

MSTP Pamphlet 3-0.1

Force Protection



MAGTF Staff Training Program (MSTP)

U.S. Marine Corps
December 2002

MSTP Pamphlet 3-0.1

Force Protection

This pamphlet supports the academic curricula of the Marine Air Ground Task Force Staff Training Program (MSTP).

U.S. Marine Corps
December 2002

UNITED STATES MARINE CORPS
MSTP Center (C 467) MCCDC
3300 Russell Road
Quantico, Virginia 22134-5069

6 December 2002

FOREWORD

1. **PURPOSE.** MSTP Pamphlet 3-0.1, *Force Protection*, provides guidance on how to plan and conduct force protection in coordination with the other warfighting functions.

2. **SCOPE.** This pamphlet is applicable across the spectrum of conflict and range of Marine air-ground task force (MAGTF) operations. It is intended for use by MAGTF and subordinate unit commanders and their staffs, although much of the material is applicable to fixed installations in the supporting establishment. It also provides force protection planning considerations to members of the operational planning team (OPT).

3. **SUPERSESSSION.** None.

4. **CHANGES.** Recommendations for improvements to this pamphlet are encouraged from commands as well as from individuals. The attached User Suggestion Form can be reproduced and forwarded to:

Commanding General (C 467)
Training and Education Command
3300 Russell Road
Quantico, Virginia 22134-5001

Recommendations may also be submitted electronically to:
opso@mstp.quantico.usmc.mil

5. **CERTIFICATION.** Reviewed and approved this date.

M.C. HAWKINS II
Lieutenant Colonel, U.S. Marine Corps
Director
MAGTF Staff Training Program Center
Marine Corps Combat Development Command
Quantico, Virginia

Throughout this pamphlet, masculine nouns and pronouns are used for the sake of simplicity. Except where otherwise noted, these nouns and pronouns apply to either sex.

USER SUGGESTION FORM

From:

To: Commanding General, Marine Corps Combat Development
Command (C 54), Quantico, Virginia 22134-5001

1. In accordance with the Foreword, individuals are encouraged to submit suggestions concerning this Pamphlet directly to the above addressee

Page _____

Article/Paragraph No. _____

Line No. _____

Figure/Table No. _____

Nature of Change:

Add

Delete

Change

Correct

2. Proposed Text: (Verbatim, double-spaced; continue on additional pages as necessary.)

3. Justification/Source: (Need not be double-spaced.)

NOTE:

1. Only one recommendation per page.
2. Locally reproduced forms may be used for e-mail submissions to:
opso@mstp.quantico.usmc.mil

This page intentionally left blank.

This page intentionally left blank.

Table of Contents

Part I	Introduction	1
1001	The Threat	1
1001a	Historical Background	2
1001b	Current Threat	3
1002	Definitions	5
1002a	Passive Force Protection	6
1002b	Active Force Protection	6
Part II	Force Protection Priorities	7
2001	Protection from the Enemy's Fires and Maneuver	7
2001a	Reducing Enemy Targeting Effectiveness	7
2002b	Physical Security	8
2001c	Nuclear, Biological, and Chemical Defense	8
2002	Health Protection	11
2002a	Healthy and Fit Force	11
2002b	Casualty Prevention	11
2002c	Casualty Care and Management	12
2003	Safety	14
2004	Prevention of Fratricide	14
2004a	Boundaries and Maneuver Control Measures	15
2004b	Fire Support Coordinating Measures	15
2004c	Enhancing Situational Awareness	17
2004d	Technological Approaches	18
Part III	Warfighting Function Support to Force Protection	19
3001	Command and Control	19
3001a	Defensive Information Operations	20
3001b	Offensive Information Operations	21
3001c	High Risk Personnel	25
3002	Maneuver	25
3002a	Mobility/Counter mobility	26
3002b	Counter mine Operations	26
3002c	Force Dispersion	27
3002d	Counter reconnaissance	27
3002e	Security Forces	28

3002f	Operational Maneuver from the Sea	29
3003	Fires	30
3003a	Antiair Warfare Operations	30
3003b	Theater Missile Defense	32
3003c	Counterfire	34
3003d	Suppression of Enemy Air Defenses	35
3004	Intelligence	35
3004a	Intelligence Preparation of the Battlespace	36
3004b	Reconnaissance	38
3004c	Counterintelligence	39
3005	Logistics	40
3005a	Active and Passive Measures	40
3005b	Sea-based Logistics	41
Part IV	Planning for Force Protection	43
4001	Mission Analysis	44
4001a	MAGTF Force Protection Officer	44
4001b	Risk Assessment	45
4002	Course of Action Development	48
4002a	Concept of Force Protection	48
4002b	Planning Tools	49
4002c	Additional Planning Considerations	50
4003	Course of Action War Game	55
4004	Course of Action Comparison and Decision	56
4005	Orders Development	56
4006	Transition	56
Appendix A	Marine Corps Component Role	57
Appendix B	Marine Corps Role in Homeland Defense	61
Appendix C	Force Protection Appendix Format and Example	65
Appendix D	JOPES Orders, Annexes, and Appendices	75
Appendix E	Force Protection Conditions	77
Appendix F	Glossary	93
Appendix G	References	103

Figures

4-1	Marine Corps Planning Process Steps	43
-----	-------------------------------------	----

Tables

4-1	Force Protection Priority Matrix	50
4-2	Force Protection Task Table	50
D-1	Force Protection Related Annexes and Appendices	76
E-1	Threat Levels and Response Forces	91

This page intentionally left blank.

Part I

Introduction

Force protection is essential to all military operations: from war to military operations other than war (MOOTW). It is conducted at the strategic, operational, and tactical levels of war. Force protection preserves vital resources—lives, equipment, and materiel—so they can be used to accomplish the mission. It includes every action or measure that preserves combat power so it can be applied at the decisive time and place. These actions include more than self-protection or base protection measures. They also include actions that reduce or eliminate the ability of the enemy to adversely affect the force’s ability to conduct successful operations.

Force protection attempts to safeguard our centers of gravity by protecting or reducing friendly critical vulnerabilities. This may include the protection of sea, air, and land lines of communications (LOC) or the protection of the host-nation infrastructure for friendly use.

Force protection is critically important to the success of MAGTF operations; it is both a command and an individual responsibility. Every Marine should be aware that the force is always subject to attack and should act accordingly. Commanders at all levels have the responsibility for protecting Marine Corps assets, information, and personnel, and are accountable for force protection within their areas of operations. The unique nature of the force protection effort requires that it be coordinated and integrated at the highest levels and across all functional areas. Integrating force protection into all aspects of operations throughout the command can be one of the greatest challenges of the commander.

1001. The Threat

Even with the downsizing of their armed forces, the United States and its allies retain conventional force dominance across all military dimensions. The inability of enemies to challenge this U.S. and allied military power

directly has lead to the use of asymmetric means of attack to deter U.S. initiatives, attack forward deployed forces, and attempt to drive a wedge between the United States and its coalition partners. These attacks are intended to weaken U.S. resolve to maintain a force presence in threatened regions and to influence U.S. public and congressional opinion. Asymmetric use of force could include employment of weapons of mass destruction (WMD) and terrorism.

a. Historical Background

On 23 October 1983, a large truck laden with the equivalent of over 12,000 pounds of explosives crashed through the perimeter of the 24th MEU compound at Beirut International Airport. It penetrated 1st Battalion, 8th Marine Regiment's headquarters building and exploded, destroying the building and resulting in the deaths of 241 U.S. Marines and Sailors. The Long Commission found that the command had failed to take adequate security measures commensurate with the increasing threat level in Lebanon. While 24th MEU had adapted to the threat from indirect fire and sniper attack, it had created an exploitable vulnerability by concentrating troops in the headquarters building. The Long Commission also determined that as the mission of the U.S. contingent to the Multinational Force and the threat to that contingent changed over time, no senior U.S. commander had compared the evolving mission with previous guidance to determine whether it was adequate to protect the Marine force on the ground.

The Riyadh and Al Khobar bombings in Saudi Arabia during 1996 resulted in 19 deaths and over 500 U.S. and Saudi casualties. The attack on USS COLE (DDG 67), in the port of Aden, Yemen, on 12 October 2000, killed 17 Sailors and wounded 39 others, demonstrating a seam in the combatant command's force protection efforts, namely in-transit forces. More than 3,000 lives were lost to terrorism by the suicide attacks on 11 September 2001 in New York City, Pennsylvania, and at the Pentagon in Washington, DC.

The Department of Defense (DOD) expects that the majority of future terrorism directed against U.S. targets will be tied to ethnic and religious conflicts. It will be primarily urban in nature, often occurring in capital cities. Terrorism for the foreseeable future will remain a weapon of choice for governments, groups, and other parties to conflict. Traditionally, terrorist movements that affected U.S. security interests were politically motivated, and even the most brutal groups usually refrained from mass casualty

operations for fear of alienating their political constituencies and potential recruits. Today, religiously motivated terrorism is increasingly on the rise. Religious zealots, when members of a terrorist group or cult, usually exhibit few such constraints and actively seek to maximize casualties. The MAGTF commander must now add terrorism to the existing normal combatant threats posed by the enemy in the battlespace.

b. Current Threat

The threat drives everything in force protection. Identifying, understanding, and assessing the threat are critical to successful force protection operations. The nature and degree of the force protection threat to MAGTF operations varies widely with geographic location, criticality, and vulnerability of the target, and level of hostile intent. The following describes the types of force protection threats most likely to be faced by the MAGTF:

- **Conventional Threat.** Regular military forces supported by a recognized government. Included in this threat are large tactical force operations including airborne, air, artillery, and missile attacks.
- **Unconventional Threat.** Military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces that are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape networks.
- **Terrorism Threat.** The calculated use of violence or threat of violence to instill fear and intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Bombings, shootings, and kidnappings are still the most likely methods used by terrorists, but there is a growing trend to use different types of weapons, with the emphasis on lethality and producing mass casualties. Other types of terrorist attacks include: arson; hostage-taking; hijacking/skyjacking; seizure or raids on facilities; commercial/industrial sabotage; hoaxes; use of WMD; information warfare; and ecological terrorism. Terrorists generally attack soft and unprepared targets that will generate the maximum amount of attention or support for their cause.
- **Criminal Threat.** Criminals range from organized to unsophisticated, and act for personal rather than political or

ideological gain. Organized criminal groups plan in detail, and possess superior security system bypass and physical security barrier breaching equipment. Their targets include: arms, ammunition, and explosives, specialized equipment, and large sums of money. However, most criminal threats directed at Marine facilities and the MAGTF are unsophisticated and focus on crimes of opportunity. Criminal activity includes drug activities, property theft, break-ins, bank robberies, kidnappings, and stolen vehicles and often indicates future enemy action.

- **Insider Threat.** This threat comes from assigned personnel (military or civilian), host-country nationals (military or civilian), third country nationals (contract employees), or other persons assigned to or transiting the area of interest. Any of these people may threaten the MAGTF by disclosing sensitive or classified information, assisting dissident groups, and by attacking with weapons, explosives, biological agents, and computers. They may target individuals, groups, facilities, weapon systems, or information systems. Insiders usually act alone without detailed planning. Their success depends upon the ability to circumvent security systems.
- **Subversive Threat.** Subversives include people or groups trying to overthrow the host nation government by force. This category includes saboteurs and spies. Sabotage, usually conducted by well-armed, well-trained guerrillas and unconventional warfare forces, is normally targeted at mission-critical personnel or equipment, information systems and military operations. Likely targets include arms, ammunition, and explosives storage and manufacturing facilities. Disgruntled employees also conduct acts of sabotage against information systems and other attractive targets. Spies operate covertly to gain access to and steal military information.
- **Environmental Threat.** Medical concerns such as disease, pestilence, and effects of the environment (to include hazardous waste areas and hazardous materials production facilities) on individuals and the MAGTF as a whole.
- **Weapons of Mass Destruction Threat.** Systems that are capable of a high order of destruction or of being used to destroy large numbers of people, such as nuclear, biological, and chemical (NBC) weapons.
- **Civil Unrest Threat.** Violent and nonviolent protest by the indigenous population. The threat can come from anti-American

groups, protests, demonstrations, refugees, and humanitarian operations, and any local tensions that may escalate into a direct threat to MAGTF operations. The primary objectives of protestors commonly include destruction and publicity by focusing their efforts on symbolic targets and authority figures.

- **Information/Data Threat.** Attempts by the enemy to achieve information superiority by attacking, disrupting, or degrading MAGTF information, information-based processes, information systems, and computer-based networks.
- **Future Threat.** New threats such as laser, microwave, acoustic weapons, or other high-technology weapons that adversaries may possess, have access to, or are developing should also be considered.

1002. Definitions

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines force protection as—

Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security [OPSEC], and personal protective services, and supported by intelligence, counterintelligence [CI], and other security programs.

Force protection relies on the integrated application of the full range of both offensive and defensive capabilities. Multidimensional force protection is achieved through the skillful combination of layered active and passive measures across the range of military operations and warfighting functions—with an acceptable level of risk.

Commanders use force protection measures to preserve the health, readiness, and combat capabilities of their force. Deep and close operations to disrupt the attacker's tempo and blind the enemy reconnaissance efforts, camouflage, terrain masking, and OPSEC to frustrate the enemy's ability to find them, all contribute to force protection. Force protection measures can be active or passive in nature.

a. Passive Force Protection

Passive force protection measures defend against or reduce the effects of hostile acts or environmental and health threats by making them more survivable. They provide a defense against the threat. This can be accomplished through training, education, hardening, camouflage, concealment, deception, information security, and OPSEC. Examples of passive measure include hardening facilities, immunizing against biological agents, comprehensive individual fitness programs, countersurveillance operations; surveillance of vulnerable points; and defeating an enemy insurgent force as it attempts to attack a facility.

b. Active Force Protection

Active force protection measures are those preemptive acts taken to degrade, deny, defeat, or destroy hostile forces or capabilities before they can attack MAGTF assets. Some examples are detecting, capturing, and detaining known terrorists, arresting network hackers prior to their affecting computer networks; counterreconnaissance operations, and destruction of terrorist bases before an attack can be launched.

Part II

Force Protection Priorities

MAGTF force protection preserves the health, readiness, and combat capabilities of the force. The commander's force protection concept must incorporate four priorities—protect the MAGTF from the enemy's fires and maneuver, maintain health, ensure safety, and prevent fratricide.

2001. Protection from the Enemy's Fires and Maneuver

The MAGTF may counter the enemy's fires and maneuver by making personnel, systems, and units difficult to locate, strike, and destroy. To ensure adequate protection, the MAGTF should also take physical actions to improve its capability to withstand the effects of an enemy attack, to include defensive actions against enemy WMD.

a. Reducing Enemy Targeting Effectiveness

Methods for reducing the enemy's targeting effectiveness focus on ways to deny the enemy information about the location of friendly units or, if the enemy has that information, making target acquisition more difficult. Those methods include:

- OPSEC to deny enemy sensor and reconnaissance assets timely acquisition and identification of friendly targets.
- Camouflage, the use of natural or artificial material on personnel, objects or tactical positions with the aim of confusing, misleading or evading the enemy.
- Deception to mislead the enemy by manipulating, distorting, or falsifying friendly actions.
- Increasing the mobility of the potential target to reduce its vulnerability and contribute to the survivability of certain systems by limiting their exposure to reconnaissance and targeting.
- Dispersion to reduce target vulnerability by decreasing concentration and making a target less lucrative.

Additional information on reducing the enemy's capability to target friendly forces is found in Part III, Warfighting Function Support to Force Protection.

b. Physical Security

Physical security is an integral part of force protection. Its objective is to provide protection from terrorists and other criminals, disaffected persons, hostile intelligence, paramilitary forces, protesters, and saboteurs. Physical security is designed to deter, detect, and defend against all of the above threats. Physical security employs physical measures such as fences, lights, cameras, blast walls, vehicle barriers and alarm systems; and procedural measures such as security checks, training and awareness programs, property accountability/inventory requirements, and inspections and PS surveys units and facilities.

Other physical security actions that may be taken to reduce vulnerability include:

- Hardening of the potential target through careful site selection, field fortifications, and other field-expedient methods.
- Developing duplicate and redundant facilities for critical capabilities that are particularly vulnerable to missile attack.
- Construction of fencing and other barriers such as bollards, walls, gates, and berms, provide the maximum protection needed for the risk level associated with targeted assets. All barriers should have and maintain an adequate clear-zone to counter any attempted breach and be covered by fire or observation.

c. Nuclear, Biological, and Chemical Defense

Force protection considerations against the enemy's potential use of NBC weapons fall into two categories: reducing vulnerability to NBC attack and preventing the enemy from employing NBC weapons in the first place. These actions will ensure that the MAGTF retains the capability to operate despite the threat or use of NBC weapons.

- **Vulnerability Reduction.** To reduce its vulnerability, the MAGTF should identify lucrative potential targets that may be subject to enemy NBC attack. Fixed facilities and relatively immobile organizations that support maneuver forces (e.g., maintenance and supply) are lucrative

targets for NBC attack. Once potential targets are identified, the MAGTF can then determine the best means to contain, mitigate, and manage the consequences of identified risks and control hazards in order to preserve combat power and minimize casualties. This could include planning for NBC branches and sequels, eliminating unique command and control (C2) nodes, assuring that multiple units are prepared to assume vital missions, and training and exercising in order to facilitate shifting missions and responsibilities to counter unanticipated NBC attacks. The use of shelters, particularly hardened shelters, offers aircraft protection from the effects of NBC weapons.

Contaminated areas must quickly be identified, delineated, and avoided. Alternate routes, assembly, and support areas must be identified during planning. To the extent possible, units should be dispersed and thereby reduce vulnerability to NBC attacks, physically massing only when required. Avoiding contamination will preclude the twin burdens of wearing protective equipment and undertaking decontamination operations.

The MAGTF should also address the dangers posed by toxic materials, including radiological contamination and other environmental contamination from industrial operations within the area of operations. Particular care must be taken in identifying the nature of such hazards. In many cases standard military NBC individual protective equipment will not provide the necessary protection. In some instances, avoiding the hazard may be the most effective or only course of action (COA).

Medical protection of the force against NBC threats involves integrated preventive, surveillance, and clinical programs. The MAGTF's plans should include preventive medicine, medical surveillance, NBC casualty control, medical evacuation, and provision for readily available treatments and supplies to counter the physical effects of NBC exposure. These plans should take into account the capabilities and requirements of host countries, multinational partners, and essential civilian workers supporting U.S. and multinational forces. Even when sufficient protection has been afforded to individuals and units, the increased number of casualties may severely tax reorganization and reconstitution systems as well as medical treatment capabilities.

Sufficient protective equipment must be available to protect not only the MAGTF but also the essential supporting U.S. civilian and host-nation work forces. Individual and unit training for proper sizing, use of, and care for this individual and crew-served equipment is required to take full advantage of its capabilities. However, the use of protective equipment degrades individuals' and units' ability to perform assigned tasks and missions. The use of protective equipment can adversely impact unit capabilities, and commanders must avoid performance degradation, such as increased movement times for tactical operations and logistics, degraded communications requiring increased numbers of electronic transmissions, longer response times on requests for fire support, and degraded C2. The impact of the use of protective equipment, such as reduced sensory awareness and work rates as well as increased fatigue and water requirements, requires that individuals and units make realistic assessments of their capabilities in an NBC environment.

- **Prevention.** The MAGTF should not rely solely on efforts to reduce the force's vulnerability to NBC attacks. It should also make every attempt to prevent the enemy from successfully delivering NBC weapons, using the full extent of actions allowed by the rules of engagement (ROE). These actions include interdiction, collateral damage planning and assessments, early and sustained operations to disrupt or destroy NBC capabilities, and establishment of multi-layered defenses against NBC weapons delivery. psychological operations (PSYOP) can decrease an enemy's perception of the utility of NBC weapons, contribute to deterring their employment, and enhance efforts to reduce an enemy's domestic and international support. Information operations (IO), including OPSEC, provides forces with a significant measure of protection by preventing an enemy from acquiring information necessary to successfully target forces and facilities. Deception, dispersion of forces, and effective use of terrain are examples of other active measures that decrease the desire or willingness of the enemy to use NBC weapons.

See Part III, Warfighting Function Support to Force Protection, for additional information on the use of warfighting function-based techniques to enhance the MAGTF's defenses against the enemy's fires and maneuver.

2002. Health Protection

The commander is responsible for keeping MAGTF personnel healthy and to maintain their fighting spirit. The three pillars of health protection are a healthy and fit force, casualty prevention, and casualty care management. The goal of health protection is to minimize the effects of wounds, injuries, disease, environment, occupational hazards, and psychological stressors on unit effectiveness, readiness, and morale. The success of casualty care management with limited medical forces is directly dependent upon the commander's aggressive enforcement of the first two pillars. A proactive preventive medicine program and a phased health care delivery system accomplish the mission that extends from actions taken prior to and at the point of injury or illness through the completion of definitive treatment. MAGTF health protection requires continuous intelligence gathering and analysis, planning, coordination, and training to ensure a prompt, effective, and unified health care effort.

a. Healthy and Fit Force

The commander should always promote a healthy and fit force and develop Marines and Sailors capable of withstanding the physical and mental rigors associated with combat and other military operations. Wellness programs, including physical and mental fitness, health promotion, and environmental and occupational health measures, guard the force against disease and nonbattle injury, combat and operational stress reactions, and other health threats. Fit military members are less likely to be injured accidentally, can more readily withstand exposure to diseases and excessive stress, and more promptly heal from wounds or injuries.

Wellness requires continuous attention before, during, and after deployment to sustain maximum readiness and operational capability. Preventive dentistry and stress management measures are examples of how to develop and maintain health within the MAGTF.

b. Casualty Prevention

Prevention of illness and injury is critical in maintaining the effectiveness of naval forces. Casualty prevention focuses on the threats posed by enemy forces and occupational and environmental health threats. Prevention is accomplished through—

- Well-designed occupational health and safety and industrial hygiene programs.
- Comprehensive pre, post and intra deployment medical surveillance programs.
- Timely, accurate and continuous medical threat assessments of the operating area and opposing forces.
- Ready availability of effective countermeasures, to include personal protective equipment, collective protective systems, immunological and chemoprophylaxis or treatment. Particular attention to food and water quality safety is required to preclude transmission of infectious disease.

There should be a comprehensive medical data collection system with continuous surveillance and preventive medicine measures (such as immunization, pretreatment, and chemoprophylaxis programs and policies) to continuously counter the health threat.

To manage or reduce combat stress, commanders should implement stress control measures. These measures include surveying the unit to identify stressors and excess stress and providing early intervention. Early intervention will reduce stress-identified personnel requiring additional help, and lessen the chances of long-term disability such as posttraumatic stress disorder. These interventions occur before, during, and after deployment of the MAGTF. The preventive medicine threats addressed include protection from and education on insects/rodents which carry diseases; weather related injuries (heat/cold/wind/humidity), and unsafe or contaminated food and water.

Casualty prevention also includes the requirement to provide an immediate medical response to reduce the severity and number of casualties resulting from threat entity use of WMD, NBC, directed-energy weapons, and conventional munitions. This can be achieved through a well-planned, coordinated, flexible, and effective medical response and consequence management program.

c. Casualty Care and Management

The basis of casualty care and management resides on the principles of essential care in theater and rapid evacuation out of theater and incorporates the following:

- A casualty prevention program based on an epidemiologic approach to combat and disease and non-battle injury casualties.
- A care-to-user approach that leverages technology to enable casualties to continue duties and avoid evacuation and/or lengthy hospitalization.
- A casualty care and management approach to clearing the battlefield using rapid stabilization, far-forward surgery, and essential care or hospitalization in-theater, all supported by a medical evacuation system that provides the required en-route care (with total in-transit visibility of casualties).

Health support elements will be capabilities based. Capability packages (personnel, supplies, equipment, and sustainment modules) must be rapidly deployable, in block or incremental form, tailored to meet the spectrum of operational requirements, using a building block, lowest denominator approach. A single capability package is a pre-established, task functional set consisting of personnel, supplies, and equipment. Capability packages must be interoperable and support afloat and ashore operations, in naval, joint and combined operations in concert with a sea-based logistics system.

Casualty care and management includes first response, forward resuscitative surgery, theater hospitalization, en-route care, and definitive care.

- **First Response.** The first response may consist of self-aid and buddy aid, combat lifesavers, combat medics, hospital corpsmen, physician assistants, physicians, or other medical personnel. It may also include advanced trauma management measures. In this phase, the focus of all health care providers is to save life and limb and stabilize the patient sufficiently to evacuate to the next level of care.
- **Forward Resuscitative Surgery.** The forward resuscitative surgery phase is the urgent initial surgery required to render a patient stabilized enough to withstand further movement to the next level of care. Forward resuscitative surgery is typically performed on patients with signs and symptoms of initial airway compromise, difficult breathing, severe bleeding and circulatory shock, and life threatening chest injuries and who do not respond to initial advanced trauma management procedures. The medical clearing and regulating assets of the combat service support usually provide this resuscitation and stabilization capability and to prepare the casualty for evacuation.

- **Theater Hospitalization.** Theater and fleet hospitals (ashore and afloat) provide essential range of services and diagnostic care to patients and prepare those who require higher care for evacuation out of theater.
- **En Route Care.** En route care involves the medical treatment of patients during movement. This provides uninterrupted care from the point of injury or initial illness until the patient arrives at the next level of care. It ensures continuing care of stabilized patients along the evacuation chain regardless of mode of transport without clinical degradation.
- **Definitive Care.** The full scope of convalescent, restorative, and rehabilitative services and care, usually provided outside the theater may by military, Department of Veteran Affairs, CONUS civilian hospitals, and theater-approved safe havens. It may include a period of minimal care and increased physical activity necessary to restore patients to functional health.

The MAGTF will be involved in the first three phases, and may provide support for the last two. Initial transport of patients to the first and second levels of medical care will also normally be a MAGTF responsibility.

2003. Safety

Although the joint force protection definition specifically excludes actions to protect against accidents, each commander should make safety an integral part of all joint training and operations. Sustained, high-tempo operations put personnel at risk. Command interest, discipline, and training lessen those risks. Safety in training, planning, and operations is crucial to successful combat operations and the preservation of combat power.

2004. Prevention of Fratricide

The commander should make every effort to reduce the potential for fratricide—the unintentional killing or wounding of friendly personnel by friendly fire. The destructive power and range of modern weapons, coupled with the high intensity and rapid tempo of modern combat, increase the potential for fratricide.

The MAGTF must be aware of situations that increase the risk of fratricide. The primary mechanisms for limiting fratricide are close coordination at all levels, command emphasis, disciplined operations, rehearsals, and situational awareness. Boundaries, maneuver control and fire support coordinating measures (FSCMs), and a thorough awareness of the locations of friendly forces will facilitate the rapid engagement of targets throughout the battlespace and at the same time provide safeguards for friendly forces.

a. Boundaries and Maneuver Control Measures

Boundaries and maneuver control measures are used to control and coordinate the operations of forces in the battlespace. These measures are usually employed to delineate areas of operation or other areas where MAGTF components will conduct their operations or to coordinate maneuver between adjacent units. Each of these measures has specific and discrete purposes. Their use normally results in the units affected by them having to do something or refrain from doing something.

The most commonly used measure is the boundary. A boundary is a line that delineates surface areas for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations or areas. They are used to define the forward, flank, and rear limits of an area of operations and when possible should be drawn along identifiable terrain to aid in recognition. Boundaries may be used to prevent fratricide and to give sufficient battlespace to a commander to protect his force by shaping and engaging the enemy.

An axis of advance is a line of advance assigned for the purpose of control; often a road, network of roads, mobility corridor, or a designated series of locations, extending in the direction of the enemy. It provides subordinate commanders with a graphic representation of the commander's intent for their scheme of maneuver. Subordinate commanders are guided by it but may deviate from it when the situation dictates. A limit of advance is an easily recognizable terrain feature beyond which attacking elements will not advance. It is assigned by the commander to subordinate maneuver commanders to control their actions and form a limit of their advance.

b. Fire Support Coordinating Measures

FSCMs ensure that fire support will not jeopardize troop safety, interfere with the delivery of other fire support means, or disrupt adjacent unit

operations. Safety measures must minimize the potential for fratricide while not limiting boldness and initiative in combat. Restrictive fire support measures that can enhance force protection include:

- **No-Fire Area.** A no-fire area (NFA) is an area where no fires or effects of fires are allowed. Two exceptions are when establishing headquarters approves fires temporarily within the NFA on a mission basis, and when the enemy force within the NFA engages a friendly force, the commander may engage the enemy to defend his force. The NFA prohibits fires or their effects in the area, normally to protect civilians or cultural areas.
- **Restrictive Fire Line.** A restrictive fire line (RFL) is a line established between converging friendly forces (one or both may be moving) that prohibits fires, or effects from fires, across the line without coordination with the affected force. It prevents fratricide between converging friendly forces. The common commander of the converging forces establishes the RFL. He may delegate establishing authority to the senior commander of the two converging forces or to the commander of the maneuvering force in a linkup operation between a moving and a stationary force.
- **Restrictive Fire Area.** A restrictive fire area (RFA) is an area in which specific restrictions are imposed and into which fires that exceed those restrictions will not be delivered without prior coordination with the establishing headquarters. The RFA controls fires into an area where friendly forces are or will be located. Any ground unit commander may establish an RFA within his own zone; however, it is not normally established below battalion level. When RFAs are used to protect a forward unit from friendly fires; e.g., reconnaissance team, the RFA size should be large enough to allow the maneuver of the unit but not so large as to needlessly restrict fire support in other areas. To facilitate rapidly changing maneuver areas, on-call RFAs may be developed during planning. Dimensions, location, and restrictions of the on-call RFA are prearranged. The RFA can be activated and deactivated either by request of the maneuvering unit, or by time or event.
- **Airspace Coordination Area.** An airspace coordination area (ACA) is a three-dimensional block of airspace in a target area, established by the appropriate ground commander, in which friendly aircraft are reasonably safe from friendly surface fires. The airspace coordination area may be formal or informal. Formal ACAs require

detailed planning. More often, informal ACAs are established using time, lateral or altitude separation between surface- and air-delivered weapon effects. The ACA ensures aircrew safety and effective use of indirect supporting surface fires by deconfliction of time and space.

- **Restricted Operations Zone.** A restricted operations zone (ROZ) is not an FSCM. It is an airspace coordination measure and an area of defined dimensions within which the operation of one or more airspace users is restricted. Examples are the platoon air hazard and target air hazard used with Army Tactical Missile System units and in the future naval gunfire ships firing extended range guided munitions and land attack standard missiles. The ROZ restricts aircraft from defined areas to prevent fratricide. They deconflict airspace for firing units by restricting aircraft from the airspace directly surrounding both the launch and impact area. Since they are airspace coordination measures, ROZs are established and disseminated by the airspace control authority.

c. Enhancing Situational Awareness

Current combat environments, characterized by non-contiguous battlespace, geographically separated units, and hard to define rear areas, require that the MAGTF gain and maintain an accurate and timely picture of friendly and enemy locations so that the fire support coordinator (FSC) can maintain an accurate representation of the battlespace. This is an essential factor in preventing fratricide and creating a picture of enemy disposition.

Situational awareness is key to the effectiveness of the MAGTF's planned procedures for the clearance of fires. These clearance procedures must be determined during planning so that the FSC and other supporting arms personnel can ensure that fires will not adversely affect friendly forces during execution. There are two methods of control: positive and passive.

- **Positive Control.** Under positive control, a verbal or automated response will be sent to the target acquisition asset and the firing unit clearing the mission for firing following an evaluation of the FSC's picture of the battlespace.
- **Passive Control.** With passive approval procedures, fires are monitored but not specifically cleared for execution. Only if the FSC determines that there is a potential fratricide problem with the requested fires will the FSC interrupt the process.

d. Technological Approaches

The Marine Corps is evaluating several combat identification technologies that have the potential to reduce fratricide. Systems such as the single-channel ground and airborne radio system improvement program plus [SINCGARS SIP+] and the Situational Awareness Data Link [SADL] system will be evaluated to determine if situational awareness and target identification functions can be improved during the critical interfaces between the forward air controller and close air support aircraft. To eliminate fratricide among dismounted Marines on the ground, eye safe laser/radio frequency combat identification systems such as the Combat Simlas Plus System [CSPS] and the Combat ID Dismounted Soldier [CIDDS (A)], will also be evaluated.

Part III

Warfighting Function Support to Force Protection

Force protection cannot provide adequate safeguards for a MAGTF in isolation. To be effective, it must have support from the other five warfighting functions: command and control, maneuver, fires, intelligence, and logistics and be completely integrated with them.

3001. Command and Control

Command, control, communications, computers and intelligence (C4I) systems that contribute to situational awareness at all levels of command are a basic requirement of force protection. By improving each commander's understanding of friendly and enemy unit locations and the tactical situation in general, these systems reduce the likelihood of fratricide and contribute to both faster and more appropriate tactical decisions.

The threat to MAGTF command and control systems consists of physical threats to the physical C2 architecture and the threat of electronic, radio frequency or computer-based attacks on the information or communications components that control or make up the C2 infrastructure. In most cases, the target of the threat is the information itself, rather than the system that transports it. The threats come from a range of sources:

- **Insiders.** Individuals with legitimate access to a data network pose one of the most difficult threats from which to defend. Whether recruited or self-motivated, the insider has access to systems normally protected against attack.
- **Hostile Intelligence/Military.** Nationally sponsored hostile intelligence services, either civil or military, are active over the entire spectrum of conflict. In peacetime, they are more likely to be targeted against U.S. commercial and scientific networks than military information infrastructures. Yet, with little additional resource

expenditure, a dissident's peacetime intrusiveness could easily be refocused on a MAGTF's data networks.

- **Terrorists (Political or Religious).** In the past, in order to gain access to, or collect intelligence on, a target, terrorist may have had to climb a security fence or pass through a locked door. Today, this same terrorist can gain access by entering through a computer network. While traditional means are still needed to protect unwanted access to information, there is a new force protection concern for the commander, and new opportunities for an enemy.

Command and control measures that support force protection consist of defensive and offensive IO and efforts to protect high risk personnel.

a. Defensive Information Operations

Since it is a practical impossibility to defend every aspect of our infrastructure and every information process, defensive IO is required to protect and defend information and information systems that the MAGTF depends on to conduct operations.

The first step to defeating a network intruder is preparing defenses. But like all defenses, network defenses only buy time and not full protection. Given enough time, an intruder can eventually acquire information that could be detrimental to friendly force operations/mission objectives. The second step to defeating these intruders, then, is to have the ability to detect when and where an intrusion attempt is being made and the type of capability being used to perform the intrusion. The third step is to have a contingency plan in place to meet and defeat this threat based on time and planning considerations established by the commander. This capability allows the commander to choose when and where to degrade, defeat, deceive, or possibly destroy the threat once it is detected, and restore any lost capabilities. Only through a comprehensive plan to defend against, detect, deceive, and defeat hostile intrusion can a network and functional capabilities that process information be truly protected.

Information assurance (IA) is the joint term applied to those security actions taken to protect friendly information and information systems. It is "all [IO] that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems

by incorporating protection, detection, and reaction capabilities” (Joint Pub 1-02). IA protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and nonrepudiation (undeniable proof of identity of originators of data). This includes IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software. Personnel and physical security measures contribute indirectly to IA.

b. Offensive Information Operations

Offensive IO attacks elements of an enemy’s information systems and attempts to degrade the quality of the information the enemy may obtain about the MAGTF. As an active force protective measure, offensive IO degrades or eliminates the enemy’s capabilities to attack the MAGTF and disrupt friendly operations. Offensive IO is composed of OPSEC, military deception, PSYOP, electronic warfare (EW), and physical attack. In an operations order, Appendix 3, Information Operations/Command and Control Warfare, to Annex C, Operations, will discuss how the MAGTF intends to conduct IO in further detail.

(1) Operations Security. OPSEC is the process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by enemy intelligence systems; (b) determine what indicators enemy intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to enemy exploitation (Joint Pub 1-02). The emphasis of OPSEC is to deny critical information necessary for the enemy commander to accurately estimate the military situation.

The OPSEC process begins when the commander and staff identify the questions that they believe the enemy will ask about friendly intentions, capabilities, and activities. These questions are the essential elements of friendly information (EEFI). EEFIs are further analyzed to determine the critical information—those specific facts about friendly intentions, capabilities, and activities—vitaly needed by the enemy to plan and act effectively. The identification of critical information is important in that it

focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all classified or sensitive information.

OPSEC indicators are those friendly actions and open sources of information that enemy intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information. They are determined by an analysis of the planned operation and the enemy collection capabilities. An indicator has five characteristics of information that make it potentially useful to an enemy.

- **Signature.** A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out.
- **Associations.** Association is the relationship of an indicator to other information or activities.
- **Profiles.** Each functional activity generates its own set of more-or-less unique signatures and associations. The sum of these signatures and associations is the activity's profile.
- **Contrasts.** Contrasts are any differences that are observed between an activity's standard profile and its most recent or current actions.
- **Exposure.** Exposure refers to when and for how long an indicator is observed.

Specific OPSEC measures are selected to reduce the probability of the enemy either collecting the indicators or being able to correctly analyze their meaning. OPSEC measures can prevent the enemy from detecting an indicator; provide an alternative analysis of an indicator; or attack the enemy's collection system. The estimated cost associated with implementing each possible OPSEC measure should be compared to the potential harmful effects resulting from an enemy's exploitation of a particular vulnerability. OPSEC measures usually entail some cost in time, resources, personnel, or interference with normal operations. If the cost to mission effectiveness exceeds the harm that an enemy could inflict, then the application of the measure is inappropriate. OPSEC measures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the enemy's intelligence system.

(2) Military Deception. Military deception consists of actions to deliberately mislead enemy military decisionmakers about friendly military capabilities, intentions, and operations, causing the enemy to take specific

actions (or inactions) that will contribute to the accomplishment of the friendly mission. Military deception is done in conjunction with the overall IO effort and closely coordinated with all of its elements. Military deception seeks to influence enemy military commanders and to degrade their C2 capabilities.

Deception operations create numerous false indicators, making it more difficult for enemy intelligence analysts to identify the real indicators that OPSEC is seeking to control. Military deception, as an integrated part of the IO plan, can protect the movement and deployment of forces by concealing the true location, purpose, or capabilities of the force. Deception can also help protect the MAGTF from enemy C2-attack efforts. An enemy commander who is deceived about friendly C2 capabilities and limitations may be more likely to misallocate resources in an effort to attack or exploit friendly C2 systems.

Deception can also include use of dummy positions, false preparations such as the misleading movement of logistics and transportation assets, use of smoke to cover movement, roving firing elements from a larger indirect fire unit, and avoidance of routine movements and resupply procedures.

(3) Psychological Operations. PSYOP are actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals. PSYOP have strategic, operational, and tactical applications, including truth projection activities that support military deception operations. PSYOP can include the distribution of leaflets, loudspeaker broadcasts, radio and television broadcasts, and other means of transmitting information that promote fear or dissension in enemy ranks. They may also shape attitudes and influence behaviors through face-to-face communication and support military deception operations. PSYOP can support the commander and force protection by:

- Discouraging enemy attacks.
- Creating uncertainty in and lower the morale and efficiency of enemy soldiers and civilians.
- Influencing enemy strategy and tactics.
- Arousing local public opinion in favor of friendly forces and increase internal political and social pressures against enemy operations.

- Promoting the activities of indigenous elements directed against the enemy, particularly those conducted by elements within enemy controlled territory.
- Encouraging disaffection among potentially dissident elements within the enemy military and civilian populace.

(4) Electronic Warfare. The three major subdivisions of EW are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EW is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Use of EA should be based not only on the commander's intent, but also on the risks of possible enemy responses and other potential effects on the operation. EA involves actions taken to attack the enemy with the intent of degrading, neutralizing, or destroying enemy combat capability to prevent or reduce an enemy's effective use of the electromagnetic spectrum. EP involves such actions as self-protection jamming and emission control taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. ES contributes to situational awareness by detecting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. EP and ES are routinely conducted during peacetime as well as during periods of crisis or conflict.

(5) Physical Attack/Destruction. Physical attack is the use of "hard kill" weapons against designated targets as an element of an integrated IO effort. By eliminating key C2 nodes of the enemy, a commander can prevent the enemy from effectively planning and executing attacks against the MAGTF.

(6) Public Affairs. Public affairs consists of public information, command information, and community relations activities directed toward both the external and internal publics with interest in the activities of the MAGTF. Although not doctrinally a component of IO, public affairs can contribute to IO by permitting the MAGTF commander to inform the enemy or a potential enemy about the friendly force's intent and capability, and deter or influence enemy actions. It can also be used to the release of information about the MAGTF and its capabilities. Public affairs activities will not be used as a military deception capability or to provide disinformation to either internal or external audiences.

c. High Risk Personnel

High risk personnel (HRP) security supports force protection by providing additional security to designated individuals who because of their rank, assignment, symbolic value, vulnerabilities, location, or specific threat are at a greater risk than the general population. A successful attack against these individuals would diminish (at least until their replacement) the ability of the MAGTF to command and control operations. HRP security consists of:

- Formal identification and designation of eligible individuals and personal security vulnerability assessments of those individuals.
- Hardened car support and domicile to duty authorization.
- Special training for HRP, their family members, and selected support personnel such as drivers.

There are two categories of HRP:

- Personnel that have such a significantly high potential as terrorist or criminal targets as to warrant assignment of full-time protective services. This would include long-term protective services based on assignment location, or short-term protective service based on a specific threat.
- Personnel that do not warrant assignment of full-time protective services but require such additional office, residential, and travel security measures as deemed appropriate based on local conditions.

HRP and their family members must be aware of risks and trained in personal protective measures they can apply. Additionally, support staff such as drivers, aides, and protective services details must be trained and properly equipped.

3002. Maneuver

Maneuver is the movement of forces for the purpose of gaining an advantage over the enemy in order to accomplish an objective. Maneuver is rarely effective without firepower and force protection. The maneuver warfighting function assists force protection through the skillful use of friendly forces to enhance mobility, reduce their visibility, complicate the

enemy's target acquisition problem, and minimize the value of any individual friendly target.

a. Mobility/Counter-mobility

Mobility is a quality or capability of military forces that permits them to move in time and space while retaining their ability to fulfill their primary mission. The MAGTF commander must be able to mass forces quickly at a chosen place and time to accomplish the assigned mission. Mobility is critical to achieving superior tempo and maintaining it for extended periods of time over great distances.

Counter-mobility is the physical shaping of the battlespace to alter the scheme of maneuver of the enemy. Counter-mobility operations block, fix, turn, or disrupt the enemy giving the MAGTF commander the opportunity to exploit enemy vulnerabilities or react effectively to enemy actions.

b. Counter-mine Operations

Land mines and very shallow water mines are a unique weapon system in the battlespace. They are inexpensive, easy to use, and as complex or simple as the user needs. Mines can be employed in large numbers to disrupt, fix, turn, or block the momentum of maneuver elements or they can be used in small numbers to cause confusion and spread terror. Psychologically, mines can unnerve a force by creating uncertainty, low morale, and even an unwillingness to fight. Although counter-mine operations are normally a subset of mobility operations, they are discussed separately in this pamphlet because of their significant impact on force protection.

Counter-mine operations are difficult because detection systems are imperfect and mine neutralization systems are only partially effective. Normally, counter-mine operations using explosive systems are conducted under enemy observation and fire. Counter-mine operations include—

- Mine detection.
- Reconnaissance for enemy minefields.
- Breaching.
- Prevention of enemy mine operations.

The most effective means of countering a mine threat is to prevent the laying of mines. Proactive counter-mine operations should be conducted to destroy

enemy mine manufacturing and storage facilities or mine-laying capabilities before the mines are laid. Enemy storage and mine production facilities and assets should always be considered as viable targets.

c. Force Dispersion

One of the characteristics of MAGTF defensive operations is mass and concentration of combat power. Mass and concentration, while facilitating local superiority at a decisive point, may mean accepting risk in other areas, particularly in regards to force protection. The massing of forces creates lucrative targets for the enemy; the dispersion of forces is a key passive measure that enhances security.

Dispersion is the spreading or separating of troops, materiel, establishments, or activities that are usually concentrated in limited areas to reduce vulnerability. It prevents an enemy from easily locating targets and reduces the likelihood that the MAGTF will be attacked with a WMD. Dispersion of forces must always be balanced with the need to mass combat power for effective operations and is dependent on the assessment of enemy capabilities. However, as technological advances continue, the ability of the MAGTF to conduct operations over greater distances with smaller dispersed forces will increase, thus enhancing force protection.

d. Counterreconnaissance

If the enemy is blinded, they will most likely fail in the attack. Therefore, a successful defense depends on finding, targeting, destroying, or suppressing enemy reconnaissance assets. Counterreconnaissance prevents the enemy from collecting sufficient information about friendly activities to interfere with them. Counterreconnaissance includes all measures taken to prevent enemy observation of a force, area or place. It focuses on denying the enemy access to EEFI, information about the MAGTF in the security area, the flanks, and the rear that would further enemy objectives.

Counterreconnaissance consists of active and passive measures. Active measures detect, fix, and destroy enemy reconnaissance elements. Passive measures conceal friendly units and capabilities and deceive and confuse the enemy. There are two components of counterreconnaissance—the detection of enemy reconnaissance forces and the targeting, destruction or suppression of those reconnaissance forces so they cannot report friendly unit positions or activities.

Counterreconnaissance includes—

- Developing named areas of interest and targeted areas of interest for likely enemy reconnaissance forces.
- Conducting continuous surveillance of designated named areas of interest and targeted areas of interest.
- Executing targeting plan against enemy reconnaissance forces.
- Recovering forward security elements.

Reconnaissance operations support counterreconnaissance through collecting information on enemy reconnaissance forces, assets, and activities. Counterreconnaissance in turn supports security operations by protecting the MAGTF from enemy collection.

e. Security Forces

MAGTF security forces aggressively and continuously seek the enemy and reconnoiter key terrain. They conduct active reconnaissance to detect enemy movement or preparations for action and to learn as much as possible about the terrain. The ultimate goal is to determine the enemy's COA and assist the main body in countering it. Security forces use a combination of ground patrols, observation posts, EW, and aviation assets.

Security in offensive operations is achieved by employing security elements to protect the MAGTF from unexpected attack, long-range fires, and observation by the enemy. The MAGTF commander can employ a wide range of forces and capabilities to conduct security operations. This can include—

- Aviation forces to screen the main force from enemy interference during fast moving offensive operations.
- Ground forces to control, seize or retain terrain to prevent enemy observation.
- Sensors (UAVs, radar and seismic sensors) to detect the enemy or his long-range fires.

In the defense, the security force engages the enemy in the security area, screening, guarding, and covering as ordered. This force maintains contact with the enemy while falling back under pressure. At a predetermined location, normally a phase line designated as a handover line, control of the battle is transferred to the main battle force.

There are three types of security missions. They vary in the degree of security provided, the forces and capabilities required, and the degree of engagement with the enemy that the commander desires. From the least degree of protection to the greatest, they are screen, guard, and cover. The forces that conduct these security missions are called a screen, a guard or a covering force and may be identified by their relation to the establishing headquarters and the location of the security force; e.g., MEF covering force, division advance guard or regimental flank screen.

- **Screen.** A screen only provides surveillance and early warning of enemy action, not physical protection. It can be employed as an economy of force measure in a low risk area because it provides security on a broad frontage with limited assets. A screen provides the least amount of protection of any security mission. It does not have the combat power to develop the situation.
- **Guard.** A guard protects the main force from attack, direct fire, and ground observation by fighting to gain time, while also observing and reporting information. A guard force protects the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body. A guard differs from a screen in that a guard force contains sufficient combat power to defeat, repel or fix the lead elements of an enemy ground force before they can engage the main body with direct fire.
- **Cover.** A cover operates apart from the main force to intercept, engage, delay, disorganize, and deceive the enemy before he can attack the main body. It prevents surprise during the advance. A covering force protects the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body. A covering force deceives the enemy about the location of the main body while disrupting and destroying his forces. This provides the main body with the maximum early warning and reaction time.

f. Operational Maneuver from the Sea

The maneuver warfare philosophy underlying the concept of operational maneuver from the sea (OMFTS) provides key defensive force protection capabilities by capitalizing on the use of the sea as maneuver space. As envisioned, seabasing of command and control, logistics, and the

preponderance of fire support functions offer an unparalleled level of force protection. Widely dispersed mobile seabased forces are far less vulnerable than those based on land. Naval forces enjoy increased security by complicating the enemy's target acquisition process. The sea also serves as a barrier to terrorists or other forces striking at established facilities in the landing force's rear area. Beyond the physical protection afforded to what would have been vulnerable areas ashore, the seabasing of those facilities eliminates the need to put Marines at risk to defend them or their LOCs. Whether major theater war or other expeditionary operations, reducing the force's footprint ashore through seabasing reduces exposure to many threats.

3003. Fires

Fires are those means used by the MAGTF to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight. In the context of force protection, fires are used to attack those enemy capabilities that have the most potential to affect friendly capabilities. The two aspects of the fires warfighting function that are key to force protection are anti-air warfare (AAW), theater missile defense, and counterfire operations.

a. Anti-air Warfare Operations

AAW is the U.S. Navy/U.S. Marine Corps term used to indicate that action required to destroy or reduce to an acceptable level the enemy air and missile threat. It is roughly equivalent to the joint term counter-air. AAW integrates all offensive and defensive actions against enemy aircraft, surface-to-air weapons, and theater missiles into a singular, indivisible set of operations. The intent of AAW is to protect and defend the MAGTF and its battlespace from enemy air and missile attack and take the fight to the enemy.

AAW serves two purposes: force protection and air superiority. It supports force protection by defending the MAGTF against enemy air and missile attacks and providing a reasonable level of confidence that maneuver can be conducted without interference from the enemy's air and missile capabilities. Force protection and air superiority actions are mutually supporting: a strong defense against enemy air attack protects the MAGTF while also achieving air superiority.

The MAGTF conducts two types of AAW operations: offensive AAW (OAAW) and air defense.

(1) Offensive Anti-air Warfare. OAAW reduces or neutralizes the enemy's air and missile threat before it launches or assumes an attacking role. In time critical targets, OAAW destroys their capability to conduct further operations after the weapon is launched. OAAW attacks the enemy's abilities to attack friendly resources with aircraft and missiles and to defend itself against attack by friendly aircraft and missiles. OAAW has two purposes: to gain air superiority and protect friendly forces. It is roughly equivalent to the joint term offensive counterair.

OAAW operations focus on a particular function of the enemy's combat potential—its air and missile forces. Because OAAW operations strive to destroy enemy air and missile resources as near to their source as possible, OAAW is the preferred method of conducting AAW.

OAAW operations are not specific to the MAGTF's aviation combat element. They are a responsibility of the entire MAGTF and impact on all MAGTF operations. The MAGTF can conduct OAAW operations with its organic resources (aircraft, EW, artillery, surveillance, and ground forces) or with support from joint force, theater, and national assets.

(2) Air Defense. Air defense operations include all defensive measures designed to destroy attacking enemy aircraft or missiles in the Earth's envelope of atmosphere or to nullify or reduce the effectiveness of such attack. (JP 1-02). Air defense operations provide the basis for force protection against attacks by enemy aircraft and missiles against the MAGTF. Air defense consists of active and passive measures.

- **Active Defense.** Active air defense is direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets. It includes layered defense-in-depth against air and missile threats through multiple engagement opportunities. Active measures also use area defense, which uses a combination of weapon systems to defend broad areas; point defense to protect limited areas (normally vital elements or installations); and self-defense, where friendly forces use organic weapons and systems. The components of an active defense system include:

- Point, area, and self-defense surface-to-air missile and gun systems
 - Aircraft primarily engaging enemy airborne launch platforms
 - EW systems
 - Voice warning
 - Surface, airborne, and space warning systems
 - Voice and data cueing
 - Command, control, communications, computers, and intelligence system
- **Passive Defense.** Passive air defense reduces or nullifies the effects of hostile air action, including theater missiles. Passive air defense provides essential individual and collective protection to friendly forces and critical assets. Passive air defense is a responsibility of commanders at all levels. Passive air defense complicates the enemy's targeting ability and ordnance delivery and increases the survivability of friendly forces under attack. Passive air defense includes:
 - Tactical warning measures to provide timely dissemination of information on the likely or imminent threat of attack by aircraft or theater missiles.
 - Reducing enemy targeting effectiveness
 - Reducing vulnerability
 - Recovery and reconstitution to the ability of a unit to be restored to a desired level of combat effectiveness commensurate with mission requirements and available resources after an attack. Recovery and reconstitution efforts may include reestablishing or reinforcing command and control; replacing personnel, equipment, and supplies; reestablishing unit cohesion, and repairing battle damage.

b. Theater Missile Defense

The proliferation and advances in ballistic missiles, cruise missiles and air-to-surface missiles and associated technologies, coupled with the pursuit of WMD capabilities, can provide adversaries with potentially decisive attack capabilities. Although theater missile defense (TMD) is a component of AAW, those force protection considerations that may be unique to TMD are discussed separately for this pamphlet.

Because of the continual advancement and proliferation of theater missiles, the threat cannot currently be countered by any single technical solution, nor will it likely be in the future. This threat can only be countered by the coordination and integration of the four operational elements of TMD (passive defense, active defense, attack operations, and TMD C4I) into cohesive and coherent combat operations.

(1) Passive Defense. Those measures taken to posture the force to reduce the vulnerability and minimize the effects of a theater missile attack. Like AAW, TMD passive defense is composed of:

- Tactical Warning. Warnings are both general (that missile launches are imminent or have occurred) and specific (that specific units or areas of the battlefield or theater are in danger of attack).
- Reducing enemy targeting effectiveness.
- Reducing target vulnerability.
- Recovery and reconstitution.

(2) Active Defense. Operations taken to protect against a theater missile attack by destroying airborne launch platforms and/or destroying theater ballistic missiles in flight.

(3) Attack Operations. Operations taken to destroy, disrupt, or neutralize theater missile launch platforms and their supporting structures and systems prior to launch. Attack operations are characterized by offensive actions intended to destroy and disrupt enemy theater missile capabilities before, during, and after launch. The objective of attack operations is to prevent the launch of theater missiles by attacking each element of the overall system, including such actions as destroying launch platforms, target acquisition platforms, C2 nodes, and missile stocks and infrastructure. Attack operations also strive to deny or disrupt employment of additional theater missiles that may be available to the enemy. Attack operations are highly dependent upon predictive and developed intelligence.

(4) Theater Missile Defense Command, Control, Communications, Computers and Intelligence. TMD C4I uses existing joint and Service C4I systems and resources to integrate the other TMD operational functions and to optimize the use of scarce resources. The C4I system links passive defense, active defense, and attack operations to provide timely assessment of the threat (to include intelligence preparation of the battlespace [IPB]); rapid

dissemination of tactical warning; and mission assignment, targeting data, and poststrike assessment to the appropriate TMD element.

For each operational element, the C4I system must provide rapid communications among intelligence assets, the fusion and decisionmaking facilities, warning systems, and weapon systems, to include a capability for rapid coordination with supporting combatant commanders. TMD C4I capabilities must support the principles of centralized planning, decentralized execution, and coordinated efforts by forces assigned TMD tasks.

c. Counterfire

Counterfire includes the attack of the enemy's cannons, rockets, and mortars, and the assets that support these weapons (target acquisition, command and control, and logistics elements). Counterfire suppresses enemy indirect fire assets and provides freedom of maneuver and use of indirect fire support for the MAGTF.

Counterfire activities are conducted using basic targeting methodology—decide, detect, and deliver. The decide function includes tasking of target acquisition assets, information processing, selection of an attack means, and determining the requirement for post-attack assessment. It results in the commander's targeting guidance and priority intelligence requirements, the high pay-off target list, target selection standards, and attack guidance. The detect phase is the execution of target acquisition, where assets are tasked to find specific enemy indirect fire targets. The main objective of the deliver phase is the attack of targets and post-attack assessment.

A key target acquisition asset in counterfire operations is the counterbattery radar platoon. Using the AN/TPQ-46A Firefinder radar, the platoon can locate enemy rocket, mortar, and artillery weapons in a timely manner for counterfire and intelligence purposes. The radars should be positioned to maximize coverage and reduce overlap and will be based on the commander's intent and priorities and known or projected enemy locations.

Radar zones are established to assist in the control of counterfire operations and to protect friendly forces. There are four different types of radar zones.

- **Critical Friendly Zone.** A critical friendly zone is an area in which are located friendly units or units that the maneuver commander designates as critical. Generates priority 1 call for fire.

- **Call for Fire Zone.** A call for fire zone is an area in enemy territory that the maneuver commander considers extremely important to neutralize fires from by immediate counterfire. Generates priority 2 call for fire.
- **Artillery Target Intelligence Zone.** An artillery target intelligence zone is an area in enemy territory that the maneuver commander wants to monitor closely. Weapon locations in this zone will be reported immediately. Their priority is exceeded only by targets in a critical friendly zone or a call-for-fire zone.
- **Censor Zone.** A censor zone is an area in which the commander wishes to ignore all target detections. Censor zones must be used judiciously, since the Firefinder computer does not report rounds originating from a censor zone to the operator. A censor zone may be used to ignore a friendly artillery position that, because of its aspect angle to the radar, could be detected as threat artillery. This situation could occur when troops are dispersed throughout the area of operations or when friendly units are in enemy territory.

d. Suppression of Enemy Air Defenses

Fires that increase survivability include suppression of enemy air defenses (SEAD) for aviation assets and proactive counter fire to ensure freedom of movement of maneuver forces. SEAD is that activity that neutralizes, destroys, or temporarily degrades enemy air defenses in a specific area by physical attack and/or EW. It may be accomplished through destructive means (indirect fire, direct fire, air attack or raids), disruptive means (EW, deception or flight tactics), or a combination of both.

The primary objective of SEAD is to destroy or degrade enemy surface-to-air defense capabilities, thereby increasing freedom of action and survivability of aircraft. SEAD is most frequently delivered in support of a specific air attack. This involves attacking air defense weapons that can threaten friendly aircraft in the immediate vicinity of the target and on the aircrafts' ingress and egress routes.

3004. Intelligence

Effective intelligence is critical to determine the threats to the force. Identifying a threat strengthens the overall force protection effort. Force protection intelligence and CI personnel must analyze a broad range of

threats. These threats may be conventional military units, special forces, terrorist groups, riotous civil populations, environmental and health hazards, chemical or biological agents, radioactive material, cyberterrorists, criminal elements, religious zealots, extremist groups, and the weapons any of these groups might select. With the extremely wide variety of threats, intelligence support to force protection should be implemented robustly, particularly through threat assessments.

The threat drives everything in force protection. Identifying, understanding, and assessing the threat are the first steps in force protection planning. Threat assessments for force protection should be systematic and continuous to reduce uncertainties concerning the enemy and the battlespace for all types of operations. A force protection threat assessment analyzes and assesses the applicable area's land, sea, and aerospace dimensions. In addition to the typical threat-related areas, force protection threat assessments should include environmental, health, infrastructure, economic, political, and cultural aspects of the particular area of interest. Force protection threat assessments should be all-source, fused analytical assessments. Intelligence may be compiled, compared, evaluated, analyzed, and assessed by a dedicated threat assessment team comprised of available force protection personnel. The end product should provide the commander with a baseline for conducting a vulnerability assessment and later for applying the appropriate force protection measures for countering the threat. Timely and accurate threat assessments are the key components in force protection planning and operations.

a. Intelligence Preparation of the Battlespace

IPB is the primary intelligence analytical process used by the MAGTF to identify enemy capabilities and potential courses of action. The IPB process identifies and evaluates the enemy's centers of gravity, critical vulnerabilities, capabilities, limitations, doctrine, and tactics, techniques, and procedures. It is readily adaptable to respond to the commander's information needs for force protection. To support force protection, the following steps are used:

(1) Define the Battlespace Environment. The battlespace, relative to force protection, may incorporate an area larger than that associated with conventional warfare operations. The battlespace should include the locations of enemy forces (particularly terrorist groups, unconventional

forces, and WMD delivery systems), as well as the likely targets of such forces (such as military housing units, transportation networks, and rear area installations).

- Consider which terrorist or potentially hostile groups are most likely to attack friendly personnel, equipment, and assets. Determine where they are normally based, and what third countries may shelter and support them.
- Anticipate how additional missions such as a noncombatant evacuation operation or peacekeeping operation may affect force protection.
- Assess the vulnerability of specific targets to attack. Consider both physical security issues and time constraints that might limit the availability of a target.
- Identify probable avenues of approach as well as infiltration and exfiltration routes.

(2) Describe the Battlespace's Effects

- Determine the demographic issues that make protected areas or personnel attractive to terrorist groups or enemy unconventional forces.
- Assess the vulnerability of specific targets to attack. Consider both physical security issues and time constraints that might limit the availability of a target.
- Identify probable avenues of approach as well as exfiltration and infiltration routes.

(3) Evaluate the Enemy. Force protection threats to the MAGTF that should be evaluated include enemy controlled agents or sympathizers, terrorism, demonstrations, and civil disturbances, guerrilla units, unconventional forces, small tactical units, conventional forces, air or missile attacks, and NBC weapons.

- Analyze the strengths and weaknesses of the enemy's target acquisition capabilities against force protection-related targets. Determine the sources of the enemy's information.
- Assess the degree of risk the enemy is willing to take in order to attack various types of force protection targets. Determine which types of targets the enemy considers most valuable.

- Identify the goals, motivations, political or social grievances, dedication, and training of terrorist groups. Evaluate how these factors may affect target selection.
- Identify the enemy's preferred methods of attack such as bombing, kidnapping, assassination, arson, hijacking, hostage-taking, maiming, raids, seizure, sabotage, or use of NBC weapons.
- Determine how and from where the enemy receives external support.

(4) Determine Enemy Courses of Action

- Identify the enemy's most likely targets by matching friendly vulnerabilities against enemy capabilities, objectives, and risk acceptance.
- Assess the status of specific types of support activities that may indicate the adoption of a specific COA.
- Identify possible infiltration routes, assembly areas, and surveillance locations near each of the enemy's likely objectives.
- Identify the enemy's most likely COA as well as the one most dangerous to the MAGTF.

b. Reconnaissance

A commander must have current information about the enemy's disposition, strength, morale, and weapons, as well as the terrain in order to employ the MAGTF effectively and prevent surprise. Reconnaissance is a continuous activity to collect information and to gain and maintain contact with the enemy. Reconnaissance activities range from passive surveillance to confirm or deny enemy courses of action or critical vulnerabilities and limitations, to aggressive measures designed to stimulate a revealing enemy response. Reconnaissance can be conducted through a variety of methods, including patrolling, armed reconnaissance, and reconnaissance by fire.

- A patrol is any detachment of ground, sea, or air forces sent out for the purpose of gathering information or carrying out a destructive, harassing, mopping-up, or security mission.
- An armed reconnaissance is a mission with the primary purpose of locating and attacking targets of opportunity (i.e., enemy materiel, personnel, and facilities in assigned general areas or along assigned ground communications routes) and not for the purpose of attacking specific briefed targets.

- A reconnaissance by fire is a method of reconnaissance in which fire is placed on a suspected enemy position to cause the enemy to disclose a presence by movement or return of fire.

c. Counterintelligence

CI is the intelligence function that is concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion, or terrorism. The objective of CI is to enhance command security by denying any enemy information that might be used to conduct effective operations against friendly forces and to protect the command by identifying and neutralizing espionage, sabotage, subversion, or terrorism efforts. CI provides critical intelligence support to command force protection efforts by helping identify potential threats, threat capabilities and planned intentions to friendly operations while helping deceive the enemy as to friendly capabilities, vulnerabilities and intentions.

CI force protection source operations are flexible and aggressive collection operations conducted by CI personnel to quickly respond to the needs of the supported command. These operations are focused on the collection of force protection information designed to assess threats from foreign intelligence collectors; provide early warning of impending attack; warn of sabotage or subversive activity against U.S. forces; identify and neutralize potential enemy infiltrations; provide information on local security forces; identify population and resource control measures; locate hostile or insurgent arms caches and safe havens; and identify local insurgent support personnel in regions where local security forces cannot or will not support U.S. operations.

At the MEF level, the CI/human intelligence (HUMINT) officer (CI/HO), with this staff, is the commander's advisor on the employment of his organic CI/HUMINT element in support of the MEF's force protection effort. The MEF's CI/HUMINT company conducts CI and HUMINT operations in support of this mission. Additionally, a Naval Criminal Investigative Service Agent is normally assigned to the CI/HO. At MEU level, an assigned HUMINT exploitation team has primary responsibility for conduction CI and HUMINT operations in support of force protection. The MEU also has a force protection officer. Prior to deployment, the force protection officer designs realistic training to meet DOD requirements. When deployed, he

conducts inspections and makes recommendations to the MAGTF commander on how to improve force protection readiness.

3005. Logistics

Logistics operations tend to be targets of enemy attacks because of the impact that a successful disruption of logistics can have on MAGTF operations. Consequently, the logistics warfighting function is extremely dependent on force protection measures to continue its ability to support the MAGTF.

a. Active and Passive Measures

Logistic units and installations are also high-value targets that must be safeguarded by both active and passive measures. Active measures must include a defense plan for logistics with provisions for reinforcement and fire support. Passive measures include dispersion, physical protection of personnel and equipment, deception, and limiting the size of an installation to what is essential for the mission.

Decentralization and redundancy can be critical to the protection of the logistic system. Decentralization disperses logistics assets throughout the battlespace. Although it can be less efficient than centralization, when appropriate due to the threat, it complicates the enemy's targeting process. Redundancy is the duplication of systems, units, or functions that provides alternate means of support if there is an interruption, failure, or loss of capability. Redundant capabilities help prevent disruption of support. However, properly planned redundancy can provide assurance of continued support. It can also contribute to enhanced responsiveness. Although redundancy improves flexibility and survivability, redundancy of systems, units, or functions should be limited to only what is essential to accomplish the mission. Survivability may dictate planning for dispersion and the allocation of protective forces at critical nodes of the logistic infrastructure.

Logistic operations are particularly vulnerable to WMD that deny or restrict the use of critical infrastructure. Planners must also consider alternate aerial ports of debarkation and seaports of debarkation in the event that WMD use denies access to the primary sites. Additionally, WMD use on points of entry may affect the ability and willingness of civilian flagged carriers, (air and

sea) to use these ports. The allocation of reserves, development of alternatives, and phasing of logistic support contribute to survivability. All force protection measures for enemy threats, especially those in the rear area, must emphasize security of the MAGTF's logistics capabilities.

b. Sea-Based Logistics

Sea-based logistics is an emerging implementing concept for executing OMFTS. Seabased logistics envisions bringing ashore only those elements of the MAGTF that are essential to mission accomplishment. Most fire support, aviation, aviation support, command and control, and logistics functions would remain sea-based throughout the operation. Sea-based logistics offers tremendous operational freedom of action to the MAGTF, reducing the need to establish and protect shore-based facilities. This results in increased operating tempo and reduced requirements for rear area security.

This page intentionally left blank.

Part IV

Planning for Force Protection

The Marine Corps Planning Process (MCP) is a procedure that supports decisionmaking by the commander and conveys the commander's decisions to his subordinates. It helps organize the thought processes of a commander and his staff throughout the planning and execution of military operations. The MCP focuses on the mission and the threat. It capitalizes on the principle of unity of effort and supports the establishment and maintenance of tempo.

The MCP organizes the planning process into six manageable, logical steps (see Figure 4-1). It establishes procedures for analyzing a mission, developing and wargaming COAs against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an operation order for execution. It provides the commander and his staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands.

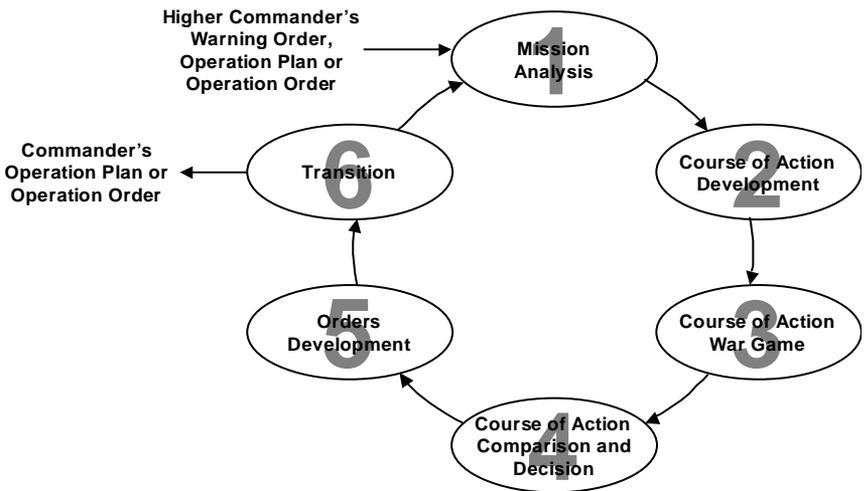


Figure 4-1. Marine Corps Planning Process steps.

Force protection planning is aligned with the MCPP steps and ensures force protection actions are coordinated and integrated with the other warfighting functions and the higher, adjacent, and subordinate commands.

4001. Mission Analysis

Mission analysis is the first step in the MCPP. The purpose of mission analysis is to review and analyze orders, guidance, and other information provided by higher headquarters and produce a unit mission statement. Mission analysis drives the MCPP. During mission analysis, force protection considerations and threats are raised and assessed by the force protection officer, with assistance from the rest of the planning staff.

a. MAGTF Force Protection Officer

Each MAGTF has an individual who is designated as the force protection officer. This may be a full-time assignment or an additional duty. It may be a responsibility assigned to an individual who is augmenting the MAGTF headquarters for the duration of the operation. Regardless, the force protection officer is responsible for ensuring that the commander's concerns and the realities of the battlespace are accounted for during the planning process. The force protection officer must raise force protection questions so that appropriate active and passive measures may be incorporated into any plan. Issues that should be addressed by the force protection officer during mission analysis include:

- **Battlespace.** Is the assigned battlespace sufficient for the execution of anticipated force protection tasks? If the battlespace is too small, too large, too small, or not appropriately located, then the force protection officer will recommend modifications. The analysis should also include an assessment of the commander's stated area of interest.
- **Friendly Center of Gravity.** Is there a logical relationship between the friendly center of gravity (COG) and the defined friendly critical vulnerabilities (CVs)? If no CVs have been identified, the force protection officer should analyze the MAGTF and the mission to determine them.
- **Implied Tasks.** Have force protection implied tasks been identified? Implied tasks—while not specifically stated in the higher headquarters

order—are performed to accomplish specified tasks. Implied tasks emerge from analysis of the higher headquarters order, the threat, and the terrain. Routine, inherent, or standing operating procedure (SOP) tasks are not included in the list of tasks. Many force protection tasks fall into this category, and should be addressed in a SOP rather than listed as an implied task. The force protection officer should review existing SOPs to ensure that they adequately address standing force protection requirements, and that new implied force protection tasks are identified.

- **Limitations.** Have limitations on the ability of the MAGTF to protect itself—such as ROE—been imposed by the higher headquarters? The impact of these limitations must be analyzed, and if the result is a critical force protection concern, then the limitations should be modified or removed.
- **Commander’s Critical Information Requirements.** Many force protection questions will be raised during mission analysis, and not all will be answered immediately. Some information gaps may be significant enough to warrant consideration as a commander’s critical information requirement (CCIR) during planning. Some, such as the status of a friendly CV, may be identified as potential CCIRs for the duration of the operation.

b. Risk Assessment

The key force protection action during mission analysis is the development of a risk assessment. The assessment, conducted by the force protection officer and assisted by representatives as needed from the other warfighting functions, consists of identifying the potential threats, analyzing MAGTF vulnerabilities, and the commander’s final determination of an acceptable level of risk.

(1) Determine Enemy Courses of Action. A force protection threat assessment is conducted for a particular area and time. Force protection threat assessments fuse intelligence, CI, environmental, medical; information/data threat, and other information into a cohesive threat picture helpful to the commander.

The threat analysis is a continual process of compiling and examining all available information concerning potential threats. A threat analysis will review the factors of a threat’s existence, capability, intention, history, and

targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying the probability of attack and results in a threat assessment.

(2) Vulnerability Assessment. Once the threats are identified, the commander should use a multifunctional vulnerability assessment team with expertise in the following areas: physical security; civil, electrical, and structural engineering; special operations; operational readiness; law enforcement and operations; infrastructure; WMD; health services; and intelligence/CI. Commanders may tailor the team composition and the scope of the assessment to meet the unique requirements of a particular activity; however, commanders should meet the intent of providing a comprehensive assessment. The assessment team conducts an evaluation of the force to reveal the vulnerabilities and potential solutions relating to present and future threats. The assessment will address the broad range of physical threats to the security of personnel and assets and it should be updated periodically.

Vulnerability assessments should determine the likelihood of enemy attack against the potential targets. They should evaluate the safety and vulnerability of local food and water sources, evaluate local medical capabilities, determine adequacy of hygiene of local billeting and public facilities, and perform an occupational and environmental risk evaluation. The assessments should identify vulnerabilities, prioritized by their criticality to the mission, and propose solutions for enhanced protection.

CARVER (criticality, accessibility, recuperability, vulnerability, effect, and recognizability) analysis can be used to conduct vulnerability assessments. It is a special operations forces technique used throughout the targeting and mission planning cycle to assess mission validity and requirements. The technique is also useful when applied to friendly forces and assets to determine if they are likely targets of enemy actions.

- **Criticality.** Criticality, or target value, is the primary consideration in targeting. The enemy will consider a target to be critical when its destruction or damage would significantly impair friendly political, economic, or military operations. The value of a target may change as the situation develops, requiring the use of time-sensitive targeting methods.

- **Accessibility.** To damage, destroy, or conduct surveillance of a target, the enemy must be able to reach it, either physically or via indirect (i.e., standoff weapons or surveillance) means. The enemy must not only be able to reach the target, but must often remain there for a period of time, and then exfiltrate out of the target area.
- **Recuperability.** Recuperability is a vital supporting element of criticality. It is important to estimate how long it will take the MAGTF to repair, replace, or bypass the damage inflicted on the target. The enemy may not consider a target to be lucrative if it can be repaired, replaced, or bypassed in a short time with minimum resources.
- **Vulnerability.** A target is vulnerable if the enemy has the means and expertise to conduct the planned mission and achieve the desired level of damage or other objectives as assigned.
- **Effect.** For targets of more purely military value (e.g., munitions depots; headquarters complexes; petroleum, oils, and lubricants facilities; LOCs; and C2 complexes), the impact of attacking the target and achieving the desired results must be assessed. For both military and civilian targets, the political, economic, legal, and psychological effects of the attack must be evaluated as well as the impact of target destruction on the health and welfare of the indigenous civilian population.
- **Recognizability.** The target must be identifiable by the enemy under various weather, light, and seasonal conditions and configurations (if applicable) without being confused with other targets or target components. Sufficient data must be available for the enemy to differentiate the target from similar objects in the target area. The same requirement exists to distinguish the target's critical damage points and stress points from their parent structures and surroundings.

(3) Commander's Assessment. Commanders should utilize the threat and vulnerability assessments produced during mission analysis to determine the level of risk they are willing to accept. The commander should also decide where and when he is prepared to accept this level of risk. Once the risk assessment is complete and all risk-level decisions made, commanders and their planners should be prepared to use this information during COA development to eliminate the risks they are not willing to accept and mitigate the risks they either cannot eliminate or have decided to accept.

4002. Course of Action Development

During COA development, the planners use the mission statement, commander's intent, and commander's planning guidance to develop the COA(s). Each prospective COA is examined to ensure that it is suitable, feasible, acceptable, distinguishable, and complete with respect to the current and anticipated situation, the mission, and the commander's intent.

During COA development, the force protection officer considers the following issues:

- **Sequence of Actions.** Do certain force protection tasks—such as implementation of TMD or military deception—suggest phasing or sequencing the operation or battle?
- **Use of Maneuver Control Measures and Fire Support Coordination Measures.** Do the proposed measures hinder or simplify force protection tasks?
- **Arrangement of Essential Tasks.** As essential tasks are arranged in time and space, and a sequence of actions developed? Are force protection tasks logically integrated into the proposed COA? Are force protection tasks prioritized?
- **Resource Allocation.** Are force protection assets dual-tasked? Are these forces adequate for the assigned force protection tasks and assessed threat levels?
- **Risk.** Does the COA assume an element of risk consistent with the commander's assessment from mission analysis? Have risk criteria been determined and used for each COA?

a. Concept of Force Protection

During COA development, planners will develop a concept of operations. As stated in MCWP 5-1, *Marine Corps Planning Process*, “the concept of operations is the basis for supporting concepts such as the concept of fires, logistics, or force protection.” The force protection officer should develop a supporting concept of force protection that captures the commander's force protection priorities, desired measures to achieve protection, and the acceptable level of risk.

The force protection concept should be an overarching security program accomplished through the integration of personnel security, information

security, protective services, law enforcement, and antiterrorism, all of which are supported by the synchronization of the other warfighting functions. The force protection concept is not developed in isolation. The force protection capabilities and actions of subordinate, adjacent, and higher commands must be fully integrated into the concept's development, coordination, and execution.

Based on the risk assessment developed during mission analysis, the concept for force protection must provide for the protection of critical assets, information, and personnel throughout the area of operations for the duration of the operation. Additionally, the concept should address units and individuals going outside of the U.S. during deployment and mobilization operations. Since the absolute and continuous protection of the many organizations, facilities, equipment, and personnel under the commander's control is unrealistic, resources and assets must be prioritized. The required level of protection, during various periods of time, should be clearly specified. Actions necessary to meet the established standards of protection must be identified, prioritized, and resourced.

b. Planning Tools

The use of planning tools such as matrices or tables can be useful to frame the scope and magnitude of the force protection requirements. Planning tools can help link the synchronization matrix developed by the planners to specific force protection activities. The following are offered as sample techniques to help frame force protection requirements.

(1) Force Protection Priority Matrix. This matrix organizes and prioritizes force protection tasks across the warfighting functions and identifies the desired effect the MAGTF wants to achieve. (See Figure 4-1.) It reverses the normal targeting methodology, and focuses the force protection officer on those capabilities that should be protected.

(2) Force Protection Task Table. This table draws out the logical consequences of a force protection task. (See Figure 4-2.) During COA development, the force protection planners may use this table to define each task and its implications. The table will be used to assign force protection tasks to appropriate units and may reveal deficiencies that require additional risk assessment and subsequent adjustments in resource allocation.

	Force Protection Task 1 “Maintain Flank Security”		Force Protection Task 2 “Maintain Security of Vital Area”	
PRIORITY	Warfighting Function	Protected Capability	Warfighting Function	Protected Capability
1	Maneuver	3d MarDiv (PD) 101 st AA Div (PD)	Logistics	FCSSA (PN) JLOTS Site (PN)
2	Intelligence	UAV Fwd Op Base (PN)	C2	MEF(Fwd) CP (PS) TACC (PN) Ground mobile force sites (PS)
3	Fires	Counterbattery Radars	Fires	Airbase A (PN) Airbase B (PN)
4	Logistics	Artillery resupply convoys	Intelligence	PW interrogation facility
5	C2		Force Protection	Tactical combat force (PD)
6	Force Protection		Maneuver	
Key	PD = Prevent Destruction PN = Prevent Neutralization PS = Prevent Suppression			

Table 4-1. Force protection priority matrix.

Force Protection Task	Condition	Desired Effect	Force Protection Activities
Maintain security of vital areas	GMF remains fully operational from H-Hour to H+24	GMF site safe from local attack and from WMD	Local security in place TCF prepared to respond to level III threat TMD coverage includes GMF site
Minimize casualties	Rapid evacuation of casualties	Air medevac less than 20 minutes; surface medevac to Regt aid stations only	Dedicate/configure 6 CH-46 for air medevac during H+10 to H+24 Ensure adequate Class VIIIIB prior to H+10

Table 4-2. Force protection task table.

c. Additional Planning Considerations

(1) Rules of Engagement. ROE provide a means for the commander to influence force protection. ROE are the directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. They regulate the use of armed force in the context of applicable political and military policy and domestic and international law. ROE are the rules that govern when, where, against whom and how force can be used.

ROE may be used to control the use of force by the MAGTF in three main areas: ROE implement the inherent right of self-defense; they define use of force for mission accomplishment; and they apply throughout the spectrum of conflict from peacetime to MOOTW to armed conflict. ROE considerations include:

- International law and domestic law.
- Operational concerns (mission requirements).
- Commander's intent (both MAGTF and higher headquarters).
- Threat capabilities and intentions.
- Tactical capabilities of the MAGTF.
- Tactics and weapons systems organic to the MAGTF.
- Host-nation law and requirements.
- U.S. policy (considering United Nations resolutions and international agreements)

The MAGTF commander should review proposed supplemental ROE and provide ROE recommendations to the higher headquarters. Mission objectives must drive the ROE formulation process and not vice versa. The proposed ROE should be developed, exercised, and modified as necessary during the COA development, analysis, and selection processes. The probable ROE impact on the COA should be wargamed, with emphasis on the impact of probable ROE restrictions and allowances for use of force. Proposed ROE must be modified as necessary to support the accomplishment of mission objectives, and should never restrict the right of self-defense.

An example of the requirement for clearly understood ROE is the issue of air and missile defense. The employment of defensive weapon systems requires early identification of friendly, neutral, or hostile aircraft and missiles to maximize beyond-visual-range engagement and avoid fratricide. The problem of distinguishing friendly, neutral, and enemy air assets and the employment of air defense systems against an enemy threat is a highly complex task and firing authorization procedures should be clearly defined. However since ballistic missiles have a distinct flight profile, ROE for this threat usually allow immediate engagement.

(2) Law Enforcement. Over the last decade, the U.S. government has developed a policy regarding terrorism states that all terrorist actions are criminal and all lawful measures to prevent such acts and to bring to justice

those who commit them will be taken. As a result, law enforcement measures addressing terrorism as well as more routine criminal acts have become a vital component of an effective force protection program.

An example of the role of military and local law enforcement can be seen in their contribution to defensive IO. By investigating information system incidents and intrusions and apprehending terrorists and criminals, damage is contained and additional attacks are deterred. Law enforcement also provides investigative resources and maintains records on incidents that may assist IO analysts in defining vulnerabilities. Law enforcement considerations should include both terrorism and criminal acts.

- **Terrorism.** By definition, terrorists do not meet the four requirements established in the 1949 Geneva Convention necessary for combatant status (wear uniforms or other distinctive insignia, carry arms openly, be under command of a person responsible for group actions, and conduct their operations in accordance with the laws of war). Only combatants can legitimately attack proper military targets. For this reason, captured terrorists are not afforded the protection from criminal prosecution attendant to prisoner of war status. In peacetime, terrorist acts are normally punishable only under domestic (local) law. However, in an internationally recognized war or MOOTW involving the use of force (regional or global), terrorists can be tried under local criminal law or under military jurisdiction by either a courts-martial or military tribunal.

Legal and policy restrictions on the use of active duty DOD military personnel, DOD civilian employees, and contractors such as DOD security police for direct enforcement of civil laws in the United States or its possessions are contained in the Posse Comitatus Act (18 USC 1385), other federal statutes (10 USC 371-382), DODDs (DODD 5525.5, “DOD Cooperation with Civilian Law Enforcement Officials”), and the SECNAVINST 5820.7 series. These laws and policies provide a general prohibition against the use of the uniformed Services of the DOD, either as part of a Posse Comitatus or in a military role other than as provided by statute, to assist local law enforcement officers in carrying out their duties. The purpose of this restrictive legislation is to maintain congressional control over the manner and circumstances under which military power could be used in domestic affairs.

Although the FBI has primary law enforcement responsibility for terrorist incidents in the United States (including its possessions and territories), installation commanders are responsible for maintaining law and order on military installations. Plans should address the use of security forces to isolate, contain, and neutralize a terrorist incident within the capability of installation resources. In the United States, installation commanders will provide the initial and immediate response to any incident occurring on military installations to isolate and contain the incident. If the FBI assumes jurisdiction, the military commander is still required to take immediate actions as dictated by the situation to prevent loss of life or to mitigate property damage before the FBI response force arrives.

For foreign incidents, the commander's responsibilities are the same as for domestic incidents—with the added requirement to notify the host nation and Department of State. Notification to the Department of State is made at the geographic combatant commander level. In all theaters, existing plans provide guidance to the installation commander regarding notification procedures. The Department of State has the primary responsibility for dealing with terrorism involving Americans abroad. The commander's response is subject to agreements established with the host nation. In addition, under standing ROE, the inherent right of self-defense still applies in situations off-base in foreign areas. If U.S. forces (or members thereof) are actually under attack, they retain the inherent right to respond with proportionate, necessary force until the threat is neutralized. The response to off-base foreign incidents is the sole responsibility of the host nation.

- **Crime.** Although crime will not normally stop a MAGTF from conducting conventional military operations, it can have a negative effect on morale, both on military personnel and indigenous civilian personnel in the area controlled by the MAGTF. Criminal acts such as looting, murders, kidnappings, and robberies can adversely affect the MAGTF as it conducts MOOTW. The primary law enforcement method of deterring and detecting criminal acts is preventive patrolling by military police. It has as its major feature the protection of people, not property. The primary emphasis of preventive patrolling is having uniformed patrols work areas where analysis shows many people gather at times when the likelihood of crime is greatest. Emphasis is placed on

establishments such as the post exchange, commissary, places where alcohol is served or sold, hospitals (especially during evening shift changes), banks, gas stations, and recreational facilities. The facility commander establishes patrol requirements based on crime patterns and the force protection threat assessment.

(3) Natural Disasters. Failed states, famines, uncontrolled migration, and other natural or man-made disasters will continue to occur, at times affecting U.S. interests and requiring the unique capabilities of a MAGTF to provide stability, disaster relief, and other forms of emergency assistance. These natural disasters could include severe thunderstorms, floods, tornadoes, hurricanes, ice storms, fires, and earthquakes. Relief operations could include dislocated civilian support (refugees, displaced or stateless persons, evacuees, and other victims) and security or technical assistance, such as communications restoration, relief supply management, provision of emergency medical care, humanitarian demining assistance, and high priority relief supply delivery.

The environment for these humanitarian operations may be permissive, uncertain, or hostile, requiring a force protection program to protect the force while assistance is being rendered. Even in a permissive environment, the MAGTF can expect to encounter banditry, vandalism, and various levels of violent activities from criminals or unruly crowds.

Force protection during natural disaster relief operations is similar to that of other operations. Effective CI and military police support is critical. All available sources of intelligence should be used for deployment planning, mission requirements, and other unforeseen taskings as they arise. Large numbers of refugee or displaced persons will require crowd control, background screening, and medical assistance to prevent the spread of disease. Strict OPSEC procedures should also be followed to prevent criminal elements or potential enemies from acting against the MAGTF.

(4) Environmental Terrorism. In the aftermath of the Persian Gulf conflict and Saddam's deliberate release of oil into the waters of the Gulf and the destruction of Kuwaiti oil wells; environmental terrorism has become a very real threat. Property and personnel loss and denial of access due to fuel or chemical spills, pollution of resources, and inadvertent or accidental release of toxins from hazardous materials production and destruction are force protection threats that a MAGTF may have to be prepared to face.

Consequence management operations in the aftermath of an act of environmental terrorism are intended to mitigate the results of the act. These operations could involve providing essential services and activities such as transportation, communications, public works, fire fighting, information planning, care of mass casualties, resources support, essential and/or routine health and medical services, urban search and rescue, hazardous materials, and the provision of food, water, and energy. Additionally, depending on the type and extent of environmental terrorism, the MAGTF may have to conduct agent identification, hazard detection and reduction, environmental monitoring, decontamination, and site restoration (environmental clean-up) operations.

4003. Course of Action War Game

COA wargaming may involve a detailed assessment of each COA as it pertains to the enemy and the battlespace. Each friendly COA is wargamed against selected threat COAs. COA wargaming assists the planners in identifying strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. COA wargaming will also identify branches and potential sequels that may require additional planning. Short of actually executing the COA, COA wargaming provides the most reliable basis for understanding and improving each COA.

The force protection officer is responsible for ensuring that friendly critical vulnerabilities are realistically stressed, and that planned protection measures are feasible and effective. Enemy capabilities and COAs should not be underestimated, and friendly capabilities must be accurately portrayed. If friendly casualty estimates are made during the war game, the force protection officer should ensure that these estimates are realistic and actions taken to reduce these casualties are incorporated into the COA.

During the war game, the force protection officer should be able to modify and validate the risk assessment developed during mission analysis. At the conclusion of the war game, the force protection officer will revise the concept of force protection for each of the friendly COA that were gamed, incorporating changes that were developed and assessed during the war game.

4004. Course of Action Comparison and Decision

In COA comparison and decision, the commander evaluates all friendly COAs—against his established criteria, then against each other—and selects the COA that he deems will best accomplish the mission. Often, risk will be a major consideration in COA comparison and decision. The force protection officer must be prepared to address specific concerns about risks to the friendly COG and CVs, which COA presents fewer force protection risks, and how the concept of force protection will be implemented.

4005. Orders Development

During orders development, the staff takes the commander's COA decision, mission statement, commander's intent, and guidance, and develops orders to direct the actions of the unit. Orders serve as the principal means by which the commander expresses his decision, commander's intent, and guidance.

The force protection officer prepares Appendix 15, Force Protection, to Annex C, Operations, which is presented in Appendix C to this pamphlet. The concept of force protection will serve as the basis for Appendix 15. Since force protection issues cross warfighting and staff boundaries, the force protection officer should be concerned with all portions of the operation order that pertain to force protection. Appendix D depicts some of the additional sections of an operation order that the force protection officer should provide input to during orders development.

4006. Transition

Transition is the orderly handover of a plan or order as it is passed to those tasked with execution of the operation. It provides those who will execute the plan or order with the situational awareness and rationale for key decisions necessary to ensure there is a coherent shift from planning to execution. The force protection officer should be prepared to brief the force protection concept and assigned tasks, and to assist in any rehearsals. The force protection officer should also be available during the transition to respond to questions about force protection priorities or tasks.

Appendix A

Marine Corps Component Role

A-1. Component Responsibilities

Marine Corps component commanders command, train, and sustain Marine Corps forces. They integrate force protection requirements into every aspect of their activities. They establish guidance, program for, coordinate, and manage all force protection requirements for the component, and coordinate with Headquarters, Marine Corps (HQMC). Centralized control of force protection resources and decentralized execution of force protection measures are essential to effectively protect Marine Corps component forces against each threat.

The Marine Corps component commander may position forces such as the Marine Corps logistics command (MLC) (if established) and some MAGTF forces (e.g., portions of the aviation combat element) in the joint rear area. The Marine Corps component commander assigns missions to the MAGTF, the MLC (if established), the rear area command (if established), and the assigned or attached forces of other Services and nations.

The Marine Corps component commander sets the conditions and establishes the environment for conducting MAGTF operations. He achieves this by providing and sustaining Marine Corps forces that execute the tasks assigned by the joint force commander. He is responsible for ensuring that the appropriate theater commander protects forces in transit—both force movement and flow of sustainment. The component commander is also responsible for planning and coordinating tasks within the rear area. He must balance the need to support the force with the need to protect it.

A-2. Marine Corps Logistics Command

To provide operational-level support to tactical operations, the Marine Corps component commander may establish a MLC. The MLC is not a standing

organization, but is task-organized to meet the operational support and sustainment requirements of the mission and is normally formed around a force service support group from another MEF. When formed, it provides logistic support to all Marine Corps forces in theater, and may provide limited support to other joint and multinational forces as directed by the combatant commander. The MLC provides operational logistics to Marine Corps forces as the Marine Corps component's logistics agency in theater. The MLC is also responsible for force protection operations to prevent the enemy from interfering with logistics operations. Although subject to mission, enemy, terrain and weather, troops and support available—time available (METT-T) considerations, specific force protection responsibilities for the MLC may include:

- Improving combat support bases and throughput infrastructure.
- Providing mobility, countermobility, and survivability support for assigned ports, airfields, and beaches.
- Health maintenance.
- Possible designation as the rear area commander.

A-3. Rear Area Commander

Successful force protection operations in the rear area must coordinate and integrate security, intelligence, area management, force movements, and host-nation support. To accomplish this complicated task requires an effective command and control organization and reliable command and control systems, including communications, intelligence, and planning. The three doctrinal options for command and control of rear area operations are for the Marine commander (Marine Corps component or MAGTF) to retain command and control, designate a rear area coordinator, or designate a rear area commander. The Marine commander determines how he will command and control rear area operations based on his analysis of METT-T factors. From a force protection perspective, when the enemy threat level (level III) in the rear area is significant enough that it requires a combined-arms task force (tactical combat force), then a rear area commander is designated. See Appendix E, Force Protection Conditions for further information on threat levels.

The rear area commander normally establishes a facility from which to command, control, coordinate, and execute rear area force protection

operations. This facility normally coordinates the force protection activities of the following organizations:

- Security forces (e.g., military police, tactical combat force).
- Fire support agencies.
- Support units (e.g., supply, engineer, medical).
- Movement control agencies.
- Other command and control facilities.
- Bases and base clusters.
- Other organizations as necessary (e.g., CI team, civil affairs group).

Base defense is an important part of rear area force protection operations. Base and base cluster commanders are designated to provide coordinated base defense. Commanders are responsible for integrating their plans and executing base defense. Base defense forces are not tactical combat forces. Base defense forces provide ongoing security for a specific location (a base) or a number of locations (a base cluster), while tactical combat forces respond to threats throughout the entire rear area.

Rear area commanders employ both active and passive measures to provide security. Active measures include organizing for defensive operations, coordinating reconnaissance and surveillance, providing security to convoys, positioning air defense units in the rear area, establishing liaison with fire support organizations, employing close air support, establishing reaction forces, developing defensive plans and positioning assets in support of them, patrolling, and training in defensive skills. Passive measures include camouflage, dispersion, and cover.

Populace and resource control operations are conducted to locate and neutralize insurgent or guerilla activities. Normally host-nation police and civilian or military units carry out these activities, but U.S. military forces, particularly military police, can also conduct or support these operations.

Reducing the potential of damage to the rear area infrastructure is a critical force protection concern. Planning and executing damage control operations should occur at the lowest possible level of command. If an enemy attack is successful and damage has been inflicted, then area damage control operations should include recovery and restoration efforts.

The tactical combat force is a task-organized combat unit used by the rear area commander to respond to enemy threats. The tactical combat force can range in size from a company to a regiment depending on the situation and factors of METT-T. It could be a combat unit temporarily in the rear area or a designated task-organized force with the capability to perform the mission. The tactical combat force should be capable of controlling ground and air fires and coordinating its actions with other Marine, joint, or host-nation forces. It should have sufficient mobility and be located in a position that allows it to respond to potential threats in a timely fashion.

Appendix B

Marine Corps Role in Homeland Defense

B-1. Headquarters, Marine Corps

HQMC exercises control over force protection programming, training, staffing, manning, and developing force protection policy. In March 2002, the Security Division (PS) was established within the Plans, Policy, and Operations (PP&O) Department of HQMC. PS is responsible for the coordination, development, and execution of Marine Corps policy for:

- Homeland defense.
- Anti-terrorism and force protection.
- Critical infrastructure protection/assurance.
- Installation security and emergency preparedness.
- Operating force and supporting establishment military police and law enforcement.
- OPSEC.
- Physical security.
- Criminal investigations.
- Marine Corps security force (MCSF), Marine security guard (MSG), and Chemical/Biological Incident Response Force (CBIRF).
- Counterdrugs.
- Military support to civil authorities.

HQMC force protection initiatives and programs include maintenance of the Marine Corps Electronic Security Systems, the procurement of an Integrated Tactical Automated Sensor System, integral involvement with the Joint Staff-sponsored Force Protection Equipment Demonstration, the distribution of funds in support of antiterrorism/force protection mobile training teams, and very close oversight of the Marine Corps antiterrorism/force protection program. The goal of this program is to establish a model which facilitates a security/preparedness posture capable of handling both man made and natural disasters. The program seeks to enable installations to smoothly transition from

normal operations to an increased readiness posture. The end state is the complete awareness of all of the program’s policies and procedures by all Marine Corps personnel—active, reserve, family members, and civilians.

B-2. Fourth Marine Expeditionary Brigade (Antiterrorism)

The 4th Marine Expeditionary Brigade (MEB) (Antiterrorism (AT)) is an organization unique to the Marine Corps with specialized antiterrorism capabilities. It consists of Marines and Sailors specifically trained to respond quickly—worldwide—to threats or actual attacks by terrorists. It is a rapidly deployable and sustainable force that can deter, detect, and defend against terrorist actions and conduct initial incident response to combat the threat of terrorism worldwide. The 4th MEB (AT) provides the following capabilities:

- Chemical, biological, radiological, nuclear, and high explosive incident response.
- Physical and electronic security.
- Integrated vulnerability assessment and threat analysis.
- Explosive ordnance detection and disposal.
- Lethal and nonlethal weapons employment and training.
- Urban search and rescue.
- Physical security and antiterrorism/force protection training.

The 4th MEB (AT) deploys a forward command element (CE)/assessment team within 6 hours of notification and maintains a task-organized antiterrorism/incident response MAGTF on 12-hour alert. The entire MEB (AT) can deploy within 72 hours of notification.

The 4th MEB (AT) may include an air contingency battalion/antiterrorism battalion, a CBIRF, MCSF battalion elements, and MSG battalion elements. Depending on the mission, it can vary in size from 1,400 to 4,800 Marines and Sailors.

a. Anti-Terrorism Battalion

The anti-terrorism battalion is an infantry battalion specially trained in antiterrorism operations and security techniques, with emphasis on urban environments. It is currently the 3rd Battalion, 8th Marine Regiment.

b. Marine Corps Security Force Battalion

The MCSF battalion provides armed antiterrorism and physical security trained forces to designated naval installations, vessels or units. The battalion's fleet antiterrorist security team (FAST) companies provide fleet commander in chiefs and fleet commanders forward-deployed FAST platoons for responsive short-term security augmentation of installations, ships or vital naval and national assets when force protection conditions have been elevated beyond the capabilities of the permanent security forces. The Khobar Towers Bombing Report specifically cited the FAST security teams as "the most impressive security forces observed in the theater. They are superbly trained, well equipped, and well led. They provide a useful model for development of service training programs."

c. Marine Security Guard Battalion

The MSG battalion provides security services to selected Department of State Foreign Service posts to prevent the compromise of classified material and equipment and to provide protection for U.S. citizens and government property. The MSG battalion exercises command, less operational control, of these Marines, in that it is responsible for their training, assignments, administration, logistical support, and discipline. MSG battalion fields over 1,000 Marines at 121 detachments organized into seven regional MSG companies and located in over 105 countries. Headquarters Company and Battalion Headquarters is located at Quantico, Virginia.

d. Chemical/Biological Incident Response Force

The CBIRF was formed in July 1995 and consolidated into the 4th MEB (AT) in 2001. It is the only U.S. force currently capable of performing counterterrorism consequence management on a large scale in a chemical and/or biological contaminated environment. CBIRF can immediately deploy to affected sites and provide a number of significant capabilities to include coordinating initial relief efforts, security, detection and identification of chemical or biological agents, expert medical advice, and limited decontamination of personnel and equipment. It is capable of detecting and identifying toxic industrial materials in addition to warfare agents.

The CBIRF includes approximately 350 Marines and Sailors organized into six elements: a command element, a chemical/ biological reconnaissance

element, a chemical/biological decontamination element, a medical element, a security element, and a service support element. The CBIRF has enhanced capabilities for detecting and identifying specific chemical and biological agents, assessing downwind hazards, conducting advanced lifesaving support, and decontaminating patients to facilitate medical treatment. It employs state-of-the-art equipment to treat casualties via a “reachback” link to civilian scientific and medical experts, conduct advanced lifesaving support, and provide communications and an enhanced transportation capability.

Appendix C

Force Protection Appendix Format and Example

This appendix provides a format and example of the force protection appendix for an operation order. The format and example are based on MCWP 5-1, *Marine Corps Planning Process*, Appendix G. The force protection appendix is Appendix 15, Force Protection, to Annex C, Operations, and applies to Marine Corps forces at all levels.

CLASSIFICATION

C-1. Force Protection Appendix Format

Copy no. ____ of ____ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 15 TO ANNEX C TO OPERATION ORDER OR PLAN
(Number) (Operation CODEWORD) ()
FORCE PROTECTION ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

1. () Situation. Summarize the overall operational situation as it relates to force protection.

a. () Enemy. Summarize the enemy situation, force disposition, intelligence capabilities, and possible courses of action. If applicable, reference intelligence estimates or summaries. Address any specific information that bears directly on planned force protection actions.

b. () Friendly. Summarize the situation of those friendly forces that may directly affect force protection actions. Address any critical limitations and any other planned force protection actions.

c. () Assumptions. List any assumptions made of friendly, enemy, or third-party capabilities, limitations, or courses of action. Describe the conditions that the commander believes will exist at the time the plan becomes an order. Omit in orders.

2. () Mission. State the force protection mission in a clear, concise statement that answers the questions: Who, what, when, where, and why.

(Page Number)
CLASSIFICATION

CLASSIFICATION

3. () Execution

a. () Concept of Operations. Summarize how the commander visualizes force protection actions throughout the operation. Describe how force protection actions will support the command's operational mission. Summarize the concepts for supervision of force protection actions.

(1) () The concept of operations may be a single paragraph or divided into two or more paragraphs depending upon the complexity of the operation.

(2) () When an operation involve various phases (i.e., peace or pre-hostilities, crisis, war, post-hostilities etc.), the concept of operations should be prepared in subparagraphs describing force protection actions in each phase.

b. () Force Protection Tasks. Identify major force protection tasks for the MAGTF. Tasks may be expanded in tabs A through C.

(1) () Combating terrorism.

(2) () Physical security.

(3) () Base defense.

c. () Coordinating Instructions. Address any mutual support issues relating to the elements of force protection.

4. () Administration and Logistics. Address any force protection-related administrative or logistic requirements.

5. () Command and Control. List any force protection-related C2 instructions. State the command structure for force protection actions. Identify any special force protection communications and reporting requirements.

ACKNOWLEDGE RECEIPT

(Page Number)

CLASSIFICATION

CLASSIFICATION

Name
Rank and Service
Title

TABS:

- A — Combating Terrorism
- B — Physical Security
- C — Base Defense

OFFICIAL:

s/

Name

Rank and Service

Title

(Page Number)
CLASSIFICATION

UNCLASSIFIED

C-2. Force Protection Appendix Example

Copy no. ____ of ____ copies
I MEF
GREENTOWN, BLUELAND
25 April 2002
ADB-1

APPENDIX 15 TO ANNEX C TO OPERATION ORDER 0002-02
(OPERATION SHARP SWORD (U))
FORCE PROTECTION (U)

(U) REFERENCES:

- (a) CJTF-Blueland OPORD 0002-02, 25 April 2002
- (b) MARFOR Blueland OPORD 0004-03, 28 April 2002
- (c) Maps and Charts: Series ONC, sheets G-2 (ORANGELAND, BLUELAND), edition 12; G-3 (ORANGELAND, BLUELAND), 1:1,000,000; Series 1501A, sheets NJ 32-10 (GREENTOWN, BLUELAND), edition 2; NJ 32-11 (JADE CITY, BLUELAND), edition 2; NJ 32-15 (PURPLETOWN, BLUELAND) 1:250,000
- (d) Joint Pub 3-0, *Doctrine for Joint Operations*
- (e) Joint Pub 3-01.5, *Doctrine for Joint Theater Missile Defense*
- (f) Joint Pub 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense*

(U) TIME ZONE: Zulu

1. (U) Situation. Marine forces have deployed to Blueland and reported OPCON to CJTF Blueland. The MEF G-2 and G-3 have jointly conducted a risk assessment of the MEF operation and the implications for force protection. The assessment is summarized below.

- (a) (U) Enemy. Current THREATCON for Blueland is DELTA; rear area threat is Level III. Prior to the deployment of U.S. forces, the

C-15-1
UNCLASSIFIED

UNCLASSIFIED

enemy demonstrated its willingness and capability to strike targets in the rear of Blueland forces. The enemy has publicly stated that it will use every means available to prevent U.S. military operations. The threat assessment has determined that the enemy will attack the MEF critical vulnerabilities, using the following capabilities

- (1) (U) Special forces—direct fire and demolition attacks by 3-5 man units.
- (2) (U) Terrorist acts—car bombs, remote controlled land mines.
- (3) (U) Scud missile attacks—conventional and chemical warheads.
- (4) (U) Computer network attack—hackers trying to disrupt operations by imbedding viruses and Trojan horse programs.
- (5) (U) Target acquisition—clandestine reconnaissance and signals intercept.

b. (U) Friendly. The MEF COG for this operation is assessed to be 3^d MAW and its ability to deliver timely fires. The associated CVs that the enemy will target are:

- (1) (U) C2—antennae, land lines, radio nets, computer data bases.
- (2) (U) Fuel distribution system—fuel tanks, trucks, and pipelines.
- (3) (U) Ammunition storage sites.
- (4) (U) Airfield runways.

c. (U) Assumptions

- (1) (U) The enemy will receive limited target acquisition and tracking assistance from sympathizers within the indigenous population.
- (2) (U) The enemy has established supply caches in the MEF rear area for use by its special force units.

C-15-2

UNCLASSIFIED

UNCLASSIFIED

(3) (U) The enemy will avoid contact with security forces and strike soft targets only.

(4) (U) Blueland will provide law enforcement and security support throughout the MEF rear area. However, there is a strong likelihood that some Blueland security elements have been infiltrated and compromised by the enemy.

(5) (U) The MEF can anticipate little warning of Scud attacks prior to launch detection.

(6) (U) The enemy will focus its efforts on the identified MEF critical vulnerabilities. However, it will not hesitate to strike other unprotected targets of opportunity that might affect MEF effectiveness, morale, or gain media attention.

2. (U) Mission. Protect the force, particularly 3^d MAW and its airfields, in order to permit the MEF to conduct its offensive operations without major impact by enemy attacks for the duration of the operation.

3. (U) Execution

a. (U) Commander's Intent. I intend to posture our force to allow no easy opportunity for special force attacks or terrorist acts against our personnel, facilities, or equipment. Safety and force protection must be paramount in every Marine's and Sailor's mind. The enemy will use stealth and surprise to strike at our CVs at a time and place of his choosing. We will deny him the ability to acquire information on our CVs by a vigorous counterreconnaissance effort and by maintaining tight security at our fixed sites.

b. (U) Concept of Operations. The focus of the MEF force protection effort will be to safeguard 3^d MAW and ensure that it can continue to provide timely air support. Protection of 3^d MAW C2 nodes will be the top priority, followed by ammunition storage sites, the fuel distribution system, and runways. Emphasis will be placed on deterrence, which will be accomplished by strong physical security presence at all

C-15-3

UNCLASSIFIED

UNCLASSIFIED

vulnerable locations. Theater missile defense alerts will be provided by CJTF BlueLand and promulgated by the most expeditious means. Extensive engineering support will be required to prevent unauthorized vehicles from penetrating the security zone. Offensive actions in the rear will be limited due to the need to coordinate actions with the host-nation security forces. CI will focus on identification of enemy intelligence collectors and provide early warning of attack. Upon completion of offensive operations, the focus of force protection will become the 1st FSSG.

c. (U) Force Protection Tasks

(1) (U) Combating Terrorism. Commanders at all levels should encourage personnel under their command to report information on individuals, events, or situations that could pose a threat to the security of the MEF. The CI/HUMINT Company will provide CI support. ROE and procedures for the screening and interrogation of suspected special forces or terrorist personnel are contained in Annex C, Appendix 6, ROE. See Tab A.

(2) (U) Physical Security. 1st FSSG and 1st MARDIV will provide combat engineering support for obstacles. Obstacles, especially minefields, will be coordinated with the MEF engineering officer and incorporated into Annex C, Appendix 22, Obstacle Plan. MPs will be provided by 1st FSSG for crowd and traffic control. See Tab B.

(3) (U) Base Defense. 1st MARDIV will provide tactical combat force of one rifle company to the rear area commander. Scout-sniper support will also be available for local security upon request. Reconnaissance and surveillance (R&S) support will be provided as required and integrated into the MEF R&S plan. See Tab C.

d. (U) Coordinating Instructions. Force protection measures will be coordinated through this headquarters. Liaison with BlueLand security forces may be conducted at MSC level, but operations must be

C-15-4

UNCLASSIFIED

UNCLASSIFIED

approved at MEF level. Consequence management and capability restoration priorities will be established by the MEF by D-1 and will be reviewed daily. ROE are as established by CJTF BlueLand.

4. (U) Administration and Logistics. Forward force protection logistical support requirements to 1st FSSG.

5. (U) Command and Control. CG, I MACE is designated as rear area commander. MEF AC/S, G-3 is designated as the MEF force protection officer and will be responsible for coordinating and integrating force protection measures with BlueLand forces. Security force commander is Capt Victor. Use existing communications systems and procedures to report incidents and request force protection support.

ACKNOWLEDGE RECEIPT

GERALD C. THOMAS
Lieutenant General, USMC
Commanding

TABS:

- A — Combating Terrorism
- B — Physical Security
- C — Base Defense

OFFICIAL:

s/
M.C. TWINING
Col., USMC
AC/S, G-3

C-15-5
UNCLASSIFIED

This page intentionally left blank.

Appendix D

JOPES Orders, Annexes, and Appendices

The following table shows some of the additional sections of an operation order that are of interest to the force protection officer during orders development. Although not exhaustive, it is provided to show the degree to which force protection permeates MAGTF operations and how these various portions of the operation order must be coordinated and integrated into a comprehensive force protection plan.

Section/Annex	Appendix/Tab	Force Protection Issue
Basic Order		Commander's intent Friendly COGs Battlespace definition
Annex B, Intelligence		Estimate of enemy capabilities, COAs
	Appendix 1, Priority Intelligence Requirements	CCIRs that pertain to enemy activity threatening friendly CVs
	Appendix 3, Tab B, Multidiscipline Counterintelligence Threat Report	Enemy collection capabilities
Annex C, Operations		Concept of operations
	Appendix 2, NMC Defense Operations	NBC defense tasks and responsibilities
	Appendix 3, Information Operations/C2 Warfare	OPSEC, military deception, PSYOP, EW
	Appendix 5, Evasion and Recovery Operations	E&R concept
	Appendix 6, Rules of Engagement	Limitations of self-defense
	Appendix 10, Noncombatant Evacuation Operations	Tasks and priorities
	Appendix 11, Escape and Evasion Operations	CSAR tasks and Responsibilities; SAFE areas
	Appendix 13, Explosive Ordnance Disposal	Safe disposal procedures
	Appendix 16, Rear Area Operations	TCF; base defense; threat levels
Annex C, Operations	Appendix 19, Fire Support	Fire support coordinating measures
	Appendix 22, Obstacle Plan	Barriers to control access and limit damage
Annex D, Logistics	Appendix 5, Civil Engineering Support Plan	Barriers to control access and limit damage; construction standards
Annex E, Personnel	Appendix 1, Enemy PWs, Civilian Internees, and Other Detained Persons	Physical control of EPWs
Annex F, Public Affairs	Appendix 3, General Ground Rules for the Media	Guidelines for release of info to the media
Annex G, Civil Affairs		Control of indigenous population
Annex K, Combat Information Systems	Appendix 1, Information Systems Security	Protection of friendly data
Annex P, Host Nation Support		Reliability of HNS personnel
Annex Q, Medical Services	Appendix 1, Joint Medical Regulating System	Hospitalization, treatment, medical regulating
	Appendix 4, Patient Evacuation	Transportation support to meet required timelines
	Appendix 11, Medical Intelligence Support to Military Operations	Environmental health and diseases

Table D-1. Force protection related annexes and appendices.

Appendix E

Force Protection Conditions

E-1. DOD Terrorism Threat Levels

The DOD terrorism threat level classification system is a set of standardized terms used to quantify terrorism threat on a country-by-country basis. The threat levels are low, moderate, significant, and high. The system evaluates the threat using a variety of analytical threat factors, such as preexistence of a terrorist threat, history, capability, intentions, targeting, and security environment.

The Defense Intelligence Agency (DIA) sets the terrorism threat levels identifying the potential risk to DOD interests in a particular country. DIA will coordinate, for clarity purposes, with the Department of State to minimize conflicting threat levels assigned by each organization. The terrorism threat levels apply whether or not U.S. personnel are present in the country. Geographic combatant commanders may also set terrorism threat levels for specific personnel, family members, units, and installations in countries within their areas of responsibility using the definitions established by DIA. Commanders at all levels shall use their own threat analysis as the basis for developing plans and programs to protect assets for which they have AT responsibility. Terrorism threat levels are estimates with no direct relationship to specific force protection conditions outlined in E-2 below.

E-2. DOD Terrorism Force Protection Conditions

A terrorism force protection condition is a security posture promulgated by the commander in consideration of a variety of factors (e.g., a terrorist threat analysis, threat level, etc.). The force protection conditions outlined in E-3 through E-5 below describe the progressive level of a terrorist threat to all U.S. military facilities and personnel under DODD 2000.12, "DOD

Combating Terrorism Program.” As approved by the Chairman of the Joint Chiefs of Staff, the terminology and definitions are recommended security measures designed to ease inter-Service coordination and support of U.S. military anti-terrorist activities. The purpose of the force protection condition system is to provide accessibility to, and easy dissemination of, appropriate information.

Commanders at all levels shall set a local force protection condition. Subordinate commanders may raise a higher-level commander's force protection condition for those personnel and assets for which they have AT responsibilities. However, subordinate commanders shall not lower a higher-level commander's force protection condition without the higher-level commander's concurrence. Commanders shall ensure proper notifications are made.

The force protection condition system applies to ground, naval, and air facilities as described below.

E-3. DOD Ground Facility Terrorist Force Protection Condition Procedures

a. Condition Normal

This condition exists when a general threat of possible terrorist activity exists but warrants only a routine security posture.

b. Condition Alpha

This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of condition Bravo measures. However, it may be necessary to implement certain measures from higher conditions either resulting from intelligence received or as a deterrent. The measures in this condition must be capable of being maintained indefinitely.

- **Measure 1.** At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for

unidentified vehicles on or in the vicinity of U.S. installations. Watch for abandoned parcels or suitcases and any unusual activity.

- **Measure 2.** The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.
- **Measure 3.** Secure buildings, rooms, and storage areas not in regular use.
- **Measure 4.** Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.
- **Measure 5.** Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.
- **Measure 6.** As a deterrent, apply measures 14, 15, 17, or 18 from Condition Bravo, either individually or in combination with each other.
- **Measure 7.** Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher conditions.
- **Measure 8.** Review and implement security measures for high-risk personnel as appropriate.
- **Measure 9.** As appropriate, consult local authorities on the threat and mutual antiterrorism measures.
- **Measure 10.** To be determined.

c. Condition Bravo

This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this condition must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

- **Measure 11.** Repeat measure 1 and warn personnel of any other potential form of terrorist attack.
- **Measure 12.** Keep all personnel involved in implementing antiterrorist contingency plans on call.
- **Measure 13.** Check plans for implementation of the next condition.

- **Measure 14.** Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.
- **Measure 15.** Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
- **Measure 16.** At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.
- **Measure 17.** Examine mail (above the regular examination process) for letter or parcel bombs.
- **Measure 18.** Check all deliveries to such locations as messes and clubs. Advise dependents to check home deliveries.
- **Measure 19.** Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.
- **Measure 20.** Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.
- **Measure 21.** At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.
- **Measure 22.** Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Identify the visitor's destination. Ensure that proper dignity is maintained and, if possible, that female visitors are inspected only by a female qualified to conduct physical inspections.
- **Measure 23.** Operate random patrols to check vehicles, people, and buildings.
- **Measure 24.** Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles
- **Measure 25.** Implement additional security measures for high-risk personnel as appropriate.
- **Measure 26.** Brief personnel who may augment guard forces on the use of deadly force. Ensure that there is no misunderstanding of these instructions.
- **Measures 27.** As appropriate, consult local authorities on the threat and mutual antiterrorism measures.
- **Measures 28 and 29.** To be determined.

d. Condition Charlie

This condition applies when an incident occurs or intelligence is received indicating that some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this condition for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

- **Measure 30.** Continue, or introduce, all measures listed in condition BRAVO.
- **Measure 31.** Keep all personnel responsible for implementing antiterrorist plans at their places of duty.
- **Measure 32.** Limit access points to the absolute minimum.
- **Measure 33.** Strictly enforce control of entry. Randomly search vehicles.
- **Measure 34.** Enforce centralized parking of vehicles away from sensitive buildings.
- **Measure 35.** Issue weapons to guards. Local orders should include specific orders on issue of ammunition.
- **Measure 36.** Increase patrolling of the installation.
- **Measure 37.** Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.
- **Measure 38.** Erect barriers and obstacles to control traffic flow.
- **Measure 39.** Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.
- **Measure 40.** To be determined.

e. Condition Delta

This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this condition is declared as a localized condition.

- **Measure 41.** Continue, or introduce, all measures listed for conditions ALPHA, BRAVO, and CHARLIE.
- **Measure 42.** Augment guards as necessary.
- **Measure 43.** Identify all vehicles within operational or mission-support areas.

- **Measure 44.** Search all vehicles and their contents before allowing entrance to the installation.
- **Measure 45.** Control access and implement positive identification of all personnel—no exceptions.
- **Measure 46.** Search all suitcases, briefcases, and packages brought into the installation.
- **Measure 47.** Control access to all areas under the jurisdiction of the United States.
- **Measure 48.** Make frequent checks of the exterior of buildings and of parking areas.
- **Measure 49.** Minimize all administrative journeys and visits.
- **Measure 50.** Coordinate the possible closing of public and military roads and facilities with local authorities.
- **Measure 51.** To be determined.

E-4. DOD Shipboard Terrorist Force Protection Condition Procedures

The measures outlined below are for use aboard vessels and serve two purposes. First, the crew is alerted, additional watches are created, and there is greater security. Second, these measures display the ship's resolve to prepare for and counter the terrorist threat. These actions will convey to anyone observing the ship's activities that the ship is prepared, the ship is an undesirable target, and the terrorist(s) should look elsewhere for a vulnerable target.

a. Condition Alpha

This condition is declared when a general threat of possible terrorist activity is directed toward installations, vessels, and personnel, the nature and extent of which are unpredictable and where circumstances do not justify full implementation of condition BRAVO measures. However, it may be necessary to implement certain selected measures from Condition BRAVO as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

- **Measure 1.** Brief crew on the threat, ship security, and security precautions to be taken while ashore.

- **Measure 2.** Muster and brief security personnel on the threat and ROE.
- **Measure 3.** Review security plans and keep them available. Keep on call key personnel who may be needed to implement security measures.
- **Measure 4.** Consistent with local rules, regulations, and status-of-forces agreements (SOFAs), post qualified armed fantail sentry and forecastle sentry. Rifles are the preferred weapon.
- **Measure 5.** Consistent with local rules, regulations, and SOFAs, post qualified armed pier sentry and pier entrance sentry.
- **Measure 6.** Issue two-way radios to all sentries, roving patrols, quarterdeck watch, and response force. If practical, all guards will be equipped with at least two systems of communication (e.g., two-way radio, telephone, whistle, or signal light).
- **Measure 7.** Issue night vision devices to selected posted security personnel.
- **Measure 8.** Coordinate pier and fleet landing security with collocated forces and local authorities. Identify anticipated needs for mutual support (security personnel, boats, and equipment) and define methods of activation and communication.
- **Measure 9.** Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier and fleet landing area—no exceptions.
- **Measure 10.** Consistent with local rules, regulations, and SOFAs, establish unloading zone(s) on the pier away from the ship.
- **Measure 11.** Deploy barriers to keep vehicles away from the ship. Barriers may be ship’s vehicles, equipment, or items available locally.
- **Measure 12.** Post signs in local language(s) to explain visiting and loitering restrictions.
- **Measure 13.** Inspect all vehicles entering pier and check for unauthorized personnel, weapons, and/or explosives.
- **Measure 14.** Inspect all personnel, handcarried items, and packages before they come aboard. Where possible, screening should be at the pier entrance or foot of brow.
- **Measure 15.** Direct departing and arriving liberty boats to make a security tour around the ship and give special attention to the waterline and hull. Boats must be identifiable night and day to ship’s personnel.

- **Measure 16.** Water taxis, ferries, bum boats, and other harbor craft require special concern because they can serve as an ideal platform for terrorists. Unauthorized craft should be kept away from the ship; authorized craft should be carefully controlled, surveilled, and covered.
- **Measure 17.** Identify and inspect work boats.
- **Measure 18.** Secure spaces not in use.
- **Measure 19.** Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline.
- **Measure 20.** Rig hawsepipe covers and rat guards on all lines, cable, and hoses. Consider using an anchor collar.
- **Measure 21.** Raise accommodation ladders, stern gates, and jacob ladders when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.
- **Measure 22.** Conduct security drills to include bomb threat and repel boarders exercises.
- **Measure 23.** Review individual actions in condition BRAVO for possible implementation.
- **Measure 24.** To be determined.

b. Condition Bravo

This condition is declared when an increased and more predictable threat of terrorist activity exists. The measures in this condition must be capable of being maintained for weeks without causing undue hardships, without affecting operational capability, and without aggravating relations with local authorities.

- **Measure 25.** Maintain appropriate condition ALPHA measures.
- **Measure 26.** Review liberty policy in light of the threat and revise it as necessary to maintain the safety and security of the ship and crew.
- **Measure 27.** Conduct divisional quarters at foul weather parade to determine the status of on-board personnel and to disseminate information.
- **Measure 28.** Ensure that an up-to-date list of bilingual personnel for the operational area is readily available. Ensure that the warning tape in the pilot house and/or quarterdeck that warns small craft to remain clear is in both the local language and English.

- **Measure 29.** Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers; (b) be alert for abandoned parcels or suitcases; (c) be alert for unattended vehicles in the vicinity; (d) be wary of any unusual activities; and (e) notify the duty officer of anything suspicious.
- **Measure 30.** Remind personnel to lock their parked vehicles and to carefully check them before entering.
- **Measure 31.** Designate and brief picket boat crews. Prepare boats and place crews on 15-minute alert. If the situation warrants, make random picket boat patrols in the immediate vicinity of the ship with the motor whaleboat or gig. Boat crews will be armed with M-16 rifles, one M-60 with 200 rounds of ammunition, and 10 concussion grenades.
- **Measure 32.** Consistent with local rules, regulations, and SOFAs, establish armed brow watch on pier to check identification and inspect baggage before personnel board ship.
- **Measure 33.** Man signalbridge or pilothouse and ensure that flares are available to ward off approaching craft.
- **Measure 34.** After working hours, place armed sentries on a superstructure level from which they can best cover areas about the ship.
- **Measure 35.** Arm all members of the quarterdeck watch and the security alert team (SAT). In the absence of a SAT, arm two members of the self-defense force.
- **Measure 36.** Provide shotgun and ammunition to quarterdeck. If the situation warrants, place sentry with shotgun inside the superstructure at a site from which the quarterdeck can be covered.
- **Measure 37.** Issue arms to selected qualified officers to include command duty officer and assistant command duty officer.
- **Measure 38.** Arm sounding and security patrol.
- **Measure 39.** Muster and brief ammunition bearers or messengers.
- **Measure 40.** Implement procedures for expedient issue of firearms and ammunition from small arms locker. Ensure that a set of keys are readily available and in the possession of an officer designated for this duty by the commanding officer.
- **Measure 41.** Load additional small arms magazines to ensure adequate supply for security personnel and response forces.
- **Measure 42.** Inform local authorities of actions taken as the condition increases.

- **Measure 43.** Test communications with local authorities and other U.S. Navy ships in port.
- **Measure 44.** Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings, and floating debris.
- **Measure 45.** Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.
- **Measure 46.** Move cars and objects such as crates and trash containers 100 feet from the ship.
- **Measure 47.** Hoist boats aboard when not in use.
- **Measure 48.** Terminate all public visits.
- **Measure 49.** Set materiel condition YOKE, main deck and below.
- **Measure 50.** After working hours, reduce entry points to the ship's interior by securing selected entrances from the inside.
- **Measure 51.** Duty department heads ensure that all spaces not in regular use are secured and inspected periodically.
- **Measure 52.** If two brows are rigged, remove one of them.
- **Measure 53.** Maintain capability to get under way on short notice or as specified by SOPs. Consider possible relocation sites (such as a different pier or anchorage). Rig brow and accommodation ladder for immediate raising or removal.
- **Measure 54.** Ensure that .50-caliber mount assemblies are in place with ammunition in ready service lockers (.50-caliber machine guns will be maintained in the armory, pre-fire checks completed, and ready for use).
- **Measure 55.** Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultralight aircraft.
- **Measure 56.** Obstruct possible helicopter landing areas in such a manner as to prevent hostile helicopters from landing.
- **Measure 57.** Review riot and crowd control procedures, asylum-seeker procedures, and bomb threat procedures.
- **Measure 58.** Monitor local communications (e.g., ship-to-ship, TV, radio, police scanners).
- **Measure 59.** Implement additional security measures for high-risk personnel as appropriate.
- **Measure 60.** Review individual actions in condition CHARLIE for possible implementation.
- **Measures 61 and 62.** To be determined.

c. Condition Charlie

This condition is declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations, vessels, or personnel is imminent. Implementation of this condition for more than a short period will probably create hardship and will affect the peacetime activities of the ship and its personnel.

- **Measure 63.** Maintain appropriate measures for conditions ALPHA and BRAVO.
- **Measure 64.** Cancel liberty. Execute emergency recall.
- **Measure 65.** Be prepared to get under way on one (1) hour's notice or less. If conditions warrant, request permission to sortie.
- **Measure 66.** Muster and arm the SAT, backup alert force, and reserve force. Position the SAT and backup alert force at designated location(s). Deploy the reserve to protect command structure and augment posted security watches.
- **Measure 67.** Place armed sentries on a superstructure level from which they can best cover areas about the ship.
- **Measure 68.** Establish .50- or .30-caliber machine gun positions.
- **Measure 69.** If available, deploy STINGER surface-to-air missiles in accordance with established ROE.
- **Measure 70.** Energize radar and establish watch.
- **Measure 71.** Ships with high-power sonars operate actively for random periods to deter underwater activity. Man passive sonar capable of detecting boats, swimmers, or underwater vehicles. Position any non-sonar-equipped ships within the acoustic envelope of sonar-equipped ships.
- **Measure 72.** Man one or more repair lockers. Establish communications with an extra watch in damage control central.
- **Measure 73.** Deploy picket boat. Boats should be identifiable night and day from the ship (e.g., by lights or flags).
- **Measure 74.** If feasible, deploy helicopter as an observation or gun platform. The helicopter should be identifiable night and day from ship.
- **Measure 75.** Activate antiswimmer watch. (Portions of watch may already be implemented by previous condition measures).
- **Measure 76.** Issue weapons to selected officers and chief petty officers in the duty section (i.e., the commanding officer, executive officer, department heads).

- **Measure 77.** Issue concussion grenades to topside rovers, forecastle and fantail sentries, and bridge watch.
- **Measure 78.** Erect barriers and obstacles as required to control traffic flow.
- **Measure 79.** Strictly enforce entry control procedures and searches—no exceptions.
- **Measure 80.** Enforce boat exclusion zone.
- **Measure 81.** Minimize all off-ship administrative trips.
- **Measure 82.** Discontinue contract work.
- **Measure 83.** Set materiel condition ZEBRA, second deck and below.
- **Measure 84.** Secure from the inside all unguarded entry points to the interior of the ship.
- **Measure 85.** Rotate screws and cycle rudder(s) at frequent and irregular intervals.
- **Measure 86.** Rig additional fire hoses. Charge the fire hoses when manned just prior to actual use.
- **Measure 87.** Review individual actions in condition DELTA for implementation.
- **Measure 88.** To be determined.

d. Condition Delta

This condition is declared when a terrorist attack has occurred in the immediate area or intelligence has been received that indicates a terrorist action against a specific location or person is likely. Normally, this condition is declared as a localized warning.

- **Measure 89.** Maintain appropriate conditions ALPHA, BRAVO, and CHARLIE measures.
- **Measure 90.** Permit only necessary personnel topside.
- **Measure 91.** Prepare to get under way and, if possible, cancel port visit and depart.
- **Measure 92.** Post sentries with fully automatic weapons to cover possible helicopter landing areas.
- **Measure 93.** Arm selected personnel of the self-defense force.
- **Measure 94.** Deploy grenade launchers to cover approaches to ship.
- **Measure 95.** To be determined.

E-5. DOD Aviation Facility Terrorist Force Protection Condition Procedures

In addition to basic force protection condition procedures, a variety of other tasks may need to be performed at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

a. Conditions Alpha and Bravo

- Review conditions ALPHA and BRAVO measures.
- Update conditions ALPHA and BRAVO measures as required.
- Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.
- Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.
- Ensure that duty officers are always available by telephone.
- Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.
- Be prepared to receive and direct aircraft from other stations.
- Perform thorough and regular inspection of areas within the perimeters from which attacks on aircraft can be made.
- Take action to ensure that no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.
- Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area—no exceptions.
- Search all vehicles, briefcases, and packages entering the area.
- Erect barriers around potential targets if at all possible.
- Maintain firefighting equipment and conduct practice drills.
- Hold practice alerts within the perimeter.
- Conduct, with local police, regular inspections of the perimeter—especially the area adjacent to flight paths.
- Advise the local police of any areas outside the perimeter where attacks could be mounted and that cannot be avoided by aircraft on takeoff or landing.
- Advise aircrews to report any unusual activity near approach and overshoot areas.

b. Condition Charlie

- Review condition CHARLIE measures.
- Update condition CHARLIE measures as required.
- Brief all personnel on the increased threat.
- Inform local police of increased threat.
- Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.
- Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.
- Inspect all vehicles and buildings on a regular basis.
- Detail additional guards to be on call at short notice and consider augmenting firefighting details.
- Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.
- Reduce flying to essential operational flights only. Cease circuit flying if appropriate.
- Escort all visitors.
- Close relief landing grounds where appropriate.
- Check airfield diversion state.
- Be prepared to react to requests for assistance from outside the perimeter.
- Provide troops to assist local police in searching for terrorists on approaches outside the perimeter of military airfields.

c. Condition Delta

- Review condition DELTA measures.
- Update condition DELTA measures as required.
- Brief all personnel on the very high levels of threat.
- Inform local police of the increased threat.
- Cease all flying except for specifically authorized operational sorties.
- Implement, if necessary, appropriate flying countermeasures.
- Be prepared to accept aircraft diverted from other stations.
- Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.
- Close military roads allowing access to the airbase.

E-6. Marine Corps Rear Area Threat Levels

Table E-1 illustrates the levels of threats likely to be encountered in combat operations in the rear area and suggests probable responses from appropriate tactical forces. Local security forces (sometimes referred to as response forces) and internal security capabilities are used to counter level I and II threats. The Marine Corps component and MAGTF commander normally establish a tactical combat force to counter level III threats.

Threat Level	Possible Threat	Response Force
Level I	Agents, sympathizers, terrorists, and saboteurs.	Unit, base, and base cluster self-defense measures.
Level II	Small tactical units, unconventional forces, and guerillas.	Self-defense measures and local response force(s) with organic supporting arms.
Level III	Large tactical units (air, helicopterborne, amphibious).	Tactical combat force.

Table E-1. Threat levels and response forces.

This page intentionally left blank.

Appendix F

Glossary

Section I Acronyms

Note: Acronyms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military acronyms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.

AAW	antiair warfare
ACA	airspace coordination area
C2	command and control
C4I	command, control, communications, computers, and intelligence
CBIRF	Chemical, Biological Incident Response Force
CCIR	commander's critical information requirement
CI	counterintelligence
CI/HO	counterintelligence/human intelligence operation
COA	course of action
COG	center of gravity
CV	critical vulnerability
DIA	Defense Intelligence Agency
DOD	Department of Defense
EA	electronic attack
EEFI	essential elements of friendly information

EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
FAST	fleet antiterrorist security team
FSC	fire support coordinator
FSCM	fire support coordinating measure
HRP	high risk personnel
HUMINT	human intelligence
HQMC	Headquarters, Marine Corps
IA	information assurance
IO	information operations
IPB	intelligence preparation of the battlespace
LOC	line of communications
MAGTF	Marine air-ground task force
MCPP	Marine Corps Planning Process
MCSF	Marine Corps security force
MEF	Marine expeditionary force
METT-T	mission, terrain, terrain and weather, troops and support available—time available
MLC	Marine Corps logistics command
MOOTW	military operations other than war
MSG	Marine security guard
NBC	nuclear, biological, and chemical
NFA	no-fire area
OMFTS	operational maneuver from the sea
OAAW	offensive anti-air warfare
OPSEC	operations security
PSYOP	psychological operations
RFA	restrictive fire area
RFL	restrictive fire line

ROE	rules of engagement
ROZ	restricted operations zone
SAT	security alert team
SEAD	suppression of enemy air defenses
SOFA	status-of-forces agreement
SOP	standing operating procedures
TMD	theater missile defense
WMD	weapons of mass destruction

Section II Definitions

Note: Definitions of military terms change over time in response to new operational concepts, capabilities, doctrinal changes, and other similar developments. The following publications are the sole authoritative sources for official military definitions of military terms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.

A

active air defense—Direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets. It includes the use of aircraft, air defense weapons, electronic warfare, and other available weapons. (JP 1-02)

antiair warfare—A U.S. Navy/Marine Corps term used to indicate that action required to destroy or reduce to an acceptable level the enemy air and missile threat. It includes such measures as the use of interceptors, bombers, antiaircraft guns, surface-to-air and air-to-air missiles, electronic attack, and destruction of the air or missile threat both before and after it is launched. Other measures which are taken to minimize the effects of hostile air action are cover, concealment, dispersion, deception (including electronic), and mobility. Also called **AAW**. (MCWP 3-22)

antiterrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. Also called **AT**. (JP 1-02)

antiterrorism awareness—Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism. (JP 1-02)

artillery target intelligence zone—An area in enemy territory that the maneuver commander wants to monitor closely. Weapon locations in this zone will be reported immediately. Their priority is exceeded only by targets

in a critical friendly zone or a call-for-fire zone. Also called **ATIZ**. (MCWP 3-16.1)

C

call for fire zone—An area in enemy territory that the maneuver commander considers extremely important to neutralize fires from by immediate counterfire. Also called **CFFZ**. (MCWP 3-16.1)

sensor zone—An area in which the commander wishes to ignore all target detections. Also called **CZ**. (MCWP 3-16.1)

centers of gravity—Those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight. Also called **COGs**. (JP 1-02)

counterair—A mission that integrates offensive and defensive operations to attain and maintain a desired degree of air superiority. Counterair missions are designed to destroy or negate enemy aircraft and missiles, both before and after launch. (JP 1-02)

counterfire—Fire intended to destroy or neutralize enemy weapons. Includes counterbattery, counterbombardment, and countermortar fire. (JP 1-02)

countermining—Tactics and techniques used to detect, avoid, breach, and/or neutralize enemy mines and the use of available resources to deny the enemy the opportunity to employ mines. (JP 1-02)

counterreconnaissance—All measures taken to prevent hostile observation of a force, area, or place. (JP 1-02)

countersabotage—That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent sabotage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting sabotage activities. (JP 1-02)

counterterrorism—Offensive measures taken to prevent, deter, and respond to terrorism. (JP 1-02)

critical friendly zone—An area in which are located friendly units or units that the maneuver commander designates as critical. Also called **CFZ**. (MCWP 3-16.1)

critical node—An element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations. (JP 1-02)

D

defensive counterair—All defensive measures designed to detect, identify, intercept, and destroy or negate enemy forces attempting to attack or penetrate the friendly air environment. Also called **DCA**. (JP 1-02)

defensive information operations—The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (JP 1-02)

E

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. (JP 1-02)

F

force protection—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive

measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called **FP**. (JP 1-02)

foreign disaster—An act of nature (such as a flood, drought, fire, hurricane, earthquake, volcanic eruption, or epidemic), or an act of man (such as a riot, violence, civil strife, explosion, fire, or epidemic), which is or threatens to be of sufficient severity and magnitude to warrant United States foreign disaster relief to a foreign country, foreign persons, or to an international organization. (JP 1-02)

H

health threat—A composite of ongoing or potential enemy actions; environmental, occupational, and geographic and meteorological conditions; endemic diseases; and employment of nuclear, biological, and chemical weapons (to include weapons of mass destruction) that can reduce the effectiveness of joint forces through wounds, injuries, illness, and psychological stressors. (JP 1-02)

I

information assurance—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called **IA**. (JP 1-02)

information operations—Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO**. (JP 1-02)

information security—The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called **INFOSEC**. (JP 1-02)

O

offensive anti-air warfare—Those operations conducted against enemy air assets and air defense systems before they can be launched or assume an attacking role. Offensive anti-air warfare operations in or near the objective area consist mainly of air attacks to destroy or neutralize hostile aircraft, airfields, radars, air defense systems, and supporting areas. Also called **OAAW**. (MCRP 5-12C)

offensive counterair—Offensive operations to destroy, disrupt, or neutralize enemy aircraft, missiles, launch platforms, and their supporting structures and systems both before and after launch, but as close to their source as possible. Offensive counterair operations range throughout enemy territory and are generally conducted at the initiative of friendly forces. These operations include attack operations, fighter sweep, escort, and suppression of enemy air defenses. Also called **OCA**. (JP 1-02)

offensive counterair attack operations—Offensive action in support of the offensive counterair mission against surface targets that contribute to the enemy's air power capabilities. The objective of attack operations is to prevent the hostile use of aircraft and missile forces by attacking targets such as missile launch sites, airfields, naval vessels, command and control nodes, ammunition stockpiles, and supporting infrastructure. Attack operations may be performed by fixed- or rotary-wing aircraft, surface-to-surface weapons, special operations forces, or ground forces. Also called **OCA attack ops**. (JP 1-02)

offensive information operations—The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities and activities include but are not limited to operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could also include computer network attack. (JP 1-02)

operations security—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced

together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called **OPSEC**. (JP 1-02)

P

passive air defense—All measures, other than active air defense, taken to minimize the effectiveness of hostile air and missile threats against friendly forces and assets. These measures include camouflage, concealment, deception, dispersion, reconstitution, redundancy, detection and warning systems, and the use of protective construction. (JP 1-02)

physical security—That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02)

psychological operations—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called **PSYOP**. (JP 1-02)

R

rear area—For any particular command, the area extending forward from its rear boundary to the rear of the area assigned to the next lower level of command. This area is provided primarily for the performance of support functions. (JP 1-02)

risk assessment—The identification and assessment of hazards (first two steps of risk management process). (JP 1-02)

risk management—The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. Also called **RM**. (JP 1-02)

rules of engagement—Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/ or continue combat engagement with other forces encountered. Also called **ROE**. (JP 1-02)

V

vulnerability assessment—A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. (JP 1-02)

W

weapons of mass destruction—Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called **WMD**. (JP 1-02)

Appendix G

References

CJCSM 3122.03. Joint Operations Planning and Execution System Volume II Planning Formats and Guidance

Joint Pub 2-0, *Doctrine for Intelligence Support to Joint Operations*

Joint Pub 2-01.3, *Joint Tactics, Techniques, and Procedures for Intelligence Preparation of the Battlespace*

Joint Pub 3-0, *Doctrine for Joint Operations*

Joint Pub 3-01.5, *Doctrine for Joint Theater Missile Defense*

Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*

Joint Pub 3-07.6, *Joint Tactics, Techniques, and Procedures for Foreign Humanitarian Assistance*

Joint Pub 3-08, *Interagency Coordination During Joint Operations*

Joint Pub 3-10, *Joint Doctrine for Rear Area Operations*

Joint Pub 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense*

Joint Pub 3-11, *Joint Doctrine for Base Defense*

Joint Pub 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical Environments*

Joint Pub 3-13, *Joint Doctrine for Information Operations*

Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare*

Joint Pub 3-53, *Joint Doctrine for Psychological Operations*

Joint Pub 3-54, *Joint Doctrine for Operations Security*

Joint Pub 3-58, *Joint Doctrine for Military Deception*

Joint Pub 4-02, *Doctrine for Health Support in Joint Operations*

Joint Pub 5-0, *Doctrine for Planning Joint Operations*

Joint Pub 5-00.2, *Joint Task Force Planning Guidance and Procedures*

MCO 3500.27, *Operational Risk Management*

ALMAR 210/97 *Operational Risk Management*

MCDP 1-0, *Marine Corps Operations*

MCWP 0-1.1, *Componency*

MCWP 2-1, *Intelligence Operations*

MCWP 2-14, *Counterintelligence*

MCWP 3-16, *Fire Support Coordination in the Ground Combat Element*

MCWP 3-17, *Engineer Operations*

MCWP 3-22, *Antiair Warfare*

MCWP 3-37, *MAGTF Nuclear, Biological, and Chemical Operations*

MCWP 3-40.2, *MAGTF Information Management*

MCWP 3-40.4, *Information Operations*

MCWP 4-1, *Logistics Operations*

MCWP 4-11.1, *Health Service Support Operations*

MCWP 5-1, *Marine Corps Planning Process*

MCRP 5-12.1C, *Risk Management*

FM 34-2-1, *Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance*

This page intentionally left blank.