovernmental organization personnel who support Army operations face the same risks as U.S. forces. Since these personnel work and often live in and among U.S. forces, commanders must include them in protection and combat identification plans.

1-18. The potential for fratricide may increase with the fluid nature of the noncontiguous battlefield and the changing disposition of attacking and defending forces. The presence of noncombatants in the area of operations further complicates the scheme of maneuver. Simplicity and clarity are often more important than a complex, detailed plan when developing fratricide avoidance methods.

1-19. The effects of fratricide can be devastating to unit moral and confidence and can quickly diminish the mission effectiveness of a unit. Known postfratricide events have resulted in the following unit behavior:

- Hesitation to conduct limited visibility operations.
- Loss of confidence in unit leadership.
- Increase of leadership self-doubt.
- Hesitation to use supporting combat systems.
- Oversupervision of units.
- Loss of initiative.
- General degradation of unit cohesiveness, morale, and combat power.

1-20. Commanders ensure that risk mitigation strategies and fratricide prevention methods are employed and trained to lessen the risk of fratricide on the battlefield. Prevention methods include fratricide prevention training, weapons control measures, rules of engagement training, assembly area procedures, reconnaissance, rehearsals, backbriefs, unexploded ordnance training and reporting procedures, field discipline, friendly troop marking procedures and, most importantly, awareness at all levels.

1-21. In any situation involving the risk of fratricide due to friendly fire, leaders must be prepared to take immediate actions to prevent casualties, equipment damage, and equipment destruction. The recommended actions in fratricide situations include—

- Identify the incident and order all parties involved to cease fire.
- Conduct an in-stride risk assessment.
- Identify and implement controls to prevent the incident from recurring.

1-22. Fratricide may be more prevalent during joint and multinational operations when communications and interoperability challenges are not fully resolved. Fratricide avoidance is normally accomplished through a scheme of protection that emphasizes prevention and is centered on awareness and target identification:

- **Awareness.** Awareness is the immediate knowledge of the conditions of the operation, constrained geographically and in time. It includes the real-time, accurate knowledge of one's own location and orientation and the locations, activities, and intentions of other friendly, enemy, adversary, neutral, or noncombatant elements in the area of operations, sector, zone, or immediate vicinity. As previously mentioned, the U.S. Army Space and Missile Defense Command joint friendly force tracking mission aids in the overall awareness of personnel location in the operational environment.
- **Target identification.** *Target identification* is the accurate and timely characterization of a detected object on the battlefield as friend, neutral, or enemy. This aspect of combat identification is time sensitive and directly supports a combatant's shoot or don't-shoot decision for detected objects on the battlefield (FM 3-20.15). Unknown objects should not be engaged; rather, the target identification process should continue until positive identification is made. An exception to this is a weapons-free zone where units can fire at anything that is not positively identified as friendly.

1-23. Fire prevention, fire suppression, and firefighting encompass all efforts aimed at preventing or stopping fires. Fire prevention programs exist at all levels, and all levels of command are responsible for the Army fire protection plan. (See FM 5-415 for more information on fire prevention, fire suppression, and firefighting.) Commanders and supervisors are responsible for fire safety policies and plans in their organizations. Army firefighting capabilities consist of general firefighting and tactical firefighting:

- **General firefighting.** General firefighting skills are embedded into all Army safety programs (annual driver's training, unit fire safety, unit fire prevention) and during the transportation of personnel, petroleum, munitions, and explosives.
- **Tactical firefighting.** Tactical firefighting requires more specialized capabilities and is typically provided by engineer, host nation, or other identified firefighting units. In addition to normal fire protection and suppression, tactical firefighting capabilities include administering first aid; providing initial response to hazmat incidents; and rescuing entrapped, sick, and injured personnel from aircraft, buildings, equipment, vehicles, water, confined spaces, and high angles.

1-24. Operational conditions often impose significant hazards to Soldiers through the increased probability of an accident. In some operational environments, these hazards raise the risk level as equipment and personnel are taxed. Leaders must know their Soldiers and trained crews, and operators must know the capabilities and limitations of their platforms and systems. To maintain a continuous tempo, commanders must know how to employ and sustain personnel and equipment. When planning operations, commanders—

- Consider human endurance limits and environmental conditions.
- Balance the possible benefits of sustained, high-tempo operations with the level of prudent risk.
- Accept no unnecessary risks.
- Conduct high-risk operations only when the potential gain or benefit outweighs the potential loss.

---

*Note.* See Army doctrine pertaining to safety and risk management for more information.

---

## IMPLEMENT OPERATIONS SECURITY

1-25. *Operations security* is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities (JP 3-13.3). 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 which could be interpreted or pieced together to derive critical information in time to be useful to adversaries or enemies.
- Execute measures that eliminate or reduce (to an acceptable level) the vulnerabilities of friendly actions to enemy or adversary exploitation.

1-26. OPSEC applies to all operations. All units conduct OPSEC to preserve essential secrecy. Commanders establish routine OPSEC measures in unit standing operating procedures. 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. The assistant chief of staff, intelligence, assists the OPSEC process by comparing friendly OPSEC indicators with enemy or adversary intelligence collection capabilities.

---

*Note.* See JP 3-13.3 for additional OPSEC information.

---

## PROVIDE INTELLIGENCE SUPPORT TO PROTECTION

1-27. This is an intelligence warfighting function task that supports the protection warfighting function. It includes providing intelligence that supports measures which the command takes to remain viable and functional by protecting itself from the effects of threat activities. It also provides intelligence that supports recovery from threat actions. It includes analyzing the threats, hazards, and other aspects of an operational environment and utilizing the intelligence preparation of the battlefield process to describe the operational

environment and identify threats and hazards that may impact protection. Intelligence support develops and sustains an understanding of the enemy, terrain and weather, and civil considerations that affect the operational environment. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations (FM 3-55). Information collection can complement or supplement protection tasks. Through information collection, commanders and staffs continuously plan, task, and employ collection assets and forces. These forces collect, process, and disseminate timely and accurate information to satisfy the commander's critical information requirements and other intelligence requirements. When necessary, information collection assets (ground- and space-based reconnaissance and surveillance activities) focus on special requirements, such as personnel recovery. (See ADRP 2-0 for additional intelligence information.)

## **IMPLEMENT PHYSICAL SECURITY PROCEDURES**

1-28. Physical security consists of physical measures that are designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. 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, defensive positions, and nonlethal capabilities.

1-29. 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 alarm systems, video surveillance systems, other types of detection systems, patrols, or fixed posts—assists in localizing and determining the size and intent of an unauthorized intrusion or activity.
- **Delay.** Delay measures protect an asset from aggression by delaying or preventing 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.

---

**Note.** See ATTP 3-39.32 for additional information on physical security procedures.

---

## **APPLY ANTITERRORISM MEASURES**

1-30. AT consists of defensive measures that are used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces. AT is a consideration for all forces during all military operations.

1-31. AT is an integral part of Army efforts to defeat terrorism. Terrorists can target Army elements at any time and in any location. By effectively preventing and, if necessary, responding to terrorist attacks, commanders protect all activities and people so that Army missions can proceed unimpeded. AT is neither a discrete task nor the sole responsibility of a single branch; all bear responsibility. AT must be integrated into all Army operations and considered at all times. Awareness must be built into every mission, every Soldier, and every leader. Integrating AT represents the foundation that is crucial for Army success.

1-32. Typical Army AT programs are composed of several adjunct and information programs, including tasks for specialized, nonprotection military occupational specialties. AT includes the following areas at a minimum:

- Risk management (threat, critical asset, and vulnerability assessments of units, installations, facilities, and bases/base camps).
- AT planning (units, installations, facilities, and bases).
- AT awareness training and command information programs.
- The integration of various vulnerability assessments of units, installations, facilities, bases/base camps, personnel, and activities.
- AT protection measures to protect individual personnel, high-risk personnel, physical assets (physical security), and designated critical assets and information.
- Resource application.
- Civil and military partnerships.
- Force protection condition systems to support terrorist threat and incident response plans.
- Comprehensive AT program review.

---

*Note.* See FM 3-37.2 for additional information on AT measures.

---

## CONDUCT LAW AND ORDER

1-33. Law and order 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. Law and order operations and the associated skills and capabilities inherent in that function provide the fundamental base on which all other military police functions are framed and conducted.

1-34. Law and order operations are conducted across the range of military operations. As the operation transitions and the operational environment stabilizes, civil control efforts are implemented and the rule of law is established. The closer the operational environment 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.

1-35. The ultimate goal is to maintain order while protecting personnel and assets. Military police Soldiers and leaders apply this policing approach when conducting all operations. The military police view shares a common general understanding of the operational environment, while adding a degree of focus on those aspects that are necessary to maintain order and enforce laws. Care should be taken to eliminate jurisdictional overlap and under lap. Law and order 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.

---

*Note.* See ATTP 3-39.10 for additional information on law and order operations.

---

## CONDUCT SURVIVABILITY OPERATIONS

1-36. Personnel and physical assets have inherent survivability qualities or capabilities that can be enhanced through various means and methods. When existing terrain features offer insufficient cover and concealment, survivability can be enhanced by altering the physical environment to provide or improve

cover and concealment. Similarly, natural or artificial materials may be used as camouflage to confuse, mislead, or evade the enemy or adversary. Together, these are called survivability operations—those military activities that alter the physical environment to provide or improve cover, concealment, and camouflage. By providing or improving cover, concealment, and camouflage, survivability operations help military forces avoid or withstand hostile actions. Although such activities often have the added benefit of providing shelter from the elements, survivability operations focus on providing cover, concealment, and camouflage. All units conduct survivability operations within the limits of their capabilities. Engineer and CBRN personnel and units have additional capabilities to support survivability operations.

1-37. Survivability operations enhance the ability to avoid or withstand hostile actions by altering the physical environment. They accomplish this by providing or improving cover, concealment, and camouflage in four areas:

- Fighting positions.
- Protective positions.
- Hardened facilities.
- Camouflage and concealment.

1-38. The first three areas focus on providing cover (although not excluding camouflage and concealment). The fourth area focuses on providing protection from observation and surveillance. All four areas, but especially the first three, often have the added benefit of providing some degree of shelter from the elements. The areas of survivability operations are often addressed in combination. For example, fighting positions and protective positions usually require camouflage and concealment also. Camouflage and concealment activities often accompany activities to harden facilities.

---

***Notes.***

1. See FM 5-103 for more information on survivability and survivability operations.
  2. See FM 3-34.400 for information on base camps.
  3. See FM 90-7 for information on obstacle integration.
- 

## **PROVIDE FORCE HEALTH PROTECTION**

1-39. Force health protection encompasses measures to promote, improve, or conserve the mental and physical well-being of Soldiers. These measures enable a healthy and fit force, prevent injury and illness, protect the force from health hazards, and include the prevention aspects of a number of 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 man).
- Combat and operational stress control.
- Dental services (preventive dentistry).
- Laboratory services (area medical laboratory support).

1-40. Army personnel must be physically and behaviorally fit. This requirement demands programs that promote and improve the capacity of personnel to perform military tasks at high levels, under extreme conditions, and for extended periods of time. These preventive and protective capabilities include physical exercise, nutritional diets, dental hygiene and restorative treatment, combat and operational stress management, rest, recreation, and relaxation that are geared to individuals and organizations.

1-41. Methods to prevent disease are best applied synergistically. Sanitation practices, waste management, and pest and vector control are crucial to disease prevention. Regional spraying and insect repellent application to guard against hazardous flora and fauna are examples of prevention methods. Prophylactic measures can encompass human and animal immunizations, dental chemoprophylaxis and treatment, epidemiology, optometry, counseling on specific health threats, and protective clothing and equipment.

1-42. The key to preventive and protective care is information—the capacity to anticipate the current and true health environment and the proper delivery of information to the affected human population. Derived from robust health surveillance and medical intelligence, this information addresses occupational, local environmental, and enemy- or adversary-induced threats from industrial hazards, air and water pollution, endemic or epidemic disease, CBRN threats or hazards, and directed-energy device weapons (high-powered microwaves, particle beams, lasers). Health service support must be capable of acquiring, storing, moving, and providing information that is timely, relevant, accurate, concise, and applicable to individuals. In summary, this information capability is crucial to force health protection. Force health protection includes—

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

---

*Note.* See ATTP 4-02 for more information on force health protection.

---

## CONDUCT CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR OPERATIONS

1-43. A CBRN environment consists of conditions found in an area that resulted from immediate or persistent effects of CBRN attacks or unintentional releases. CBRN operations include the employment of tactical capabilities that counter the entire range of CBRN threats and hazards through—

- Weapons of mass destruction (WMD) proliferation prevention (security cooperation and partner activities and threat reduction cooperation).
- WMD counterforce (interdiction, offensive operations, and elimination).
- CBRN defense (active and passive defense).
- CBRN consequence management.

1-44. CBRN operations support operational and strategic objectives to combat WMD and operate safely in a CBRN environment. They include—

- **Providing WMD security cooperation and partner activities support.** WMD security cooperation and partner activities improve or promote defense relationships and the capacity of allied and partner nations to execute or support other military mission areas to combat WMD through military-to-military contact, burden-sharing arrangements, combined military activities, and support to international activities.
- **Providing WMD threat reduction cooperation support.** WMD threat reduction cooperation activities are undertaken with the consent and cooperation of host nation authorities in a permissive environment to enhance physical security and to reduce, dismantle, redirect, and/or improve the protection of an existing state WMD program, stockpiles, and capabilities.
- **Conducting WMD interdiction operations.** WMD interdiction operations track, intercept, search, divert, seize, or otherwise stop the transit of WMD, WMD delivery systems, or WMD-related materials, technologies, and expertise.
- **Conducting WMD offensive operations.** WMD offensive operations disrupt, neutralize, or destroy a WMD threat before it can be used; or they deter the subsequent use of a WMD.
- **Conducting WMD elimination operations.** WMD elimination operations are conducted in a hostile or uncertain environment to systematically locate, characterize, secure, disable, or destroy WMD programs and related capabilities. (See ATTP 3-11.23 for more information.)
- **Conducting CBRN active defense.** CBRN active defense includes measures to defeat an attack with CBRN weapons by employing actions to divert, neutralize, or destroy those weapons or their means of delivery while en route to their target.
- **Conducting CBRN passive defense.** CBRN passive defense includes measures taken to minimize or negate the vulnerability to, and effects of, CBRN incidents. This mission area

focuses on maintaining force ability to continue military operations in a CBRN environment. Commanders use measures that implement the principles of contamination avoidance (see FM 3-11.3), protection (see FM 3-11.4), and decontamination (see FM 3-11.5).

- **Conducting CBRN consequence management operations.** CBRN consequence management consists of actions taken to plan, prepare, respond to, and recover from a CBRN incident that requires forces and resource allocation beyond passive defense capabilities (see FM 3-11 and FM 3-11.21).

1-45. 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.

---

*Note.* See FM 3-11 for additional information on CBRN operations.

---

## **PROVIDE EXPLOSIVE ORDNANCE DISPOSAL AND PROTECTION SUPPORT**

1-46. The role of EOD is to eliminate or reduce the effects of explosive ordnance and hazards to protect combat power and the freedom of action. Explosive ordnance and hazards are ever-present dangers in most areas of operation. They limit mobility, deny the use of critical assets, and potentially injure or kill Soldiers and civilians. The U.S. and multinational use of munitions that disperse submunitions across a wide area has led to increased amounts of unexploded ordnance on the battlefield. EOD forces have the capability to render-safe and destroy explosive ordnance and hazards across the range of military operations. EOD units are specifically trained in render-safe procedures and the disposal of explosive ordnance, explosive hazards, and CBRN munitions. 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 normally—

- Identify and collect information on explosive ordnance and hazards.
  - Perform an initial assessment of found munitions, which include 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 weapons technical intelligence on explosive ordnance and hazards, including first-seen items of interest.
- Render-safe and dispose of explosive ordnance and hazards.
  - 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.
  - Support responses to nuclear and chemical accidents and incidents, including technical advice and procedures to mitigate hazards associated with such items.
  - Provide EOD Soldiers in support of humanitarian assistance efforts that involve explosive ordnance and hazards.

---

*Notes.*

1. EOD is the only force equipped, manned, and trained to positively identify, render-safe, and dispose of U.S. and foreign explosive ordnance and improvised explosive devices.

2. See ATTP 4-32 for additional EOD information.

---

## COORDINATE AIR AND MISSILE DEFENSE

1-47. Air and missile defense protects the force from missile attack, air attack, and aerial surveillance by ballistic missiles, cruise missiles, conventional fixed- and rotary-wing aircraft, and unmanned aerial systems. It prevents enemies from interdicting friendly forces, while freeing commanders to synchronize movement and firepower. All members of the combined arms team perform air defense tasks; however, ground-based air defense artillery units execute most Army air and missile defense operations. Air and missile defense elements coordinate and synchronize defensive fires to protect installations and personnel from over-the-horizon strikes. Army air and missile defense capabilities increase airspace situational understanding and complement the area air defense commander.

1-48. Indirect-fire protection systems protect forces from threats that are largely immune to air defense artillery systems. The indirect-fire protection intercept capability is designed to detect and destroy incoming rocket, artillery, and mortar fires. This capability assesses the threat to maintain friendly protection and destroys the incoming projectile at a safe distance from the intended target.

1-49. The air and missile defense task consists of active and passive measures that protect personnel and physical assets from an air or missile attack. Passive measures include camouflage, cover, concealment, hardening, and OPSEC. Active measures are taken to destroy, neutralize, or reduce the effectiveness of hostile air and missile threats. The early warning of in-bound missile threats is provided in theater by the globally located, joint tactical ground stations.

1-50. Protection cell planners coordinate with the Air Defense Airspace Management Cell for Air and Missile Defense for the protection of the critical asset list (CAL) and defended asset list (DAL) and for other air and missile defense protection as required. There is continuous coordination to refine the CAL and DAL throughout operations, ensuring the protection of critical assets and forces from air and missile attack and surveillance. (The CAL and DAL are further discussed in chapter 2.)

1-51. The air and missile defense assets integrate protective systems by using the six employment guidelines—mutual support, overlapping fires, balanced fires, weighted coverage, early engagement, and defense in depth—and additional considerations necessary to mass and mix air and missile defense capabilities. These employment guidelines enable air defense artillery forces to successfully accomplish combat missions and support overall force objectives.

---

*Note.* See ADRP 3-09 for more information on air and missile defense operations and airspace control.

---

## CONDUCT PERSONNEL RECOVERY

1-52. Army personnel recovery is the sum of military, diplomatic, and civil efforts to prevent isolation incidents and to return isolated persons to safety or friendly control. Personnel recovery is the overarching term for operations that focus on recovering isolated or missing personnel before they become detained or captured.

1-53. Personnel recovery operations are conducted to recover and return personnel who are isolated, missing, detained, or captured in an operational area. These personnel consist of U.S. forces, Army civilians, or other personnel (as designated by the President or the Secretary of Defense) who are in an operational environment 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.

1-54. Commanders must understand the operational environment and the impact of PMESII-PT to ensure that personnel recovery is incorporated into and supports each mission. This includes the characteristics of the particular operational environment and how aspects of the environment become essential elements in shaping the way that Army forces conduct operations. Threats to isolated Soldiers will vary based on the operational environment.

1-55. Personnel recovery is not a stand-alone mission; it is incorporated into mission planning. Personnel recovery operations are supported through joint friendly force tracking activities. Personnel recovery guidance must synchronize the actions of commanders and staffs, recovery forces, and isolated individuals.

In order to synchronize the actions of all three, commanders develop personnel recovery guidance based on command capabilities to conduct recovery operations. By knowing what actions they have dictated to potential isolated Soldiers, commanders develop situational understanding and provide guidance to their staffs and recovery forces to synchronize their actions with those of isolated personnel.

1-56. Commanders must integrate personnel recovery throughout operations. This requires an understanding of the complex, dynamic relationships between friendly forces and enemies and the other aspects of the operational environment (including the populace). This understanding helps commanders visualize and describe their intent for personnel recovery and helps them develop focused planning guidance. As commanders develop personnel recovery guidance for subordinate units, they must ensure that subordinates have adequate combat power for personnel recovery. Commanders must also provide resources and define command relationships with the requisite flexibility to plan and execute personnel recovery operations.

1-57. Commanders provide personnel recovery planning guidance within their initial guidance. Personnel recovery guidance provides a framework for how the unit and subordinates will synchronize the actions of isolated personnel and the recovery force. Effective personnel recovery planning guidance accounts for the operational environment and the execution of operations. Personnel recovery guidance is addressed in the synchronization of each warfighting function. It broadly describes how the commander intends to employ combat power to accomplish personnel recovery tasks within the higher commander's intent.

---

**Note.** See FM 3-50.1 for additional information on personnel recovery operations.

---

## **CONDUCT INTERNMENT AND RESETTLEMENT**

1-58. Internment and resettlement operations are conducted by military police to shelter, sustain, guard, protect, and account for populations (detainees, dislocated civilians, and U.S. military prisoners) as a result of military or civil conflict and natural or man-made disasters or to facilitate criminal prosecution:

- **Internment.** Internment involves the detainment of a population or group that pose some level of threat to military operations.
- **Resettlement.** Resettlement involves the quartering of a population or group for their protection.

1-59. These operations inherently control the movement and activities of their specific population for imperative reasons of security, safety, or intelligence gathering. The Army is the DOD executive agent for all detainee operations and for the long-term confinement of U.S. military prisoners.

1-60. Internment and resettlement operations include—

- Performing internment.
- Interning U.S. military prisoners.
- Supporting host nation corrections reform.
- Conducting resettlement operations.
- Conducting enemy prisoner of war operations.
- Conducting detainee operations.

---

**Note.** See FM 3-39.40 for more information on internment and resettlement operations.

---

## **TASKS AND SYSTEMS INTEGRATION**

1-61. In order 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.

1-62. The protection warfighting function tasks and systems, when integrated throughout the operations process, help establish control measures against potential threats and hazards. The layering of protection tasks and systems, some even redundant, ensures a comprehensive scheme of protection. The layered approach of protection provides strength and depth. Units utilize their available capabilities to defend the protection priorities and a layering of capabilities reduces the destructive effect of threats and hazards.

1-63. 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. Implementing AT and physical security measures, enhancing survivability measures, and applying active and passive defense operations add to the next layer of a comprehensive, integrated, layered scheme of protection. Implementing the protection tasks and utilizing protection systems in a comprehensive, layered scheme of protection preserves the critical assets throughout the range of military operations in any operational environment.

**This page intentionally left blank.**

## **Chapter 2**

# **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 set protection priorities for each phase or critical event of an operation. The military decisionmaking process or troop leading procedures provide a deliberate process and context to develop and examine information for use in the various continuing activities and integrating processes that comprise the operations process. An effective scheme of protection and risk decisions are developed based on the information that flows from mission analysis, allowing a thorough understanding of the situation, mission, and environment. Mission analysis provides a context to identify and analyze threats and hazards, the situational understanding of the operational environment, and the development of the 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**

2-1. Initial protection planning requires various assessments to support protection prioritization; namely, threat, hazard, vulnerability, criticality, and capability. These assessments are used to determine which assets can be protected given no constraints (critical assets) and which assets can be protected with available resources (defended assets). Commanders make decisions on acceptable risks and provide guidance to the staff so that they can employ protection capabilities based on the CAL and DAL. All forms of protection are utilized and employed during preparation and continue through execution to reduce friendly vulnerability.

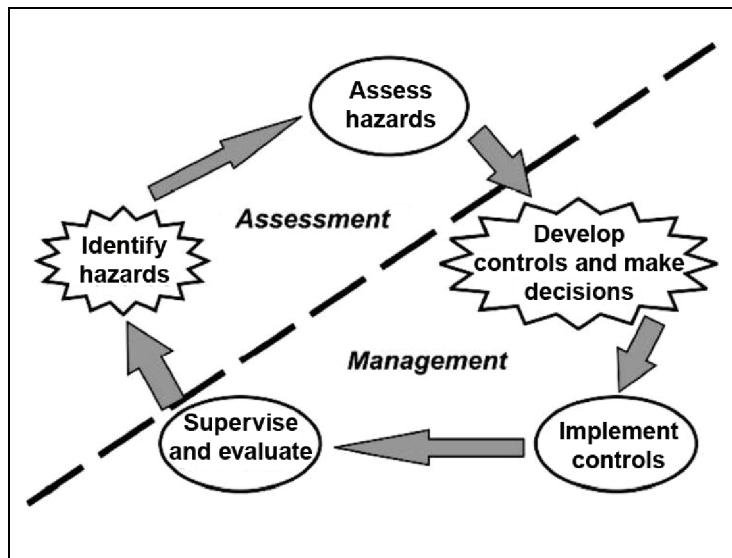
### **INTEGRATING PROCESSES**

2-2. The integrating processes of intelligence preparation of the battlefield, targeting, and risk management 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.

2-3. The intelligence preparation of the battlefield is a systematic process of analyzing and visualizing the mission variables of threat, terrain, weather, and civil considerations in a specific area of interest and for a specific mission. By applying the intelligence preparation of the battlefield, commanders gain the information necessary to selectively apply and maximize operation effectiveness at critical points in time and space.

2-4. The targeting process integrates commander guidance and priorities to determine which targets to engage and how, when, and where to engage them in order to assign friendly capabilities to achieve 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, that are necessary to minimize the chance of these events. The protection priorities must be integrated within the targeting process to achieve the desired effects while ensuring the preservation of combat power.

2-5. Risk management (figure 2-1) is the process of identifying, assessing, and controlling risks that arise from operational factors and making decisions that balance risk cost with mission benefits. Threat, hazard, capability, vulnerability, and criticality assessments are utilized to evaluate the risk to the force, determine the critical assets, ascertain available resources, and apply security or defensive measures to achieve protection. Risk management helps commanders 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 courses of action (COAs). Risk management integration during operations process activities is the primary responsibility of the unit protection officer or operations officer.



**Figure 2-1. Risk management process**

## THREATS AND HAZARDS

2-6. The protection warfighting function preserves the combat power potential and survivability of the force by providing protection from threats and hazards.

2-7. 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 upon personnel, physical assets, or information. These threats may include improvised explosive devices, suicide bombings, network attacks, mortars, asset theft, air attacks, or 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, OPSEC violations, network compromises, equipment malfunctions, or accidental CBRN incidents.
- **Environmental conditions.** Environmental hazards associated with the surrounding environment could potentially degrade readiness or mission accomplishment. Weather, natural disasters, and diseases are common examples. The staff also considers how military operations may affect noncombatants in the area of operations. Such considerations prevent unnecessary collateral damage and regard how civilians will affect the mission. Heavy civilian vehicle or pedestrian traffic adversely affects convoys and other operations.

2-8. Commanders use the METT-TC mission variables to describe the operational environment, including threats that may impact protection. In most cases, they can draw the relevant information from an ongoing analysis of the operational environment using the PMESII-PT operational variables.

## THREATS

2-9. The various actors in any area of operations can qualify as a threat, enemy, adversary, neutral, or friendly. Land operations often prove complex because actors intermix, often with no easy means to distinguish one from another.

- 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 (ADRP 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.
- An *enemy* is a party identified as hostile against which the use of force is authorized (ADRP 3-0). An enemy is also called a combatant and is treated as such under the law of war.
- An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0).
- A *neutral* is a party identified as neither supporting nor opposing friendly or enemy forces (ADRP 3-0).
- A *friendly* is a contact positively identified as friendly (JP 3-01).

2-10. The term *hybrid threat* has evolved to capture the seemingly 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, and/or criminal elements unified to achieve mutually benefitting effects (ADRP 3-0). Hybrid threats combine regular forces, who are governed by international law and military traditions and customs, with unregulated forces who 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

2-11. 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.

## THREAT AND HAZARD ASSESSMENT

2-12. 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 area of operations. 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 operational environment changes.

2-13. Considerations for the threat and hazard assessment include—

- Enemy and adversary threats.
  - Operational capabilities.
  - Intentions.
  - Activities.
- Foreign intelligence and security service threats.
- Crimes.

- Civil disturbances.
- Medical and safety hazards.
- CBRN weapons and toxic industrial material.
- Other relevant aspects of the operational environment.
- Incident reporting and feedback points of contact.

2-14. 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 or hazard. Table 2-1 shows examples of potential threats and hazards in an area of operations. 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 2-1. Potential threats and hazards**

<b>Area of Concern</b>	<b>Potential Threats and Hazards</b>
Area security	<ul style="list-style-type: none"> <li>● Assassination of, or attacks on, important personnel</li> <li>● Enemy, adversary or terrorist attacks on facilities</li> <li>● Ambushes or attacks on convoys</li> <li>● Enemy or adversary attacks on convoy routes</li> </ul>
Safety	<ul style="list-style-type: none"> <li>● Hazards associated with enemy or adversary activity</li> <li>● Accident potential</li> <li>● Weather or environmental conditions</li> <li>● Equipment</li> </ul>
Fratricide avoidance	<ul style="list-style-type: none"> <li>● Poor or reduced awareness</li> <li>● Inexperienced or poorly equipped or disciplined personnel</li> <li>● Complex or poorly defined mission against an experienced enemy or adversary</li> </ul>
OPSEC	<ul style="list-style-type: none"> <li>● Accidental friendly release of essential elements of friendly information</li> <li>● Enemy or adversary collection and exploitation of essential elements of friendly information</li> <li>● Enemy or adversary capture of unclassified friendly information</li> <li>● Physical security violations</li> <li>● Enemy or adversary intelligence gathering</li> </ul>
AT	<ul style="list-style-type: none"> <li>● Improvised explosive devices</li> <li>● Suicide bombs</li> <li>● Mail bombs</li> <li>● Snipers</li> <li>● Standoff weapons</li> <li>● WMD</li> <li>● Active shooters</li> <li>● Insider threats</li> </ul>
Survivability	<ul style="list-style-type: none"> <li>● Environmental conditions</li> <li>● Capabilities of threat weapons and sensors</li> </ul>
Force health protection	<ul style="list-style-type: none"> <li>● Endemic and epidemic diseases</li> <li>● Environmental factors</li> <li>● Diseases from animal bites, poisonous plants, animals, or insects</li> <li>● Risks associated with the health, sanitation, or behavior of the local populace</li> </ul>
CBRN	<ul style="list-style-type: none"> <li>● CBRN weapons</li> <li>● Toxic industrial materials</li> </ul>
EOD	<ul style="list-style-type: none"> <li>● Explosive ordnance and hazards (friendly and enemy)</li> <li>● Adversary attacks on personnel, vehicles, or infrastructure</li> </ul>

**Table 2-1. Potential threats and hazards (continued)**

<b>Area of Concern</b>	<b>Potential Threats and Hazards</b>
Air and missile defense	<ul style="list-style-type: none"> <li>• Artillery</li> <li>• Mortars</li> <li>• Rockets</li> <li>• Ballistic and cruise missiles</li> <li>• Fixed- and rotary-wing aircraft</li> <li>• Unmanned aerial systems</li> </ul>
Personnel recovery	<ul style="list-style-type: none"> <li>• Events that separate or isolate individuals or small groups of friendly forces from the main force</li> </ul>
<b>Legend:</b>	
AT	antiterrorism
CBRN	chemical, biological, radiological, and nuclear
EOD	explosive ordnance disposal
OPSEC	operations security
WMD	weapons of mass destruction

## CRITICALITY ASSESSMENT

2-15. 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) which 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 giving 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.

2-16. The protection cell staff continuously updates the criticality assessment during the operations process. As the staff develops or modifies a friendly COA, information collection efforts confirm or deny information requirements. As the mission or threat changes, initial criticality assessments may also change, increasing or decreasing the subsequent force vulnerability. The protection cell monitors and evaluates these changes and begins coordination among the staff to implement modifications to the protection concept or recommends new protection priorities. Priority intelligence requirements, running estimates, measures of effectiveness (MOEs), and measures of performance (MOPs) are continually updated and adjusted to reflect the current and anticipated risks associated with the operational environment.

## VULNERABILITY ASSESSMENT

2-17. A vulnerability assessment is an evaluation (assessment) to determine the magnitude of a threat or hazard effect against an installation, personnel, unit, exercise, port, ship, residence, facility, or other site. It identifies the areas of improvement necessary to withstand, mitigate, or deter acts of violence or terrorism. The staff addresses **who** or **what** is vulnerable and **how** it is vulnerable. 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. Vulnerability is the component of risk over which the commander has the most control and greatest influence. 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.

2-18. Vulnerability evaluation criteria may include the degree to which an asset may be disrupted, quantity available (if replacement is required due to loss), dispersion (geographic proximity), and key physical characteristics.

2-19. DOD has created several decision support tools to perform criticality assessments in support of the vulnerability assessment process, including—

- **MSHARPP (mission, symbolism, history, accessibility, recognizability, population, and proximity).** MSHARPP is a targeting analysis tool that is geared toward assessing personnel vulnerabilities, but it also has application 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.
- **CARVER (criticality, accessibility, recuperability, vulnerability, effect, and recognizability).** 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) determine assets that are more critical to the success of the mission.

---

**Note.** See FM 3-37.2 for more information on MSHARPP and CARVER.

---

## **CAPABILITY ASSESSMENT**

2-20. A capability assessment of an organization determines its current capacity to perform protection tasks based on the integrated material and nonmaterial readiness of the assets. A capability assessment considers the mitigating effects of existing manpower, procedures, and equipment. It is especially important in identifying capability gaps, which may be addressed to reduce the consequences of a specific threat or hazard. A capability assessment—

- Considers the range of identified and projected response capabilities necessary for responding to any type of hazard or threat.
- Lists force resources, by type, and corresponding protection tasks.
- Determines which assets are necessary to defend key areas.

## **CRITICAL AND DEFENDED ASSET LISTS**

2-21. Initial assessments identify threats and hazards to the force, determine the criticality of systems and assets, and assess protection capabilities to mitigate vulnerabilities. The CAL and DAL are key protection products developed during initial assessments; they are dynamic lists that are continuously revised.

### **CRITICAL ASSET LIST**

2-22. The *critical asset list* is a prioritized list of assets, normally identified by phase of the operation and approved by the joint force commander, that should be defended against air and missile threats (JP 3-01). Once the threat, criticality, and vulnerability assessments are complete, the staff presents the prioritized CAL to the commander for approval. Commanders typically operate in a resource-constrained environment and have a finite amount of combat power for protecting assets. The protection cell/working group determines which assets are critical for mission success and recommends protection priorities based on the available resources. The CAL will vary depending on the mission variables.

2-23. During threat assessment, members of the protection cell/working group identify and prioritize the commander's critical assets using the vulnerability assessment, criticality assessment, and plan or order. Critical assets are generally specific assets of such extraordinary importance that their loss or degradation would have a significant and debilitating effect on operations or the mission. They represent what should be protected. The protection cell/working group uses information derived from command guidance, the intelligence preparation of the battlefield, targeting, risk management, warning orders, and the restated

mission to nominate critical assets from their particular protection functional area. Vulnerability and criticality assessments are generally intended to be sequential. However, the criticality assessment can be conducted before, after, or concurrent with threat assessments. The vulnerability assessment should be conducted after the threat and criticality assessments to orient protection efforts on the most important assets. These assessments provide the staff with data to develop benchmarks, running estimates, commander's critical information requirements, change indicators, variances, MOEs, and MOPs.

2-24. CAL development may require the establishment of evaluation criteria, such as—

- Value (impact of loss).
- Depth (proximity in distance and time).
- Replacement impact (degree of effort, cost, or time).
- Capability (function and capacity for current and future operations).

2-25. The lack of a replacement may cause a critical asset to become the first priority for protection. Not all assets listed on the CAL will receive protection from continuously applied combat power. Critical assets with some protection from applied combat power become part of the DAL.

## DEFENDED ASSET LIST

2-26. The *defended asset list* is a listing of those assets from the critical asset list prioritized by the joint force commander to be defended with the resources available (JP 3-01). Critical assets that are reinforced with additional protection capabilities or capabilities from other combat power elements become part of the DAL. It represents what can be protected, by priority. The DAL allows commanders to apply finite protection capabilities to the most valuable assets. The combat power applied may be a weapons system, electronic sensor, obstacle, or combination.

## SCHEME OF PROTECTION DEVELOPMENT

2-27. 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.

2-28. 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.

2-29. The scheme of protection is developed after receiving guidance and considering the principles of protection in relation to the mission variables, the incorporation of efforts, and the tasks that comprise the protection warfighting function. The scheme of protection is based on the mission variables, thus includes protection priorities by area, unit, activity, or resource. It addresses how protection is applied and derived during the conduct of operations. 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 and press the offensive. These conditions, areas, or situations are anticipated; and the associated risks are mitigated by describing and planning for the use of response forces.

2-30. The staff 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.
- Intelligence focus and limitations for security efforts.
- Areas or events where risk is acceptable.

- Protected targets and areas.
- Civilians and noncombatants in the area of operations.
- Vehicle and equipment safety or security constraints.
- Personnel recovery actions and control measures.
- Force protection condition status.
- Force health protection measures.
- Mission-oriented protective posture guidance.
- Environmental guidance.
- Information operations condition.
- 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.

## **PROTECTION PRIORITIES**

2-31. Criticality, vulnerability, and recuperability 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.

2-32. 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 be the most important decisions that commanders make and that staffs support. There are seldom sufficient resources to simultaneously provide the same level of protection to all assets. For this reason, commanders use risk management to identify increasingly risky activities and events, while other decision support tools assist in prioritizing protection resources.

2-33. 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. Event-driven operations may be short in duration, enabling a formidable protection posture for a short time; while 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.

## **RUNNING ESTIMATE**

2-34. The protection cell develops and refines the protection running estimate (figure 2-2). The protection estimate provides a picture to the command on the protection warfighting function. 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, essential elements of friendly information, CALs, DALs, protection priorities, risk decision points, supporting tasks) feed updates to the running estimate.

Past 24 hours	Protection common operational picture <ul style="list-style-type: none"> <li>• CAL/DAL</li> <li>• Threats/hazards</li> <li>• Incidents</li> <li>• Asset locations</li> </ul>			CAL/DAL
Next 48 to 72 hours				Asset task organization
Issues/risk decision points				Provost marshal officer
Protection priorities				Engineer
Essential elements of friendly information	FPCON INFOCON	AMD ADW WCS	CBRN and EOD MOPP OEG	Safety
Security banner				
<b>Legend:</b>				
ADW	air defense warning			
AMD	air and missile defense			
CAL	critical asset list			
CBRN	chemical, biological, radiological, and nuclear			
DAL	defended asset list			
EOD	explosive ordnance disposal			
FPCON	force protection condition			
INFOCON	information operations condition			
MOPP	mission-oriented protective posture			
OEG	operation exposure guide			
WCS	weapons control status			

**Figure 2-2. Sample protection running estimate**

## PROTECTION CELL AND WORKING GROUP

2-35. 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

2-36. At division level and higher, the integration of the protection function and tasks is conducted by a designated protection cell and the chief of protection. At brigade level and below, the integration occurs more informally, with the designation of a protection coordinator from among the brigade staff or as an integrating staff function assigned to a senior leader. Chiefs of protection and protection coordinators participate in various forums to facilitate the continuous integration of protection tasks into the operations process. This occurs through protection working groups, staff planning teams, and staffs conducting integrating processes.

### PROTECTION WORKING GROUP

2-37. 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 across the staff.

2-38. The protection working group is led by the chief of protection and normally consists of the following:

- Air and missile defense officer.
- AT officer.

- CBRN officer.
- Engineer officer.
- Electronic warfare element representative.
- EOD officer.
- Fire support representative.
- OPSEC officer.
- Provost marshal.
- Safety officer.
- Intelligence representative.
- Civil affairs officer.
- Personnel recovery officer.
- Public affairs officer.
- Staff judge advocate.
- Surgeon.
- Medical representative.
- Veterinary representative.
- Subordinate unit liaison officers.
- Operations representative.
- Area contracting officer.

2-39. Commanders augment the team with other unit specialties and unified action partners depending on the operational environment and the unit mission. The protection officer determines the working group agenda, meeting frequency, composition, input, and expected output.

## **ROLES AND RESPONSIBILITIES**

2-40. The protection cell/working group is 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/working group helps develop a concept of protection tailored to the type of operation the unit is conducting.

2-41. During the planning process, the protection cell/working group provides input to the commander's military decisionmaking process by integrating the threat and hazard assessment with the commander's essential elements of friendly information, the CAL, and the DAL. While the planning cell develops plans, the protection cell/working group attempts 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/working group provides vulnerability mitigation measures to help reduce risks associated with a particular COA and conducts planning and oversight for unified land operations.

2-42. 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, such as the CAL.
- Provides recommendations for the CAL and DAL.
- Reviews and coordinates unit protection measures.
- Recommends force protection conditions 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.
- 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 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.

2-43. The approved vulnerability reduction mitigation measures, commander's decisions for acceptable risks, CAL, and DAL 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.

2-44. 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 the threshold variances.
- Recommendations for the commander's critical information requirements that reflect decision criteria from protection tasks and systems.
- CAL and DAL.
- Decision points based on the commander's risk tolerance level.

## COORDINATION AND RELATIONSHIPS

2-45. The protection cell/working group ensures the integration of protection equities throughout the operations process via integrating processes, continuing activities, the military decisionmaking process, 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/working group provide input and conduct actions (table 2-2, page 2-12) 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 protection officer based on mission variables and military decisionmaking process integration.

**Table 2-2. Protection working group actions**

<b>Key Input</b>	<b>Protection Actions</b>	<b>Steps</b>	<b>Protection Output</b>	<b>Key Output</b>
<ul style="list-style-type: none"> <li>• Higher HQ plan or order</li> <li>• New mission anticipated by the commander</li> </ul>	<ul style="list-style-type: none"> <li>• Consolidate protection-related running estimates from staffs</li> <li>• Review consolidated protection array of assets</li> <li>• Determine protection working group members</li> <li>• Ensure protection planner integration within the unit planning team</li> </ul>	<p>Step 1: Receipt of Mission</p> <p style="border: 1px solid black; padding: 2px;">Warning Order</p>	<ul style="list-style-type: none"> <li>• Protection working group</li> <li>• Warning and reporting systems</li> <li>• Protection running estimate</li> </ul>	<ul style="list-style-type: none"> <li>• Commander's initial guidance</li> <li>• Initial allocation of time</li> </ul>
<ul style="list-style-type: none"> <li>• Higher HQ plan or order</li> <li>• Higher HQ knowledge and intelligence products</li> <li>• Knowledge products from other organizations</li> <li>• Design concept (if developed)</li> </ul>	<ul style="list-style-type: none"> <li>• Provide input on critical networks or nodes that can be influenced</li> <li>• Identify requests for information</li> <li>• Determine available assets</li> <li>• Conduct and consolidate initial assessments</li> <li>• Conduct protection working group</li> <li>• Recommend and coordinate information collection assets for protection</li> <li>• Develop OPSEC indicators</li> <li>• Identify EEFI, and establish how long they need to be protected</li> <li>• Develop essential survivability and other engineering tasks</li> <li>• Identify available information on routes and key facilities</li> <li>• Analyze protection considerations of civilians in the area of operations</li> <li>• Determine available unified action partner capabilities</li> <li>• Determine funding sources, as required</li> <li>• Determine availability of construction and other engineering materials</li> </ul>	<p>Step 2: Mission Analysis</p> <p style="border: 1px solid black; padding: 2px;">Warning Order</p>	<ul style="list-style-type: none"> <li>• Consolidated HVT list</li> <li>• RFIs</li> <li>• Initial assessments</li> <li>• Recommended CAL</li> <li>• Recommended EEFI</li> <li>• Initial protection priorities</li> <li>• Input into information collection plan</li> </ul>	<ul style="list-style-type: none"> <li>• Problem statement</li> <li>• Mission statement</li> <li>• Initial commander's intent</li> <li>• Initial planning guidance</li> <li>• Initial CCIRs and EEFIs</li> <li>• Updated IPB and running estimates</li> <li>• Assumptions</li> </ul>

**Table 2-2. Protection working group actions (continued)**

<b>Key Input</b>	<b>Protection Actions</b>	<b>Steps</b>	<b>Protection Output</b>	<b>Key Output</b>
<ul style="list-style-type: none"> <li>• Mission statement</li> <li>• Initial commander's intent, planning guidance, CCIRs, and EEFIs</li> <li>• Updated IPB and running estimates</li> <li>• Assumptions</li> </ul>	<ul style="list-style-type: none"> <li>• Determine array of protection assets</li> <li>• Integrate protection tasks into COA</li> <li>• Determine initial scheme of protection</li> <li>• Coordinate health support requirements</li> <li>• Ensure that link architecture meets requirements and have been allocated from respective agents</li> <li>• Recommend appropriate level of survivability effort for each COA based on the expected threat</li> <li>• Determine alternate construction location, methods, means, materials, and timelines to give the commander options</li> <li>• Determine real-property and real estate requirements</li> </ul>	Step 3: COA Development	<ul style="list-style-type: none"> <li>• Recommended updates to CAL</li> <li>• Recommended updates to EEFIs</li> <li>• Initial scheme of protection</li> </ul>	<ul style="list-style-type: none"> <li>• COA statements and sketches</li> <li>• Tentative task organization</li> <li>• Broad concept of operations</li> <li>• Revised planning guidance</li> <li>• Updated assumptions</li> </ul>
<ul style="list-style-type: none"> <li>• Updated running estimates</li> <li>• Revised planning guidance</li> <li>• COA statements and sketches</li> <li>• Updated assumptions</li> </ul>	<ul style="list-style-type: none"> <li>• Identify limitations and shortfalls of protection tasks for each COA</li> <li>• Determine branches, sequels, decision points, unintended consequences, and second and third order effects</li> <li>• Develop risk management and decision points for risk tolerance</li> <li>• Develop MOE and MOP</li> </ul>	Step 4: COA Analysis (War Game)	<ul style="list-style-type: none"> <li>• Initial DAL</li> <li>• Refined EEFI</li> <li>• Refined information collection plan</li> <li>• Initial risk management and risk tolerance decision point matrix</li> <li>• Refined scheme of protection</li> </ul>	<ul style="list-style-type: none"> <li>• Refined COAs</li> <li>• Potential decision points</li> <li>• War-game results</li> <li>• Initial assessment measures</li> <li>• Updated assumptions</li> </ul>
<ul style="list-style-type: none"> <li>• Updated running estimates</li> <li>• Refined COAs</li> <li>• Evaluation criteria</li> <li>• War-game results</li> <li>• Updated assumptions</li> </ul>	<ul style="list-style-type: none"> <li>• Compare economy-of-force and risk reduction measures</li> </ul>	Step 5: COA Comparison	<ul style="list-style-type: none"> <li>• Refined protection priorities</li> <li>• Refined CAL/DAL</li> <li>• Refined EEFI</li> <li>• Refined scheme of protection</li> </ul>	<ul style="list-style-type: none"> <li>• Evaluated COAs</li> <li>• Recommended COAs</li> <li>• Updated running estimates</li> <li>• Updated assumptions</li> </ul>
<ul style="list-style-type: none"> <li>• Updated running estimates</li> <li>• Evaluated COAs</li> <li>• Recommended COA</li> <li>• Updated assumptions</li> </ul>	<ul style="list-style-type: none"> <li>• Brief scheme of protection</li> <li>• Brief protection task specifics, as required</li> </ul>	Step 6: COA Approval  Warning Order	<ul style="list-style-type: none"> <li>• Refined protection priorities</li> <li>• Refined EEFI</li> <li>• Refined CAL/DAL</li> <li>• Refined scheme of protection</li> </ul>	<ul style="list-style-type: none"> <li>• Commander-selected COA and modifications</li> <li>• Refined commander's intent, CCIRs, and EEFIs</li> <li>• Updated assumptions</li> </ul>

**Table 2-2. Protection working group actions (continued)**

<b>Key Input</b>	<b>Protection Actions</b>	<b>Steps</b>	<b>Protection Output</b>	<b>Key Output</b>
<ul style="list-style-type: none"> <li>• Commander-selected COA with any modifications</li> <li>• Refined commander's intent, CCIRs, and EEFIs</li> <li>• Updated assumptions</li> </ul>	<ul style="list-style-type: none"> <li>• Refine and develop protection annex and supporting appendixes</li> </ul>	Step 7: Orders Production, Dissemination, and Transition	<ul style="list-style-type: none"> <li>• Protection annex and supporting appendixes</li> </ul>	<ul style="list-style-type: none"> <li>• Approved operation plan or order</li> <li>• Subordinate understanding of plan or order</li> </ul>

**Legend:**

CAL	critical asset list
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
RFI	request for information

## **Chapter 3**

# **Protection in Preparation**

The force is often most vulnerable to an enemy or adversary surprise attack during preparation. Preparation creates conditions that improve friendly force opportunities for success. It requires commander, staff, unit, and Soldier actions to ensure that the force is trained, equipped, and ready to execute operations. Preparation activities help commanders, staffs, and Soldiers understand a situation and their roles in upcoming operations. During the preparation phase, the protection focus is on deterring and preventing the enemy or adversaries from actions that would affect the combat power. The implementation of protection tasks with ongoing preparation activities helps prevent negative effects. Commanders ensure the integration of protection warfighting function tasks to safeguard bases, secure routes, and protect the force while it prepares 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 the threat and hazard effects and accelerates the mitigation of those effects.

## **CONSIDERATIONS**

3-1. As the staff monitors and evaluates the performance or effectiveness of friendly COA, ground- and space-based information collection operations 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 and 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. Chiefs of protection and planners stay alert for changing indicators and warnings in the operational environment that would signal new or fluctuating threats and hazards.

3-2. 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, 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 critical information requirements could be required based on changes to asset vulnerability and criticality when conjoined with the threat assessment.

3-3. Commanders who are exercising mission command direct and lead throughout the entire operations process as they provide supervision in concert with the process. Commanders' actions during preparation may also include—

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

3-4. 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—

- Superior, subordinate, and adjacent units.
- Civilian agencies and personnel that are part of the force or those that may be impacted by the task or control.

3-5. 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 during mission preparation through training, rehearsals, task organization, and resource allocation. Rehearsals, especially those using opposing force personnel, can provide a measure of protection plan effectiveness.

## **PROTECTION WITHIN PREPARATION ACTIVITIES**

3-6. Commanders, units, and Soldiers conduct preparation activities (as described in ADRP 5-0) to help ensure that the force is protected and prepared for execution. Protection is incorporated throughout the following preparation activities, 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 preoperation checks and inspections.
- Prepare terrain.
- Continue to build partnerships and teams.
- Conduct confirmation briefs.

### **CONTINUE TO COORDINATE AND CONDUCT LIAISON**

3-7. Coordination and liaison help ensure that leaders, internal and 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**

3-8. 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.

3-9. Information collection assets develop and refine the common operational picture of the area of interest. Relevant information from information collection helps protection cells and working groups fill information gaps, refine potential threats and hazards data into facts, validate assumptions, and finalize the plan before execution in order to improve protection efforts.

## INITIATE SECURITY OPERATIONS

3-10. Commanders and staffs continuously plan and coordinate security operations throughout the conduct of operations. 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.

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

3-12. 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 combined arms units in combat, fighting to gain time with differing levels of capability and autonomy for independent action. Operational area security focuses on the protected force, installation, route, or area. Local security protection ranges from echelon headquarters to reserves and sustainment forces. Local security can be part of the sustaining base or part of the area infrastructure.

## MANAGE AND PREPARE TERRAIN

3-13. Terrain management is the process of allocating terrain by establishing areas of operation, designating assembly areas, and specifying locations for units and activities to deconflict activities that might interfere with each other. Staffs deconflict operations, control movements, and deter the fratricide of units and unified action partners as they maneuver through the area of operations. The secure movement of theater resources is essential to ensure that commanders receive the forces, supplies, and equipment needed to support the operation 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.

## PROTECTION CELL AND WORKING GROUP

3-14. Preparation includes increased application and emphasis on protection measures. During preparation, the protection cell/working group—

- Provides recommendations to refine the scheme of protection.
- 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 on survivability position improvement.
- Liaisons and coordinates with adjacent and protected units.
- Determines protection indicators and warnings for information collection operations.
- Monitors defended asset training.
- Confirms backbriefs.
- Analyzes and proposes vulnerability reduction measures.

- Provides recommended revisions to tactical standing operating procedures.
- Disseminates personnel recovery guidance.

3-15. During preparation, the protection cell/working group ensures that the controls and risk reduction measures developed during planning have been implemented and are reflected in plans, standing 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 cell and working group maintain a list of prioritized threats, adverse conditions, and hazard causes. The challenge is to find the root cause or nature of a threat or hazard so that the most effective protection solution can be implemented and disseminated.

3-16. Subworking groups feed information to the protection working group and incorporate elements from the other warfighting functions. Commanders augment the working groups with other unit specialties and unified action partners depending on the operational environment 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, essential elements of friendly information, CALs, DALs, and the scheme of protection.

### **ANTITERRORISM WORKING GROUP**

3-17. 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—

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

### **COUNTER IMPROVISED EXPLOSIVE DEVICE WORKING GROUP**

3-18. The counter improvised explosive device working group is led by the EOD officer and includes members from 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 area of operations improvised explosive device networks.
- Recommends the protection working group improvised explosive device defeat initiatives relating to equipment, intelligence, and operations.
- Identifies improvised explosive device defeat requirements and issues throughout the unit, including separate and subordinate units.

### **CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR WORKING GROUP**

3-19. The CBRN working group is led by the CBRN officer and includes members from 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 consequence management and remediation efforts.
- Refines the CBRN threat, hazard, and vulnerability assessments.

## **Chapter 4**

# **Protection in Execution**

Commanders exercising mission command direct, lead, and assess organizations and Soldiers during execution. As operations develop and progress, commanders interpret information that flows from systems for indicators and warnings that signal the need for execution or adjustment decisions. Indicators and warnings can come from products such as space-based imagery and signals intelligence, among others. Commanders may direct and redirect the way combat power is applied or preserved and may adjust the tempo of operations through synchronization. Effective execution is aided by seizing the initiative through action and accepting prudent risk to exploit opportunities. 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. The synchronization of applied protection warfighting function tasks and systems helps prevent threat and hazard effects to the force. Employed mitigation measures, 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.

## **PROTECTION IN UNIFIED LAND OPERATIONS**

4-1. Unified land operations is the Army operating concept and its contribution to unified action. The central idea of unified land operations is how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability or defense support of civil authorities operations to prevent or deter conflict, prevail in war, and create conditions for a favorable conflict resolution. Where possible, military forces and unified action partners seek to prevent or deter threats. However, if necessary, military forces possess the capability to prevail over aggression in unified land operations.

4-2. Commanders and leaders must be flexible and adaptive as they seek opportunities to seize, retain, and exploit the initiative. 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 area of operations. 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.

4-3. Commanders must accept risk to exploit 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 technological advancements, such as geospatial intelligence products or processes, to minimize fratricide and increase the probability of mission accomplishment.

4-4. Accurate assessment is essential for effective decisionmaking 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 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 and systems that comprise the protection warfighting function.

## **OFFENSE**

4-5. An *offensive task* is a task conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers (ADRP 3-0). They 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 tasks compels the enemy or adversary to react, creating or revealing additional weaknesses that the attacking force can exploit.

4-6. Protection can be derived through audacity, 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.

4-7. Seizing, retaining, and exploiting initiative and opportunity are the essences of the offense. 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.

4-8. Protection measures and tasks are applied within the principles of protection and are conducted to preserve combat power by reducing risk or mitigating vulnerability. Air and missile defense systems defend maneuver forces, critical infrastructure, and logistics bases/base camps. Although all commanders have some organic capability for air defense and warning, enhanced capabilities are often provided by higher-echelon commanders and air component organizations utilizing ground- and space-based systems.

4-9. The preservation of combat power often requires the immediate restoration of critical skills and capabilities. All mission-capable personnel contribute to combat power in operations, but certain skills and capabilities can turn the tide of a battle or an engagement, and immediate personnel recovery becomes essential. Therefore, personnel recovery operations are closely integrated into all phases, branches, and sequels associated with operations to ensure that isolated and captured Soldiers are quickly recovered and returned to the fight. Personnel recovery operations can be facilitated through coordination with the U.S. Army Space and Missile Defense Command Mission Management Center, the proponent for joint friendly force tracking. Combat arms crews and aviation crews and pilots are often a high-demand personnel asset during offensive operations, and their recovery may require specific guidance.

4-10. 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.

4-11. An enemy or adversary 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, while ensuring that food and water are safe for consumption.

4-12. Offensive tasks are executed with 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. An increased information operations

condition during the offense enhances mission command and protection posture through prevention and situational understanding. 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.

4-13. Increased operating tempo can result in combat identification errors and fratricide. Deliberate precautions are taken to prevent surface-to-surface, surface-to-air, and air-to-surface friendly fire incidents through positive and procedural control mechanisms, standard unit marking schemes and patterns, and sound navigation and reporting procedures. Friendly and enemy or adversary forces often use obscurants for protection during movement and maneuver or to create surprise through diversion.

4-14. The protection of critical combat power systems requires survivability assets that alter the physical environment to provide or improve cover, concealment, and camouflage. Such terrain modifications may require significant amounts of time, making them unfeasible 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.

4-15. 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 force protection condition), but may be vulnerable to enemy or adversary remnant forces requiring a response that is beyond base camp capabilities. 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. 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

4-16. A *defensive task* is a task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks (ADRP 3-0). Commanders can use the defense to gain time and economize forces so that offensive tasks can be executed elsewhere. Defensive tasks—

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

4-17. No matter which defensive task is performed, the survivability of mission command 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 or adversary 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 force protection conditions 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.

4-18. In 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 or adversary reconnaissance while creating standoff distances from enemy or adversary 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.

4-19. Mobile defensive schemes are 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 protects the force from fratricide by 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 and are, therefore, typically well rehearsed.

4-20. Defense could potentially begin with enemy or adversary bombardment, resulting in a siege that could 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.

4-21. Commanders integrate air defense sensors and intelligence assets into a comprehensive network to provide effective early warning of an aerial attack to friendly forces. They develop or contribute to an airspace management 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.

4-22. 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.

4-23. 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. All 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. Fire support should engage the enemy or adversary well forward, before it gets to friendly delaying positions. Inflicting maximum casualties reduces enemy or adversary combat power, disrupts its approach, and suppresses and destroys accompanying indirect-fire assets. Massed fires on avenues of approach and canalizing terrain destroys high-priority targets, limits enemy or adversary maneuver, and prevents enemy or adversary attacks from gaining momentum from any limited successes.

4-24. Effective and disciplined OPSEC protects essential elements of friendly information, preventing enemy or adversary reconnaissance and other information collection capabilities from gaining an advantage through identifiable or observable pieces of friendly information or activities. This is key during defensive and retrograde operations to prevent surprise. OPSEC and information protection activities deny the enemy or adversary access to information systems and prevent network intrusion, degradation, or destruction through computer network defensive TTP. Electronic protection capabilities prevent an attacking enemy or adversary from using the electromagnetic spectrum to degrade, neutralize, or destroy friendly combat capabilities.

4-25. Preventable accidents can thwart mission success during combat operations. Leaders must continue to assess the environment and routine activities for the evidence of hazards that can lead to the preventable loss of combat power through accidents and events. Personnel rest and recovery plans, leader experience, and skill levels are safety considerations that influence risk management decisions during combat operations.

## STABILITY

4-26. *Stability operations* is an overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-0). Stability tasks are conducted during decisive action. They support a host nation or interim government or a transitional military authority when no government exists. Stability tasks involve coercive and constructive actions, help establish or maintain a safe and secure environment, and facilitate reconciliation among local or regional adversaries. Stability tasks can also help establish political, legal, social, and economic institutions while supporting the transition to legitimate host nation governance. Stability tasks cannot succeed if they only react to enemy or adversary initiatives; they must maintain the initiative by pursuing objectives that resolve the causes of instability.

4-27. Military forces must quickly seize and retain the initiative when conducting stability tasks 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.

4-28. Fragile states suffer from institutional weaknesses that threaten the survival of their central government (see FM 3-07 for more information). Stability strategies are developed to achieve conflict resolution by enhancing host nation legitimacy, civil institution development through capacity-building activities, and progress toward justice 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:

- Safe and secure environment.
- Established rule of law.
- Social well-being.
- Stable government.
- Sustainable economy.

4-29. When conducting stability tasks, protection is essential for success at all operating levels, from tactical to strategic. Like offensive and defensive tasks, stability tasks 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 tasks may require a scheme of protection that is more resource-intensive and more prescribed than typical security operations.

4-30. Stability tasks 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. Enemies 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 tasks 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.

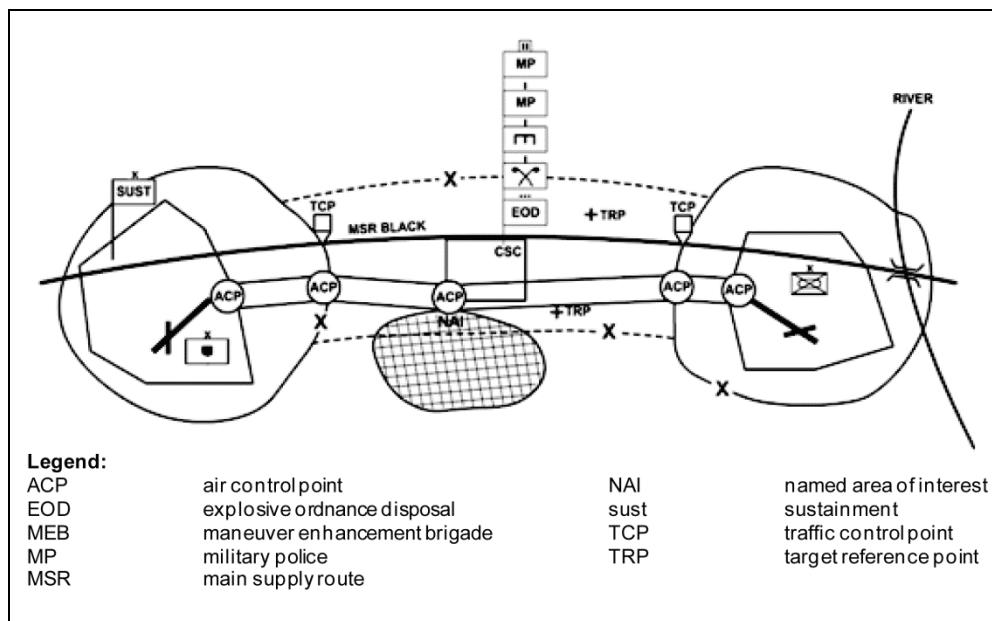
4-31. Army units should account for the protection of civilians from other hazards, in addition to their own direct and indirect fires. Particularly in counterinsurgency and stability situations, population support may be the center gravity; and it is unlikely that support can be achieved if the population is not protected.

Across the entire range of military operations, 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.

4-32. 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 is a high density of civilians throughout the area, in unexpected locations, and outside the common 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, the adoption of a similar mind-set regarding civilian casualty avoidance is crucial.

4-33. Stability tasks 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, operational security, and AT based on METT-TC.

4-34. Adversaries often blend in with the local populace and are difficult to identify, making heightened levels of awareness the norm. 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 may also expose vulnerabilities that enemies and adversaries will 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 (figure 4-1).



**Figure 4-1. Sample movement corridor**

4-35. Inform and influence activities are essential during operations characterized by stability tasks and are a key protection enabler. Commanders and Soldiers engage 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. Leaders and Soldiers conduct inform and influence tasks to facilitate the delivery of friendly messages (matched by actions on the ground) to key leaders and population groups.

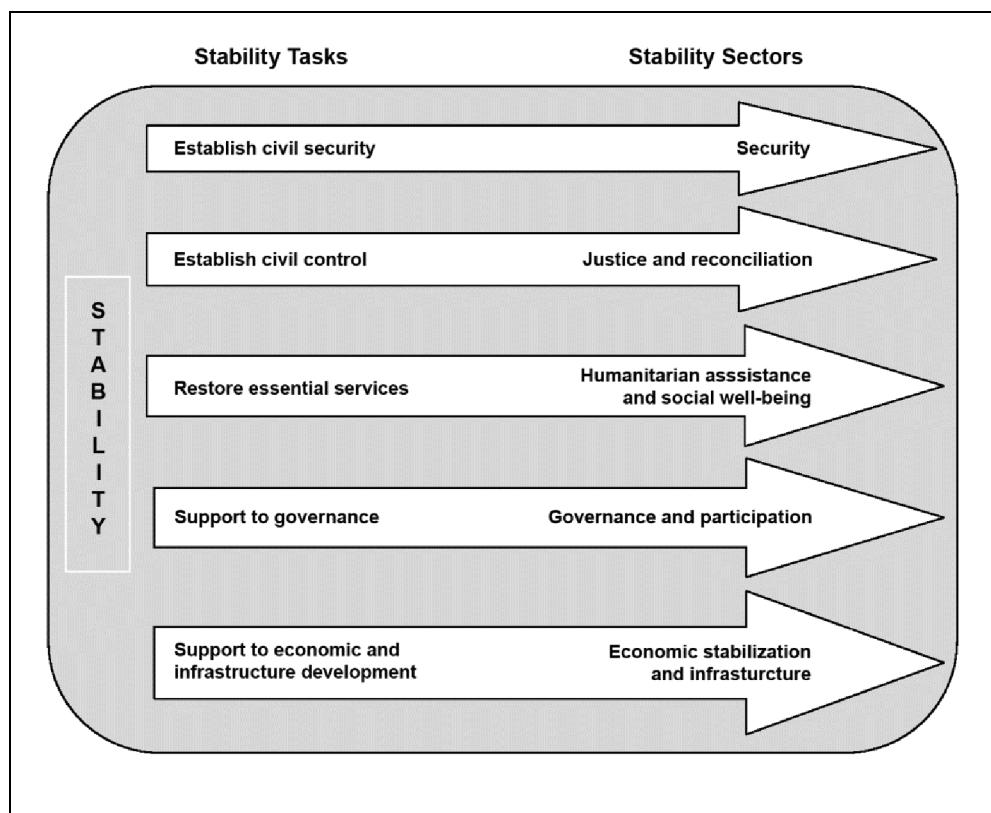
4-36. The close proximity of civilians and Soldiers can also promote force health protection issues (such as communicable disease) through close contact with local civilians, detainees, or local foods. Stability

operations are often enduring missions that 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.

4-37. 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-government approach that sets the conditions necessary to enable the elements of national power (diplomatic, information, military, and economic). Stability operations tasks include—

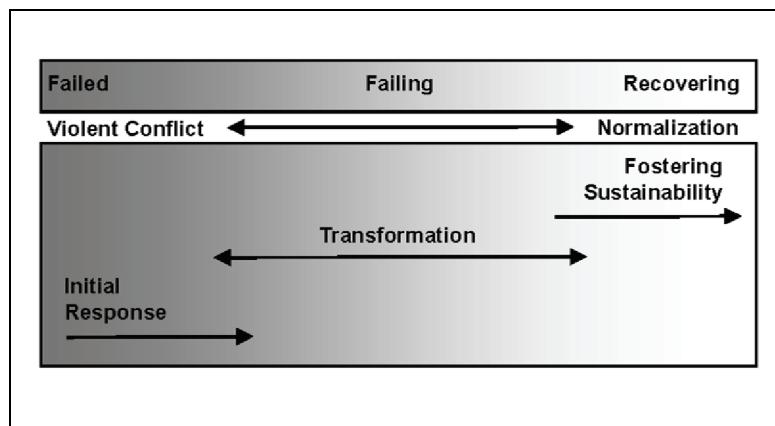
- Establishing civil security.
- Establishing civil control.
- Restoring essential services.
- Supporting governance.
- Supporting economic and infrastructure development.

4-38. Inform and influence activities are also essential to the success of these operations. Unified action and interagency participation are achieved by nesting the five stability tasks with the five stability sectors identified by the Department of State (figure 4-2).



**Figure 4-2. Whole-government, integrated approach to stability**

4-39. In order to support operations characterized by stability tasks, the scheme of protection is developed and refined to link operational goals and end states with stability and protection tasks. Stability tasks and security sectors are integrated within the stability framework (figure 4-3) 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—which are the fundamental measures of success in conflict transformation.



**Figure 4-3. Stability framework**

4-40. 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.

---

*Note.* See JP 3-07 and FM 3-07 for more information on stability operations.

---

## CIVIL SECURITY

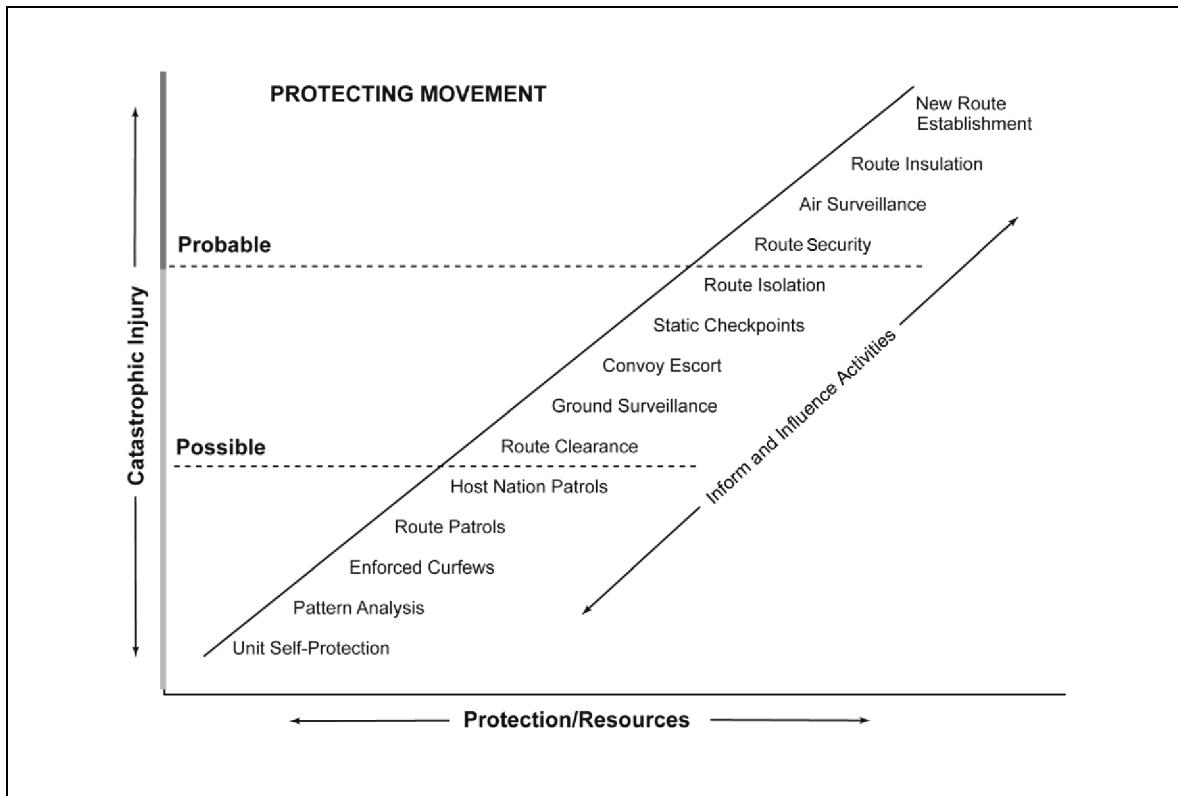
4-41. An initial response to civil security operations conducted in a failing state may emphasize the establishment of civil security as a means of protecting critical assets, facilities, personnel, or the freedom of movement. Border or boundary control operations protect the integrity and sovereignty of the host nation while providing protection against illegal entrants, contraband, disease, and the enemy or adversary. Border operations can be conducted as a type of area defense operation or through area security tasks and TTP integrating checkpoints, mobile patrols, and designated fixed sites.

4-42. Civil security focuses on establishing a stable security environment and developing legitimate institutions and infrastructure to maintain that environment. While securing 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.

4-43. Stability tasks in decisive action are often characterized by retaining the initiative. Tactical and nontactical movement occurs throughout the area of operations as a matter of military necessity and as a component of a normalized society. Controlling and maintaining the freedom of movement (figure 4-4) in the area of operations—

- 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 law and order operations as a function of traffic regulation enforcement.

4-44. Commanders should employ pattern analysis to identify patterns of activities, associations, and events within the area of operations. The basic premise of pattern analysis uses activities, associations, and events to identify the components of the threat to discern similarities of time, geography, personnel, victims, and *modus operandi*. Deliberate inform and influence activities are often essential when implementing movement or traffic controls and restrictions on a given population in an area of operations. Commanders can leverage host nation security, police, and civic organizations through inform and influence 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 supporting troops engaged in controlling or limiting movement take deliberate precautions to prevent fratricide.



**Figure 4-4. Freedom-of-movement control**

4-45. 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. Until a legitimate civil government can assume responsibility for the security sector, military forces perform the tasks associated with civil security. At the same time, they help develop host nation security and police forces. Building partnership capacity is essential in order to develop host nation capabilities and capacities related to security tasks. This type of assistance spans from individual training and education to unit exercises that conduct training assistance. Building host nation capacity for civil security is paramount to establishing the foundation for lasting civil order. Community-oriented police services under civilian control that 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.

4-46. 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. They must also know sound AT and OPSEC procedures that are included in their personnel recovery plans and battle drills. 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 during heightened awareness. 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 ordnance, explosives, and CBRN threats and hazards may exist in the operational environment at the cessation of hostilities or may be introduced deliberately or accidentally. These threats and hazards may require an integrated EOD, demining, or foreign consequence management response.

## **CIVIL CONTROL**

4-47. Transformation occurs in the stability framework as civil security is achieved and certain risks are reduced, making other stability tasks possible. Civil control regulates behavior in an area of operations and builds the foundation for order, justice, and the rule of law. There is 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 host nation while a patriotic event could lead to the massing of civilians at key governmental locations. The end of the academic school period may increase the number of adolescents in the streets of certain regions.

4-48. 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 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 technologies provide commanders with the ability to demonstrate a measured force response, which can contribute to the protection of the force and the civilian populace. The presence of well-trained, -equipped, and -disciplined troops with lethal or violent capability can often be sufficient to deter violence, confrontation, or conflict while conducting stability tasks. Law enforcement activities transition from military personnel to civilian police who are supplied by the host nation or as part of a third-world or international policing effort. Police training, development, and mentoring may continue until normalization is achieved. Commanders may authorize, develop, and train civilian volunteers to augment civil control efforts or to serve as a police auxiliary.

4-49. In order to successfully provide for the safety and security of the populace, an effective judiciary branch and a functioning corrections system must complement the state security institutions. Together with governance and civil security, civil control is a core element of security sector reform. This reform sets the foundation for broader government and economic reform and for successful humanitarian relief and social development.

4-50. 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**

4-51. Areas that have been neglected or damaged as a result of conflict may require the protection of essential infrastructure. Power generation, water treatment, 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 TTP. 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 operational environment.

Inform and influence activities also involve significant Soldier and leader engagement with the local population as a means of informing the public while also gathering information on the environment.

4-52. By integrating military and host nation police forces early on, commanders get police or street level information on local criminal elements, including organized crime. Through combined police operations, commanders help establish a safe and secure environment for U.S. forces, host nation forces, and civilians. Such multinational operations also improve 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.

4-53. Efforts to restore essential services ultimately contribute to achieving a stable democracy, a sustainable economy, and the social well-being of the population in a secure environment. It provides legitimacy to the government and gives a sense of normalcy back to the population.

## GOVERNANCE SUPPORT

4-54. When conditions in a failed or failing state become extreme and prevent the host nation government from conducting civic functions, military forces must be capable of providing support to governance and civic functions while acting as a transitional military authority according to the international law or mandate. In this capacity, 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 the 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.

4-55. High-risk personnel, AT, OPSEC, and personnel recovery plans and procedures should include considerations for the protection of key civil leaders.

---

*Note.* See FM 3-07 for more information on providing support to governance.

---

## ECONOMIC AND INFRASTRUCTURE DEVELOPMENT

4-56. Protection capabilities are often applied to support economic and infrastructure developmental efforts during stability tasks to foster sustainability. 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 semipredictable cycle that may be seasonal, coinciding with events such as agricultural harvests or conditions that make commodity gathering or production optimal. 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.

4-57. 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 of infrastructure include construction services, engineering, and physical infrastructure in the following sectors:

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

## **DEFENSE SUPPORT OF CIVIL AUTHORITIES**

4-58. The defense support of civil authorities is 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. The 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 authorities tasks in support of homeland operations when the size and scope of events exceed the capabilities or capacities of domestic civilian agencies.

4-59. Leaders must understand the unique operational and mission variables associated with this complex operational environment and be able to rapidly transition—from conventional wartime and stability roles to the constraints inherent to the homeland—in order 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 Act* (Title 18, U.S. Code, Chapter 67, Section 1385), information collection, and the standing rules for the use of force. The integration of Army capabilities into the guidance and parameters set forth by national policy will require the innovative integration of mission command and other warfighting functions in order 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 will result in protecting Soldiers (in various duty statuses) and civilian personnel from hostile actions while conducting defense support of civil authorities tasks. The requirement to deploy into a constrained operational environment and operate with joint and interagency elements requires a unity of command, with flexible Soldiers who are able to improvise and adapt systems intended for combat into a robust civilian disaster response system based on the National Incident Management System.

4-60. Soldiers who are engaged in the defense support of civil authorities may face threats or hazards from criminals, disease, 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. An accurate, ongoing assessment of risk is vital in determining whether and how the commander will provide the defense support of civil authorities.

4-61. The CBRN response conducted by the 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 is tiered response packages to support state and federal authorities.

4-62. 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.

4-63. 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 probable. 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.

---

*Note.* See FM 3-28 for more information of the defense support of civil authorities.

---

## PROTECTION CELL AND WORKING GROUP

4-64. The protection cell/working group monitors and evaluates several critical ongoing functions associated with the execution of operational actions or changes that impact protection cell proponents. The protection cell/working group—

- Ensures that the protection focus supports the decisive operation.
- Reviews and adjusts the commander's critical information requirements derived from protection tasks.
- Reviews changes to graphic control measures and boundaries for the increased risk of fratricide.
- Evaluates the effectiveness of battle tracking for constraints on personnel recovery.
- Monitors the employment of security forces for gaps in protection or unintended patterns.
- Evaluates the effectiveness of liaison personnel for protection activities.
- Evaluates movement coordination and control to protect critical paths.
- Monitors adjacent unit coordination procedures for terrain management vulnerabilities.
- Monitors readiness rates of response forces involved in fixed-site protection.
- Monitors force health protection.
- Coordinates with the U.S. Army Space and Missile Defense Command for issues regarding personnel recovery operations.

4-65. Staff members are also particularly alert for reports and events that meet the commander's critical information requirements. Once a threat to a critical or defended asset is detected by monitoring and evaluating running estimates and MOEs for indicators and warnings, the protection cell alerts the unit responsible for protecting the asset or recommends additional protective action. Unit commanders respond to the assessment of the threat or deliberate warning and then execute contingency or response plans. For example, if a threat force attacks an asset, the commander applies combat power to defeat it. Commanders are alerted by the commander's critical information requirements if the capability of the threat force reflects a variance that exceeds anticipated and projected combat power ratios. They may respond to the increased risk by rendering an execution or adjustment decision to commit additional assets in the form of response forces or fires that are necessary to defeat or neutralize the threat.

4-66. Events frequently occur that prompt commanders to reevaluate assessed threats and their vulnerabilities. These reevaluations are normally due to a significant change in the situation; for example, a change in the mission, the loss of a critical asset, a newly discovered enemy or adversary capability, an environmental change, a political or civil event, or a change in the rules of engagement. Commanders must stay as sensitive to the risk calculus as they are to changes in readiness rates or available manpower in terms of immediate combat power. When commanders adjust or change their risk calculation, the process begins anew. The staff compares the new friendly situation to the known enemy or adversary situation, develops controls, recommends priorities and decision points, and then implements the decisions. The protection cell/working group determines—

- Where protection assets can best help mission accomplishment with acceptable risk.
- If protection assets should be committed to the mission immediately or be held in reserve.
- If assets should be moved due to a change in the DAL.
- If the commander needs to request assistance and, if so, for what purpose.

4-67. There may be a change in the rules of engagement or the political, civil, or environmental situation. A failure to understand and comply with established rules of engagement can result in fratricide, mission failure, or national embarrassment. Commanders and Soldiers must limit collateral damage and apply force precisely to accomplish the mission without causing the unnecessary loss of life, suffering, or damage to property and infrastructure. The unanticipated changes may not require immediate action. However, commanders must consider how changes relate to the mission as they mitigate the vulnerability to civilians and the environment. They must—

- Determine if immediate actions will minimize damage.
- Decide if actions will affect mission accomplishment.
- Determine if the staff balance requires protective actions.
- Ensure overall mission accomplishment.

## **Chapter 5**

# **Protection Assessment**

Protection assessment is an essential, continuing activity that 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. Commanders and staffs monitor the current situation to—

- Collect data to assess.
- Evaluate the progress toward attaining the end-state conditions, achieving objectives, and performing tasks.
- Recommend or direct actions for improvement.

## **CONTINUOUS ASSESSMENT**

5-1. *Assessment* is the determination of the progress toward accomplishing a task, creating an effect, 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 operational environment to determine what changes might affect the conduct of operations.

5-2. 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.

5-3. The assessment plan is enabled by monitoring and evaluating criteria derived from the protection warfighting function tasks. Criteria used to monitor and evaluate the situation or operation may be represented as a MOE or a 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 essential elements of friendly information and may generate information requirements. MOEs and MOPs can be significant decision support tools and may drive transition periods, resource allocations, and other critical decisions.

## **ASSESSMENT DURING PLANNING**

5-4. The staff conducts analysis to assess threats, hazards, criticality, vulnerability, and capability to assist commanders in determining protection priorities, task organization decisions, and the integration of protection tasks.

5-5. The protection cell evaluates the COA during the military decisionmaking process against 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**

5-6. Assessment occurs during preparation and includes activities required to maintain situational understanding; monitor and evaluate running estimates, tasks, MOEs, and MOPs; and identify variances for decision support. These assessments generally provide commanders with a composite estimate of preoperational force readiness or status in time to make adjustments.

5-7. During preparation, the protection cell focuses on threats and hazards that can influence preparatory activities, which includes monitoring new Soldier integration programs and movement schedules and evaluating live-fire requirements for precombat checks and inspections. The protection cell may evaluate training and rehearsals or provide coordination and liaison to facilitate effectiveness in high-risk or complex preparatory activities, such as movement and logistics preparation.

## **ASSESSMENT DURING EXECUTION**

5-8. The protection cell monitors and evaluates the progress of current operations to validate assumptions made in planning and to continually update changes to the situation. The protection cell and protection working group continually meet to monitor threats to the CAL and DAL, 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 unforeseen threat or hazard or to mitigate a developing vulnerability. They also track the status of protection assets and evaluate the effectiveness of the protection systems as they are employed. Additionally, the protection cell and protection working group monitor 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.

5-9. The protection cell and protection working group monitor and evaluate—

- 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 AT measures.

## **MEASURES OF EFFECTIVENESS AND PERFORMANCE**

5-10. Criteria in the forms of MOEs and MOPs help determine the progress toward attaining end-state conditions, achieving objectives, and performing tasks. A MOE helps determine if a task is achieving its intended results, and a MOP helps to 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**

5-11. 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). A MOE helps measure changes in positive and negative conditions and is oriented to mission accomplishment, focuses on the results or consequences of an action, and is used to assess changes in the operational environment. This is more often a subjective assessment as it tends to measure long-term results. As a result, MOEs may consist of a series of indicators that are used to judge success or failure.

5-12. Significant changes in some conditions of the operational environment are subtle and only occur over a long period of time, yet 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 risk.

5-13. 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 military decisionmaking process allows commanders to accelerate decisionmaking 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 essential elements of friendly information and indicators or warnings that relate to the development of protection priorities.

5-14. 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 anticipated threat combat power ratio, resulting in an increased risk equation.
- Ineffective supporting efforts, leading to a cumulative failure of more critical elements.

5-15. 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

5-16. A *measure of performance* is a criterion used to assess friendly actions that is tied to measuring task accomplishment (JP 3-0). A 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 whether a task was performed successfully. FM 7-15 provides a table with MOPs that can be used to develop standards for each task. Some specific MOPs may be altered for their relevance to the operational environment, or they may be omitted; however, all changes to established MOPs should be disseminated vertically and horizontally among headquarters and participants in an operation or activity.

## LESSONS LEARNED INTEGRATION

5-17. The way that 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 sound stewardship practices and risk management principles required to ensure the minimal losses 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 cell 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 decisions accurate?
  - 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 ADRP 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

<b>ADP</b>	Army doctrine publication
<b>ADRP</b>	Army doctrine reference publication
<b>AR</b>	Army regulation
<b>AT</b>	antiterrorism
<b>ATTN</b>	attention
<b>ATTP</b>	Army tactics, techniques, and procedures
<b>CAL</b>	critical asset list
<b>CARVER</b>	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
<b>CBRN</b>	chemical, biological, radiological, and nuclear
<b>COA</b>	course of action
<b>DA</b>	Department of the Army
<b>DAL</b>	defended asset list
<b>DC</b>	District of Columbia
<b>DOD</b>	Department of Defense
<b>DODI</b>	Department of Defense instruction
<b>EOD</b>	explosive ordnance disposal
<b>FM</b>	field manual
<b>IDN</b>	initial distribution number
<b>JP</b>	joint publication
<b>MANSCEN</b>	Maneuver Support Center of Excellence
<b>METT-TC</b>	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
<b>MO</b>	Missouri
<b>MOE</b>	measure of effectiveness
<b>MOP</b>	measure of performance
<b>MSHARPP</b>	mission, symbolism, history, accessibility, recognizability, population, and proximity
<b>NBC</b>	nuclear, biological, and chemical
<b>OPSEC</b>	operations security
<b>No.</b>	number
<b>PMESII-PT</b>	political, military, economic, social, information, infrastructure, physical environment, and time
<b>TTP</b>	tactics, techniques, and procedures
<b>UXO</b>	unexploded ordnance
<b>WMD</b>	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)

**assessment**

Determination of the progress toward accomplishing a task, creating an effect, 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 US forces. (JP 3-10)

**convoy security operation**

A specialized kind of area security operations conducted to protect convoys. (FM 3-90)

**critical asset list**

A prioritized list of assets, normally identified by phase of the operation and approved by the joint force commander, that should be defended against air and missile threats. (JP 3-01)

**\*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.

**defended asset list**

A listing of those assets from the critical asset list prioritized by the joint force commander to be defended with the resources available. (JP 3-01)

**defensive task**

A task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks. (ADRP 3-0)

**enemy**

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

**force protection**

Preventative 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 friendly. (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, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0)

**information collection**

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

**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)

**neutral**

(Army) A party identified as neither supporting nor opposing friendly or enemy forces. (ADRP 3-0)

**offensive task**

A task conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers. (ADRP 3-0)

**operations security**

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. (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. (ADRP 3-0)

**stability operations**

An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 3-0)

**target identification**

The accurate and timely characterization of a detected object on the battlefield as friend, neutral, or enemy. This aspect of combat identification is time sensitive and directly supports a combatant's shoot or don't-shoot decision for detected objects on the battlefield. (FM 3-20.15)

**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. (ADRP 3-0)

**This page intentionally left blank.**

## **References**

Field manuals and selected joint publications are listed by new number followed by old number. Most Army doctrinal publications are available online: <<http://www.apd.army.mil/>>. Most joint publications are available online at <[http://www.dtic.mil/doctrine/new\\_pubs/jointpub.htm](http://www.dtic.mil/doctrine/new_pubs/jointpub.htm)>.

## **REQUIRED PUBLICATIONS**

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

ADRP 1-02. *Operational Terms and Military Symbols*. 31 August 2012.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

## **RELATED PUBLICATIONS**

These documents contain relevant supplemental information.

ADP 3-0 (FM 3-0). *Unified Land Operations*. 10 October 2011.

ADP 3-09. *Fires*. 31 August 2012.

ADP 3-37. *Protection*. 31 August 2012.

ADP 6-0 (FM 6-0). *Mission Command*. 17 May 2012.

ADRP 2-0. *Intelligence*. 31 August 2012.

ADRP 3-0. *Unified Land Operations*. 16 May 2012.

ADRP 3-09. *Fires*. 31 August 2012.

ADRP 5-0. *The Operations Process*. 17 May 2012.

ADRP 6-0. *Mission Command*. 17 May 2012.

AR 525-28. *Personnel Recovery*. 5 March 2010.

Army Directive 2011-04. *Army Protection Program*. 31 January 2011.

ATTP 3-11.23. *Multi-Service Tactics, Techniques, and Procedures for Weapons of Mass Destruction Elimination Operations*. 10 December 2010.

ATTP 3-39.10. *Law and Order Operations*. 20 June 2011.

ATTP 3-39.32. *Physical Security*. 3 August 2010.

ATTP 3-90.4. *Combined Arms Mobility Operations*. 10 August 2011.

ATTP 4-02. *Army Health System*. 7 October 2011.

ATTP 4-32. *Explosive Ordnance Disposal Operations*. 19 December 2011.

DODI 2000.16. *DOD Antiterrorism (AT) Standards*. 2 October 2006.

FM 3-07. *Stability Operations*. 6 October 2008.

FM 3-11. *Multiservice Doctrine for Chemical, Biological, Radiological, and Nuclear Operations*. 1 July 2011.

FM 3-11.3. *Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Contamination Avoidance*. 2 February 2006.

FM 3-11.4. *Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection*. 2 June 2003.

FM 3-11.5. *Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination*. 4 April 2006.

FM 3-11.21. *Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Consequence Management Operations*. 1 April 2008.

FM 3-20.15. *Tank Platoon*. 22 February 2007.

FM 3-28. *Civil Support Operations*. 20 August 2010.

## **References**

---

- FM 3-34.400. *General Engineering*. 9 December 2008.
- FM 3-37.2. *Antiterrorism*. 18 February 2011.
- FM 3-39. *Military Police Operations*. 16 February 2010.
- FM 3-39.40. *Internment and Resettlement Operations*. 12 February 2010.
- FM 3-50.1. *Army Personnel Recovery*. 21 November 2011.
- FM 3-55. *Information Collection*. 23 April 2012.
- FM 3-90. *Tactics*. 4 July 2001.
- FM 4-01.45. *Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations*.  
5 January 2009.
- FM 5-103. *Survivability*. 10 June 1985.
- FM 5-415. *Fire-Fighting Operations*. 9 February 1999.
- FM 7-15. *The Army Universal Task List*. 27 February 2009.
- FM 27-10. *The Law of Land Warfare*. 18 July 1956.
- FM 90-7. *Combined Arms Obstacle Integration*. 29 September 1994.
- JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 16 June 2009.
- JP 3-0. *Joint Operations*. 11 August 2011.
- JP 3-01. *Countering Air and Missile Threats*. 23 March 2012.
- JP 3-07. *Stability Operations*. 29 September 2011.
- JP 3-07.2. *Antiterrorism*. 24 November 2010.
- JP 3-10. *Joint Security Operations in Theater*. 3 February 2010.
- JP 3-13.3. *Operations Security*. 4 January 2012.
- JP 3-33. *Joint Task Force Headquarters*. 16 February 2007.
- Title 18, United States Code. *Crimes and Criminal Procedure*.

## **RECOMMENDED READING**

- DODI 6055.17. *DOD Installation Emergency Management (IEM) Program*. 13 January 2009.
- FM 2-0. *Intelligence*. 23 March 2010.
- FM 3-01. *U.S. Army Air and Missile Defense Operations*. 25 November 2009.
- FM 3-19.12. *Protective Services*. 11 August 2004.
- FM 3-52. *Army Airspace Command and Control in a Combat Zone*. 1 August 2002.
- FM 3-90.31. *Maneuver Enhancement Brigade Operations*. 26 February 2009.
- FM 4-02.17. *Preventive Medicine Services*. 28 August 2000.
- FM 4-30.51. *Unexploded Ordnance (UXO) Procedures*. 13 July 2006.
- FM 5-19. *Composite Risk Management*. 21 August 2006.
- JP 2-0. *Joint Intelligence*. 22 June 2007.
- JP 3-08. *Interorganizational Coordination During Joint Operations*. 24 June 2011.
- JP 3-11. *Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments*.  
26 August 2008.
- JP 3-27. *Homeland Defense*. 12 July 2007.
- JP 3-28. *Civil Support*. 14 September 2007.
- JP 3-50. *Personnel Recovery*. 20 December 2011.
- JP 3-52. *Joint Airspace Control*. 20 May 2010.
- JP 6-0. *Joint Communications System*. 10 June 2010.

## **REFERENCED FORMS**

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

**This page intentionally left blank.**

# **Index**

## **A**

area of operations, 1-6

## **C**

camouflage, 1-10

chemical, biological,  
radiological, and nuclear,  
1-10

command and control, 4-13

commander's critical  
information requirements,  
4-13

composite risk management,  
1-4, 2-8

cover, 1-10

critical asset security, 1-4

definition, 1-4

## **F**

fratricide, 1-5, 1-6  
definition, 1-5

## **H**

hostile actions, 1-10

## **M**

movement corridor, 4-6

## **O**

operational area security, 1-3

## **P**

protection coordinator, 2-9,  
2-10

## **S**

situational awareness, 1-6

situational understanding, 1-5

stability, 1-3

survivability, 1-1

survivability operations, 1-10

## **T**

tactics, techniques, and  
procedures, 4-5

terrain, 1-9

## **W**

warfighting function, 4-5

**This page intentionally left blank.**

**ADRP 3-37**  
**31 August 2012**

By order of the Secretary of the Army:

**RAYMOND T. ODIERNO**  
*General, United States Army*  
*Chief of Staff*

Official:



**JOYCE E. MORROW**  
*Administrative Assistant to the  
Secretary of the Army  
1218003*

**DISTRIBUTION:**

*Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve:* To be distributed in accordance with the initial distribution number (IDN) 110502, requirements for ADRP 3-37.

**PIN: 102966-000**