WWW.SURVIVALEBOOKS.COM

FM 90-12
FMFRP 2-73
TACP 50-50
PACAFP 50-50
USAFEP 50-50
AACP 50-50
2 OCTOBER 1989

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

WILLIAM J. MEEHAN II
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-11 E, requirements for FM 90-12, Joint Base Defense (Qty rqr block no. 4377); FM 90-14, Rear Battle (Qty rqr block no. 1235); FM 100-16, Support Operations: Echelons Above Corps (Qty rqr block no. 1241); FM 3-3, NBC Contamination Avoidance (Qty rqr block no. 3829); FM 100-20, Low Intensity Conflict (Qty rqr block no. 513).

WWW.SURVIVALEBOOKS.COM

CONTENTS

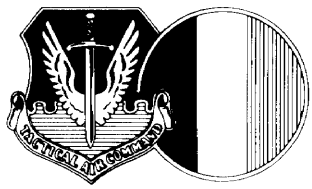
CHAPTER 1.	**OPERATIONAL CONCEPTS**	1-1
	Types of Conflict	1-1
	Levels of Threat	1-2
	The Fundamentals of Base Defense	1-3
CHAPTER 2.	**ANALYSIS AND PLANNING**	2-0
	Analysis	2-0
	Planning	2-3
CHAPTER 3.	**COMMAND AND CONTROL**	3-1
	Section I Responsibilities	3-1
	Theater Command	3-1
	Area Command	3-4
	Joint Base Command	3-4
	Section II Legal Constraints	3-8
	International Agreements	3-8
	United States Laws	3-8
	Host-Nation Laws	3-9
	Laws of War	3-9
	Rules of Engagement	3-9
CHAPTER 4.	**INTELLIGENCE AND COMMUNICATIONS**	4-0
	Section I Intelligence	4-0
	Responsibilities	4-0
	Support	4-1
	Operations	4-1
	Section II Communications	4-2
	Planning and Construction Considerations	4-3
	Capabilities	4-4
CHAPTER 5.	**HOST-NATION SUPPORT**	5-1
	Planning Factors	5-1
	Facilities and Systems	5-1
	Supplies, Services, and Equipment	5-2
	Command and Control	5-2
	NBC Defense	5-2
	Training	5-2
	Intelligence	5-2
	Civil Affairs	5-3
	Public Affairs	5-3

WWW.SURVIVALEBOOKS.COM

APPENDIX A.	**SAMPLE BASE DEFENSE PLAN**	A-1
APPENDIX B.	**SECURITY**	B-0
	Section I Tactical Security	B-0
	Patrols	B-0
	Roadblocks	B-1
	Urban Defense	B-1
	Convoy Defense	B-2
	Searches	B-2
	Ambushes	B-3
	Response to Attacks	B-4
	Crowd Control	B-4
	Section II Unit Security	B-5
	Predeployment	B-5
	Deployment	B-7
	Redeployment	B-8
	Section III Operations Security	B-8
	Objectives	B-9
	Measures	B-9
	Intelligence Indicators	B-9
APPENDIX C.	**SPECIALIZED EQUIPMENT AND MATERIEL**	C-1
APPENDIX D.	**TERRORISM**	D-1
	Unit Vulnerability	D-1
	Threat Conditions and Responses	D-2
	Base Terrorism Response	D-6
GLOSSARY		Glossary-1
	Acronyms and Abbreviations	Glossary-1
	Terms	Glossary-3
REFERENCES		References-1
	Army Publications	References-1
	Marine Corps Publications	References-1
	Navy Publications	References-1
	Air Force Publications	References-2
	Joint and Multi-Service Publications	References-2
INDEX		Index-1

WWW.SURVIVALEBOOKS.COM

FM 90- 12/FMFRP 2-73/TACP 50-50/PACAFP 50-50/USAFEP 50-50/AACP 50-50





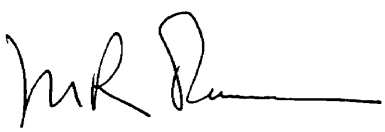




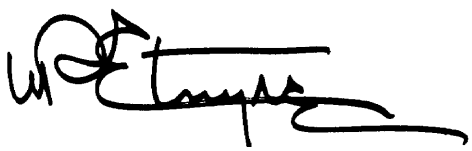


FOREWORD

This publication may be used by the Army, Marine Corps, and Tactical Air Forces during training, exercises, and contingency operations.



M.R. THURMAN
General, USA
Commanding
Training and Doctrine Command



W. R. ETNYRE
Lieutenant General, USMC
Commanding General
Marine Corps Combat Development Command



ROBERT D. RUSS
General, USAF
Commander
Tactical Air Command

WWW.SURVIVALEBOOKS.COM

TACTICAL AIR FORCES AUTHORIZATION

The procedures contained in this publication are authorized for use throughout the Tactical Air Forces as indicated below. For overseas theaters, the procedures set forth in this publication are applicable only in US unilateral operations. Forcombineci operations, applicable multinational procedures apply.

The Air Force distribution symbol for TAC is "X" (stocked and issued by TAC/DAPD); PACAF, USAFE, and AAC distribution is "X." Additional copies or new requirements should be requested through TAC/XPJA. Reprints are not authorized. Send requests to TAC/DAPD, Langley Air Force Base, VA 23665-5583.

US Air Forces Europe



GERALD N. GUNTER
Colonel, USAF
Director of Administration

MICHAEL J. DUGAN
General, USAF
Commander in Chief

Pacfic Air Forces



DAVID N. THOMPSON
Colonel, USAF
Director of Administration

MERRILL A. McPEAK
General, USAF
Commander in Chief

Alaskan Air Command

OFFICIAL

HUGH M. McAWEENEY, JR.
Major, USAF
Director of Administration

THOMAS G. McINERNEY
Lieutenant General, USAF
Commander

ARMY DISTRIBUTION RESTRICTION AND DESTRUCTION NOTICE

ARMY DISTRIBUTION RESTRICTION: Distribution authorized to DOD components only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 21 January 1988. Other requests for this document will be referred to HQ TRADOC, A_fTN: ATDO-J, Fort Monroe, VA 23651-5000 or HQ TAC, AITN: XPJ, Langley Air Force Base, VA 23665-5001.

ARMY DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

WWW.SURVIVALEBOOKS.COM

Army, Marine Corps, Tactical Air Forces

FM 90-12/FMFRP 2-73/TACP 50-50/PACAFP 50-50/USAFEP 50-50/AACP 50-50

Base Defense

Multi-Service Procedures for Defense of a Joint Base

EXECUTIVE SUMMARY

This publication provides doctrinal guidelines commanders and staffs may use to establish the defense and security of joint bases. The joint base defense coordination requirements and basic principles described herein should remain relatively constant, although variations in size and type of US forces, host-nation agreements, and unique command relationships may require modification of selected procedures.

OPERATIONAL CONCEPTS

Joint bases could be setup almost anywhere in the world to support a wide variety of missions and national objectives. The threats to such bases can range from terrorism to large conventional forces. For purposes of defense planning, these threats are divided into three levels. A thorough knowledge of types of conflict and levels of threat are fundamental to base defense.

ANALYSIS AND PLANNING

Base defense includes all active and passive measures that commanders can take to secure their facilities, equipment, and personnel. They must analyze, organize, and plan their defenses using the same tenets of any successful military operation. They must use the terrain effectively, position facilities and equipment advantageously, create an effectual in-depth defense, and provide defense forces with clear areas of responsibility. They must assess such concerns as enemy avenues of approach, fields of fire, entrance control, and fire support.

COMMAND AND CONTROL

Commanders and staffs must understand the command relationships for base defense precisely. They must organize their available forces in the most effective manner possible for defense. They must outline and transmit defense missions and responsibilities for all elements assigned to or transiting the base. Because of the special threat that terrorism poses, commanders must make it a particular concern. From commanders on down, personnel should be familiar with the legal aspects of base defense deriving from international laws, US laws, and host-nation laws, as well as from treaties and agreements.

INTELLIGENCE AND COMMUNICATIONS

Success in countering the threat depends on the ability of intelligence activities to collect, analyze, produce, and disseminate user-specific threat information as quickly as possible. Commanders of bases must use all

WWW.SURVIVALEBOOKS.COM

available assets to develop viable intelligence programs for defense. They must develop reliable and redundant communications systems flexible enough to support the overall security scheme.

HOST-NATION SUPPORT

Integrating US base defense assets and HNS is vital to a successful base defense. HNS will help relieve US assets for other missions and complement the overall base security program. Planning for HNS must occur within the framework of established nation-to-nation agreements; however, HNS must still function as an effective component of a sound defense.

WWW.SURVIVALEBOOKS.COM

FM 90-12	**US Army Training and Doctrine Command Fort Monroe, Virginia**
FMFRP 2-73	**US Marine Corps Combat Development Command Quantico, Virginia**
TACP 50-50	**Tactical Air Command Langley Air Force Base, Virginia**
PACAFP 50-50	**Pacific Air Forces Hickam Air Force Base, Hawaii**
USAFEP 50-50	**US Air Forces Europe Ramstein Air Base, Germany**
AACP 50-50	**Alaskan Air Command Elmendorf Air Force Base, Alaska**

2 October 1989

Base Defense

Multi-Service Procedures for Defense of a Joint Base

PREFACE

PURPOSE

This publication provides operating procedures and security precautions for the defense of joint bases outside the continental United States (OCONUS).

SCOPE

This publication describes the actions required to defend joint bases in an area of operations and contains information that will assist staff officers and subordinate commanders in carrying out their commanders' guidance.

APPLICABILITY

This publication is for use by tactical operating forces of the Army, Air Force, Navy, and Marine Corps. Although the Navy is not signatory to this document, naval information has been coordinated with Headquarters, Atlantic Fleet. Generic in nature, it provides multi-service command coordinated and approved information. It can serve either as a source document for developing multi-service and service manuals, publications, and curricula or as a stand-alone document. It has been developed for four-service planning and war-fighting personnel at all echelons. Although it addresses host-nation support (HNS), it is a US unilateral-only document, and it may have to be modified for use in combined operations.

IMPLEMENTATION PLAN

The offices of primary responsibility (OPRs) of participating major commands will review this publication for multi-service procedural information. Once they validate the information, OPRs should reference and incorporate it in the following manner:

WWW.SURVIVALEBOOKS.COM

Army

The doctrine and procedures contained in this document will be incorporated in US Army doctrinal and training publications as directed by the Commander of the Training and Doctrine Command.

Marine Corps

The doctrine and procedures contained in this document will be incorporated in US Marine Corps doctrinal and training publications as directed by the Commandant of the Marine Corps (OPR: MAGTF, Warfighting Center).

Tactical Air Command

TAC will incorporate procedures according to AFR 5-8 and HQTAC OI5-1 (OPR: TAC/XPJ). USAFE, PACAF, and AAC will validate and incorporate appropriate procedures in accordance with applicable MAJCOM and other governing directives.

USER INFORMATION

The TAC-TRADOC Air Land Forces Application (ALFA) Agency developed this publication with the joint participation of the approving service commands. ALFA will review and update this publication as necessary. We encourage you to recommend changes for improving this publication. Key your comments to the specific page and paragraph, and provide a rationale for each recommendation. Send changes or comments to—

Army:	HQ TRADOC ATTN: ATDO-J Fort Monroe, VA 23651-5000
Marine Corps:	HQ MCCDC ATTN: WF12E Quantico, VA 22134-5001
Air Force:	HQ TAC ATTN: XPJ Langley AFB, VA 23665-5576

Unless this publication states otherwise, masculine pronouns do not refer exclusively to men.

WWW.SURVIVALEBOOKS.COM

CHAPTER 1

OPERATIONAL CONCEPTS

A joint base could be established in support of treaties and agreements between the US and a friendly country or in support of a military mission. US bases present lucrative targets because friendly forces and equipment performing mission-essential functions concentrate there. To disrupt such operations, the enemy will devote a high degree of effort, ranging from conventional military attacks to random terrorism. Joint base defense prevents degradation of base functions by detecting, engaging, and destroying enemy forces before they can succeed in accomplishing their mission. In most parts of the world this objective will be met not only by joint operations but also by combined operations that depend heavily on host-nation support (HNS) assets and coordination. Due to the unique environment of low-intensity conflict (LIC) and the special challenges it represents, considerations peculiar to LIC are highlighted throughout. For purposes of base defense operations, significant definitions are shown in Figure 1-1.

Joint Base.
A *joint base* is a locality from which operations of two or more of the armed forces of the Department of Defense are projected or supported and which is manned by significant elements of two or more services or in which significant elements of two or more services are located. (JCS Pub 1-02)

Base Defense.
Base defense includes those local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base to ensure that the maximum capacity of its facilities is available to US forces. (JCS Pub 1-02)

Figure 1-1. Significant Definitions

TYPES OF CONFLICT

An in-depth understanding of the threat to the joint base is vital in the overall development of a defensive plan. Therefore, both military and civilian intelligence and security forces must coordinate closely when planning the base defense and when they carry it out.

Mid- and High-Intensity Conflicts

During full-scale war, nations will use conventional forces to seek a satisfactory conclusion of hostilities. Forces will conduct large-scale operations. Joint bases that support US operations will likely be prime targets for attack. During mid- and high-intensity conflicts, bases could be subjected to large-scale air attacks; nuclear, biological, chemical (NBC) attacks; or major ground attacks. Such attacks intend to disrupt base operations, discredit US forces, and display enemy prowess. The enemy may also try to sway US public opinion against the conflict by inflicting heavy losses on US personnel and equipment.

DEEP OPERATIONS

Soviet doctrine stresses the concept of deep operations. So do many Warsaw Pact nations whose leaders are trained in Soviet doctrine, whose equipment follows Soviet design, and whose forces are generally configured after the Soviet model. Soviet doctrine stresses a

WWW.SURVIVALEBOOKS.COM

combination of massed fires on key objectives and rapid concentration of maneuver forces to seize the offense after opening a breach in order to conduct high-speed, deep attacks into the opponent's rear area. These operations are executed in close coordination with airborne, heliborne, and amphibious assault landings, tactical missile employment, and high-speed, deep ground penetrations. These operations may use conventional and nuclear arms, chemical fires, and deep recon. The purpose of such operations is to disrupt our rear area, reducing our efficiency and ability to support close and deep operations.

RECON AND SABOTAGE

Special purpose forces, such as Soviet *spetsnaz* or North Korean commando-rangers, are specifically trained for recon and sabotage. They may secretly try to enter and disrupt a joint base. They may also activate sleeper agents and cell networks to develop and control partisan operations in the rear area.

Low-Intensity Conflicts

Low-intensity conflicts (LICs) are political-military confrontations between contending states or groups below conventional war and above the routine, peaceful competition among states. They frequently involve protracted struggles of competing principles and ideologies. LICs range from subversion to the use of armed forces. They are waged by a combination of means employing political, economic, informational, and military instruments. LICs are often localized, generally in the third world, but contain regional and global security implications.[1]

LIC involves the actual or contemplated use of military capabilities up to, but not including, sustained combat between regular forces. The factors which lead to LIC are complex. Often, short-term actions cannot resolve them. Success in a LIC environment depends upon applying all elements of national power effectively and defining goals and objectives clearly. Political objectives establish the limits and constraints for military operations and for social, political, and economic programs.

LIC is not a new form of aggression. Throughout history, groups have sought to achieve their goals through various limited actions: embargoes, blockades, demonstrations of military capabilities, incitement of and support for insurgents, harassment at borders, incursions, and intimidation. Conflict remains at the LIC level when at least one of the belligerents has limited resources or when both want to avoid either the greater cost or greater risk involved in a more intense effort, LICs may arise as an integral part of East-West worldwide rivalry or may develop independently of US-USSR competition.

In LIC, US military forces may have four general kinds of missions: peacekeeping operations, combating terrorism, peacetime contingency operations, and insurgency-counterinsurgency (see Glossary). Forces may have to conduct several of these missions at the same time and in the same area of operations (AO).

During several LICs, US resolve has been highlighted in all parts of the world. For future LICs, the US will probably use a joint force incorporating elements from all the services. To support such a force, the US may need to establish a base from which to conduct operations.

The US could establish a joint base in a passive or potentially hostile HN. In such a case, the political environment in the US, HN, and the world could generate low-intensity conflicts that would adversely affect joint base defense operations. Restrictions and constraints on our ability to reinforce, buildup, or enhance security at a joint base could result. Therefore, the entire chain of command, including State Department representatives, constantly needs to know about any possible situations which may adversely affect our ability to safeguard US personnel and equipment.

LEVELS OF THREAT

Defense is normally an incremental response to perceived threats. As the threat increases, so does the level of defense. Defenders hope that threat increases will occur well ahead of an actual attack. Dividing enemy actions into three levels serves to guide base defense planning. All three levels that could confront a joint base are discussed below.

Level I

Level I threats are those which can be defeated by base or base cluster self-defense measures.

Level II

Level II threats are those which are beyond base or base cluster self-defense capabilities but which can be defeated by response forces, normally military police with supporting fires.

[1] *DOD Dictionary of Military and Associated Terms,* JCS Pub 1-02.

WWW.SURVIVALEBOOKS.COM

Level III

Level III threats are those which necessitate the command decision to commit a combined arms tactical combat force (TCF) to defeat the threat.

THE FUNDAMENTALS OF BASE DEFENSE

Understand the Enemy

Defenders must be thoroughly familiar with the capabilities and limitations of enemy weapons and equipment. They should know enemy force organization, deployment, and tactics. Ultimately, the US commander must determine the intent of enemy activity.

See the Battlefield

Prior to the battle, defending commanders must organize to defeat any type of attack from all possible directions. During the intelligence-preparation-of-the-battlefield (IPB) process, commanders acquire knowledge of the enemy and terrain. Using this knowledge, they predict threat operations. They must then conduct operations to learn enemy location, organization, direction of movement, and strength. Commanders must have a continuous flow of information on which to base decisions. They must also have effective operations security (OPSEC) to deny similar friendly information to the enemy (see Appendix B, Section III).

Use the Defenders' Advantages

Defenders' advantages are numerous and could permit a numerically inferior force to defeat a much larger one. Defenders must become totally familiar with the terrain before battle. If possible, they must prepare the ground in advance by building obstacles, firing positions, and routes between positions. Defenders can—

- Fight from cover.
- Fire from stationary platforms or positions.
- Shift forces among prepared positions.
- Plan communications, control measures, fires, and logistical support to fit any predictable situation.

Defenders must force attackers to canalize their forces and minimize their chances to maneuver. Attackers must be forced to adhere to their initial plans or risk annihilation. Attackers may also have to alter plans as the situation develops and risk an uncoordinated effort. Defenders can also camouflage their positions and use deceptive measures.

Concentrate at Critical Times and Places

Commanders who understand the enemy see the situation and the developing battle better than the enemy and use the defenders' advantages to shift forces quickly. Commanders must concentrate forces at critical points so that locally engaged forces can generate combat power to defeat enemy attacks. Locally engaged forces must then shift to other positions to concentrate combat power against other threats during the battle.

Coordinate Available Defense Assets

Indirect fire systems, air defense artillery, tactical aircraft, engineers, dismounted troops, armored vehicles, and helicopters can each make a vital contribution to overall base security. But none by itself is the answer to a successful base defense. They must combine with one another in order to maximize their strengths and minimize their vulnerabilities.

Balance Base Security with Political Constraints

In LIC, base security measures must balance with political constraints. This fundamental can be the most frustrating but the most critical in joint base defense during a LIC. Base security will have to be designed around numerous political constraints and often under the scrutiny of the press. For example, constraints could involve restrictions on defensive construction, limitations on the number of security personnel, or stringent rules of engagement (ROE). Coordination between US State Department officials and the staff of the area commander in chief (CINC) will be essential to ensure that base defense is within US strategic objective guidelines. Finally, the presence of friendly civilians in the area requires commanders to use minimum force against the enemy. Unintentional harm to local civilians could enhance support for the enemy and adversely affect the success of military operations.

Know the Law and Rules of Engagement

US commanders an senior advisors and their subordinates must be familiar with the legal basis for their presence in a foreign country in order to assist its government and armed forces. US personnel should understand the basics of international and domestic law that authorize base defense operations and the restrictions the law imposes upon personnel (see Chapter 3). Further, the theater CINC will develop clearly stated, specific ROE for all US forces.

WWW.SURVIVALEBOOKS.COM

CHAPTER 2

ANALYSIS AND PLANNING

Commanders at all levels must continuously monitor local threat indicators and essential elements of enemy information. They must ensure that their intelligence officers develop realistic priority intelligence requirements (PIRs) (see Chapter 4). Timely receipt and proper analysis of such information enable commanders to tailor their active defense plans while maintaining their primary missions. Local commanders must set up both active and passive plans to defend bases against conventional operations and various LIC threats.[2]

ANALYSIS

After carefully reviewing the threat against the base, commanders and leaders at all levels must organize their defenses using active and passive measures, such as—

- Establishing guard posts in the immediate vicinity of vital areas.
- Deploying forward patrols to prevent insurgents from closing vital areas.

This defense should be based on mission, enemy, terrain, troops, and time available (METT-T).

Mission

The unit mission statement should specify—

- **Who** will defend.
- **Where** the unit will defend.
- **When** it will be prepared to defend.
- **Why** it will defend.
- **What** it will defend.

The unit mission or other missions on base may seem more important to US efforts than the base defense mission. However, base defense is fundamental to the success of missions that support the overall operation. Therefore, commanders must stress the importance of base defense to all personnel and ensure their direct involvement.

The five essential actions of the base defense mission are—

- Detect. An enemy attempt must be detected in its earliest stages.
- Warn. The detected attempt must result in an alarm. The base must be warned that an attack is imminent or under way, and all US forces must report to their assigned base defense positions.
- Deny. Allowing the enemy to damage its target jeopardizes the defense mission. The defenders must minimize the damage and deny the enemy's attempt at the target.
- Destroy. To prevent future attempts by the same force, defenders must destroy the enemy before it can withdraw. In LIC, the enemy may be hard to identify and may blend into the population. Thus, collateral civilian casualties are possible in LIC and could adversely affect the overall success of military operations. Defenders must take great care to identify the enemy and to point combat efforts directly at it.
- Delay. If the initial defenders cannot deny or destroy the enemy alone, they must delay it until adequate combat power arrives.

Enemy

Commanders consider how their defenses will—

- Identify and counter the location, direction, size, and method of attack.

  Anticipate enemy ground and aerial avenues of approach.
- Counter the effects of enemy firepower, mobility, and electronic warfare (EW).
- Negate the enemy's strengths such as speed of attack and numerical superiority.
- Exploit the enemy's weaknesses such as command and control difficulties and rigid scheme of maneuver.

[2] This chapter describes an ideal security posture. Political and military situations may dictate more austere and restricted measures. Use this chapter as the basis for a viable security plan. See also the sample base defense plan in Appendix A and the additional unit tactical security precautions in Appendix B.

WWW.SURVIVALEBOOKS.COM

Terrain

The US could establish a base almost anywhere, from an existing HN airfield or port to a jungle clearing. The choice of terrain may be more significant than subsequent improvements or decisions.

When selecting a base location, commanders should consider elevation. Occupying or controlling high ground is especially important to deny an enemy direct observation or fire into the base. Commanders should also consider the economic, political, and psychological impact on the local area as well as on the HN in general. HN agreements and considerations may restrict base construction and security enhancements. Before site selection and construction, defenders should conduct an extensive IPB analysis. Such an analysis will prevent construction in major threat areas and place the base in defensible, trafficable terrain. A list of specialized base defense equipment and materiel is at Appendix C.

Terrain forms the natural structure of the battlefield. Joint base defense force commanders must recognize terrain limitations and possibilities, using them to protect base operations and to put the enemy at a disadvantage. To do so, they and commanders at all levels must personally examine the terrain, starting with map recon, reinforced by terrain walks and, if possible, aerial surveys. Commanders analyzing terrain must consider all military aspects, including observation and fields of fire, cover and concealment, obstacles and movement, key terrain, and avenues of approach (OCOKA).

OBSERVATION AND FIELDS OF FIRE

Contour and vegetation affect observation and fire. Our direct-fire weapons are less effective, and the enemy can move with less risk where visibility is limited by—

- Large forests.
- Jungles.
- Built-up areas.
- Tracts of broken ground.

Commanders increase the defensive posture of their bases by having vegetation cleared, by properly siting observation posts and direct-fire weapons, and by compensating with indirect fire and aerial observation. For example, hilltops and the tops of buildings make excellent observation posts or radar sites but are rarely satisfactory positions for direct-fire weapons. Tanks, direct-fire missiles, and machine guns must be sited where they have the best fields of fire and their effects are greatest. Indirect fire can cover areas not directly observable. Remote sensors can detect enemy movement and cue artillery. Aircraft can provide overwatch from flanking positions in woods and valleys inaccessible to ground troops.

COVER AND CONCEALMENT

Cover is protection from observation and fire. Whether maneuvering on the ground or in the air, forces should seek the best protection of covering terrain. Slopes, folds, and depressions can protect a unit from observation and fire or hide forces, serving to preserve the strength of the force. Covered positions are as important to command posts, indirect fire units, reserves, combat support (CS) units, and combat service support (CSS) units as they are to close combat units. Dispersing units among multiple covered positions can provide considerable cover.

Concealment is protection from observation. Urbanized terrain, broken hills, high ground, and forests can be used to hide forces, but terrain alone cannot conceal a force or facility in operations against sophisticated forces. To conceal units and headquarters, commanders must also—

- Limit electronic and thermal emissions.
- Use camouflage to conceal personnel and equipment.
- Use covert relocation to help prevent the detection of hidden units.

Even in fluid conditions, forces will be able to find concealment for short periods. Concealing a force can be a great tactical advantage. Defenders can use concealment to draw the enemy deep into prepared defensive areas. Attackers can use it to avoid being detected or engaged as they approach defended positions. Deceptive measures such as decoys or simulated forces also give a significant tactical advantage.

OBSTACLES AND MOVEMENT

Few areas are truly impassable. Thus, commanders should protect difficult approaches into their positions against surprise enemy attacks. Roads, ridgelines, river valleys, and plains are high-speed approaches on which fluid battles may develop rapidly. Combat elements move slowly on soft sand and through swamps, thick forests, and broken or mountainous terrain traversable only through defiles or by dismounted forces. Urban areas also can constitute formidable obstacles.

WWW.SURVIVALEBOOKS.COM

Season and weather can affect trafficability. Snow and ice on hills can slow a mounted movement considerably. Thaws or rains can quickly change plains to quagmires. Fog and snow not only adversely affect trafficability but can be excellent concealment for a terrorist attack.

Normally, an AO will contain a mixture of obstructing terrain and avenues suitable for air assault, mounted movement, or dismounted movement. Terrain that canalizes movement allows defenders to economize in difficult ground and to concentrate on the dangerous approaches. If the terrain is open, the attacker will be able to choose among many different approaches, and defenders may have to fight a mobile battle in-depth.

Natural or man-made obstacles parallel to the direction of movement can protect the flanks of attacking or counterattacking forces. Obstacles across an avenue of approach form lines of resistance for the defenders. Rail lines, small streams, and villages along roads do not significantly impede dismounted forces but can significantly slow mounted ones. Adequately guarded forests and marshes are difficult for unassisted armored forces to penetrate, but dismounted infantry can traverse them and air assault forces can envelope them.

The best approaches are often those which appear unlikely. Forces can often gain access to a high-speed ridge approach by crossing difficult terrain immediately to its front. Old roadbeds also offer good movement potential because they follow solid ground and are usually not as well defended as improved routes.

KEY TERRAIN

Key terrain is any feature, locality, or area that affords a marked advantage to the controlling force. Since such an advantage is situational, the commander designates key terrain only after analyzing the mission. The commander may designate certain key terrain as decisive terrain if the mission depends on retaining it. The commander designates decisive terrain in the concept of operation to communicate its importance to the staff and subordinate commanders. Many areas will not have decisive terrain.

AVENUES OF APPROACH

Defenders must determine the main approaches to the base that attackers might use, as well as internal avenues that permit maneuver against attackers. Defenders must evaluate avenues of approach in terms of—

- Speed of movement along their entire length.
- Potential to accommodate enemy forces of a specified number and type.
- Access to important areas and adjacent avenues.
- Degree of canalization.
- Cover and concealment.
- Effect on line-of-sight communications.
- Obstacles.

Defenders must also consider likely drop zones (DZs) and landing zones (LZs) for threat airborne or heliborne insertions.

Troops

DEFENDING AGAINST LEVEL I THREATS

Each base must defend itself against low-level threats. Base defense forces should be organized, trained, and equipped to defeat Level I threats. They must also maintain a limited capability to detect, delay, and disrupt Level II and III forces until friendly response or tactical combat forces (TCFs) arrive.

Many rear-area personnel do not have the training or resources to conduct sustained defensive operations against threat Levels II and III. Conducting such operations could disrupt vital support functions and, in effect, permit threat forces to accomplish their goals. However, bases must provide their own self-defense until friendly response forces arrive.

Defeating enemy incursions in rear areas could be a US command responsibility, or HN agreements may place primary responsibility upon the HN. Such agreements, however, do not negate or lessen the responsibilities of US commanders to defend their bases against Level I threats and to respond to Level II and III threats.

DEFENDING AGAINST LEVEL II AND III THREATS

Designated area response forces will be called upon to defeat Level II threats directed against bases. These response forces could be military police or combat forces located in the area. A TCF is required to defeat a Level III force whose capabilities exceed organic base defense forces or area security assets. As a combined arms organization assigned to fight a specific threat, a

WWW.SURVIVALEBOOKS.COM

TCF may contain its own organic artillery or attack helicopters. The appropriate echelon commander task-organizes the TCF through operational channels.

The TCF commander is assigned an AO and normally assumes operational control (OPCON) of all external base defense forces in the AO until the threat is neutralized. The commander of the base may need to retain control of sufficient assets to maintain security of critical resources. Such needs will be closely coordinated with the area security force, the commander of the base and TCF commanders. Once the threat is neutralized, control of external base defense forces will revert to the established command channels.

EVALUATING THE DEFENSE

Commanders of bases must evaluate how the defense will—

- Use organic and HN or other US service-supporting indirect fires to maximum advantage.
- Use organic and supporting direct-fire weapons to maximum advantage.
- Provide for its own low-altitude air defense.
- Be affected by the mobility of its own combat and CS elements.
- Use supporting engineers in countermobility and survivability roles.
- Use a reserve, considering its location, type of force, and size.
- Employ counterattacks.
- Be affected by soldiers' training, discipline, physical condition, and morale.
- Be affected by the state of maintenance and the effectiveness of logistics to sustain combat operations.
- Request additional assets.
- Avoid, detect, protect, and recover from enemy use of chemical or biological weapons.

Time Available

Commanders of bases consider how the time available will affect—

- Planning (recon, coordination, task organizing, planning of fires, issuance of orders down to squad level).
- Preparation (movement to positions, occupation and preparation of positions, coordination between units, logistics support).

For specific LIC security precautions during the predeployment, deployment, and redeployment phases of an operation, see Appendix B, Section II. For estimating base vulnerability to terrorist attacks, see Appendix D.

PLANNING

After considering the factors of METT-T, joint base defense force commanders develop a defense plan that they and leaders at all levels should use in organizing a defense.

Employing Forces in Base Defense Areas

Successful defense of a base depends on an aggressive, all-around, in-depth defense. The base defense operations center (BDOC) normally plans such a defense. (For specific details on BDOC responsibilities, see Chapter 3.) To provide an in-depth defense, commanders of bases establish defense forces within a series of defensive rings: the screening force area (SFA), the main defense area (MDA), and the close defense area (CDA). See Figure 2-1. They also establish a mobile reserve

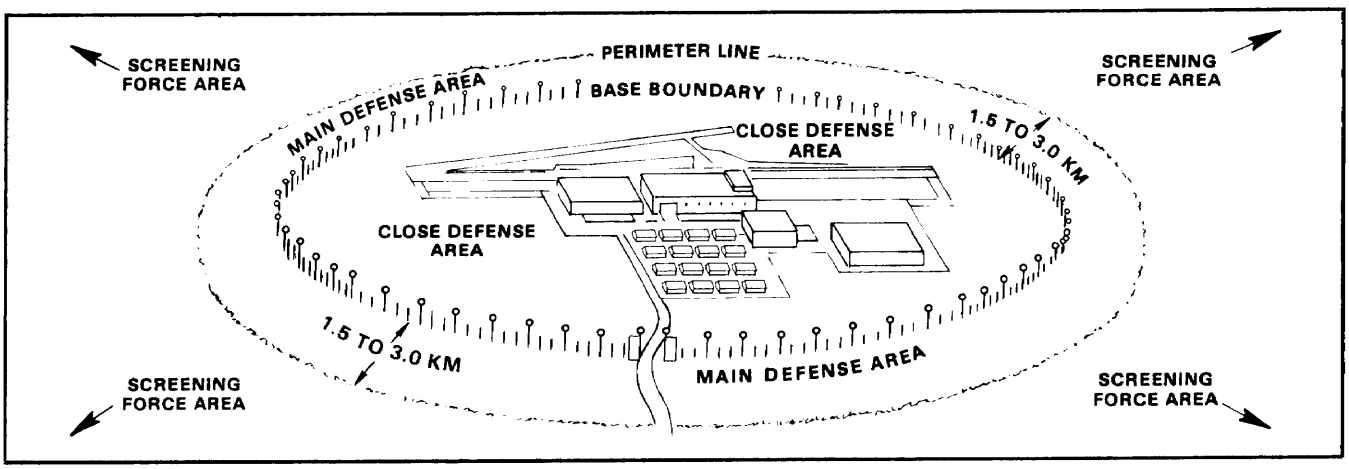


Figure 2-1. Base Defense Areas

WWW.SURVIVALEBOOKS.COM

(MR) or reaction force in reinforce any of these areas. Defense forces in each area must develop fields of fire and no-fire areas and use other control measures, keeping in mind the locations of other friendly elements. Doing so prevents friendly casualties and ensures that fires overlap to create an in-depth layered defense.

SCREENING FORCE AREA

The screening force area is the outer defense ring, extending from the MDA far enough to keep attackers from surprising base defense forces. SFA forces provide early warning to the remaining base defense forces. Screening forces (SFs) maintain surveillance over the entire front of the defensive perimeter. Screening forces—

- Provide timely warning of enemy approach.
- Gain and maintain visual contact with attackers and report their movement.
- Destroy or repel small enemy forces.
- Impede the advance of larger enemy forces by en-gaging them with long-range organic and supporting fire.

Screening forces use a series of dismounted observation posts (OPs), listening posts (LPs), and mounted and dismounted patrols in front of the perimeter line. OPs and LPs detect the enemy as far out from the perimeter as possible, report sightings to the commander, and, where rules of engagement allow, engage with organic weapons or call for indirect fire on the enemy.

Whenever possible, OPs and LPs will be equipped with remote sensors, ground surveillance radar (GSR), forward-looking infrared radar (FLIR), night-vision goggles (NVG), night-observation devices (NOD), trip flares, and other items that will aid in establishing a continuous detection capability across the front.

To be effective, OPs and LPs must have sufficient personnel to operate for sustained periods and good radio and telephone communications. OPs and LPs should report to their sector command post at predetermined intervals, taking care not to reveal or highlight their locations.

For maximum observation, OPs and LPs should be positioned in front of the perimeter line. The distance from the line should be determined by—

- The terrain.
- The mobility of the OPs and LPs.
- The availability of fire support.
- The availability of communications.
- The location and mobility of the enemy.
- HN agreements.

Patrols will cover areas that stationary elements cannot observe and the areas between OPs and LPs.

The SF usually consists of elements from, or attached to, the main defense force (MDF). Depending on METT-T, the commander may elect to use elements from the MR to perform all or part of the SF mission. In such a case, the commander should task-organize the forces to place the SF elements from the MR under the operational control of the security elements who have been tasked to perform the MDF mission. Unit integrity should be maintained to the maximum extent possible.

When available, aviation assets can add flexibility, response, and extended observation to the SF. For the most effective employment and integration of aviation assets into the SF, commanders must coordinate with the BDOC to request aviation assets early enough to permit proper coordination and mission planning. Once integrated into the plan, such assets normally coordinate directly with the leadership of the SF to ensure unity of effort.

Where possible and where nation-to-nation agreements exist, HN forces should be used as the SF. When HN forces are the SF, they must be in constant touch with the BDOC for early warning and overall defense coordination. To ensure effective coordination, US liaison officers and NCOs should be attached to the HN force.

MAIN DEFENSE AREA

The MDA extends from the CDA to form the background of the base defense. Forces in the MDA, referred to as the MDF, usually comprise the bulk of the defense force. The MDF depends on METT-T, but normally it deploys in an area from 1.5 to 3 kilometers past the base perimeter. These distances are representative and based on the typical effective range of most man-carried weapons. Main defense forces—

- Detect enemy forces and warn the defense force and the base command post of impending attack.
- Destroy the enemy when possible or delay, disorganize, and canalize the enemy into areas suitable for counterattack by the MR.

WWW.SURVIVALEBOOKS.COM

Portions of the MDF may reinforce the MR to counter direct landings on the base by airborne, airmobile, airlanded, or sealanded forces.

MDFs are assigned to defend specific portions or sectors of the perimeter. The width and depth of these sectors are determined by—

- The terrain to be held to keep the enemy from curtailing or terminating friendly operations.
- The size, location, and type of enemy force.
- The likely avenues of approach into the perimeter.
- The key terrain within the perimeter.
- Concealment and cover from direct and indirect fire that the perimeter area provides for the MDF and priority resources.

MDFs deploy so as to provide mutual support. Doing so keeps the enemy from penetrating the perimeter or bypassing forward elements undetected. Figure 2-2 suggests how to divide a perimeter into sectors of operation.

Commanders may defend from a series of supplementary positions along key avenues of approach or from well prepared, mutually supporting fixed fighting positions. Choices depend on the—

- Size and mobility of the MDF.
- Type, size, and mobility of the enemy.
- Terrain in the MDA.

In any case, MDFs must use surprise to their advantage. To optimize the capabilities of their weapon systems and to be most effective against the enemy, they must select blocking and fixed fighting positions carefully and clear fields of fire out as far as possible. By doing so, they can—

- Restrict enemy freedom of movement.
- Disrupt enemy leadership.
- Engage the enemy in a series of small actions that sap its strength and impair its ability to carry out its mission.

Essential to the MDA defense plan, fire support planning includes mortar, field artillery, naval gunfire, EW, and tactical aircraft (TACAIR) assets. Defenders plan fires on likely avenues of approach, as well as in front of, on top of, and behind likely objectives. Defenders also need to plan indirect fires to cover and take advantage of all natural and man-made barriers and obstacles. In-depth coordination with fire support assets from each service must occur during planning. The BDOC has overall responsibility for base defense fire support. Fire support planners must make collateral damage and possible civilian casualties primary considerations. Fire support planners must consider countermortar and counterbattery assets. Their radar can provide quick response to enemy indirect fires.

Aviation assets could be integral to the MDF. Both fixed- and rotary-wing assets can extend observation and give immediate combat response in the outer areas of base defense. Planned for and

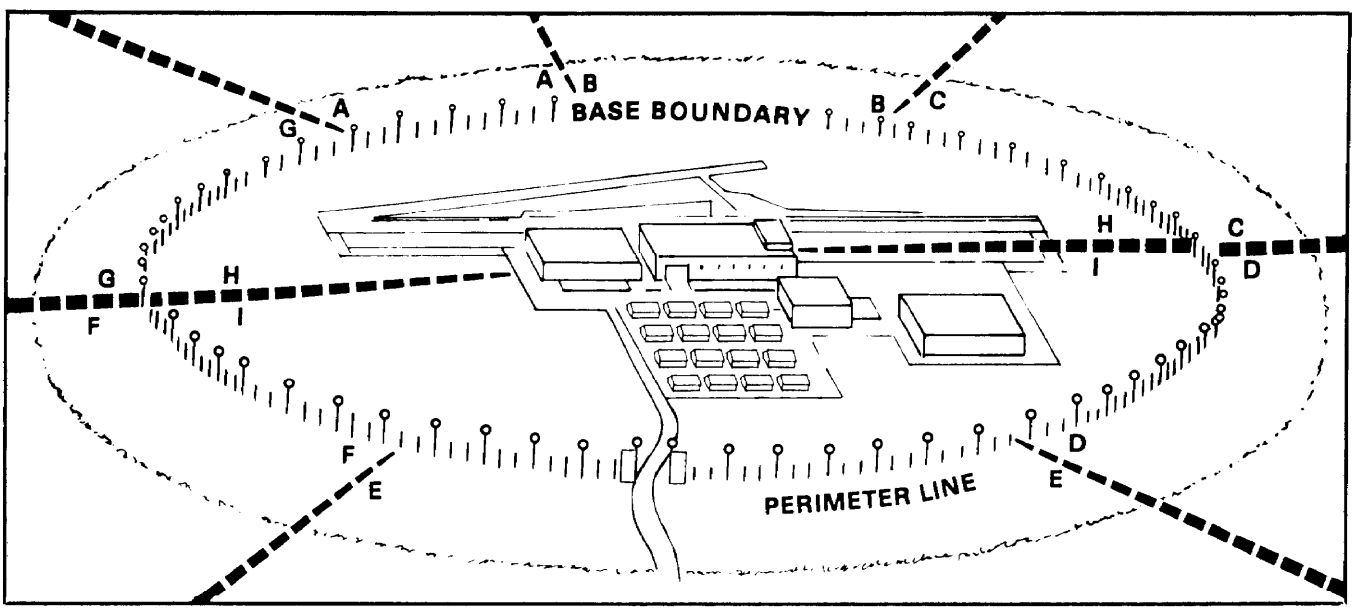


Figure 2-2. Sample Defense Sectors

WWW.SURVIVALEBOOKS.COM

requested early, aviation assets add flexibility and combat power to the defense.

Where possible and where nation-to-nation agreements exist, HN forces may serve as the MDF.

CLOSE DEFENSE AREA

The CDA is the innermost ring. It contains all elements essential for day-to-day base operations. Unless a legal base boundary exists, commanders determine the base perimeter on a case-by-case basis to accommodate local conditions. Regardless of the legal base boundary, the perimeter along which the defense is prepared and conducted should be determined by the terrain and the forces available to conduct the defense. The CDA perimeter is usually within the base perimeter. The CDA may be adjusted along the most defensible terrain and the terrain from which best to detect the enemy. Forces assigned to defend in the CDA protect the most critical base elements.

Forces in the CDA are the close defense force (CDF). Its soldiers occupy positions on the perimeter and perform internal security missions against sabotage and covert threat. To increase observation and security, the CDA can be sectored according to base dimensions and internal security missions. Mobile patrols in the CDA also enhance overall security. CDF may occupy—

- Entry control posts, boundary sentry posts, and base entry control posts.
- Static defense positions around fuel depots, ammunition depots, communication centers, supply facilities, medical facilities, and other high-value targets and along likely avenues of approach into the CDA.

They also provide a security response force for aircraft parking areas or other restricted or sensitive areas, as well as a mobile patrol throughout the CDA.

Also, the CDF must help the MR to prevent hostile forces from landing aircraft, helicopters, amphibious craft, or troops directly on the base. If the base is an airfield, the CDF will perform a runway denial mission by positioning forces at covered and concealed, mutually supporting positions around active runways. On naval installations the CDF will be positioned around ships and vital harbor facilities. These combat elements engage any attacker that may have survived engagements with the MDF and MR.

Heavy weapons teams will support the CDA. Antiarmor teams will occupy strong points along likely avenues of approach for vehicles attempting to crash through the defensive perimeter. Machine gun teams will augment critical positions, strong points throughout the CDA, and static positions around the perimeter.

An HN force on a base should be directly integrated in the CDA in sector or around its own restricted or sensitive resource areas. Its organic indirect fire weapons must be integrated into the commander's defense plans. Except in special cases, its chain of command should be used to preserve unit integrity and unique logistical and administrative systems.

Employing the Mobile Reserve

Forces penetrating the MDA will be met by additional vehicle-mounted forces performing as the MR. Its main mission is to block any penetration of the base or any direct landing on it until the enemy can be repelled or destroyed. The MR must concentrate enough firepower to destroy the enemy force. To function as a blocking force, the MR must be positioned where it can best respond to the most likely avenues of approach into the CDA and other critical areas. Its composition should be based on METT-T; for example, on flat, open terrain, an MR in lightly armored vehicles could be the most effective.

The MR will counterattack to regain critical battle positions or terrain or to reestablish the base perimeter. Counterattacks can restore integrity to the defense when penetration or disintegration threaten it or when the enemy gains terrain from which it can place direct weapons fire on the base. The MR should launch counterattacks immediately to eliminate small penetrations or infiltrations while the enemy is weak, disorganized, and susceptible to isolation.

Part of the MR may also reinforce a forward MDA when heavy enemy pressure or casualties reduce its relative combat power. The MR may also perform part or all of the SF mission. The commander prescribes what SF responsibilities the MR will have and the command and control relationship between the MR and the MDF. The MR may be moved by helicopters to increase its flexibility and responsiveness.

HN forces on US bases may be directly integrated by unit into the MR. Agreements spell out the command relationships for such units, MR planners should consider having them reinforce or counterattack in their own sectors or areas of

WWW.SURVIVALEBOOKS.COM

responsibility to avoid language problems. US and HN forces of the MR should exchange personnel to provide language translation ability and disseminate orders and information. Such liaison must start as early as possible and be available from then on. If HN forces are not integrated into US operations, the tendency may be to Americanize LIC, especially during a counterinsurgency. This tendency may be counterproductive. In most cases, therefore, US forces cannot operate unilaterally in LIC.

Employing Antiarmor Weapons

To employ antiarmor weapons, defenders should—

- Identify avenues of approach that enemy armored vehicles could use.
- Cover the approaches by assigning positions and sectors of fire for antiarmor weapons.
- Select primary, alternate, and supplementary positions.
- Select routes to and from all the positions so that crews can occupy and vacate them quickly without unnecessary exposure.
- Plan obstacles that force the enemy into open areas where antiarmor and antipersonnel fires can target them. The obstacles, too, must be covered by fire.

Alternate positions, located to the rear of primary positions, provide depth to the antiarmor defense. Likewise, supplementary positions protect against an armored attack not covered from primary positions. These positions provide for all-around security.

Positions should use all the cover and concealment advantages that the terrain can provide. Fields of fire should be unobstructed out to the maximum effective range of the weapon. Crew members may have to clear them.

Employing Mortars and Other Indirect Fire Systems

Mortar, field artillery, and naval gunfire could support the MDF. To ensure immediate fire support and complete coverage, defenders must preplan indirect fires on likely targets throughout the SFA and MDA. Such targets include enemy avenues of approach and areas in front of, on, and behind friendly blocking and fixed fighting positions in the MDA. Defenders planning indirect fire must consider minimizing collateral damage and possible civilian casualties.

FIRE SUPPORT PLANNING

Defenders will plan targets—

- On likely LZs and DZs near their bases.
- On avenues of approach from such zones to the base.
- In support of man-made and natural obstacles.
- On critical terrain features.
- On possible enemy positions.
- For support of the perimeters.

The BDOC is the focal point for defense of the base. It coordinates and executes all action necessary to secure the base and its support facilities. A BDOC maybe responsible for several subordinate bases in the area. In such case, it would be in charge of all the bases in what is called a *base cluster*. The BDOC reviews and incorporates the target lists and fire plans of surrounding bases into an overall fire plan. The base forwards a copy of the target list and fire plans to the command post of the commander responsible for the commitment of response forces. Response or TCF commanders and the supporting fire support element must have a copy of the target list and fire plans before the forces are committed.

Fire support planners must consider and publish any restrictions on the type of munitions. Some, though excellent for destroying an attacker, could inhibit or prevent continuation or resumption of the base mission. If such munitions are to be used as a last resort, the approving authority and command channels must be clearly delineated. Generally, indirect fire should not be used against Level I threats since they are usually individual or small-unit operations, limited in scope and duration, and too fleeting to be engaged successfully. Larger enemy forces could be Level II or III threats. They have the size, combat power, and identifiability which might require fire support assets.

Response forces and TCFs used to counter Level II and III threats maybe tailored to include attached or direct support (DS) artillery. They will include observers and may have fire support elements (FSEs) with communication equipment. They may also include Air Force tactical air control parties (TACPs) with associated maneuver units of the TCF. The TACPs will perform their primary mission of directing offensive air power against an enemy force.

FIRE SUPPORT COORDINATION MEASURES

Fire support coordination measures permit or restrict fires in and around bases. Where HN

WWW.SURVIVALEBOOKS.COM

support is used, these measures can restrict fires without revealing the functions of classified sections of the base not accessible to HN forces. For all bases, and especially those in or near populated areas, US and HN commanders will have to coordinate—

- The types of fires authorized into surrounding areas.
- The severity of fires.
- The circumstances that permit return fires.

Permissive fire support coordination measures can increase the response to requests for indirect fires.

Employing Aviation Assets

When available, aviation assets should be integral to base defense. Both fixed- and rotary-wing aircraft can extend the range of observation in the SFA and give immediate combat response in the outer areas of base defense. Specially designed aircraft, such as those equipped with FLIR or the Air Force AC-130 gunship, are particularly well suited for supporting base defense. Planned for and requested early, aviation assets can add flexibility and combat power to the base defense.

Using Mines and Obstacles

Antitank and antipersonnel mines complement obstacles and indirect fires. Defenders should emplace them on all enemy avenues of approach to break up assault formations and inflict heavy casualties. Mines and obstacles such as barbed wire canalize and slow the enemy to increase exposure to defensive fire. Defenders should employ obstacles in depth, reinforce them to increase their effectiveness, and cover them by observation and fire. The commander exercising control over response forces and the TCF must obtain obstacle overlays and obstacle target lists before committing a response force in an area of dangerous obstacles.

Establishing Security Measures

The commander of the joint base defense force sets up a security system to prevent observation and surprise. The SF should provide early warning. However, security measures must be in force throughout the entire area of operations. Identifying and setting priorities for critical base assets will emphasize likely targets and help economize defense force efforts.

ACTIVE

Active security measures include OPs, LPs, patrols, and stand-to alerts. The defense force commander may direct a set number of OPs and LPs or let subordinate commands decide their needs. OPs and LPs must be placed strategically. However, careful random positioning of them will help to confuse enemy recon forces and frustrate an attacking force. In terrain that restricts fields of fire and during periods of limited visibility, more OPs and LPs are necessary.

Security requires aggressive patrolling. Patrols reconnoiter dead space in sectors and gaps between sectors.

Stand-to alerts, held both morning and evening, ensure that all soldiers in the defense force—

- Adjust to the changing light and noise.
- Are awake, dressed, and equipped.
- Check their weapons and are ready for combat.

Morning alerts should start before first light; evening alerts should continue until after dark. The starting and ending times should vary to prevent establishing a pattern, but each alert must last long enough to serve its purpose.

The commander may also specify a set number of troops to be on security at all times. The number will vary with the enemy situation, terrain, and visibility. When an attack is expected, the entire defense force should be on security. Such high security should not continue for long periods because troops need rest in order to function. Security, however, cannot be sacrificed for rest.

PASSIVE

Passive security measures include—

- Camouflage.
- Concealment.
- Movement control.
- Light and noise discipline.
- Proper radiotelephone procedures.
- Ground surveillance radars and ground sensors.

Establishing Work Priorities

The commander must set priorities for the many tasks involved in base defense. Work may occur on several tasks at the same time. See the sample that follows in Figure 2-3.

WWW.SURVIVALEBOOKS.COM

Priority 1:	Establish initial base security.
Priority 2:	Position crew-served weapons and troops and assign sectors of fire.
Priority 3:	Clear fields of fire and prepare range cards.
Priority 4:	Prepare fighting positions.
Priority 5:	Install communications.
Priority 6:	Emplace obstacles and mines.
Priority 7:	Improve primary fighting positions to include overhead cover.
Priority 8:	Prepare alternate and supplementary positions.
Priority 9:	Stockpile ammunition, food, and water.
Priority 10:	Prepare routes and trenches between positions.
Priority 11:	Develop a counterattack plan.

Figure 2-3. Priorities

Developing a Counterattack Plan

Reserves or lightly committed forward elements conduct counterattacks. Counterattacks begin after the enemy's main effort has been identified and an assailable flank has been created. Their timing is especially important because they must synchronize with the overall defensive effort. Like spoiling attacks, they usually revert to the defense after local exploitation rather than turn into full exploitation and pursuit. In some cases, they may be the first step in resuming offensive operations by the larger defending force. Counterattacks may be counterattacks by fire only. Such tactical actions position a force so it can bring flanking or rear fires against the enemy, but it does not assault enemy positions.

Establishing Area Damage Control Measures

Area damage control (ADC) includes the measures taken before, during, and after hostile action or natural disasters to reduce the probability of damage, minimize its effects, and aid in the continuation or reestablishment of normal operations. Engineers perform most of these tasks. Other forces and assets contributing to ADC include ordnance, policy, NBC, civil affairs, maintenance, medical, signal, supply, transportation, and transiting units.

Establishing Air Defense Measures

Air defense nullifies or reduces the effectiveness of attack or surveillance by hostile aircraft or missiles after they are airborne.[3] Air defense assets on or near a base will be integrated into the overall defense plan for the theater. The commander of the joint base should set up a communications link with the air defense net for earl y warning of impending air attack. If the joint base is also an air base, local air defense units and the air base operations center must coordinate and establish return-to-force and identification, friend or foe (IFF) procedures.

Establishing NBC Defense Measures

Commanders of bases must ensure that their facilities can operate with maximum individual and unit effectiveness in an NBC environment. They must understand the NBC threat, including likely weapon systems and threat tactics, and they must ensure all soldiers know precisely how to use their own NBC equipment.

They must enforce strict OPSEC procedures to reduce the enemy's ability to acquire lucrative targets against which it may use NBC munitions.

All personnel and units must be prepared and trained to operate under the worst possible battlefield conditions. Training must be realistic, continually reinforced, and fully integrated into unit exercises. To survive, personnel must maintain their equipment properly and use it. Training in the use of detectors and mission-oriented protective posture (MOPP) ensembles and procedures is the key to protecting the force. Operating with suits, masks, detectors, and alarms is a necessary part of base NBC defense.

Defenders look for both enemy activity and contamination when they establish an NBC defense plan. Personnel should be assigned additional duties of various chemical detection and radiological monitoring or survey. The data they collect gives the BDOC a picture of NBC activity in the area. They mark and report detected contamination so others will not encounter it.

Nuclear weapons will cause heavy casualties, materiel damage, and obstacles to movement. They will restrict the use of critical facilities, communications, and terrain. The effects of initial nuclear radiation can range from temporary mild radiation sickness to immediate incapacitation

[3] *Joint Doctrine for Air Defense, .ICS* Pub 3-01.3; *Joint Doctrine for Theater Counterair Operations,* JCS Pub 2-01.2.

WWW.SURVIVALEBOOKS.COM

and early death. Thermal radiation can severely burn exposed personnel. Enhanced radiation weapons dramatically increase radiation casualties without corresponding increases in materiel destruction. Fallout and neutron-induced contamination will require defenders to expend time and resources for monitoring and survey, radiation exposure control, and decontamination operations.

The primary means of protecting US forces against biological weapons is maintaining current inoculation status as they process for overseas deployment. Once deployed, they counter biological threats through—

- A rigorous field sanitation program incorporating water and food inspection by qualified personnel.
- A certification program for hiring local nationals.
- Medical programs to closely monitor the health of the command.

Medical personnel must be alert to any significant increase in infectious disease rates and keep the commander informed as they occur. Medical observation continues to be the primary warning method because reliable field detectors for biological agents are not widely available.

Protective measures against chemical attack fall into two categories: sanitary inspection and physical protection. A thorough food and water sanitation program greatly reduces the chances of covert chemical assaults achieving their goal. To counter overt chemical attacks or indirect exposure, base commanders have readily available physical protection measures and supporting equipment for detection, protection, and decontamination.

Developing a Threat Response Contingency Plan Combating Terrorism

The threat response contingency plan outlines specific duties and responsibilities to combat terrorism. It describes the—

- Circumstances for its implementation.
- Notification procedures.
- Concept of operations.
- Mission priorities.
- Options for using forces.
- Decision making parameters (local and higher levels).
- Resource requirements.

It provides checklists of actions to be taken by emergency operations center (EOC) members, crisis management team (CMT) members, and the threat management force (TMF). (See Appendix D.) The defense force commander normally develops the plan in coordination with the installation staff, including the staff judge advocate. The G3 or deputy chief of staff for operations and plans (DCSOPS) normally implements, trains, tests, and revises the plan. All concerned, including all potential response agencies, must understand and coordinate the plan.

Determining the Physical Layout of the Base

The physical layout and placement of equipment on a base can be as significant to its defense as the size of the force guarding its perimeter. Commanders must always stress continuous upgrading for base physical security. Surveys of the defense, including intruder drills and mock attacks, must be part of defense training and serve to identify any shortcomings of base defense. Defenders, especially those in high-threat areas, must be cautious not to confuse a drill with an actual attack.

Plans for base construction must consider ADC. Defenders need to use fire fighting equipment and practice procedures often to maintain ADC proficiency should an attack occur.

INTRUSION DETECTION

Defenders can emplace sensors on likely avenues of approach, locating them as far forward as the SFA. Directed GSR and airborne FLIR systems can improve the chances of detecting intrusions early. Remotely monitored sensors, trip flares, and other nonlethal warning devices can also be useful. Depending on the threat situation and ROE, antipersonnel and antivehicle mines may also be emplaced. Noncombatants nearby may restrict their use.

OBSERVATION

To improve observation, defenders should clear the ground to the front of the CDA and from near the base perimeter fences by cutting foliage or applying defoliant. Using defoliant or cutting foliage can expose the base to aerial observation. Balancing the needs of ground defense and aerial defense is best. Defoliant must be used only on areas immediately around the defensive perimeter because it can affect large areas and destroy food production.

WWW.SURVIVALEBOOKS.COM

Bromacil is the defoliant of choice inmost cases. Presidential approval is mandatory prior to using herbicides (Executive Order 11850). Perimeter roads on either side of the base fence improve observation. A combination of concrete barriers, concertina wire, lighting, surveillance cameras, and intrusion sensors should be used to form a solid, mutually supporting defense (see Figure 2-4). Observation sites in guard towers or atop buildings can increase the surveillance capabilities of perimeter guards.

COMMUNICATIONS

Defenders should install a reliable and redundant communications system at all guard locations. It should consist of—

- A land line.
- A telephone hookup to a central switch in the base operations center.
- Radio links to the BDOC.
- Some type of duress or general alarm signal (fire alarm or loud speaker) to alert the entire base and activate the MR.

The base should also have alarms for NBC and air attacks.

ENTRANCES

The base should have as few entrances as possible. Offset concrete barriers at the entrance will prevent vehicles from accelerating. A counterbalance beam should be used as a gate. In addition, a heavy vehicle, bus, or dump truck should be stationed nearby to be driven in front of the entrance as an additional barrier.

Hydraulic barriers can improve entrance security. Entrance guards can use telescoping poles with mirrors attached to check under vehicles. Dogs trained in explosive detection are also useful. Dogs must be tested often, especially in extreme weather conditions when their abilities may be severely degraded.

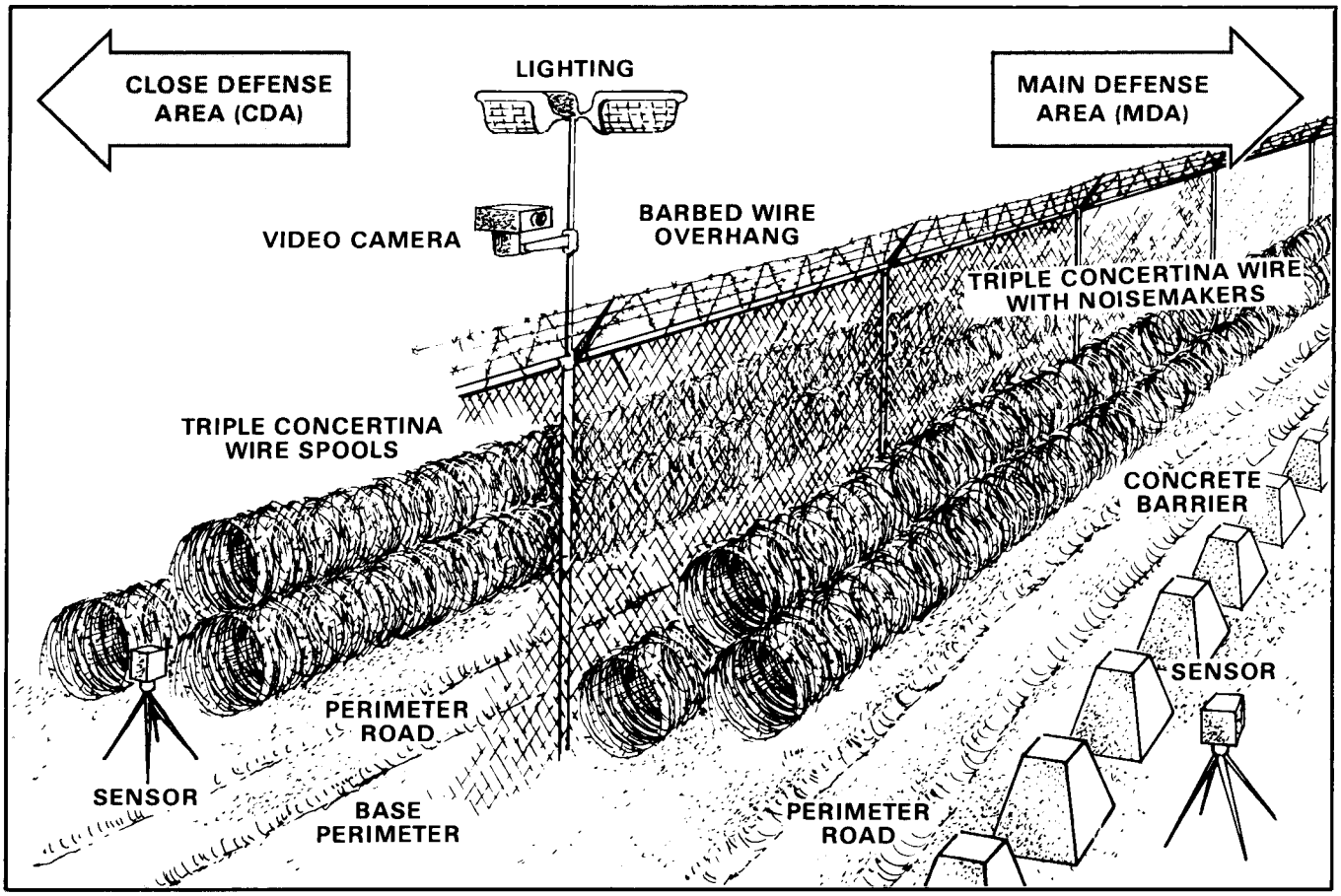


Figure 2-4. Sample Physical Perimeter Defense Measures

WWW.SURVIVALEBOOKS.COM

Personnel on foot should have a separate entrance. An encased turnstyle would provide effective control, especially where foot traffic is heavy. A badge system of identification should be established, and personnel need to be time-logged in and out. Security personnel must constantly guard against complacency in such a system and be alert for any paperwork mistakes. An area for searching personnel should be established and equipped with portable metal detectors.

Buildings housing personnel and sensitive equipment should be out of grenade-throwing range from the exterior fence and, if possible, away from direct sight.

Protecting the Base

WORKING AND LIVING AREAS

Bunkers with reinforced and sandbagged roofs should be near all working and living areas. They should not only provide protection but also serve as fighting positions. Trenches between bunkers would increase safety. The bunkers should be equipped with communications and first aid kits. The defense of on-base dependent housing areas and other nonmilitary facilities could require extraordinary security precautions.

PERSONNEL AND EQUIPMENT

In a LIC environment the defense must protect both US and allied personnel and equipment without degrading the overall objective. Given political constraints such as limits on security personnel or restrictions on building defenses, commanders will probably have to translate broad strategic guidance into definitive operational objectives and viable security plans.

Terrorists and other dissidents who wish to embarrass the HN or the US may target US military personnel for attack or incite behavior discrediting to the US. Commanders must consider the following in defending deployed units:

- The potential threat for terrorist attack.
- HN agreements on responsibilities and procedures for protecting personnel on leave, liberty, or pass.
- Coordination between HN civil authorities and military law enforcement agencies.
- Actions expected of officers and NCOs in a developing situation.
- Advance training in personal defense techniques for deploying units.
- Organization of those on leave, liberty, or pass into two- or four-person teams with each member responsible for the well-being of the others.

INTERNAL AND EXTERNAL TERRITORIES

Defenders must retain or deny terrain, facilities, and activities and preserve forces essential to base functions while minimizing the impact of security efforts on local politics. Area security forces, which defend territory outside the base and base defense area, could consist of US or HN personnel. They respond to requests for assistance in base defense. They could be placed under OPCON or attached to the base.

MEDICAL FACILITIES

Medical facilities should be well marked and placed away from possible lucrative targets. These facilities must have their own means of security since they could be primary terrorist targets. They must have backup energy sources ready to use in case of a power failure. The backup system must be at a separate site from the primary source.

PORT AND HARBOR FACILITIES

Port and harbor facilities can be attractive targets. Because access is so varied and activity is normally so heavy, defense is difficult. Developing mutually supporting elements to control access and to defend against air, land, and surface or subsurface waterborne attacks requires in-depth planning. The area commander coordinates with the commander of the base to plan, organize, and equip resources for port security and available naval and special operations forces (SOF) assets. Because port and harbor facilities are inherently complex, no single set of defensive measures can apply to all of them. Defenders integrating port and harbor security with land-based security must pay close attention to the concerns in Figure 2-5.

Protection for Choke Points

Security forces should be placed where an entering or exiting vessel's maneuvering is restricted, making it susceptible to a shore-based attack.

Protection Against Attack from High Ground

Security forces need to identify high ground and protect against attacks from such sites.

WWW.SURVIVALEBOOKS.COM

Protection of Structures

Structures, especially if they could be effective sniper locations, must be secured or manned by security forces.

Protection of Fuel Supplies

Fuel supplies should have remote closure valves for cutting off the flow of fuel in case of an attack.

Tides and Currents

Local tides and currents must be studied. Their effects on swimmers and floating explosive devices must be handled by the overall defense plan.

Water Clarity and Depth

To plan the use of antiswimmer devices or nets, security forces should be familiar with the clarity of the water and consider the chances of swimmer-delivered attacks.

Pier Clearance

If the pier's clearance above the water and piling configuration is such that a small boat or swimmers could operate under it, it must be barricaded or patrolled.

Lighting

Lighting must be adequate and positioned so as to illuminate incoming personnel but shadow security forces.

Vehicle Control Points

Security forces should set up such points at all roads into or out of the facility.

Use of Patrol Boats

Defenders must have patrol boats equipped with searchlights, radios, appropriate weapons, and concussion grenades. The number of boats will vary based on facility size and level of threat. Picket or patrol boats must guard vessels at anchor. Defenders must establish a security perimeter on the water and patrol it to keep all unauthorized boating clear of the security zone. For deployment checks, see Figure 2-6.

Communications Net

All elements of the security forces should have access to a common communications net.

Check for Explosive Devices

Swimmers and divers should be available and trained to check the hulls of vessels for explosive

1. Aerial photos, if available.
2. Current tides and current chart.
3. Current depth-sounding chart.
4. From 1, 2, and 3, the locations where—
   - A vessel's maneuvering may be restricted, making it susceptible to attack.
   - Floating devices could be placed and consequently drift into vessels moored or at anchor.
   - Vessels are susceptible to attack from high ground.
5. Commander's choice of locations for establishing defensive positions.

Figure 2-5. Predeployment Checks of the Port or Harbor Area

1. Areas under piers secured by temporary fencing, lighting, and patrol boats as necessary.
2. Surrounding structures examined to ensure the identity of the occupants.
3. *Unoccupied structures secured.*
4. Any structure that could serve as a base for sniper attacks routinely checked by roving patrol.
5. Remote closure valves for fuel supplies operational and protected.
6. Nighttime survey conducted to check the adequacy of lighting; lights repaired or replaced as required.

Figure 2-6. Deployment Checks

WWW.SURVIVALEBOOKS.COM

devices when they arrive and periodically during their stay in port. For port checks, see Figure 2-7.

Inspection Station Checkpoints

Checkpoints should be established to inspect incoming and outgoing cargo.

Rail and Highway Entrances Security

Clear lines of demarcation must separate port areas. They should be fenced and patrolled.

Air Defense Measures

If an air attack is probable or anticipated, defenders should establish defensive positions and point air defense weapons.

Security for Individual Vessels

Maintain the engineering plant so the vessel can get under way as quickly as possible. Each unit should have an internal security force, and the facility security officer should be informed of its size and capabilities. The commanding officer or master of each vessel should inform the facility commander of the support it can provide to existing security forces.

The facility should be aware of what weapons, if any, a vessel can employ in support of security forces. The commanding officer or master of each vessel must be briefed on actions to be taken in the event of an attack. All crew members must be given an up-to-date briefing on terrorism awareness and personal security. For individual vessel checks, see Figure 2-8.

1. Vehicle control points.
   - Only minimum amount of access necessary.
   - Manning by two armed personnel.
   - Barricades in place or available.
   - Communications available.
   - Entry requirements available.
2. Picket and patrol boats equipped with—
   - Searchlight.
   - Radios.
   - Weapons and ordnance.
   - Two-person crew (minimum).
   - Harbor charts.
   - Location and names of vessels in port.
   - Information concerning vessel movement.
3. Swimmers and devices.
   - Number available.
   - Capabilities.
   - Response time.

Figure 2-7. Port Checks

Using Tactical Deception

The use of deception is a proven force multiplier that can improve base security. Deception operations should include visual, sonic, olfactory, and electronic measures. The measures must be mutually supporting and believable.

Dummy minefield can be integrated with actual minefield. Sonic simulators can imitate armor convincingly if tanks can periodically deploy in the MDA. Olfactory, electronic, sonic, and visual measures can simulate defenses in depth. These measures are especially effective at night.

To degrade enemy intelligence, defenders should—

- Vary guard rotations.
- Vary internal patrol times and routes.
- Move high value items such as aircraft to different locations on an unscheduled basis.
- Use camouflage for sensitive areas.

Mockups of living areas, weapons, and fuel storage tanks and deception operations can further degrade the enemy's ability to successfully attack base assets. Tactical deception is also critical within the CDA and must be integrated with the overall deception plan as directed by the commander of the base.

1. Crew briefed on the threat and actions to take if attacked or provoked.
2. Point of contact provided for security issues.
3. Security forces informed of the amount of time vessel needs to get under way, if required.
4. Capabilities of ship's internal security force determined.
   - Number of personnel.
   - Types of weapons.
   - Response time.
   - Specific capabilities.
5. Ability of ship's weapons to stop a shore-based attack determined.
6. Ship's antiair capabilities determined.

Figure 2-8. Individual Vessel Checks

WWW.SURVIVALEBOOKS.COM

CHAPTER 3

COMMAND AND CONTROL

Defending a joint base involves normal command and control responsibilities. However, commanders of bases in foreign countries must be familiar with the legal constraints imposed by international and domestic law.

SECTION I

RESPONSIBILITIES

The potential complications of the presence of multi-service bases in an area must be overcome by effective communications, responsive reporting, and timely reaction if base defense is to be successful. A situation which includes base defense will probably also place other concurrent, high priority requirements upon military forces. The base defense task organization can incorporate available regular force units and provisional units organized from base resources to provide maximum defense. A sample defense organization of a joint base is shown on the next page in Figure 3-1.

THEATER COMMAND

The following are the normal country and command responsibilities and relationships for a theater of operations.

National Security Council

The National Security Council advises the president on all national security matters and critical foreign policy issues.

Secretary of State

The president's representative in supervising, directing, and coordinating US foreign policy affairs is the secretary of state. The Department of State is the lead agency responsible for developing policy and operational guidelines for dealing with terrorist incidents involving US citizens and US interests abroad.

Ambassador and Country Team

The president's representative in each country is a US ambassador. The president gives the ambassador full responsibility for directing and coordinating the activities of all elements of the US diplomatic mission. The ambassador promotes positive program direction by ensuring that all US government activities in the HN are efficiently and economically administered and effectively interrelated so that they will contribute fully to US interests in that country, as well as to our regional and international objectives.

The ambassador's overall authority (Title 22, US Code, Section 3927) must be recognized unless the military commander's troops are actually in combat. The ambassador is responsible for initiation of noncombatant evacuation operations; however, he does not have the authority to direct US military forces under the command of a US area military commander.

The term *country team* describes in-country interdepartmental coordination among key members of the US diplomatic mission. In practice, the composition of country teams varies widely, depending on the—

- Desires of the chief of the diplomatic mission.
- Local situation.
- US departments and agencies represented in-country.
- Problems that the team has to consider.

WWW.SURVIVALEBOOKS.COM

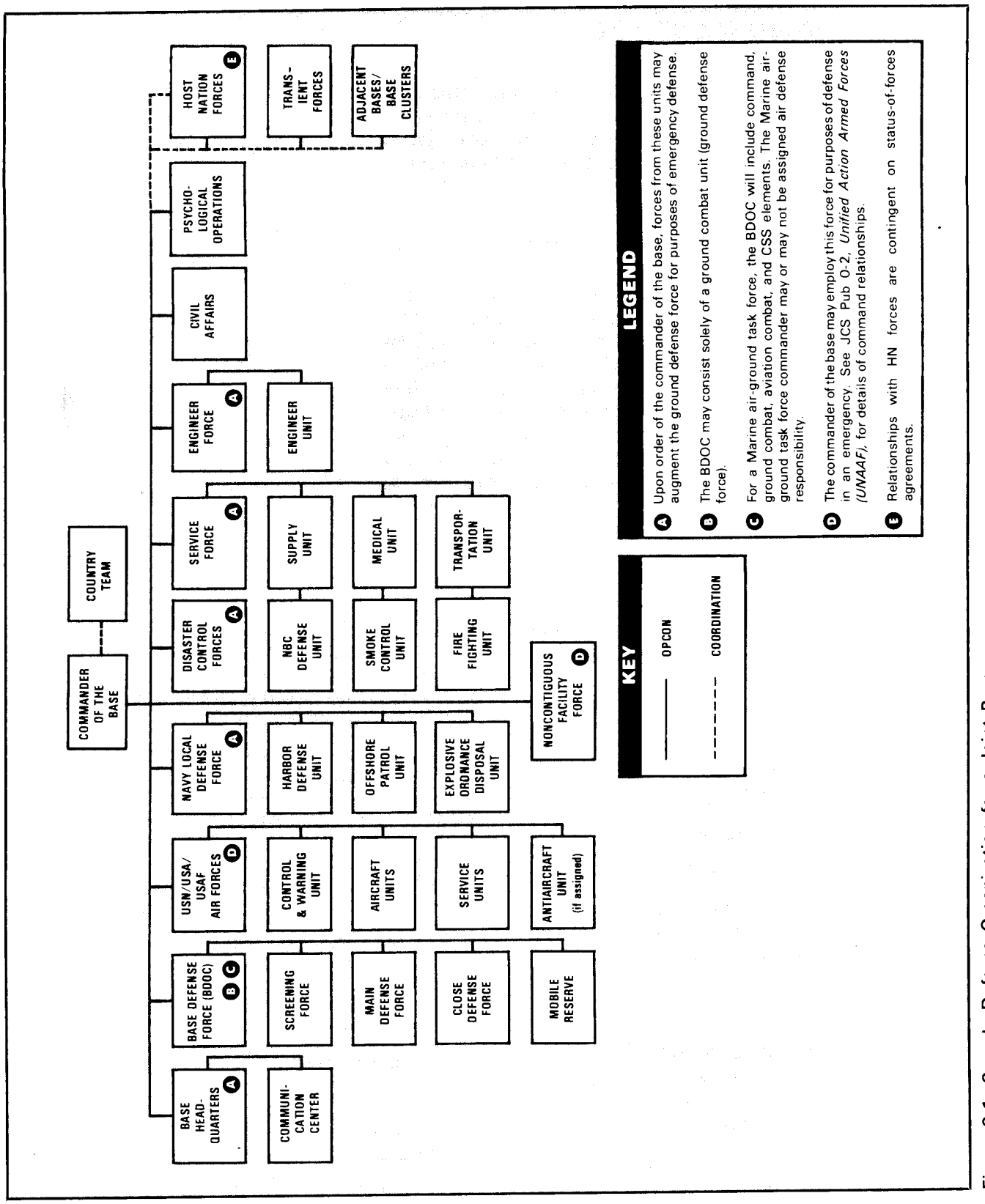


Figure 3-1. Sample Defense Organization for a Joint Base

WWW.SURVIVALEBOOKS.COM

An appointed contact officer, who is usually the Chief, Security Assistance Organization (SAO), or, in some cases, the defense attache, represents the unified commander on the country team.

Chief, Security Assistance Organization

SAOs manage security assistance functions in foreign countries. SAOs are responsible for foreign military sales and other forms of materiel assistance. The SAO chief is under the command of the CINC. As a member of the country team, however, the SAO chief is under the direction and control of the ambassador. The CINC normally appoints the SAO chief as his point of contact to the ambassador. In certain countries, the defense attache may have security assistance management responsibilities as an extra mission. The SAO may be known as the office of defense cooperation (ODC), the military assistance advisory group (MAAG), or another name mutually acceptable to the US and HN governments.

Joint Chiefs of Staff

The JCS assists the secretary of defense by developing joint plans to guide unified commands. Also, program recommendations coming from the SAOs and unified commands are fully coordinated through the JCS to ensure consistency with US global security plans. Only the national command authority (NCA), representing the executive branch of government, has the authority to commit US military forces. Combat forces assigned to a geographic area are usually under the operational command of the appropriate unified CINC.

Commanders in Chief

The CINCs of various unified commands are critical in committing US forces. They advise the JCS on significant events in their areas of responsibility. CINCs have operational and regional responsibility. The exception is the CINC, United States Special Operations Command, who has a global responsibility. CINCs must identify and apply the necessary resources for achieving US national strategic goals. CINCs have the responsibility and authority to communicate with the chiefs of the military services, the JCS, and the secretary of defense on all military-related matters. CINCs have an established linkage with the ambassadors in their AO through their appointed contact officers, and close coordination through them is essential (see Figure 3-2).

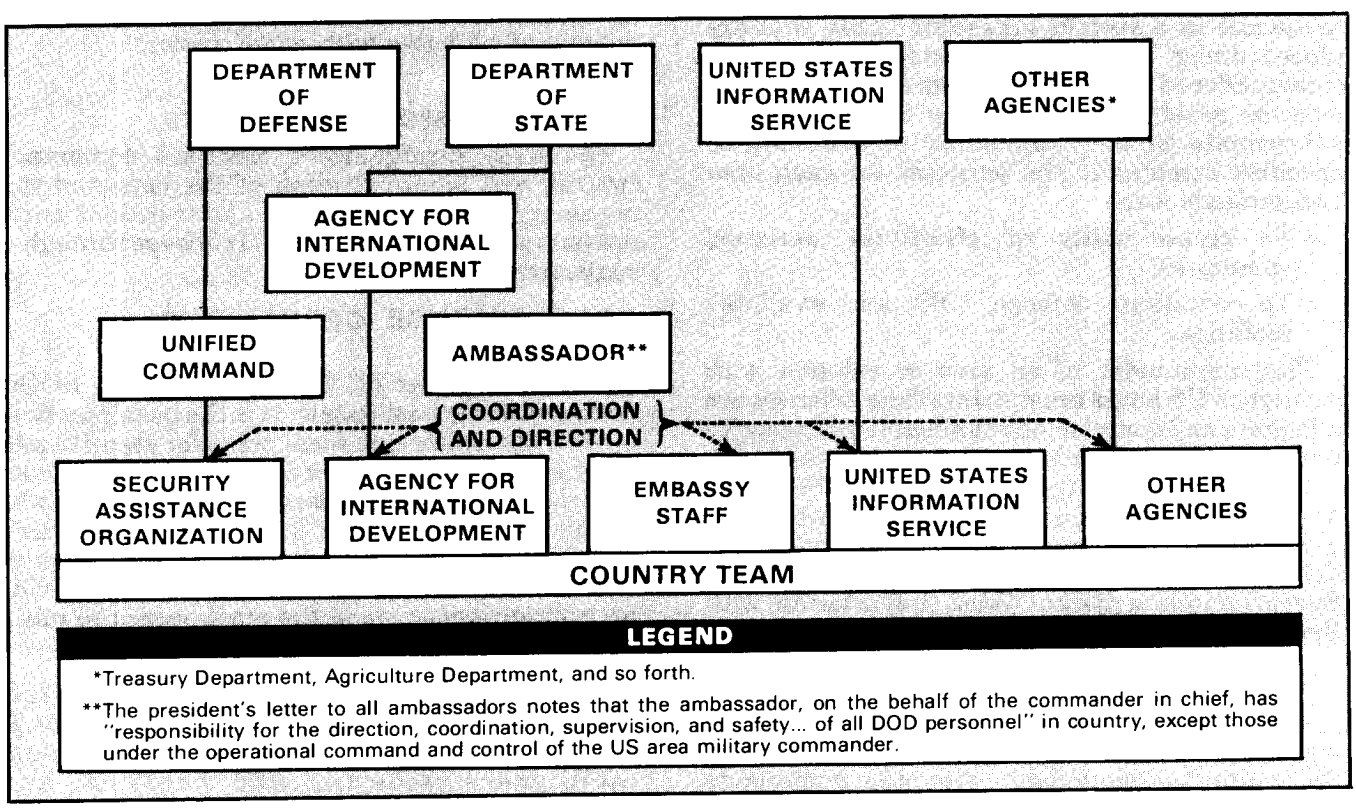


Figure 3-2. Country Team Relationships

WWW.SURVIVALEBOOKS.COM

Joint Task Force Commander

CINCs will normally delegate authority and responsibility for a particular operation to a joint task force (JTF) commander. If the JTF needs a base, a single commander for security and operations will normally be placed in charge. Regardless of the level of service involvement at a particular base, a clearly defined chain of command for controlling operations must be established to ensure unity of effort.

To provide for the effective defense of a base within his command or for joint planning within his area of responsibility, the JTF commander—

- Assigns the responsibility for local defense of the base.
- Establishes the method of command or coordination to be used by the local base defense commander.
- Ensures that appropriate command relationships between subordinate area and local base defense commanders are established.
- Ensures that local defense areas are delineated.
- Ensures that defense plans are published.

AREA COMMAND

An area command consists of the organized elements of one or more armed services, designed to operate in a specific geographic area, that are placed under a single commander such as the commander of a unified command. Smaller areas may be assigned as necessary to commanders subordinate to the commander of a unified or specified command. The purposes for such area assignments are—

- To secure unity of effort for assigned operations.
- To coordinate defense, CSS, and available facilities.

The commander of an area or subarea with numerous US bases must ensure their defenses are adequate and complement applicable HN security plans. The commander may be responsible for overall security of the area outside US bases, depending on local HN agreements and capabilities. The commander must ensure US base defense plans are properly focused against enemy forces, including distant forces that interfere with the operation or security of the bases.

JOINT BASE COMMAND

The designation of a commander of a joint base is influenced in part by the purpose of the base and its geographic relationship with other commands and bases. Overall command responsibilities for joint base defense are specifically defined in the directives activating the base. (In some cases a commander of a base may also be an area commander.)

The commander of the base establishes the defense organization as well as the planning, preparation, and execution of all defense measures. The base may support or protect the operations of two or more services at noncontiguous facilities within the base. As base defense coordinating authority, the commander of the base plans and directs the use of noncontiguous facility forces in base defense roles.

The primary mission of base support elements usually conflicts with planning and training for its secondary role in ground defense. The commander of the base coordinates both, thus ensuring that time and effort are equitably allocated. The current threat against the base influences this decision, necessitating greater emphasis upon accurate intelligence.

The base command can consist of a single base or a cluster of bases organized under one commander. It may be a land mass, an island, an island group, or combinations of them. A commander of a joint base who is also designated as a cluster commander must coordinate the defense of all bases within the cluster.

Base Headquarters

The base headquarters exercises command, control, and administration of the base and the necessary control of resident and transient units not part of the base command. It does so through a centralized BDOC.

BASE DEFENSE OPERATIONS CENTER

The commander of the base creates a BDOC from available base assets. It is the base's tactical operations center and focal point for security and defense. It frees the senior unit staff to concentrate on primary support missions. The BDOC may be composed of elements of the senior commander's headquarters (HQ) alone, elements from each of the tenant units, or both. Each tenant will provide an appropriate share of the staff needed to run a functional operations cell around the clock.

The BDOC plans, directs, coordinates, integrates, and controls all base defense efforts. It has three critical functions: operations, intelligence-gathering and analysis, and communication.

WWW.SURVIVALEBOOKS.COM

Operations.

The operations section is primarily concerned with planning and coordinating current and future operations. It prepares and implements base defense plans and serves as the central point of contact for coordination with—

- Higher echelon area defense counterparts.
- Other bases.
- Area security and response by military police (MP) forces.
- TCFs.
- HNS.
- ADC teams.

Large bases occupying critical sites or performing sensitive missions may receive permanently stationed liaison teams. Such teams help coordinate defensive efforts with adjacent bases, HNS, and area security elements. The operations section—

- Maintains defensive status boards.
- Prepares overlays.
- Develops and/or coordinates response force plans.
- Prepares fire support plans and requests.

It requests response forces or a TCF from higher echelons when attacks exceed the capability of base forces. The operations section is the interface for the commanders of the TCF and the base during combat operations against sustained Level II and Level III threats.

Intelligence-Gathering and Analysis.

The BDOC intelligence cell may or may not be distinct from the operations section, depending on the size of the BDOC. This cell serves as the conduit through which the commander of the base receives and transmits intelligence information about the AO. It develops information through exploitation of—

- All indigenous sources.
- Area security patrols (MP).
- Convoys.
- Adjacent bases.
- Theater intelligence.
- Communications.
- Higher echelon sources.

It also serves as a focal point for the base's contamination control effort.

If bases are near population centers, transportation routes, communication links, their intelligence assets can provide higher echelons with early warning and real-time assessment of local NBC conditions. Such information enables the overall rear area commander to discern potential problems and develop responses to minimize the impact of threat NBC operations in the rear area. Intelligence is then analyzed to give the commander the best advantage possible over the enemy.

Communications.

Dedicated communications assets must closely link all base defense activities. The communications system among the BDOC, higher echelons, and base defense elements must be secure, robust, redundant, and highly efficient. An automated battlefield communication system that includes inter- and intracommunications links is essential to base defense operations. Communication systems of HN and US response forces must interface for a coordinated response.

ALTERNATE BASE DEFENSE OPERATIONS CENTER

Defenders should set up an alternate BDOC if possible. If the base does not have the resources to support this requirement, headquarters elements of units OPCON to the base for defense may be designated for this purpose. The alternate BDOC can be located on or off the base, but command, control, and communications (C^3) of base defense should be the main factor in decisions about the alternate BDOC.

EMERGENCY OPERATIONS CENTER

The commander of the base has operational control of base resources during a terrorist incident. Counterterrorism actions, however, are typically planned, coordinated, and directed by an EOC, which is activated immediately when terrorist incidents occur. JCS has defined four terrorist threat conditions (THREATCONs) in combating terrorism. As progressive levels, they place units in increased postures of defense to reduce the vulnerability of US military personnel, their dependents, facilities, and equipment. For specific information on the THREATCONs and EOC, refer to Appendix D.

Base Defense Forces

Base defense forces are those specifically charged with the security of the base. They are under operational control of or attached to the BDOC. They include the SF, MDF, CDF, MR, and any other immediate response forces that are part

WWW.SURVIVALEBOOKS.COM

of the base defense plan. Base defense forces must—

- Detect an impending attack as soon as possible.
- Repulse or disorganize all forms of ground attack.
- Contain enemy forces that have established a lodgment in the base area.
- Repulse or destroy the enemy by counterattack.

The responsibilities of the base defense force include—

- Preparation of ground defense plans.
- Organization of defensive elements.
- Execution of security tasks.
- Execution of ground defense plans.
- Preparation and execution of local air defense plans and tasks.

A defense force commander is normally appointed by the commander of the base to supervise the preparation of ground defense plans, conduct the required training, provide for CSS, and conduct and control ground defense operations. As a special staff officer of the commander of the base, during planning he coordinates the efforts of all elements scheduled to defend the base, and during the defense, exercises operational control of them. Commanders of base elements may be given responsibility for defense training of their force or for making their forces available to the commander of the base for training. They may be given additional requirements such as—

- Procurement and storage of essential supplies.
- Construction of defense installations.
- Medical care.
- Communication assistance.

If a terrorist situation develops, special considerations, tactics, and coordination are necessary. Given the unique threat that terrorism poses and the worldwide attention it brings, US forces require specific handling, For specific information, see Appendix D.

SCREENING AND MAIN DEFENSE FORCES

The defense force commander normally exercises decentralized operational control of the SF and the MDF. Doing so permits SF and MDF leaders to exercise their own command and control in their sectors to carry out their missions. The SF and the MDF in sector are task-organized to meet the needs of the mission and generally operate semiautonomously by engaging the enemy with available firepower and reasonable tactics. In-depth coordination and control measures are essential, however, to ensure that adjacent elements do not receive friendly fires. Depending on the situation and ROE, each subelement of the SF and the MDF can engage the enemy without prior permission of the defense force commander. The subelement must make an immediate report of the engagement.

CLOSE DEFENSE FORCES

The defense force commander exercises operational control of the CDFs during operations, thus ensuring they can respond quickly, efficiently, and effectively to enemy attacks but avoid firing on the SF, the MDF, and the MR.

MOBILE RESERVE

The defense force commander should exercise centralized operational control and decentralized execution of the MR. The commander keeps close control over when and where the MR deploys, preventing premature use of the reserve caused by an enemy feint. Once the MR is deployed to its designated sector, it is free to engage enemy forces within that sector without prior approval from the defense force commander. Such decentralized execution allows the MR force leader to use proper tactics to defeat the enemy.

Naval Forces

Naval local defense forces are comprised of units having local naval tasks in base defense. These tasks include harbor defense, offshore patrolling, explosive ordnance disposal (EOD), search and rescue operations, and additional tasks as required. Navy security forces, mobile construction battalions (Seabees), and administrative, maintenance, and supply units and personnel are expected to perform ground defense force duties. Certain related operations affecting base defense such as strike force operations, submarine and antisubmarine activities, and the control and protection of shipping are normally outside the responsibility of the commander of the base and are not usually directly connected with local naval defense operations. However, the commander of the base may be authorized to employ such elements in emergencies.

Air Forces

Air force elements stationed in the base area could augment base defenses. Security police, supply and maintenance units, and personnel stationed on the base can also augment base

WWW.SURVIVALEBOOKS.COM

defenses. USAF security police normally act as part of the CDF. As such, they have primary responsibility for providing entry control, boundary sentries, and security response forces in and around USAF resources.

Disaster Control Forces

Disaster control consists of measures taken to minimize the effects of damage caused by hostile action. The disaster control forces include—

- Fire fighting units.
- NBC defensive units.
- Engineer units.
- Medical units.[4]
- EOD units.
- Other units capable of satisfying disaster control requirements.

Further, all units initiate passive defensive measures such as the employment of shelters, dispersion, camouflage, and blackout. These same units can help minimize the effects of damage caused by natural disasters.

Base Service Forces

Base service forces support the active defense. They furnish food, water, ammunition, and other supplies of common demand. The major elements of the industrial and maintenance forces are assigned to the ground defense force. Storage points should be hardened and guarded depending on the threat.

Base Engineer Forces

Base engineer forces consist of construction units and civilian engineer operations. These forces perform construction and destruction tasks, prepare the base demolition plan, and supervise the installation of demolitions. Their support in building firing positions and clearing fields of fire saves critical time for the defense force.

Civil Affairs Authorities

Civil affairs includes all interactions between the military and civil authorities or people in the area. Such interactions may range from military-civic action projects to the exercise of authority that normally belongs to the local government (see Chapter 5). PSYOP assets and units may augment civil affairs personnel.

[4] In the defense, medical personnel should protect their patients, themselves, and the medical facilities and provide medical support to defense forces.

Host-Nation Forces

Diplomatic agreements between the US and HNs determine whether HN forces will support the defense. They may be totally integrated in the base defense force or in any part of the defense. They may have total authority and man the SF, MDF, or MR. They could be responsible for the perimeter with US forces sharing control of internal security.

The relationships and authority that the commander of the joint base has with HN forces are decided at the NCA level. For a totally integrated security plan, the commander of the base must coordinate closely with the HN.

The HN is responsible for responding to terrorist activities. Status-of-forces agreements, however, may grant to US forces the right-not the responsibility—to do anything necessary to maintain order and security on the base. US response procedures to terrorist activity on the base are set up according to US and HN law and status-of-forces agreements and in coordination with HN governmental agencies.

Psychological Operations Forces

Defenders must plan and coordinate PSYOP with appropriate US diplomatic mission and HN personnel to ensure a unified approach to our tactical and strategic objectives, PSYOP missions include—

- Developing campaigns to provide positive explanation of the goodwill intent of ongoing US activities.
- Providing assistance to HNs to gain the support of their people through various local programs and incentives.
- Identifying local sensitivities to US occupation activities; identifying local key leaders, tribes, clans, religions, population and political groupings, and their susceptibilities to hostile or US propaganda efforts.
- Positively exploiting the temporary nature of US involvement and maximizing publicity of plans for and execution of US rapid withdrawal of forces.
- Projecting an image of the US as a neutral third party between hostile groups during peacekeeping operations.

Transient Forces

Transient forces, or other forces not a part of the base command, may be assigned to the operational control of the commander of the base for emergency defense. These forces may be assigned missions using their organic capability;

WWW.SURVIVALEBOOKS.COM

they may be assigned as elements of the ground defense force. The authority, mutual responsibility, and command relationships for using such forces during an attack or under threat of an attack are covered in JCS Publication 0-2.

Adjacent Bases and Base Clusters

A totally integrated security plan requires all bases and base clusters in an area to coordinate their defense efforts. Area commanders will normally establish command and control for bases within their area. Liaison between bases and base clusters will be essential in developing an overall security plan.

Tactical Combat Forces

TCFs will normally assume OPCON of any forces outside the base perimeter in sustained combat operations against Level II and III threats. Once the threat has been defeated, base defense forces revert to base control.

A TCF near a base maybe used for base defense even if the threat is only Level I. Normally it would be given a separate AO, such as the SFA or sector, and retain control of its own forces. Close coordination and integration of the TCF's C^3I system would have to take place with the BDOC. The base and TCF headquarters must exchange liaison personnel and set up direct communications links. They must also coordinate the TCF's movement in and out of the base defense structure to ensure continuity of security.

SECTION II

Legal Constraints

Treaties agreements, and national interests determine relationships-and support among allies and friendly nations and provide a basis for specific ROE issued by competent military authority. ROE must be clearly stated and disseminated to all US forces.

Commanders at all levels must be very concerned about the legal aspects of base defense. Three types of law relevant to base defense are international agreements, US law, and HN law. Together, these laws regulate the status and activities of the forces in all levels of conflict. Should legal questions arise, defenders should consult the staff judge advocate or other official legal advisor.

INTERNATIONAL AGREEMENTS

International agreements are the most important source of rules of international law applicable to US, allied, and HN forces. They prescribe most of the reciprocal rights, powers, duties, privileges, and immunities of the US forces stationed abroad and of the governments of the host and allied nations and their respective armed forces. They also regulate, to some extent, the relationship between the opposing parties in internal conflicts.

The four relevant types of agreements are those concerning the law of war, SAO agreements, stationing agreements, and HN support agreements. US armed forces are committed to conducting foreign internal defense operations according to the applicable provisions of the law of war, including those of the Geneva Convention of 1949 and others set forth in FM 27-10 and DA Pam 27-1.[5]

UNITED STATES LAWS

US forces in an HN follow US law as expressed in statutes, executive orders, DOD directives and instructions, military regulations, and directives issued by the unified command and by the separate component commands subject to applicable status-of-forces agreements (SOFAs). US domestic law regulates such areas as military justice, control of public funds, procurement of supplies, and disposition of property. Copies of

[5] *Legal Guide for Commanders; Treaties Governing Land Warfare.*

WWW.SURVIVALEBOOKS.COM

publications containing applicable US laws and SOFA should be on file at the headquarters of the SAO in the HN or with the command judge advocate.

HOST-NATION LAWS

HN laws control the conduct of counterinsurgency operations. Such laws emanate from the various levels of government and from the agencies functioning at each echelon. US advisors, commanders, and staff officers must understand these critical HN laws and responsibilities. Other HN laws that apply include those governing—

- The use of labor.
- Currency.
- Foreign exchange transactions.
- Separation of powers.
- Local purchases.
- Judicial procedures.
- Control of the populace and resources.
- Emergency legislation.

The command must adhere to and publicize appropriate agreements between the US and the HN. Detailed guidance on HN law is normally available from the local US consul, a legal advisor or local attorney employed by the US diplomatic mission, or judge advocate. The laws of a sovereign HN apply to all US forces stationed in that country unless modified by international or bilateral agreements.

LAWS OF WAR

Treatment of Belligerents

During a conventional war, the treatment of belligerents is governed by the laws of war and relevant HN and US domestic laws. Enemy personnel acting in accordance with the laws of war will be accorded prisoner-of-war (PW) status and afforded all the considerations thereof.

Treatment of Insurgents

Insurgency occurs within a particular state when people band together to displace the established government by force. Under international laws, another country is not permitted to assist the insurgents inside the threatened country's territory.

For insurgents held in US military custody during counterinsurgency operations, US policy requires and directs humane care and treatment from the moment they are detained until they are released or repatriated. This policy is fully and equally binding upon US personnel whether serving as the capturing troops, as the custodial personnel, or in some other capacity.

This policy also applies to all detained or interned personnel. It applies whether they are known or suspected to have committed acts of espionage, sabotage, terrorism, or other war crimes. Their punishment is adjudicated and administered only under due process of law and by legally constituted authority. Inhumane treatment, even under stress of combat and with deep provocation, is a serious and punishable violation under international law and the *US Uniform Code of Military Justice.*

In combating an insurgency, defenders must accord humane treatment to any civilians involved and scrupulously observe the laws to demonstrate government concern for individuals. Improper treatment of these people serves the enemy's cause. For conditions that may suggest a potential for politically motivated violence, see Appendix D.

Treatment of Prisoners

The treatment of PWs is outlined in the 1949 Geneva Convention. However, PW status is granted to insurgents on a case-by-case basis. The status of prisoners and the interpretation of the law will be made in close coordination with legal advisors. Should PW status be accorded captured personnel, Article III of the 1949 Geneva Convention protects them by prohibiting—

- Violence to life and person, in particular, murder of all kinds, mutilation, cruel treatment, and torture.
- Hostage-taking.
- Outrages upon personal dignity, in particular, humiliating and degrading treatment.
- Sentences and executions without previous judgment pronounced by a regularly constituted court that affords all the judicial guarantees considered indispensable by civilized peoples.

RULES OF ENGAGEMENT

ROE are directives issued by competent military authority. They delineate the circumstances and limitations under which US forces may initiate or continue combat engagement with other forces encountered (JCS Pub 1-02). Theater commanders establish ROE in coordination with US Department of State representatives. ROE must conform to HN laws concerning defense of others, self-defense, and protection of military facilities.

WWW.SURVIVALEBOOKS.COM

CHAPTER 4

INTELLIGENCE AND COMMUNICATIONS

Intelligence is the cornerstone for base defense in any theater. Communications, and the numerous challenges it involves, is also fundamental to base defense.

SECTION I

Intelligence

Joint base intelligence activities are conducted in coordination with lead US agencies and HN intelligence activities. Intelligence agencies comply with federal laws, presidential executive orders, status-of-forces agreements, memorandums of understanding, and applicable US military regulations.

IPB, the primary responsibility of the intelligence organization, is a continuous process that should begin before combat operations do. IPB enables the commander of the base to determine vulnerable areas, analyze the threat, upgrade facilities and procedures, and prepare contingency plans. For a detailed discussion of IPB, see FMs 34-3 and 34-130.[6]

RESPONSIBILITIES

Intelligence Officer (J2 or C2)

Intelligence officers who support a deploying unit need to carefully consider the information in Figure 4-1 when developing PIRs. At theater level, intelligence officers—

- Direct, coordinate, and control all theater intelligence collection operations targeted against the threat.
- Collect, receive, process, and disseminate all-source intelligence on the threat.
- Perform liaison and coordination as required with national law enforcement, intelligence, and other government agencies.

Intelligence Representative

The intelligence representative on the base staff and crisis management team—

- Facilitates the flow of threat-related information.
- Normally forms the BDOC intelligence cell.
- Conducts liaison with local and HN law enforcement.
- Provides on-scene intelligence support to the commander of the base in coordination with law enforcement elements.
- Maintains contact, provides information, and receives information from higher level commands.
- Arranges and provides threat information and intelligence training to other members of the joint base and to supported units.
- Expeditiously provides locally developed information to higher commands.
- Warns the supported commander of all threats to the command.
- Provides for realistic intelligence play during periodic exercises.

Tactical Unit Intelligence Staff

In wartime, the tactical unit intelligence staff collects and processes information according to current joint doctrine.

[6] *Intelligence Analysis; Intelligence Preparation of the Battlefield.*

WWW.SURVIVALEBOOKS.COM

SUPPORT

Trained intelligence personnel provide a variety of services, including—

- Presenting threat awareness training to military personnel and their families.
- Processing information into intelligence and disseminating it to users.
- Collecting intelligence information and analyzing it in support of counterterrorist operations.
- Providing the support detailed below.

Threat Briefings

Briefings about specific regional threats make personnel aware of enemy activity in the area of assignment or travel. Such briefings prepare personnel to observe and report unusual activity and may include measures they can take to reduce their vulnerability to attack.

1. Organization, size, and composition of group.
2. Religious, political, or ethnic affiliation.
3. Recruiting methods, locations, and targets.
4. Group intelligence capabilities.
5. Important dates (religious holidays, martyrdom anniversaries).
6. Preferred tactics and operations.
7. Group skills (sniping, demolitions, disguises, forged documents, industrial sabotage, aircraft and boat operations, tunneling, underwater electronic surveillance, poisons, and contaminants).
8. Medical support availability.
9. Motivation, long-range goals, and short-range goals.
10. International and national support (moral, physical, financial).
11. Identities of group leaders, opportunists, and idealists.
12. Sources of supply and support.
13. Planning competence.
14. Degree of discipline.
15. Willingness to kill.
16. Transportation on hand and required.
17. Freedom of access to media and skill in using it.

Figure 4-1. PIR Considerations

Translation and Interrogation

Linguists and interrogators translate important documents, interpret or participate in negotiations, and interrogate captured and detained personnel.

Use of Specialized Equipment and Collection Methods

Specialized equipment and methods of obtaining information are employed in strict compliance with federal law, US military regulations. status-of-forces agreements, and the applicable US-HN agreements. For example, when authorized, personnel may use technical surveillance countermeasures, providing the area commander with the ability to detect the activities of hostile intelligence services in the target area. The requirement for monitoring, however, must be consistent with the appropriate regulations. only service-level departments can authorize such methods.

OPERATIONS

To counter the threat, intelligence agencies collect, analyze, produce, and disseminate user-specific threat information quickly. The resources and methods used to do so divide into four disciplines: counterintelligence (CI), human intelligence (HUMINT), imagery intelligence (IMINT), and signal intelligence (SIGINT). Each provides pieces for completing an all-source intelligence picture. Integrating them with information from other civilian, military, and government agencies may produce a composite so the commander can see what is happening or what is about to happen and plan accordingly.

Collecting and Storing Information

To provide critical and timely information, the intelligence system must not only collect and process information efficiently but also organize, store, and retrieve information rapidly. Coupled with early warning, careful observation, and effective analysis, these functions enhance the intelligence officer's ability to predict the types and timing of strikes at the base.

Order-of-battle factors can be a logical starting point to guide information collection and to organize intelligence files. They include composition, disposition, strength, objectives, tactics, training, logistics, and personality.

The collection process is dynamic and constantly modified as intelligence accumulates.

WWW.SURVIVALEBOOKS.COM

As intelligence improves in depth and detail, collection management efforts are refined in focus and orientation, files are constantly reviewed and updated, and information is quickly disseminated to users.

Exchanging Information

Intelligence activities are a team effort. For instance, many US federal agencies actively involved in combating terrorism are sources for technical support, evaluation, and shared information. Controlled liaison with civilian and HN police and intelligence agencies is essential to exchange information, prevent duplication of effort, and reduce the likelihood of compromising ongoing collection efforts. Air defense units, air recon assets, the provost marshal, and security police also have intelligence-gathering capabilities. The intelligence section at the BDOC must establish close and constant liaison with these and other activities to develop the most accurate intelligence information possible for base defense.

CRIMINAL INFORMATION

Civilian and military agencies maintain information on known criminal incidents in their jurisdictions. This data is of vital interest to military intelligence. Military law enforcement, criminal investigators, military intelligence, and civilian police agencies must coordinate with one another. Outside the US, the first three elements conduct liaison with HN and allied law enforcement and intelligence agencies according to status-of-forces agreements. The local commander must be briefed about any exchange of information and intelligence.

OPEN-SOURCE INFORMATION

The news media maintains the world's most extensive information collection system. Relevant threat-related open-source material is disseminated through intelligence channels to the theater J2 or C2 and appropriate law enforcement agencies. Personnel assigned to conduct PSYOP and civil affairs activities will routinely contact civilian personnel such as local officials, clergy, farmers, and police. These sources can often provide useful information.

LOCAL HUMAN INTELLIGENCE

Local HUMINT can be one of the most effective sources of information. Such information can come from friendly locals and those sympathetic to the US presence. Base intelligence may have to pay for such information and organize the sympathizers into a local HUMINT network. Normally, such networks have a few key local figures who recruit other sympathizers, developing a system to gather local information in support of base intelligence efforts. These efforts must be in line with theater level J2 or C2 intelligence collection operations which reimburse and ultimately approve them.

SECTION II

Communications

Base communications is similar to that of any fixed administrative unit of equal size and scope. It involves centralized communication agencies that furnish services for all users from available resources. Some tactical communications, such as those for offshore or aviation patrols, may operate through or in conjunction with the base operational communication system. Other tactical communications should not be integrated into the base communication system, although physical facilities may collocate with base communications.

Communications for joint base defense presents numerous challenges such as the inability to net different service radios and a lack of secure radios which must be resolved. The BDOC, as the central point for base defense C^2, is normally the hub for the base defense communications system. See Figure 4-2 for a sample BDOC communications net.

WWW.SURVIVALEBOOKS.COM

PLANNING AND CONSTRUCTION CONSIDERATIONS

Defenders must plan, coordinate, and construct fixed-base communications facilities to not only provide for base defense communications but also for other necessary communications. Considerations include—

- Organization and integration of communications capabilities and resources.
- Compatibility of equipment and systems.
- Selection and preparation of locations for communication installations and facilities, including hardening plans for communication survivability.
- Determination of sources and types of communication augmentation available to base defense forces.
- Coordination and control of air support operations and communications requirements among controlling agencies.
- Communication systems and responsibilities pertaining to defense sectors, areas, and mobile defense plans; command and communication responsibilities for counter-terrorist actions.
- Ability to operate in an electronic countermeasure (ECM) environment.
- Frequency management to coordinate HN and augmented forces.
- Secure voice communications.
- Communications links to the country team and US federal agencies.
- Entry to the defense communications system, when necessary.
- Development of communication-electronic operation instructions (CEOI) by the theater commander responsible for each base, to include all units committed to base defense, tenants units, and sufficient spare CEOIs to facilitate an ingress and egress of transient units during a fluid situation.
- Coordination and exchange of communications information with HN, TCF, and transient units.

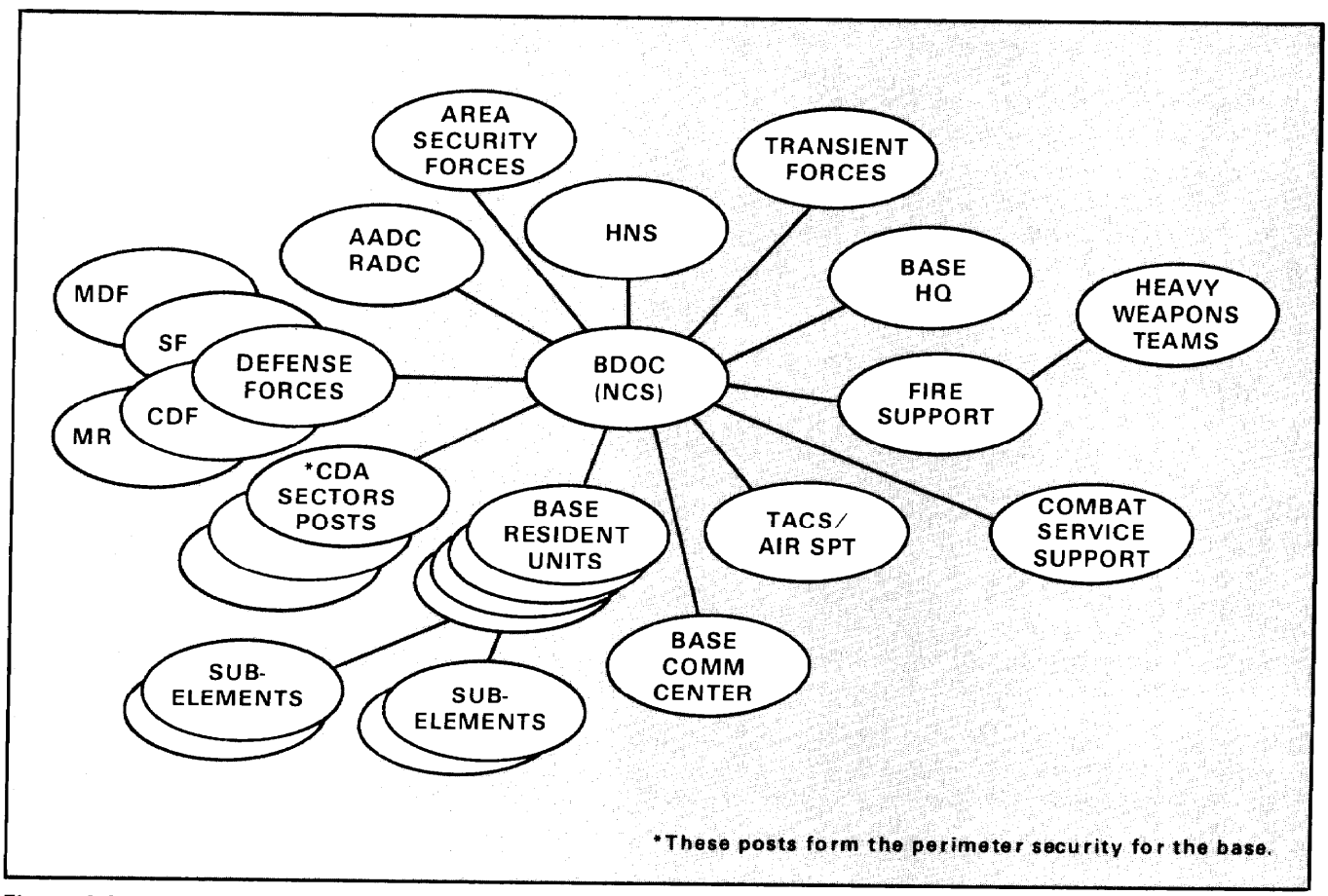


Figure 4-2. Sample BDOC Communications Net

WWW.SURVIVALEBOOKS.COM

CAPABILITIES

Plans provide for using base communications facilities to the maximum extent practicable. Plans also set up any alternate means of communication and cover their maintenance and use.

Augmentation forces will rarely have the personnel or equipment for their tactical communications. Normally, the base communications officer or J6 is responsible for meeting these needs.

The base defense communications system should be extended and improved to the maximum capability of the personnel and materiel available. The success of communications will reflect the effort expended between the initiation of communications planning and the onset of hostile activity.

The primary carrier of internal communications is wire. Wire lines should be laid to primary and alternate defensive positions. A duress signal system, such as a buzzer or alarm, should be installed among all posts and linked to the next higher command post to give instantaneous notice of attack. The base should have a loudspeaker or siren system to notify all personnel of ground, air, or NBC attack. The base should use different signals for air and ground attacks so that personnel can differentiate between the two and know how to respond.

WWW.SURVIVALEBOOKS.COM

CHAPTER 5

HOST-NATION SUPPORT

HNS is normally based on agreements that commit the HN to provide specific support in prescribed conditions. Agreements occur at various levels: nation, component command, major command, service, and unit. Although formal agreements are the preferred means of obtaining and documenting HNS, they are not absolutely necessary. Overall, HNS will depend on the situation. For example, US bases could be located in countries whose governments fully support US policies. In other cases, the HN may show little interest in commiting forces to meet the threat.

In the vast majority of cases, US bases locate in friendly HNs. Treaties, agreements, or any of the four LIC missions could be the reasons for US involvement. US bases may also locate in friendly states adjoining the AO.

Once a joint base is established, close cooperation with the HN and special considerations for its people, culture, and territory could be vital in attaining strategic US military goals. The proper use of HNS is a key in conducting joint base defense.

PLANNING FACTORS

The primary purposes of US involvement are to fulfill treaty agreements in support of US national interests. Thus, commanders must not destroy the image of HN political control. Providing HNS gives credibility to the HN and enhances the abilities of US forces to perform their missions. HNS can reduce requirements for US personnel, materiel, and services, allowing flexibility in assigning forces to other missions or other theaters. Diplomatic agreements, political situations, or the mission itself may restrict the number of US military personnel allowed at a joint base. In such a case, HNS would be necessary to supplement US security forces. US forces should expect HNS where the HN has total sovereignty, for example, within the communications zone (COMMZ) during wartime.

Factors to evaluate or consider in determining whether to use HNS for specific missions and functions include—

- Capability, dependability, and willingness of the HN to provide and sustain resources.
- Shortfalls in US forces supplemented by HNS and reductions in US forces made possible by using HNS.
- Effects of HNS on the morale of US soldiers.
- Effects of HNS on the political structure within the HN.
- Reliability of support and effects on security, including OPSEC. US intelligence and security personnel, in conjunction with HN authorities, must develop a system to check the background and loyalty of HN personnel employed on the base. Qualified personnel to inspect for quality and to ensure that goods have not been tampered with may be required.
- HN agreements and treaties that specify US involvement in the AO.
- Capability of US forces to accept and manage HNS.
- Availability of HNS in the type and quantity agreed even if the level of threat should change.

FACILITIES AND SYSTEMS

HN government agencies build, operate, and maintain facilities and systems, such as utilities and telephone networks, and provide their services in support of US forces. Police, fire companies, and border patrols may be available to support US forces.

WWW.SURVIVALEBOOKS.COM

US forces use HN facilities for hospitals, headquarters, billets, and maintenance shops. The facilities may be owned by the HN, controlled by the HN, or provided by a contract.

SUPPLIES, SERVICES, AND EQUIPMENT

Bases may acquire supplies and services such as laundry, bath, bakery, transportation from US, HN, or third-country contractors. Located in the theater, such contractors use HN or third-country personnel.

Bases need such support personnel as laborers, stevedores, truck drivers, supply handlers, equipment operators, mechanics, linguists, medical aides, computer operators, and highly skilled managers. Many will be available from the HN labor pool. OPSEC certification for such workers should be coordinated and prescribed in nation-to-nation status-of-forces agreements. HN military or paramilitary units support US forces with functions such as traffic control, convoy escort, base security, and cargo and troop transport.

HNS may be for a special function in a designated area or for particular organizations within national boundaries. Rail operations, convoy scheduling, air traffic control, and harbor pilot services are examples. Certain services may come under host-government control by authority of national power acts. To avoid shipping supplies and equipment from the US, bases may acquire them locally.

COMMAND AND CONTROL

US and HN personnel command their respective units and normally work in cooperation with but not under OPCON of each other. However, OPCON relationships between US and HN commanders may occur when appropriate agreements are negotiated to address specific circumstances.

The degree of command and control that US forces exercise over HNS depends on the type of HNS involved; the location, tactical situation, and political environment; and any agreements. Personnel who know the languages provide the interface between US and HNS elements. Implementing plans must include request procedures and legal restrictions imposed by the HN.

The US coordinates its control of HN resources through local officials, when possible, and defines control through treaties or HNS agreements. Civil affairs personnel nurture this civil-military cooperation by providing an interface with HN authorities or military forces.

Depending on the agreements, the HN may provide both exterior and interior security to US bases or share the responsibility for base security with US forces. Such situations require close coordination, common communications, and a credible base defense plan.

NBC DEFENSE

When required, HN military, paramilitary, and civilians and third-country civilians providing support are equipped and trained to operate in an NBC environment. Provisions for training and equipping are negotiated rather than unilaterally imposed by US forces.

TRAINING

US personnel at all levels should be trained in HNS functions. All of them should get orientations on HN government regulations, business practices, social customs, and military procedures. Proficiency in the HN language is vital to coordinating HNS. Defenders should integrate HNS into training exercises whenever possible.

INTELLIGENCE

Friendly nations normally operate separate intelligence systems in support of their own police and military forces. However, the products of national collection that affect operations should be shared (within limits of national security), and early coordination of the intelligence operations of allies should be assured. Specific provisions for combined intelligence operations and the use of national systems are generally arranged at the highest levels.

For operational and tactical purposes, defenders must arrange to disseminate military intelligence rapidly and to make intelligence assets available to all partners in the operation. Doing so usually requires—

- Formatting a combined intelligence staff at theater level.
- Establishing an intelligence network with dedicated communications and liaison officers to link allied headquarters.
- Assigning tactical intelligence units throughout the force so as to optimize their use.

WWW.SURVIVALEBOOKS.COM

Technical intelligence collectors such as drones, direction finders, radars, and EW assets of the partners will differ. The combined intelligence staff should consider their capabilities and, if advantageous, distribute them throughout the force to ensure the command's full potential for intelligence collection. HNS will be particularly vital for data collection from the HN's own HUMINT sources.

Commanders of joint bases must ensure that the intelligence sections link closely to the theater intelligence staff and to local HN assets such as police and paramilitary units. Current and accurate intelligence from those sources helps provide the best base security against the threat.

PSYOP forces can identify—

- Key local leaders.
- Significant tribes, clans, and religions.
- Important local sensitivities.

PSYOP can develop and conduct information and education programs to project a positive image to HN citizens as to why US forces are in the area. In so doing, PSYOP forces can collect intelligence while in contact with the local populace.

CIVIL AFFAIRS

Commanders at all levels can expect to be involved in civil affairs (CA) operations. These include any activity involving relationships between the military forces and HN civil authorities or local population. Activities may range from a military civic action project to the exercise of authority normally belonging to the local government.

The type of local government and the legal basis for US presence influence the scope of CA operations as do the economic, social, and political background of the country and people.

CA personnel monitor and assist efforts of PSYOP, engineer, medical, logistics, MP or SP forces, base defense forces, and administrative elements as these elements work—

- To restore stability.
- To coordinate security operations.
- To contribute to national development.
- To promote support for the government.

CA efforts coordinate closely with and directly support civilian efforts. They supplement civilian efforts with activities such as construction in remote areas and extension of the lines of communications (LOCs).

CA operations require good relationships with the population. Troop discipline, courtesy, and honesty are essential to good relationships. In third world countries, US soldiers want to hand out food or money, especially to children. An organized CA program should do this, not individual soldiers. Indiscriminate giving can interfere with operations and harm relations with the host government. Where sound rapport has been established between HN forces and the population, properly administered CA operations will materially enhance base security. PSYOP assets such as loudspeakers and media production facilities can assist in actively promoting CA programs.

PUBLIC AFFAIRS

Public affairs (PA) are closely linked to civil affairs. PA are not directly relevant to base defense, but they are very important in all operations because of their effects on public opinion.

US adversaries seek to exploit public opinion via news media. When they succeed, their results may far exceed their investment in time, resources, and personnel. They use propaganda and disinformation to intimidate and dishearten those they attack. They try to shape public opinion to oppose the national policies that they oppose. Because a fixed US base can attract a lot of publicity, the commander has to be particularly concerned about PA.

Responsibilities

COMMANDERS

Commanders are directly responsible for PA and often seek counsel from the public affairs officer (PAO). A member of the personal staff, the PAO has direct access to the commander. The commander should include the PAO in all planning. The commander and his staff should be readily available for media queries and interviews whenever such requests do not infringe on the mission, security, or safety. When they deal with the news media, all members of the command should be friendly and professional, not adversarial.

PUBLIC AFFAIRS OFFICER

PAOs counsel commanders and staff on the positive or negative impact of actions proposed to carry out the mission. In LIC environments, they

WWW.SURVIVALEBOOKS.COM

assess the capacity of the insurgent or terrorist to exploit situations through news media and propaganda. Where such exploitation already exists, PAOs advise commanders and staff on the best way to counter it, PAOs plan flexible internal, external, and community relations programs that support the mission in a dynamic threat environment. PAOs advise commanders and staff on PA-related matters across a wide range of possible threats and disasters.

STAFF

The staff must coordinate with the PAO on all significant matters that may impact on internal or external policies. Along with other key staff members, thePAO should be notified of serious incidents and casualities.

Considerations

High levels of insurgent or terrorist activity may justify requests for augmenting public affairs at a higher level than normally provided by tables of organization.

Before their units deploy, PAOs may need briefings on extremely sensitive missions by special staffs at Departments of the Army, Navy, and Air Force; Headquarters, Marine Corps (HQMC); and Department of Defense (DOD).

All news media contact and requests for interviews or information should be routed through the PAO. Responses to media queries should be accurate and timely. They should be staffed through appropriate staff sections. Certain information may be delayed or withheld only for security reasons, accuracy, propriety, or policy.

The advance party should contact the host-country team at the American embassy or consulate to determine local sensitivities and political concerns. The host-country team should help evaluate proposed civic action and community relations projects.

HN media should be categorized by political religious, and ethnic beliefs.

PAOs must consider these beliefs when granting access or agreeing to interviews.

A joint information bureau may improve dissemination and simplify news media control. The prevailing situation should determine bureau location and staffing. In no instance should the bureau be adjacent to the BDOC. When circumstances permit, a joint information bureau annex may be located near media concentrations and away from tactical units in order to reduce unit profile and accessibility.

Base personnel should always escort news media and control their access sensibly and tactfully. Media visits are opportunities—

- To support the unit's mission.
- To increase public awareness and support.
- To thwart terrorist initiatives and propaganda.

Being forthright, open, and ethical is the best way to establish credibility with the public while countering insurgent or terrorist propaganda.

Defenders redeploying to a familiar area should make every effort to exploit previous contacts between members of the command and friendly media and community leaders.

The commander's priority of public affairs concerns should be as follows:

- National security.
- Mission.
- Unit safety.
- Internal and external information (public's right to know).
- Countering propaganda and disinformation.
- Community relations and civic action.

WWW.SURVIVALEBOOKS.COM

APPENDIX A

SAMPLE BASE DEFENSE PLAN

(In Joint Operations Order [OPORD] Format)

SECURITY CLASSIFICATION

Copy No. _____
Issuing Headquarters
Place of Issue (may be in code)
Date/time group of signature
Message Reference Number

Type and Serial Number of Operations Order.

References: a. Maps or Charts.

b. Time Zone of Referenced Documents. (Insert the time zone used throughout the order.)

Task Organization. (List this information here or in paragraph 3. Under this heading, as appropriate, give the subdivision of the force, including attached units, together with the names and ranks of the commanders.)

1. ( ) Situation. (Under the following headings, briefly state the general objective so that the subordinate commanders will understand the current situation.)

a. ( ) Enemy Forces. (Give the composition, disposition, location, movements, estimated strengths, identification and capabilities, to include terrorist organizations.)

b. ( ) Friendly Forces. (List information on friendly forces, other than those covered by the operation order, which may directly affect the action of subordinate commanders, for example, MP and SP, medical, engineer, NBC decontamination units, EOD, or HN.)

c. ( ) Attachments and Detachments. (When not listed under Task Organization, list units attached to or detached from the issuing units, by this order, together with the times they are effective.)

2. ( ) Mission. (Give a clear, concise statement of the commander's tasks and the purpose of each task.)

3. ( ) Execution. (In the first subparagraph, give a summary of the overall course of action intended. In subsequent subparagraphs, assign specific tasks to each element of the command that executes tactical duties. Give details of coordination and the task organization and grouping, if not already included under the heading Task Organization. Place instructions that apply to two

CLASSIFICATION

SAMPLE

WWW.SURVIVALEBOOKS.COM

or more elements of the command in a final subparagraph headed Coordinating Instructions.)

a. ( ) Concept of Operation. (Briefly describe how the commander believes the overall operation should progress. Define the areas, buildings, and other structures considered critical and establish priorities for their protection.)

(1) ( ) (Set forth the phases of the operation as they are anticipated from the commander's decision.)

(2) ( ) (Describe schemes of maneuver for major subordinate task elements. State precisely what the commander expects to be done both in defense and in a counterattack (SFA, MDA, and MR forces). Work priorities may also be listed here.)

(3) ( ) (State general plans for employing supporting fire and weapons (mortars and other indirect fire systems, antiarmor weapons, aviation assets).

b. ( ) Defense Force. (In this and subsequent subparagraphs of paragraph 3, assign specific tasks to each element of the command.)

c. ( ) Remainder of Forces. (List as shown in the Task Organization.)

d. ( ) Reserve or Transient Forces. (List instructions to any reserve or transient forces in the next to last subparagraph of paragraph 3.)

e. ( ) Coordinating Instructions.

(1) ( ) Control Measures. (Define and establish restrictions on access to and movement into critical areas. These restrictions can be categorized as personnel, material, and vehicles. Security measures may also be outlined here.)

(a) ( ) Personnel access. (Establish control pertinent to each area or structure.)

1 ( ) Authority. (Give authority for access.)

2 ( ) Criteria. (Give access criteria for unit personnel, visitors, maintenance or support personnel, contractor personnel, and local police and armed forces.)

3 ( ) Identification and control.

a ( ) (Describe the system to be used in each area. If a badge system is used, give a complete description to disseminate requirements for identification and control of personnel who conduct business on the base.)

SAMPLE

WWW.SURVIVALEBOOKS.COM

b ( ) (Describe how the system applies to unit personnel, visitors to restricted or administrative areas, vendors, tradesmen, contractor personnel, and maintenance or support personnel.)

(b) ( ) Materiel Control.

1 ( ) Incoming.

a ( ) (List requirements for admission of materiel and supplies.)

b ( ) (List special controls on delivery of supplies and/or personnel shipments in restricted areas.)

2 ( ) Outgoing.

a ( ) (List required documentation.)

b ( ) (List special controls on delivery of supplies and/or personnel shipments in restricted areas, as outlined above for incoming materiel control.)

c ( ) (List classified shipments.)

(c) ( ) Vehicle control.

1 ( ) (State policy on registration of vehicles.)

2 ( ) (State policy on search of military and privately owned vehicles.)

3 ( ) (State policy on parking.)

4 ( ) (State policy on cases of suspected abandoned vehicles.)

5 ( ) (List the controls for entering restricted and administrative areas.)

a ( ) Privately owned vehicles.

b ( ) Military vehicles

c ( ) Emergency vehicles.

(2) ( ) Security Aids. (Indicate the manner in which the following security aids will be implemented on the base.)

SAMPLE

WWW.SURVIVALEBOOKS.COM

(a) ( ) Protective barriers.

1 ( ) Definition.

2 ( ) Clear zones.

a ( ) Criteria.

b ( ) Maintenance.

3 ( ) Signs.

a ( ) Types.

b ( ) Posting.

4 ( ) Gates.

a ( ) Hours of operation.

b ( ) Security requirements.

c ( ) Lock security.

(b) ( ) Protective lighting system.

1 ( ) Use and control.

2 ( ) Inspection.

3 ( ) Direction (points in or out).

4 ( ) Action to be taken during a commercial power failure.

5 ( ) Action to be taken during an alternate source power failure.

6 ( ) Emergency lighting systems.

a ( ) Stationary.

b ( ) Portable.

(c) ( ) Intrusion detection systems.

1 ( ) Security classification.

2 ( ) Inspection.

3 ( ) Use and monitoring.

SAMPLE

WWW.SURVIVALEBOOKS.COM

4 ( ) Action to be taken in the event of alarm conditions.

5 ( ) Maintenance.

6 ( ) Alarm logs or registers.

7 ( ) Sensitivity settings.

8 ( ) Fail-safe and tamper-proof provisions.

9 ( ) Monitor panel location.

(d) ( ) Communications.

1 ( ) Locations.

2 ( ) Use.

3 ( ) Tests.

4 ( ) Authentication.

(3) ( ) Interior Guard Procedures. (Include general instructions that apply to all interior guard personnel, fixed and mobile. Attach detailed instructions such as special orders and SOPs as annexes. Ensure randomness is incorporated in guard procedures.)

(a) ( ) Composition and organization.

(b) ( ) Tour of duty.

(c) ( ) Essential posts and routes.

(d) ( ) Weapons and equipment. (Live ammunition? Magazines in weapons? Round in chamber?)

(e) ( ) Training.

(f) ( ) Sentry and patrol dogs.

(g) ( ) Method of challenge (with sign and countersign).

(h) ( ) Alert force.

1 ( ) Composition.

2 ( ) Mission.

3 ( ) Weapons and equipment.

SAMPLE

WWW.SURVIVALEBOOKS.COM

4 ( ) Location.

5 ( ) Deployment concept.

(4) ( ) Rules of Engagement.

(5) ( ) Contingency Plans. (Indicate actions in response to various emergency situations. List as annexes any detailed plans, such as combating terrorism, responding to bomb threats, negotiating hostage situations, dealing with disasters, and responding to fire.)

(a) ( ) Individual actions.

(b) ( ) Alert force actions.

(c) ( ) Security alert status.

(6) ( ) Security Alert Status.

(7) ( ) Air Surveillance.

(8) ( ) Noncombatant Emergency Evacuation Plan.

(9) ( ) Integration with host-nation plans or nearby military base plans (liaison and coordination.)

(a) ( ) Local civil authorities.

(b) ( ) Federal agencies.

(c) ( ) Military organizations.

(10) ( ) Operation plan (OPLAN) Examination Dates. (Give tentative dates for OPLAN examination in this subparagraph. In the case of an order that is not effective on receipt, indicate the date and time the order will become effective.)

SAMPLE

4. ( ) Administration and Logistics. (State the administrative and logistical arrangements applicable to the operation. If the arrangements are lengthy or not ready for inclusion in the operation order, issue them separately and reference them here. This paragraph sets forth the manner of logistics support for the base defense plan. Include enough information in the body of the order to make clear the basic concept for logistics support. Include the subparagraphs below.)

a. ( ) Concept of Combat Service Support. (Include a brief summary of the overall operation from the combat service support point of view. In some cases, you may only have to include this subparagraph and a reference to the logistics and personnel annex. Area damage control and NBC considerations may also be listed here.)

WWW.SURVIVALEBOOKS.COM

b. ( ) Materiel and Services. (List supply, maintenance, transportation, construction, and allocation of labor for logistics purposes.)

c. ( ) Medical Services. (List plans and policies for hospitalization and evacuation of both military and civilian personnel.)

d. ( ) Personnel. (List unit strengths, replacements, and personnel policies and procedures, including those pertaining to civilians and prisoners of war. Brief all personnel on economic and political impact of US presence in the country. Brief information on exchanging US dollars into military script and local currency.)

e. ( ) Civil Affairs. (Describe control of civil populations, refugees, and related matters.)

f. ( ) Miscellaneous.

5. ( ) Command and Signal. (Give signal recognition and identification instructions, electronic policy, headquarters locations and movements, code words, code names, liaison, and acknowledgement instructions.)

a. ( ) Command, Control, and Communications. (Give information about pertinent command, control, and communications nets, operating procedures, recognition and identification procedures, electronic emission constraints, and so on. A separate annex may be required.)

b. ( ) Command.

(1) ( ) Joint and combined operations. (Joint and combined operations, by their nature, have complex command relationships. Joint and combined operation orders must be specific concerning such relationships, including shifts that may take place as the operation progresses from one phase to another. Detail command relationships out in chart form and include them as an annex to the operation order.)

(2) ( ) Command posts and alternate command posts. (List command posts and alternate command posts, along with their times of activation and deactivation, in this paragraph.)

6. ( ) Acknowledgement Instructions. (Normally, the word acknowledge is sufficient to indicate that the recipient is to acknowledge receipt and understanding of the order by sending the message reference number in the heading back to the originator. If other measures are to be used, prescribe them here.)

(Signed) _____

WWW.SURVIVALEBOOKS.COM

Commander

ANNEXES:

A - Intelligence

B - Base Security Status Map and Area Commander Map

C - Contingency Plans

D - Interior Guard

E - Screening Force

F - Main Defense Force

G - Close Defense Force

H - Air Defense Plan

I - Area Damage Control Plan

J - Disaster Preparedness Plan

K - Mines and Obstacles Plan

L - Fire Support Plan

M - NBC Plan

N - General Base Information (see sample annex)

O - Rules of Engagement (if not complete in coordinating instructions subparagraph)

P - Combating Terrorism Plan

Q - Alert Notification Plan

DISTRIBUTION: (By policy and procedures of the issuing headquarters.)

AUTHENTICATION: (According to local staff practice, normally the J3 or 5.)

SAMPLE

WWW.SURVIVALEBOOKS.COM

Annex N

General Base Information
(Sample)

Base Information to OPORD: _____

Base: _____ Date: _____

Commander of the Base: _____

Units Within Base	POC	Switchboard and Number
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

BDOC Location: _____

Telephone Number: _____

Defensive Responsibilities of Each Unit:

Unit	Sector (Use Hours of Clock, 1200 is N)
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

SAMPLE

WWW.SURVIVALEBOOKS.COM

Additional Base Defense Forces: (Composed of Base Assets)

	Members	Unit	Weapon
OIC or NCOIC:	_____	_____	_____
	_____	_____	_____
	_____	_____	_____
	_____	_____	_____
	_____	_____	_____

Assembly Area: _____

Signal for Assembly: _____

Date Base Defense Drill Was Last Tested: _____

Crew-Served Fighting Positions Assigned:

Position	Personnel	Weapon	Range Card*	
_____	_____	_____	Y	N
_____	_____	_____	Y	N
_____	_____	_____	Y	N
_____	_____	_____	Y	N
_____	_____	_____	Y	N
_____	_____	_____	Y	N

*Range cards included as Enclosure 2.

SAMPLE

MP, SP, Tenant Unit Response Forces:

MP, SP, Tenant Unit Company, Platoon, Fleet Which Will Provide Response Forces: _____

POC: _____

Switchboard Designator or Number: _____

Location: _____

Last Coordination Made: _____

WWW.SURVIVALEBOOKS.COM

Barriers and Obstacles Placed:

Type	Location	Date

LP and OP Placement:

Location	When Occupied	Communications

Designated Report Times: _____

Air Defense Available Within Base:

_____

_____

_____

_____

_____

SAMPLE

WWW.SURVIVALEBOOKS.COM

ADC Response Force:

	Members	Unit	Equipment
OIC or NCOIC:			

Assembly Area: _____

Signal for Assembly: _____

Date of Last Rehearsal: _____

Medical Facilities and Evacuation:

Type of Facility	Location

Evacuation Mode	Unit	How Contacted

SAMPLE

WWW.SURVIVALEBOOKS.COM

NBC Monitoring and Decontamination Teams:

	Radiological Monitoring	Unit
OIC or NCOIC:	_____	_____
Members:	_____	_____
	_____	_____
	_____	_____

Signal and Assembly Area: _____

	Chemical Monitoring	Unit
OIC or NCOIC:	_____	_____
Members:	_____	_____
	_____	_____

Signal to Assemble: _____

Assembly Area: _____

	Decontamination Team	Unit
OIC or NCOIC:	_____	_____
Members:	_____	_____
	_____	_____
	_____	_____

Signal to Assemble: _____

Assembly Area: _____

Indirect Fire Support Assets Available Within or Close to Base:

Unit	Weapons	How Contacted	Last Coordination
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

SAMPLE

WWW.SURVIVALEBOOKS.COM

Adjacent Base Coordination:

Base Organization	Location	Last Coordination
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Host-Nation Support (Base Level):

POC	Support Available	Last Coordination
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Tactical Combat Force:

Commander or POC	Support	Last Coordination
_____	_____	_____
_____	_____	_____

Command and Signal:

CP Located: _____

Telephone Number: _____

Personnel Authorized to Act or Sign for the Commander of the Base:

_____

_____

_____

_____

SAMPLE

WWW.SURVIVALEBOOKS.COM

Signals Authorized:

Ground Attack: _____

Air Attack: _____

Chemical Attack: _____

Assemble All Additional Base Defense Force: _____

Recall Additional Base Defense Force: _____

Assemble ADC Response Force: _____

Recall ADC Response Force: _____

SAMPLE

WWW.SURVIVALEBOOKS.COM

APPENDIX B

SECURITY

This appendix provides information on how units can protect themselves from attack when they have been deployed to either an urban or suburban environment. It also includes guidance on maintaining operations security. The security measures discussed here are not all inclusive. They are included only as a reference. For more detailed guidance, commanders and staffs should refer to their individual service publications.

SECTION I

Tactical Security

Units deployed to an area of operations must be constantly aware of the threat and take protective measures to minimize the danger of attack.

PATROLS

Patrolling may be necessary outside the base to provide additional base security. The patrol's main mission may be to show US presence. Other possible tasks may include—

- Supporting police operations.
- Gathering information on local terrorist groups.
- Checking clubs and restaurants.
- Coordinating planned apprehensions with local law enforcement agencies.
- Conducting hasty searches.
- Deploying hasty roadblocks with local law enforcement agencies.

Patrolling urban areas involves different risks and considerations than patrolling open or cleared uninhabited areas. The security operation may require the use of patrol dogs. Patrol dogs are the most versatile security dogs. They are trained to assist the handler, attack on command, and track suspects. The two types of patrols are the foot patrol and the vehicle patrol.

Foot Patrols

Foot patrols are normally carried out by fire teams. Multiple teams usually remain within 100 yards of one another. Patrol members should walk with relaxed confidence and be ready to talk to locals. However, they should also be prepared to take up proper firing positions, keeping rifles constantly ready, which is known as hard targeting. Hard targeting is appropriate under the following circumstances: when crossing obstacles; when reacting to a possible enemy intrusion; when leaving or entering a static base, observation post, or area with a history of high-threat contact; and when breaking up movement patterns.

Vehicle Patrols

Vehicle patrols normally consist of two vehicles moving within sight of each other but not presenting a double target. Vehicles should travel at no more than 10-15 MPH. Vehicle crews should dismount at every stop to provide security and employ appropriate dismount tactics. In order to reduce the risk of assault, vehicle patrols should avoid establishing patterns. Defensive precautions include—

- Being particularly alert for strange people, vehicles, or incidents close to the beginning or end of the patrol route.
- Avoiding the same daily routes and times.
- Avoiding isolated routes and stops.
- Locking the doors.
- Stopping short of any unusual object or incident.
- Detouring around suspicious cars and obstacles.

WWW.SURVIVALEBOOKS.COM

- Continually checking to ensure nobody is following.
- Being aware of the vehicle's dimensions and ability to sustain damage.
- Being able to make full use of the vehicle's acceleration and turning capacity.

ROAD BLOCKS

Roadblocks may be constructed of permanent or semipermanent materials (deliberate) or rapidly out of materials at hand (hasty). Roadblocks may be used—

- To check identification.
- To obstruct passage.
- To perform spot-checks, with or without prior intelligence.
- To achieve surprise.

Sentries should be assigned to protect roadblocks. They should stop cars well short of the main search area to minimize the effects of possible car bombs. The commander should assign an appropriate number of troops to meet the threat and effectively handle the expected volume of traffic. Local police, females for searching females, interpreters, and EOD experts may also be employed. Troops protecting roadblocks must be aware of their legal authority and their duties and limitations regarding search, seizure, arrest, and use of force, Roadblocks require direct communication with the BDOC and any supporting defense forces in the area.

Roadblocks should not unnecessarily hamper the movement of civilians. Troops employed on roadblocks will enhance public relations if they know their jobs thoroughly and act quickly and methodically. They must be polite and considerate at all times and hand suspects over to the civil police quickly and efficiently. When stopping a vehicle for search at a roadblock, sentries should use the following procedure:

- Move occupants away from the vehicle and search the driver, passengers, and loose baggage. Once the personal search incomplete, hold the occupants under guard nearby within sight of the roadblock commander while searching the vehicle.
- Direct the driver to open the trunk and identify its contents. Look under and around the spare wheel, tool boxes, luggage, partitions, spare wheel housing, and spare tire (check inflation).
- Direct the driver to open the hood. Look for items taped to the bulkhead or hood. Examine all containers and look behind the sound-proofing, front grill, and heater.
- When searching the interior, be suspicious of strong odors such as perfume or deodorant.
- Check methodically. Look behind the dash, radio, and cassette fittings; look in the glove compartment; look behind panels, under floor mats, and between seats and cushions; look in open windows, in toys, and in decorative animals and ashtrays.
- When searching the exterior, look in wheel wells and fenders, behind bumpers, around headlights, and in hubcaps.
- When searching commercial vehicles, look in the following additional hiding places: driver's cab, space between body and cab, external storage bins, wooden bodies, false floors and sides, rear double wheels, and wheel chocks that can be hollowed.
- If possible, use explosive detectors or dogs to search vehicles.

URBAN DEFENSE

Base forces may be employed in urban areas for security operations or for other tasks short of conventional combat, for example, protection of facilities or equipment required for base operations. Masonry structures and other urban features can be adapted to provide protection.

Security Precautions

When employed in urban areas, commanders must estimate the threat (see Chapter 1) and plan for the defense (see Chapter 2). In addition, they should consider the following security precautions:

- Wire fences or barriers for additional protection.
- Screens made of canvas or corrugated iron for use outside buildings or inside windows. Mesh or chain-link barriers placed in front of bunkers or above ground fighting positions aid in premature detonation of rocket-propelled grenades and other similar shaped, charged explosive devices.
- Canopies of chain link, weld mesh, or corrugated iron will protect roofs if they are placed at least 1 meter above the roofs. Sandbags placed directly on roofs will absorb shrapnel.
- Obstacles in the approaches will slow or stop vehicles and personnel approaching the defended area. However, the entrance gate

WWW.SURVIVALEBOOKS.COM

design must allow access to those authorized, deny access to others, and provide protection to those who must have access. If possible, illuminate fences, entrance gates, and obstacles. Cover with observation and fire.

- Sentry posts for round-the-clock security. If field fortifications are required, dig fighting positions rather than build towers. Ordinarily, sentry posts are doubled during darkness or poor visibility. Sentries should report at irregular intervals within a specified time period and be posted at—
  - Entrances, in order to check entry permits.
  - Observation posts or rooftops, in order to observe all avenues of approach and dominate buildings and grounds.
  - Perimeter sites.

Employment of Sentries

Sentries must be properly trained and equipped. They must pay particular attention to ROE and appropriate use of force. They must always have an MR on which they can call for immediate assistance. Sentries employed in urban areas must—

- Detect and deter anyone seeking to gain unauthorized access to the secured area.
- Prevent damage, arson, and looting within the secured area.
- Ensure maintenance of essential services.
- Remain on post until properly relieved.

The duties and conduct of sentries are detailed in FM 22-6, AFR 125-3, and FMFM 6-4.[7]

Some security operations may require the use of sentry dogs. Sentry dogs are extremely aggressive and may work without a handler. They are best assigned to critical areas to prevent unauthorized penetration. (Although no longer available in DOD inventory, sentry dogs may be available as a part of HNS.)

CONVOY DEFENSE

Depending on route classification, convoys are arranged for control and protection using armored, organic vehicles and military police escort, if available. Road movement is always vulnerable in high-threat areas. The convoy commander should plan convoy movements and practice using hardened vehicles if support from other units such as infantry and armor is not available. Convoys are organized into an advance party, main body, and trail party.

The convoy commander estimates the situation and develops a plan. The plan must include a thorough predeparture briefing for all convoy members. The briefing must include—

- Composition and order of march.
- Chain of command.
- General posture.
- Communications and special signals.
- Objectives.
- Routes and schedules.
- Emergency actions and actions to be taken at halts.

Convoy orders follow a conventional six paragraph format as shown in Figure B-1.

SEARCHES

Personnel

Many times, personnel searches will be required to ensure the safety and security of operations. When performing a personnel search—

- Extend proper respect to the person detained. The aim is to provide security without creating animosities which can be exploited in the future.
- Immobilize the person detained in a position of disadvantage.
- Always work from behind the detainee.
- Employ two searchers, one to cover while the other searches.

The quick-body search, or frisk, and the detailed body search are the two types of personnel searches.

QUICK-BODY SEARCH OR FRISK

This type of search is used most often by base defenders. The quick-body search is a preliminary search to detect weapons in low threat areas. Follow the logical sequence from top to toe. If possible, use a metal detection system. Be sure to carefully check—

- Hair.
- Armpits.
- Inside legs.
- Half-clenched hands.
- Medical dressings.
- Bags or cases.
- Walking sticks, umbrellas, crutches.
- Shoes, boots.

[7] *Guard Duty; Security Police Handbook; Marine Rifle Company/Platoon.*

WWW.SURVIVALEBOOKS.COM

1. Situation.
   a. Friendly forces.
   b. Support units.
   c. Enemy situation.
2. Mission.
   a. Type of cargo.
   b. Origin.
   c. Destination.
3. Execution.
   a. General organization of convoy.
   b. Time schedule.
   c. Convoy speed.
   d. Catch-up speed.
   e. Vehicle distance.
   f. Emergency measures
      (1) Accidents.
      (2) Breakdowns.
      (3) Separation from convoy.
      (4) Ambush.
         (a) Action of convoy personnel in the event of an ambush.
         (b) Action of the security forces during ambush.
         (c) Medical support during ambush.
      (5) Air attack (include actions in (4)(a) through (c) above, plus the following):
         (a) Weapons employment procedures.
         (b) Air sentinels during the convoy.
         (c) Air attack alerting procedures.
4. Administration and Logistics.
   a. Personnel control.
   b. Billeting arrangements.
   c. Messing arrangements.
   d. Vehicle refueling.
   e. Vehicle servicing.
5. Command and Signal.
   a. Location of convoy commander.
   b. Designation of assistant convoy commander.
   c. Action of the security force commander.
   d. Responsibilities of serial commander.
   e. Use of arm and hand signals.
   f. Use of other prearranged signals.
   g. Use of radio frequencies and call signs for—
      (1) Control personnel.
      (2) Security force commander.
      (3) Fire support elements.
      (4) Reserve security elements.
      (5) Medical evacuation support.
6. Safety.
   a. Hazards of route.
   b. Weather conditions.
   c. Defensive driving.

Figure B-1. Format for Convoy Order

DETAILED BODY SEARCH

This type of body search is best left to law enforcement officials. A special room or area should be set aside. A medic and a female should be available to assist with the searches.

Buildings

Planning for search operations should include—

- The reason for the search.
- Team composition.
- Order of priority.
- Team tasking and specialist tasking.
- Damage limitation.
- Expected assistance and guards or escorts.

When preparing to search buildings, use radios (search net and command net) and call signs for teams and specialists. Use grid references for location of teams, control points, and headquarters. In addition, consider electronic countermeasure constraints.

Assume that any unoccupied house or building is booby-trapped. Visually scan the exterior for suspicious signs. Set up a command post outside and detail one pair of searchers to make the initial entry. Avoid the obvious entryways. If possible, use holes in walls or roofs as entryways. If you must use doors and windows, check for booby traps before entering. Traps can be activated in many ways. Clearly mark with white tape the routes through the building which have been cleared of traps. Once the building is cleared of traps, the team leader will make a plan and allocate pairs of searchers to make detailed room searches. Figure B-2, shown on the next page, lists common booby traps.

Explosive detector dogs can be used to search for arms, ammunition, explosive caches in buildings, vehicles, open areas, and routes to be cleared. However, dog teams do not work in buildings that have not been cleared of booby traps. Handlers must never touch materials the dogs have indicated are explosive. Figure B-3, shown on the next page, is a list of do's and don'ts for troops discovering unexploded devices or arriving at the scene of an explosion.

AMBUSHES

Like patrolling, setting ambushes demands patience, skill, and outstanding soldiering ability. Planned ambushes are primarily defensive.

WWW.SURVIVALEBOOKS.COM

Urban ambushes are intended to arrest a wanted person or persons, not to kill them. Urban ambushes are always more difficult than combat ambushes because of the concentration of civilians.

It may not be possible to site an ambush in a tactically sound position. Sites such as houses where wanted people are gathering may have to be used. Information about enemy movements is essential. Planners must know the routine movement patterns of local inhabitants and have an intimate knowledge of area terrain.

Terrorist bombings or bomb threats may be intended to draw security forces away from protected assets into an area as targets for a shooting ambush. Therefore, security forces must always be cautious.

RESPONSE TO ATTACKS

When responding to an attack from an urban area, defenders must try to kill or capture assailants while keeping the base secure. In addition, they must consider local use-of-force requirements. During immediate follow-up, they must also consider—

- Returning fire according to ROE.
- Submitting a contact report, including the location, number of casualties, and estimate of opposition.
- Dispatching a fire team to engage the opposition force.
- Estimating the civilian situation.
- Establishing roadblocks on likely escape routes.
- Deploying cordon sentries as necessary.
- Alerting local authorities.
- Recovering and aiding hostages, if necessary.
- Securing the scene for collection of evidence if you can--establish a firing point.

CROWD CONTROL

Crowd violence may be a spontaneous emotional eruption, or it may be a planned event. In the latter case, the purpose may be to draw attention away from something else or to draw people to a location where attack is easier. Crowd violence may involve civilian group interaction. Mob violence is highly contagious. The aim of riot control is to restore order as quickly as possible with a minimum of force and return control to civilian authorities as quickly as possible. HN police agencies should assume principal responsibility

- **Pull**—triggered by opening a drawer or cupboard. Use a handline to open drawers and cupboards. Then leave them open.
- **Pressure**—triggered by standing on a particular floor board or sitting in a chair. Look for loose floor boards or lumps under carpets or in chairs.
- **Release/antilift**—triggered by picking up a book or bottle. Look for attractive items in the open.
- **Tilt**—triggered by turning an object on its side to look underneath.
- **Trembler**—triggered by any vibration or movement.
- **Collapsed circuit**—triggered by cutting or breaking the circuit in an electronic device. May also be triggered by a worn-down battery.
- **Light-sensitive**—triggered by exposure to or denial of light.
- **Antisubmerge**—triggered by placing the device in water.
- **Antiprobe**—triggered by the searcher's probing.

Figure B-2. Common Booby Traps

- Establish a control point and coordinate with civil authorities.
- Clear the area of people at least 300 meters from the bomb.
- Divert traffic from the scene.
- Assemble witnesses, suspects, and home owners at the control point.
- Send for an EOD team.
- Alert fire fighters and emergency medical personnel.
- Gather as much information as possible about the situation.
- Dominate possible firing points to protect response from snipers.
- Allow no more than one person to approach the suspicious device.
- Treat the press respectfully, but keep them from the scene.
- Don't touch or approach the device.
- Don't assume that one explosion means the area is safe.
- Don't press or hurry the EOD team.
- Don't wear or permit excessive amounts of metal, including metal helmets, in the vicinity of the device.

Figure B-3. Security Procedures On Encountering Unexploded Devices

WWW.SURVIVALEBOOKS.COM

for countering actions of indigenous personnel. US forces should come into direct conflict with indigenous personnel only in emergency situations when HN police or military personnel are not present.

The best way to disperse rioters is to make key arrests and make it clear that further rioting will result in physical discomfort to lawbreakers. Leave an escape route open to allow rioters to disperse. The HN police force must assist. Once the crowd has dispersed and all is quiet, return the troops to the assembly or base area. Exert caution not to escalate the violence by misuse of force. Use of chemical agents such as tear gas for riot control must follow stated national policy and HN agreements. Close coordination with legal counsel and US diplomatic missions is vital to the successful conclusion of such hostilities.

SECTION II

Unit Security

The threat to unit security exists throughout a deployment whether personnel are on liberty, leave, or pass; in transit; on training exercises; or on operations. Commanders must include security in their guidance and deter or create an obvious risk for terrorists through effective security programs. The operations section should coordinate all security actions. The following predeployment, deployment, and redeployment considerations are relevant factors in ensuring unit security.

PREDEPLOYMENT

Fit, alert, and well-trained soldiers are the best protection against the threat in any conflict. Expand tactical thinking to include security against terrorism. Include security against insurgency and terrorism in all orders, plans, and training. The following predeployment considerations are relevant factors in implementing unit security.

Planning

Ensure all personnel are prepared for overseas movement—verify immunizations and give instruction on the appropriate preventive medicine tasks.

MISSION ANALYSIS

To perform a mission analysis, ask the following questions:

- How can the mission be adversely affected by insurgent or terrorist attack?
- What are the security aspects of both specified and implied tasks?

Continue to review unit vulnerability throughout predeployment, deployment, and redeployment (see Appendix D).

THREAT ASSESSMENT

Identify insurgent and terrorist groups operating in the deployment area. Develop a list of PIRs (see Chapter 4), to include—

- Methods of operation.
- Attack methodology.
- Preattack indicators.

Identify sources of information on insurgent and terrorist groups. Know how to access these sources quickly and routinely. Include threat assessment in intelligence estimates as a continuing process.

COMBAT SERVICE SUPPORT CONSIDERATIONS

To implement unit security, consider the CSS areas below.

Supply

Procure special security equipment such as detectors, portable barriers, and intrusion devices (see Appendix C). Protect storage and distribution areas.

WWW.SURVIVALEBOOKS.COM

Maintenance
Maintain special equipment and provide security of maintenance unit if separate from the main body.

Transportation
Provide security during movement and in staging areas and provide liaison with security agencies such as MP movement control centers.

Engineer
Provide security and ADC measures (strong points, barriers, obstacles, reinforcement, clearing construction) and special engineer equipment (see Appendix C).

Base Military or Security Police
Check, inspect, and improve unit physical security. Identifying what is wrong is not enough; doing something about it is the key. Provide liaison with local police and security personnel, a source of intelligence that must be tapped. Assist in security planning and training. Ensure all personnel know what to do and why. Screen civilian employees. Be continuously cautious of HN employees, no matter how loyal they appear to be.

Civilian Employees
If possible, avoid employing civilians. If they are employed, establish special security procedures for screening and monitoring them.

Fiscal Needs
In some environments, inconspicuous rental cars may be an operational necessity. Funding should be a planning consideration. Consider random exchanges the rental agency is not aware of. Do not take what they offer you. Randomly select from their fleet of vehicles. Also in many countries, a fee for information is expected when collecting intelligence data.

Health Services Support
Ensure security of medical facilities, secure supplies and equipment, and safeguard patients during movement.

OPERATIONAL CONSIDERATIONS
To implement unit security, consider the operational areas below.

Unit Plans
Include security in every plan and standing operating procedures (SOP), operations orders (OPORDs), movement orders.

Security Plans
Prepare and continuously review and update specific security plans such as physical security plans and individual security plans.

Programs
Develop specific security programs: threat awareness, OPSEC (see Section III of this appendix).

Special Skills
To counter the terrorist threat, special skills not normally found in the unit may be required: linguists, foreign area specialists, EOD specialists, and PA specialists. Some of these will need to be included in advanced parties. See Figure D-9.

Special Teams
The terrorist threat may require a task organization that would not normally be considered (search teams, special reaction teams, protective service teams). See Figure D-10.

Command Relationships
Command relationships (State Department, host nation, country team) may differ from the routine relationships. Command relationships between the advance party and other agencies need to be resolved before deployment.

Training

Consider the following training:

- Institutional training (specialized skills instructor qualification, evasive driving, physical security, protective services).
- Individual training (threat awareness, additional weapon familiarization, search techniques, roadblocks, sentry duties, refreshment of basic soldier skills).
- Collective training (include terrorist play in all exercises, Marine Corps Combat and Readiness Evaluation System [MCCRES], Army Training and Evaluation Program mission training plan [AMTP], and USAF major command [MAJCOM] or local operation readiness inspections [ORIs]).
- Training support (training tapes, war games, correspondence courses, tactical exercises without troops).

WWW.SURVIVALEBOOKS.COM

Transit to Deployment Area

Consider the following overall security of the unit throughout the entire movement:

- Command, control, and communication.
- Emergency action procedures.
- Alternative routes or diversions.
- Organic protection parties with each movement element.
- En route planning and training. Include security briefings and training in normal en route procedures. Immediately update the intelligence threat assessment prior to arrival.

DEPLOYMENT

Advance Parties

COMPOSITION

Consider additional personnel necessary for security or liaison with HN security agencies such as military or security police protective service teams, public affairs officer, foreign area specialists, linguists, additional intelligence for terrorism. For advance party deployment, consider whether it should be standard or low profile (uniform or plain clothes, military or civil transport, reception party or not).

PRIORITY INTELLIGENCE REQUIREMENTS

Validate mission and PIRs by asking if the terrorist threat seen from in country affects our ability to accomplish our mission and if the country team perceives our mission as we do. After the PIRs are validated, review them and verify planned ROE.

OPERATIONS SECURITY

If possible, avoid advertising the time and place of main body arrival; if unavoidable, increase security. Avoid establishing patterns of behavior or operation for advance party and main body. Establish secure communications with main body.

Liberty, Leave, and Pass

Maintain a low profile, both unit and individual. Coordinate with local authorities on security measures in the liberty and leave area. Provide troop information and threat briefings to military personnel before they depart on liberty and leave. Establish individual security measures for personnel on liberty and leave. Provide security for billeting or assembly areas (ships in port, hotels, HN accommodations, aircraft). Provide security during transit to liberty and leave areas. Do not forget security for morale support activities.

Training Exercises

Determine the threat assessment to the exercise or training area. Coordinate with security forces designated to protect exercise forces (military police, HN forces, exercise-directing staffs). If necessary, dedicate part of the unit to security vice exercise participation (counterintelligence team, guards, sentries, traffic controller). If possible avoid likely target areas (populated areas, heavily used routes). Avoid creating lucrative targets (troop concentrations, motor pools, large static logistics installations). Remain alert during nontactical phases. Consider separate security communications. Emphasize terrorist threats before and during the exercise.

Transit Within the Deployment Area

Perform continuous threat assessments along routes for each movement. Include security in all movement orders (rail, road convoy, sea, air). Provide security at departure and arrival points (ports, airfields, assembly areas, railway stations). Employ security forces with quick-reaction capabilities during transit. Establish liaison and coordinate with all security agencies along the route.

Operational Contingencies

FACTORS WHICH CAN DEGRADE SECURITY

The following factors can degrade security:

- Required access to VIPs, media representatives (see Chapter 5), and drain on the commander's time.
- An established routine or pattern of life (change of guards, formation, time of reveille, meals).
- Inability to restrict access (main roads passing through the position).
- Inability to choose unit location based on security considerations.
- Restrictions on the employment of security forces (inability to patrol or establish observation posts, intelligence collection).
- Required presence of nonunit personnel (civilian employees, vendors, contractors).

  Inadequate coordination or liaison (intelligence sharing, disclosure of security measures, local police and armed forces).

WWW.SURVIVALEBOOKS.COM

MEASURES THAT CAN ENHANCE SECURITY

The following measures can enhance security:

- Continually reassessing the mission, change in national policy, threat, attitude of the locals.
- Using table of organization and equipment (TOE) and specialized security equipment such as closed circuit TV, detection devices, sensors, lighting, barriers, and barricades (see Appendix C).
- Assigning physical security responsibilities to special staff personnel who are trained physical security officers.
- Knowing applicable regulations (guard orders, ROE, local restrictions).
- Being aware of training and the troop information program.
- Organizing unit positions by providing good defensive and barrier plans, dispersing high value targets (HVTs) away from access roads and perimeter fences.
- Maintaining a low profile (restricting liberty and leave parties).
- Restricting access of unassigned personnel (media, visitors) to the unit location, permitting a minimum number of vehicles within the perimeters, parking away from buildings, and requiring stringent identification checks.
- Exhibiting an image of professionalism and readiness.

REDEPLOYMENT

Advance Parties

Maintain security alert and awareness until all of the unit has returned to base. Develop PIRs for return to home base.

Reverse Deployment

Consider the security of the port of entry and lines of communication for the return trip. Consider whether the mission has changed the situation at home. An unpopular political decision may expose the unit to a threat upon its return to the US. Adopt the same type of security measures used during transit to, and movement within, the deployment area (movement orders, security of ports, airfields, railway stations). Coordinate reaction capabilities with security agencies along the route.

Public Affairs Policy

Release a maximum amount of information to the media with a minimum amount of delay. Information released should fall within the limitations of OPSEC. Brief troops regarding release of information to outside agencies. Stress that release is to be made by authorized public affairs personnel only.

Trainer's Debriefing

Brief personnel to reorient them for the return to the US. Do not overlook inspection procedures aimed at recovering maps, souvenirs, ordnance, weapons, or other contraband.

After-Action Report

Provide lessons learned on security to appropriate authorities as part of the report. Remember to include terrorism counteraction items in the report.

SECTION III

Operations Security

Throughout base defense planning, preparation, and execution, defenders must make every effort to maintain security. OPSEC is an integral part of planning and conducting base defense training and day-to-day operations at all levels of command.

The OPSEC program is designed to deny access to intelligence and information which the threat can use to learn about plans and operations. The program consists of—

- Continuous estimation of the threat.
- Training in measures to deny an enemy information.
- Supervision, evaluation, and corrective action.

WWW.SURVIVALEBOOKS.COM

OBJECTIVES

OPSEC objectives are—

- To avoid stereotyped operations.
- To understand methods threat forces use to collect intelligence.
- To deny intelligence and information to the enemy.
- To integrate OPSEC into physical and personnel security and protection programs.

OPSEC requires close coordination between the operations officer, who provides staff cognizance, and the intelligence officer, who—

- Estimates the threat.
- Is responsible for counterintelligence.
- Determines unit vulnerabilities (see Figure B-4).
- Identifies exploitable sources of information.
- Recommends countermeasures.

MEASURES

Defenders must—

- Develop essential elements of friendly information (EEFI) on those items and activities of planning and operations that terrorists can use.
- Develop a counterrecon plan by determining the assets that the threat is likely to reconnoiter, their locations, and their physical destruction.
- Vary locations such as patrol routes, check points, and sentry or guard positions; vary schedules for activities such as patrols, meetings, meals, religious services, sentry relief, and resupply.
- Use perimeter and internal protective barriers.
- Check the identification of everyone entering or leaving the base or perimeter.
- Use additional security for restricted areas such as communication posts, communication centers, motor parks, high-density troop areas.
- Control itineraries and schedules of VIPs and high-risk personnel.
- Locate dismount points and parking areas away from buildings, preferably at sites where they cannot be observed from outside the base.

INTELLIGENCE INDICATORS

Insurgents or terrorists might use indicators such as those below to gather intelligence on a unit.

Operational indicators could include—

- Troops restricted to the post before a move or an operation.
- Increased patrolling and air recon.
- No patrolling at all.
- Increased movement between locations caused by task organizations prior to an operation.
- Special requisitions to increase rations, transport, ammunition.

HUMINT indicators could include—

- Newspaper or other media coverage.
- Farewells and last-minute visits by VIPs or senior officers.
- Church services the night before an operation.

Sources	Activities	Countermeasures
Human Intelligence	Casual conversations, planning agents	Training for personnel, countersurveillance, and counterintelligence
Signal intelligence	Interception of communications signals	Communications security and information security
Imagery intelligence	Photography of activities from aircraft or high terrain or from cars or bicycles or from other unobtrusive vantages	Counterintelligence, countersurveillance, and access control
Operational patterns	Observation of stereotyped operations	Randomized operations; use of deception

Figure B-4. Unit Vulnerabilities and Countermeasures

WWW.SURVIVALEBOOKS.COM

- Bulletins announcing that enforced rest is required or that dispensary hours are changed.
- Public signs announcing changes in procedures such as restricting civilian travel or access.
- Photographs developed by local contractors showing in-camp scenes and preparations.

Communication indicators could include—

- Changed call signs and frequencies prior to an operation.
- New aerials that suggest repositioned auxiliary communication equipment.

WWW.SURVIVALEBOOKS.COM

APPENDIX C

SPECIALIZED EQUIPMENT AND MATERIEL

The following lists of equipment and materiel specific to joint base defense are not all inclusive. Base mission, threat, and environment may dictate other requirements.

GENERAL

- Pyrotechnic pistols
- Riot guns
- Tear gas launchers
- Tear gas grenades (exploding rather than canister)
- Hand-held flashlights
- Riot helmets
- Shields (3 feet 6 inches)
- Police batons
- Handcuffs and flexicuffs
- Body armor
- Leg armor
- Binoculars
- Marshaling wands
- Telescopes and tripods
- Infrared devices
- Listening devices
- Loudspeakers
- Fire extinguishers
- Cameras with flash attachments and tripods
- Telescopic sights
- Photographic filters
- Polaroid cameras
- Whistles
- Hand-held radios (for use in urban areas)
- Defoliant
- Grass cutting equipment
- Tactical deception equipment (camouflage nets, false structures and equipment, false fencing)
- Vehicle intrusion alarms
- Manuals on threat and personal protection
- Manuals on locale, people, and customs
- Medical equipment (to include litters and equipment for combat lifesavers)
- Tactical maps: If 1:50,000 standard maps are not available. The Defense Mapping Agency must be tasked to develop tactical maps from the base center out to 35 kilometers at minimum. Procedures for map development must be coordinated to be done as soon as possible, if not immediately.
- Ground surveillance equipment
- Forward looking infrared radar (available in some aircraft)
- Trip flares
- Night vision devices
- IR spotlights and goggles
- Fire fighting equipment
- High pressure hoses and equipment
- Closed circuit television (CCTV) camera
- Low light level CCTV camera

ROADBLOCKS AND GATES

- Portable lamps, lights
- Traffic signs
- Lightweight barriers
- Steel cable
- Concertina wire
- Marker lights
- Visor sleeves
- Mirrors
- Badge system at all entry points
- Traffic cones
- Tire puncture chains
- Portable and stationary metal detectors

WWW.SURVIVALEBOOKS.COM

SEARCHES

- Ladders
- Wrecking bars
- Telescopic mirrors
- Mine markers
- White tape
- Measuring tape
- Knives
- Safety harnesses
- Flashlights
- Hand tools (hammers, pliers, screwdrivers)
- Mine detectors
- Metal cutting tools
- Saws
- Picks, shovels
- Magnets
- Axes
- Helmets
- Eye shields
- Chisels
- Mine probes

SPECIALISTS

- Explosive detectors
- Remote light units
- Remote controlled EOD devices
- Video periscopes
- Endoscopes
- Engineer heavy equipment
- Concrete mixers
- Portable compressors
- Hydraulic platform
- Engineer tractors
- Platform hoists
- Command destruct munitions—(thermite grenades)[8]
- EOD equipment
- Guard dogs
- Patrol dogs
- EOD dogs

STATIC DEFENSE (ENGINEERS)

- Portable sensors
- Portable alarms
- Portable lighting systems
- Barriers (drop arm, swing arm, and counterbalance)
- Roadblock equipment for exit and entry control
- CCTV
- Shot direction indicator
- Wire (barbed, concertina)
- Wire netting
- Corrugated iron
- Fencing
- Steel girders
- Scaffolding
- Mines (antivehicle, antipersonnel)
- Piping for personnel turnstile
- Video monitoring system
- Duress signal systems at guard stations at EOC (doorbell, radio)
- Call to arms system (fire alarm, loudspeakers)
- Sandbags
- Telephone system and switch backup energy sources (that is, generators)
- Water purification system
- PSP matting

PORTS

- Mine sweeping equipment
- Diving equipment
- Underwater demolition equipment
- Percussion grenades
- Special warfare swimmer qualified personnel
- Patrol boats (Zodiac, F-470)
- Sonar buoys
- Antisubmarine nets
- Antiswimmer nets
- Mines

To obtain Navy ammunition for defense or training, bases need to submit requests for an allowance list consistent with armament available. NAVSEAINST C8011.3A and NAVSEAINST 8011.2 apply.

[8] Equipment under static defense applies.

WWW.SURVIVALEBOOKS.COM

APPENDIX D

TERRORISM

Terrorism is the unlawful use or threatened use of force against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives. Terrorism involves a criminal act that is often symbolic and intended to influence an audience beyond the immediate victims. Combating terrorism consists of taking actions to counter the terrorist threat both offensively and defensively.

UNIT VULNERABILITY

Commanders should evaluate how vulnerable their units are to terrorist attack during deployment. Vulnerability changes as units change locations, activities, and quarters and as reinforcements are available or VIPs conduct visits. Thus, commanders need to update their evaluations continually.

The questionions in Figure D-1 are not all-inclusive. Rather, they serve to suggest whether units are susceptible. All negative answers do not guarantee that the unit is safe from terrorist attacks.

GENERAL

Mission Sensitivity

- Is the mission a heavily publicized national security mission?
- Is it a sensitive mission with limited publicity?
- Is it a covert mission?

Presence of Very Important Persons

- How many general and flag officers are in the area?
- How many diplomats and politicians?

Current Threat Analysis

- What is the current analysis by the military police?
- What is the current analysis by intelligence, by the State Department?

World attitude toward Mission

- Is there general agreement or general disagreement with the purpose?
- Is there disagreement by a hostile country such as the Soviet Union, Cuba, North Korea, Iran, Libya, or Syria?

Status of Unit Training

- Does a terrorism security plan exist?
- Do we have terrorism trained personnel, is specialist equipment available, and are all regularly exercised?

Unity of Security Effort

- Is the force from a single service?
- Does it have a terrorism counteraction plan and organization?
- Do we have a multi-service force and a coordinated plan?

REGIONAL

Area of Deployment

- Is the deployment to a high threat area such as Europe, the Middle East, Central or South America?
- Is it to the Caribbean, the Phillipines?
- Is it to somewhere else OCONUS?

Country Team Guidance

- Is good intelligence and security advice or assistance available; is there no conflicting mission?
- Is there no intelligence or security assistance; does a mission conflict?

Other US Military Assistance

- Is air, naval, and land assistance available within 1 hour?
- Is it available in the region?
- Is assistance unavailable?

Figure D-1. Questions to Help Determine Susceptibility

WWW.SURVIVALEBOOKS.COM

LOCAL

Defenses and Nonmilitary Law Enforcement Agencies

NOTE: Make an assessment for each subunit located separately.

- Are the agencies on site?
- Do they react in 30 minutes?
- Do they react in 1 hour?
- Is the area urban, undefended, and inhabited by civilians?
- Is the area urban, defended with perimeter fencing, rocket screens, mortar protection, barriers?
- Is the area rural, undefended, and close?
- Is the area rural, undefended, and open?
- Is the area rural, defended with perimeter fencing, rocket screens, observation towers, fire trenches, patrols?

Access to Site

- Are the roads primary roads or secondary?
- Can the airfields handle high-performance aircraft, small aircraft, or only helicopters?
- Are the waterways navigable or not?

Personnel and Vehicle Access

- Do civilian workers and media have free access?
- Are they allowed access, controlled by the HN?
- Are they allowed access, controlled by US military?
- Are unassigned personnel denied access?

Communications

- Is access to outside communications easy?
- Do we have communications with higher, lateral, and lower elements?
- Are land lines dedicated to secure communications available?
- Are dedicated radio communications available?

Tactical Limitations

- Is live ammunition allowed?
- Are magazines in weapons allowed?
- Are outside patrols, operations, and intelligence-gathering allowed?
- Are we allowed to build barricades, harden buildings, dig trenches?
- Are stereotyped patterns of life required?

Figure D-1. Questions to Help Determine Susceptibility (continued)

THREAT CONDITIONS AND RESPONSES

Warnings of terrorist activity against US bases will normally come from US security authorities or through the security agencies of the HN. Warnings may come from local police or even from terrorist organizations themselves. In combating terrorism, bases should use common terrorist THREATENS, each with its measures and required responses.

Assessment Factors

Commanders of bases may declare a THREATCON and take implementation measures upon receiving intelligence through official sources or anonymous messages. THREATCONs are disseminated laterally and vertically to ensure all potentially affected areas are warned. To assess the nature of the threat, defenders use the factors in Figure D-2.

Many of the indicators in Figure D-3 may appear to be normal rights until put in context with other activities. They may then become indicators of potential violence.

Threat Levels

Positive evidence for any or all of the assessment factors above requires an appropriate THREATCON.

The following guidelines apply only in assessing terrorist threats against US or DOD interests. Each service may translate the THREATCONS into a code applicable to its own forces. Local orders will include specific instructions on issuing weapons and live ammunition. These orders must comply with the policy of the US command or agency concerned. The detailed measures to be

WWW.SURVIVALEBOOKS.COM

Existence
A terrorist group is present in an area of concern. It need not have posed a threat to US or DOD interests in the past.

Capability
The group has the ability to carry out an operation against US interests in areas of concern, including resources such as intelligence, mobility, personnel.

History
The group's history of terrorist acts and behavior reveal an anti-US stand.

Trends
Over the past year, the group's activity appears to be continuing or increasing. Activity may be violent or merely verbal or involve the issuance of threats.

Targeting
The group has known plans or confirmed intentions to target US or DOD interests. Targeting can be either specific or nonspecific. If targeting is not against US or DOD interests, this factor does not apply.

Figure D-2. Assessment Factors

- Dissent for political, social, or ethnic reasons; charges brought against local government.
- Formation of radical groups, branches of national subversive groups, or secret societies.
- Antigovernment, anti-US agitation; identification of government or US as the root of the problem.
- New spokesperson for the cause emerging; out-of-town organizers arriving.
- Meetings, rallies, and demonstrations being organized; grievances taking political overtones; inflammatory speeches and charges made; provocation of authorities to intervene, overreact; police or military brutality charged.
- Appearance of antiestablishment posters, leaflets, underground press, taking people's concerns into political areas, politicalization of social causes.
- Use of known personalities as draws for rallies, especially those that have been identified with radical causes.
- Demonstrations, civil disobedience, protest marches with the actual causes overshadowed by political rhetoric.
- Increased recruiting, especially by known front groups and radical organizations; support sought among workers.
- Increased activism in political spheres at colleges and universities.
- Speeches and communications advocating violence as the only means of solution.
- Identification of foreign influence or aid.
- Threats against public works, utilities, transportation; threats of violence against prominent personalities.
- Agitation in refugee, minority, or foreign communities; polarization; arming segments of society.
- Reports of stolen firearms and explosives; raids on armories, sporting goods stores.
- Violence against property, looting, destruction, arson, especially during demonstrations, marches, mob actions.
- Violence against persons, murders, attempted murders, beatings, threats, abductions, public targeting of people.
- Increased purchases of high-performance weapons; appearance of automatic weapons, especially of foreign manufacture.
- Discovery of weapons, ammunition caches, explosives; indication of terrorist training; increased terrorist surveillance.
- Open attacks on police, military, and other symbols of authority.
- Discovery of enemy communications equipment or interception of radio signals which point to buildup of threat.

Figure D-3. Local Insurgent and Terrorist Indicators

WWW.SURVIVALEBOOKS.COM

adopted by US headquarters sharing facilities with HN organizations must be coordinated with those organizations. For the measures and required actions for each THREATCON, see Figure D-4.

THREATCON ALPHA: LOW

Existence and capability are factors. THREATCON Alpha applies if bases and personnel are subject to a general terrorist threat, the nature and extent of which are unpredictable. Such possibilities do not justify full implementation of the measures of THREATCON Bravo. However, defenders may have to implement selected measures from THREATCON Bravo in response to intelligence received or as a deterrent. Defenders must be able to maintain the measures in this THREATCON indefinitely.

THREATCON BRAVO: MEDIUM

Existence and capability are factors. History or trends must also be evident. Targeting of US or DOD interests is not evident. THREATCON Bravo applies when an increased and more predictable threat of terrorist activity exists. Defenders must be able to maintain the measures in this THREATCON for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

THREATCON CHARLIE: HIGH

Existence, capability, trends, and targeting are factors. Targeting is not specific or immediate. History may be a factor. THREATCON Charlie applies when an incident occurs or when intelligence indicates an imminent terrorist action against bases and personnel. Implementation measures for more than a short period will probably create hardship and will affect the peacetime activities of the unit and its personnel.

THREATCON DELTA: IMMINENT

Existence, capability, immediate and specific targeting of US or DOD interests, and trends are factors. History may be a factor. THREATCON Delta applies in the immediate area after a terrorist attack or when intelligence indicates a likely threat against a specific location or person. THREATCON Delta is a rare assessment, normally issued as a localized warning.

Measure	Required Action	Measure	Required Action
THREATCON ALPHA			
1	Regularly remind all personnel, including dependents, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers; be alert for unidentified vehicles on, or in the vicinity of, US bases; and be alert for abandoned parcels or suitcases or any unusual activity.	4	Increase security spot checks of vehicles and persons entering the base and unclassified areas under the jurisdiction of the US command and agency.
		5	Limit access points for vehicles and personnel compatible with a reasonable flow of traffic.
2	Ensure that immediate contact is possible with the duty security officer or other appointed personnel who have access to plans for evacuating buildings and areas in use and for sealing off areas where an explosion or attack has occurred. Keep on call key personnel needed to implement security plans.	6	As a deterrent, apply Measure 14, 15, 17, or 18 from THREATCON Bravo individually and randomly.
		7	Review all plans, orders, personnel details, and logistic requirements related to the introduction of the higher THREATCON.
3	Secure buildings, rooms, and storage areas not in regular use.	8	Review and implement security measures for high-risk personnel.
		9	Spare.

Figure D-4. THREATCON Actions

WWW.SURVIVALEBOOKS.COM

Measure	Required Action
THREATCON BRAVO	
10	Repeat Measure 1 and warn personnel of any other form of attack to be used by terrorists.
11	Keep all personnel involved in implementing antiterrorist contingency plans on call.
12	Check plans for implementation of the measures contained in the next THREATCON.
13	Where possible, move cars and such objects as crates and trash containers at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider requiring centralized parking.
14	Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
15	At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.
16	Qualified personnel (US mail, trained military police) examine all mail for letter or parcel bombs. This examination is increased above normal.
17	Check all deliveries to facilities such as messes and clubs. Advise dependents to check all home deliveries.
18	As far as resources allow, 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.
19	Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.
20	At an early stage, inform members of local security committees of any action being taken and why.
21	Upon entry of visitors to the unit, physically inspect them and a percentage of their suitcases, parcels, and other containers.
22	Wherever possible, operate random patrols to check vehicles, people, and buildings.
23	Protect off-base personal and military vehicles according to prepared plans. Remind drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive a car.
24	Implement additional security measures for high-risk personnel.
25	Brief personnel who may augment guard force on use of deadly force. Make this part of the individual training program.
26 to 29	Spare.
THREATCON CHARLIE	
30	Continue all THREATCON Bravo measures or introduce those outstanding.
31	Keep available at their places of duty all personnel who are responsible for implementing antiterrorist plans.
32	Limit access points to an absolute minimum.
33	Strictly enforce control of entry and search a percentage of vehicles.
34	Enforce centralized parking of vehicles away from sensitive buildings.
35	Issue weapons and ammo to guards. Local orders should include specific orders on issue of ammo.
36	Increase patrolling of the base.
37	Protect all designated vulnerable points (VPs) and give special attention to VPs outside the base.
38	Erect barriers and obstacles to control traffic flow.
39	Spare.
THREATCON DELTA	
40	Continue or introduce all measures listed for THREATCONs Bravo and Charlie.
41	Augment guards as necessary.
42	Identify all vehicles already on the base within operational or mission support areas.
43	Search all vehicles entering the base; search vehicle contents.
44	Control all access and positively identify all personnel.

Figure D-4. THREATCON Actions (continued)

WWW.SURVIVALEBOOKS.COM

Measure	Required Action	Measure	Required Action
THREATCON DELTA (continued)			
45	Search all suitcases, briefcases, and packages brought into the base.	48	Minimize all administrative trips and visits.
46	Take measures to control access to all areas under the jurisdiction of the US command or agency concerned.	49	Consult local authorities about closing public and military roads and facilities that might make sites vulnerable to terrorist attack.
47	Check parking lots and the exterior of buildings frequently.	50	Spare.

Figure D-4. THREATCON Actions (continued)

BASE TERRORISM RESPONSE

The commander of the base has operational control of base resources during a terrorist incident. Necessary actions, however, are typically planned, coordinated, and directed by an EOC, which is activated immediately when terrorist incidents occur.

Emergency Operations Center

The EOC is subordinate to the BDOC. The EOC is an on-scene command post for the BDOC. The EOC exerts operating control over the forces assigned to it and directs the military response.

See the base terrorism response model for command and control in Figure D-5. It shows the relationship of the EOC to subordinate threat response activities.

Once the BDOC is established, then it coordinates with higher, lower, and adjacent military headquarters and organizations. For planning considerations and measures for combating terrorism on military bases, commanders and staffs must refer to their individual service publications.

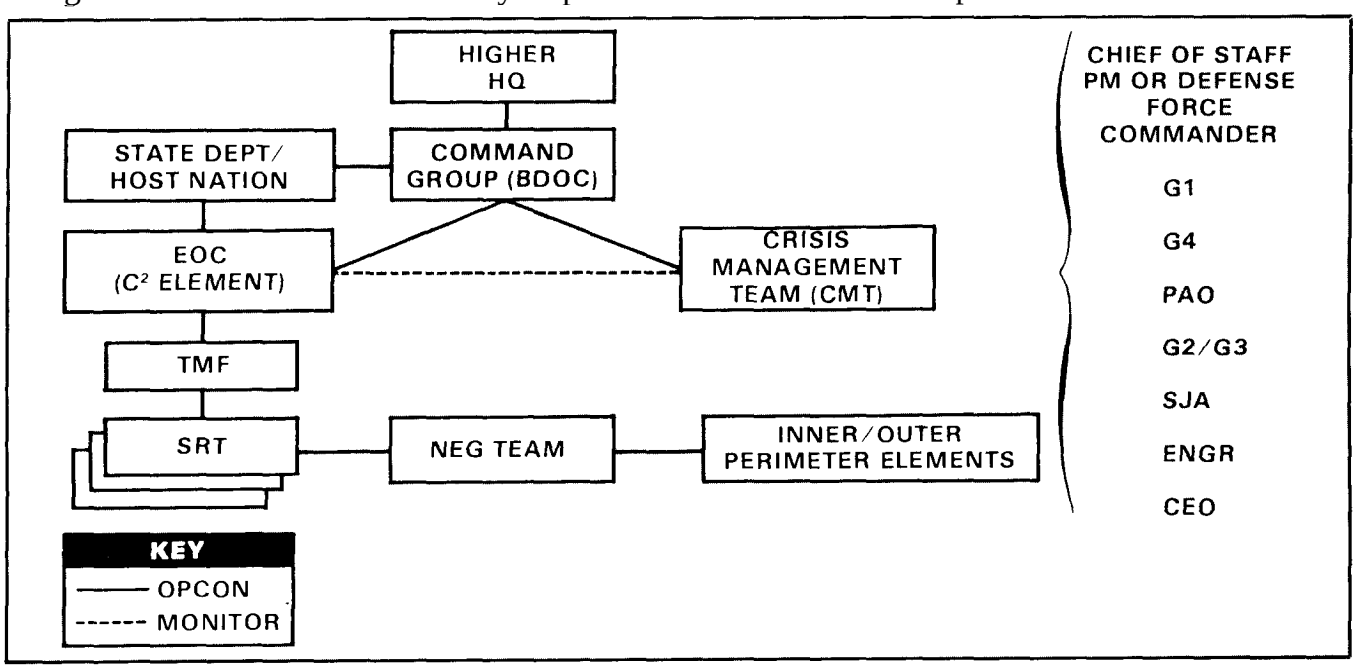


Figure D-5. Operational Control of Base Terrorism Response

WWW.SURVIVALEBOOKS.COM

Crisis Management Team.

The crisis management team (CMT) is composed of selected representatives from the base staff. This team assists the commander in controlling the incident. The CMT consists of the—

- Provost marshal (PM), senior MP, or security police (SP) commander.
- G1 (personnel).
- G2 (intelligence).
- G3 (operations).
- G4 (logistics).
- Staff judge advocate.
- Public affairs officer.
- Psychological operations officer.
- Civil affairs officer.
- Engineer.
- Country team representative.
- Medical staff officer.
- Communications officer.

THREAT MANAGEMENT FORCE.

The threat management force (TMF) is the tactical element of the EOC. The TMF commander has operational control of all base military forces at the incident site. The TMF is composed of-

- Special reaction teams which isolate and contain the incident, report information, rescue hostages and nonparticipants, and assault terrorist positions (see Figures D-9 and D-10). Teams perform rescue and assault missions only under special circumstances or when a more qualified force is not available.
- Inner and outer perimeter elements that secure the incident site, control access to the area, and provide security to the remainder of the installation (Figure D-6).
- Hostage negotiation teams trained to conduct direct communication with the terrorists. Negotiations are conducted to further develop the situation for key decision makers.

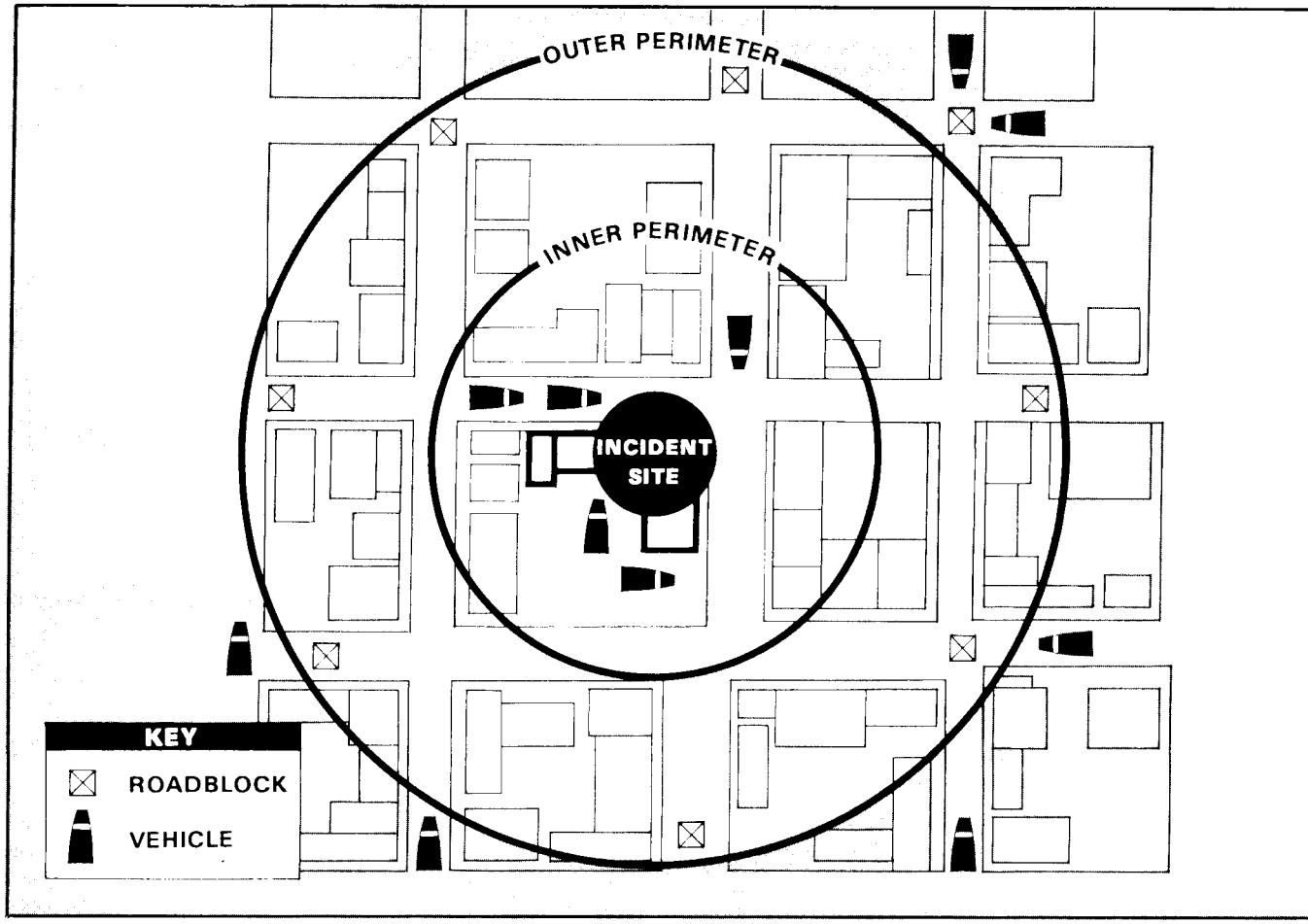


Figure D-6. Inner and Outer Perimeters at Incident Site in a Built-up Area

WWW.SURVIVALEBOOKS.COM

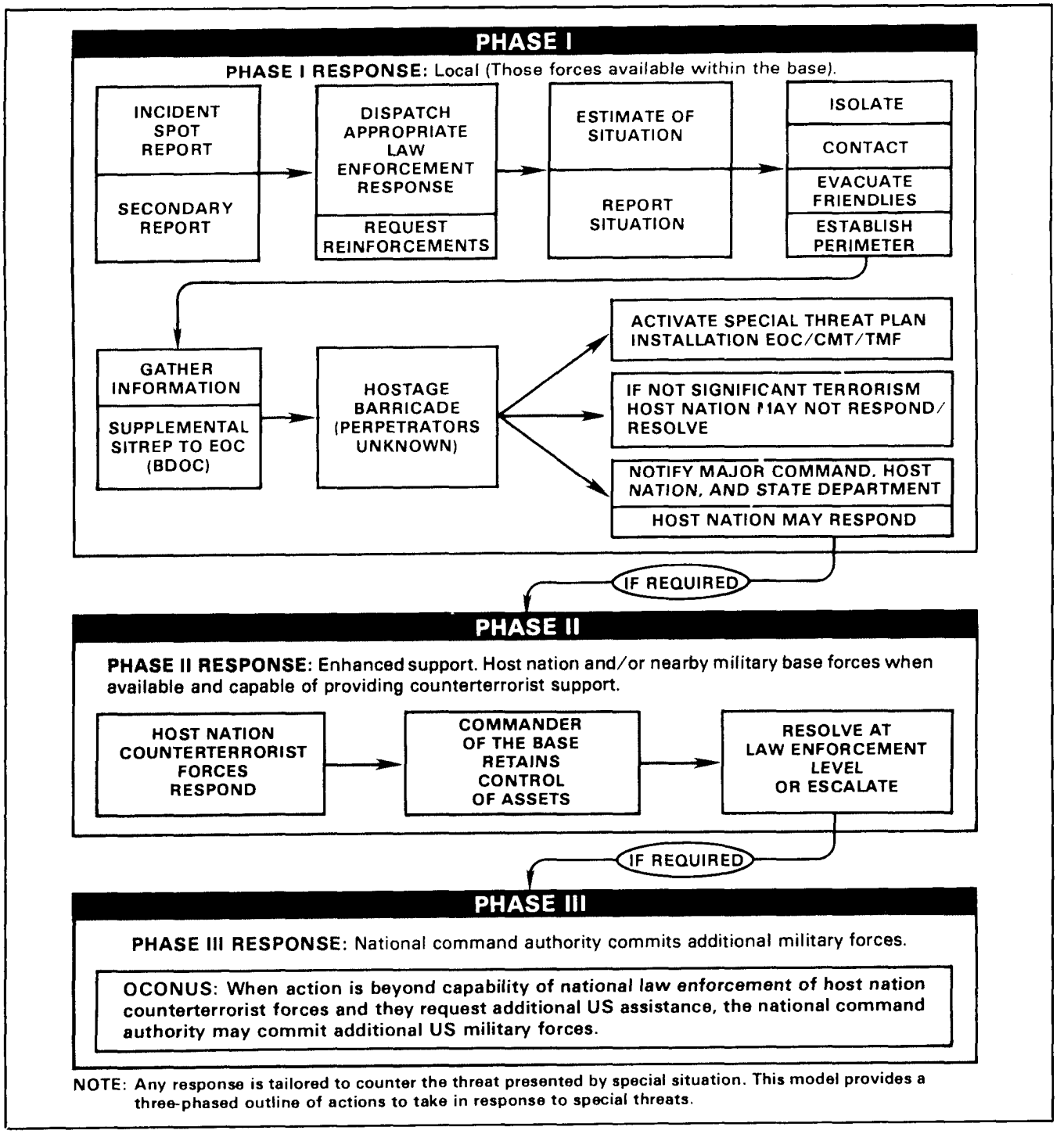


Figure D-7. Special Threat Decision Model

The typical military response on bases outside the US consists of three phases:

- Phase I, the initial response by base law enforcement, other military resources, and HN law enforcement agencies.
- Phase II, an enhanced response by other in-country US military forces or HN forces.
- Phase III, the highest level of response by specially trained forces.

Figure D-7 shows a special threat decision model for these three response phases to terrorist incidents. Figure D-8 shows the alert notification process for terrorist incidents on overseas bases.

WWW.SURVIVALEBOOKS.COM

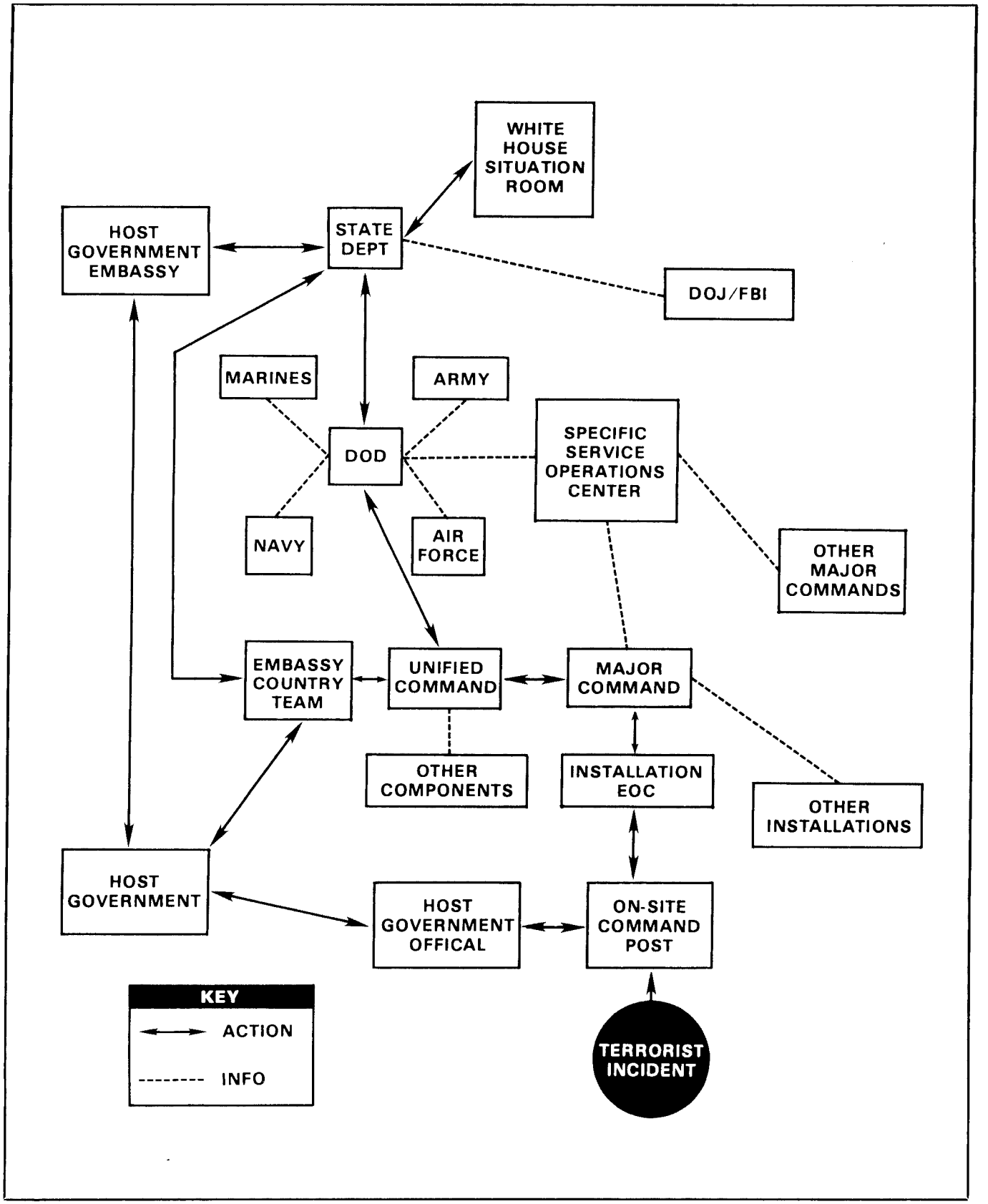


Figure D-8. Alert Notification Process

WWW.SURVIVALEBOOKS.COM

Special Skills and Special Teams

Once a terrorist situation has developed, special considerations, tactics, and coordination are necessary. Given the unique threat that terrorism poses and the worldwide attention it brings, US forces require specific handling (see paragraph on page D-6 on Emergency Operations Center). Figures D-9 and D-10 list additional special skills and special teams that may be needed to react to terrorist incidents.

Photography (developing, telescopic photography, photographers down to company level)

Intelligence (intelligence personnel at lower levels, some counterintelligence capability)

Public affairs officer

Language and foreign area specialization

Environmental engineering

Explosive ordnance disposal

Nuclear, biological, and chemical monitoring

Search advising (at least one advisor with each company)

Military police or security police support

Civil affairs

Psychological operations (PSYOP)

Engineering (camp structures, defenses and reinforcements, permanent roadblocks)

NOTE: Each defense force member deploying to a high-threat area must learn the basic skills listed in Appendix B.

Figure D-9. Special Skills

Search team (for each company or squadron at least one four-to-five-person team trained in house, car, and area searches)

Special reaction team (SRT), USAF Security Police, Army Military Police Emergency Service Team (EST) (trained to react to a terrorist incident)

Protective service team (specialist protection for commanders, very important persons (VIPs), and sensitive convoys)

Close observation team (for close observation capability, especially in urban areas, a recon platoon or flight, or a surveillance and target acquisition platoon or flight)

Photographic team (a large team or several teams)

Snatch team or arrest team (a team in each company or squadron trained in hand-to-hand combat)

Hostage negotiation team

Explosive or advanced demolition team

Judge advocate

Intelligence team (because of extended threat throughout a deployment and need for continual assessment, a larger team or teams to provide 24-hour cover)

Crisis management team (in a unit, the unit headquarters to provide the crisis mangement team in a terrorist incident FM 100-37, OH 7-14, AFR 208-1, AFM 125-7[a])

[a]FM 100-37, *Terrorism Counteraction;* OH 7-14, *Terrorism Counteraction;* AFR 208-1, *USAF Antiterrorism Program;* AFM 125-7, *Emergency Service Team Operations.*

Figure D-10. Special Teams

WWW.SURVIVALEBOOKS.COM

GLOSSARY

ACRONYMS AND ABBREVIATIONS

AADC	area air defense commander
ABGD	air base ground defense
ADC	area damage control
AFM	Air Force manual
AFR	Air Force regulation
AMTP	Army Training and Evaluation Program mission training plan
AO	area of operation
BDOC	base defense operations center
C^2	command and control
C2	intelligence officer at a combined headquarters
C^3	command, control, and communications
C^3I	command, control, communications, and intelligence
CA	civil affairs
CCD	camouflage, concealment, and deception
CCTV	closed circuit television
CDA	close defense area
CDF	close defense force
CEOI	communications-electronics operation instructions
CGSC	Command and General Staff College
CI	counterintelligence
CINC	commander in chief
CMC	commandant, Marine Corps
CMT	crisis management team
COMMZ	communications zone
CONUS	continental United States
CSS	combat service support
DA	Department of the Army
DCSOPS	deputy chief of staff for operations and plans, G5
DOD	Department of Defense
DOJ	Department of Justice
DS	direct support
DZ	drop zone
ECM	electronic countermeasure
EEFI	essential elements of friendly information
EOC	emergency operations center
EOD	explosive ordnance disposal
EST	emergency service team
EW	electronic warfare
FBI	Federal Bureau of Investigation
FLIR	forward-looking infrared radar
FM	field manual
FMFM	fleet marine force manual
FORSCOM	LJS Army Forces Command
FOUO	for official use only
FSE	fire support element
G1	assistant chief of staff, personnel
G2	assistant chief of staff, intelligence
G3	assistant chief of staff, operations and plans
G4	assistant chief of staff, logistics
GO	general officer
GSR	ground surveillance radar
HEAT	high explosive, antitank
HN	host nation
HNS	host-nation support
HQ	headquarters
HQMC	Headquarters, Marine Corps
HUMINT	human intelligence
HVT	high value targets
IFF	identification, friend or foe
IMINT	imagery intelligence
IPB	intelligence preparation of the battlefield
IR	infrared
J2	intelligence directorate at a joint headquarters
J3	operations directorate at a joint headquarters

WWW.SURVIVALEBOOKS.COM

J4	logistics directorate at ajoint headquarters
J5	plans and policy directorate ata joint headquarters
J6	communications-electronics directorate ata joint headquarters
JBD	joint base defense
JCS	Joint Chiefs of Staff
JTF	joint task force
km	kilometer
LAV	land amphibious vehicle
LIC	low-intensity conflict
LOC	line of communication
LP	listening post
LZ	landing zone
MAAG	military assistance advisory group
MCCRES	Marine Corps Combat and Readiness Evaluation System
MDA	main defense area
MDF	main defense force
METT-T	mission, enemy, terrain, troops, and time available
MOPP	mission-oriented protective posture
MOS	military occupational speciality
MPH	miles per hour
MP	military police
MR	mobile reserve
NAVSEAINST	naval sea instruction
NBC	nuclear, biological, chemical
NCA	national command authority
NCO	noncommissioned officer
NCOIC	noncommissioned officer in charge
NCS	net control station
NOD	night observation device
NVG	night vision goggles
OCOKA	observation and fields of fire, cover and concealment, obstacles and movement, key terrain, and avenues of approach
OCONUS	outside continental United States
ODC	office of defense cooperation
OH	operational handbook
OIC	officer in charge OP observation post
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPREP	operational report
OPSEC	operations security
ORI	operation readiness inspection
PA	public affairs
pam	pamphlet
PAO	public affairs officer
PIR	priority intelligence requirement
PM	provost marshal
POC	point of contact
PSP	perforated steel plate
PSYOP	psychological operations
pub	publication
PW	prisoner of war
RADC	regional air defense commander
ROE	rules of engagement
SAO	security assistance organization
SF	screening force
SFA	screening force area
SIGINT	signal intelligence
SOF	special operations forces
SOFA	status-of-forces agreement
SOP	standing operating procedure
SP	security police
SRT	special reaction team
TAC	US Air Force Tactical Air Command
TACAIR	tactical aircraft
TACP	tactical air control party
TC	training circular
TCF	tactical combat force
THREATCON	threat condition
TMF	threat management force
TOE	table of organization and equipment
TRADOC	US Army Training and Doctrine Command

WWW.SURVIVALEBOOKS.COM

TV television
TVT television tape

UNAAF Unified Action Armed Forces
US United States
USA US Army
USAF US Air Force
USMC US Marine Corps
USN US Navy
USSR Union of Soviet Socialist Republics

VIP very important person
VP vulnerable point

TERMS

base command
An area containing a military base or group of such bases organized under one commander (JCS Pub 1-02).

civil affairs
Those activities conducted during peace and war that facilitate relationships between US forces, civil authorities, and people of the nation in which the US military forces are operating (TRADOC Pam 525-44).

civil war
An internal conflict which meets the following criteria:

1. The insurgents occupy and control territory.
2. The insurgents have a functioning government.
3. Other states offer some type of recognition to the insurgent government and define their attitude toward the conflict.
4. The insurgents have armed forces which are commanded by a person responsible for their actions, carry their arms openly, wear a distinctive emblem, and conduct their operations in accordance with the laws of war.
5. A state of general hostilities accompanied by a military confrontation of major proportions is taking place. (FM 100-20)

combating terrorism
Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum (JCS Pub 1-02).

command

1. The authority that a commander in the military service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel.
2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action.
3. A unit or units, an organization, or an area under the command of one individual.
4. To dominate by a field of weapon fire or by observation from a superior position (JCS Pub 1-02).

counterguerrilla warfare
Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas (JCS Pub 1-02).

counterinsurgency
Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency (JCS Pub 1-02).

counterintelligence
Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, or subversion (JCS Pub 1-02).

crisis management team
A team found at a major command or installation level concerned with plans, procedures, techniques, policies, and controls for dealing with terrorism, special threats, or other major disruptions occurring on government installations or facilities. The team considers the local, national, and international implications of major disruptions and establishes contact with the appropriate operations center as the situation escalates, requiring higher level involvement and guidance. Normally at installation level, the CMT is established at or in proximity to the designated emergency operations center.

WWW.SURVIVALEBOOKS.COM

defense
Defense is normally an incremental response to perceived threats. As the threat increases, so does the level of defense. Hopefully, increases occur well ahead of an actual attack. Defense is a balanced and coordinated effort by all forces assigned to a site to defeat an attacker and prevent it from achieving its objectives.

developing nation
Sometimes referred to as a *less developed country,* a developing nation is a nation that is progressing beyond a traditional society and is experiencing the turbulent process of economic, social, military, political, and psychological change (FM 100-20).

foreign internal defense
Participation by civilian and military agencies of a government in any of the action programs taken by another government to free and protect its society from subversion, lawlessness, and insurgency (JCS Pub 1-02).

foreign military sales
That portion of United States security assistance authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended. This assistance differs from the Military Assistance Program and the International Military Education and Training Program in that the recipient provides reimbursement for defense articles and services transferred (JCS Pub 1-02).

guerrilla warfare
Military and paramilitary operations conducted in enemy held or hostile territory by irregular, predominantly indigenous forces (JCS Pub 1-02).

host nation
A nation in which representatives or organizations of another state are present because of government invitation or international agreement.

human intelligence
A category of intelligence derived from information collected and provided by human sources. Also called HUMINT (JCS Pub 1-02).

insurgency
An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict (JCS Pub 1-02).

intelligence
The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas (JCS Pub 1-02).

internal defense
The full range of measures taken by a government to free and protect its society from subversion, lawlessness, and insurgency (JCS Pub 1-02).

internal development
Actions taken by a nation to promote its growth by building viable institutions (political, military, economic, and social) that respond to the needs of its society (JCS Pub 1-02).

joint base
A locality from which operations of two or more of the armed forces of the Department of Defense are projected or supported and which is manned by significant elements of two or more services or in which significant elements of two or more services are located (JCS Pub 1-02).

low-intensity conflict
A limited politico-military struggle to achieve political, social, economic, or psychological objectives. It is often protracted and ranges from diplomatic, economic, and psychosocial pressures through terrorism and insurgency. Low-intensity conflict is generally confined to a geographic area and is often characterized by constraints on the weaponry, tactics, and level of violence. Also called LIC (approved definition for JCS Pub 1-02).

military assistance advisory group
A joint service group, normally under the military command of a commander of a unified command and representing the Secretary of Defense, which primarily administers the US military assistance planning and programming in the host country. Also called MAAG (JCS Pub 1-02).

Military Assistance Program
That portion of the US security assistance authorized by the Foreign Assistance Act of 1961, as amended, which provides defense articles and services to recipients on a nonreimbursable (grant) basis (JCS Pub 1-02).

military civic action
The use of preponderantly indigenous military forces on projects useful to the local population at all levels in such fields as education, training, public works, agriculture, transportation, communications, health, sanitation, and others contributing to economic and social development, which would also serve to improve the standing of the military forces with the population (US forces may at times advise or engage in military civic actions in overseas areas) (JCS Pub 1-02).

national command authorities (NCA)
The president and the secretary of defense or their duly deputized alternates or successors. Commonly referred to as NCA (JCS Pub 1-02).

operational control
Operational control includes directive authority for joint training. Operational control should be exercised through the commanders of assigned

WWW.SURVIVALEBOOKS.COM

normal organizational units or through the commanders of subordinate forces established by the commander exercising operational control. Operational control normally provides full authority to organize forces as the operational commander deems necessary to accomplish assigned missions and to retain or delegate operational control or tactical control as necessary. Operational control may be limited by function, time, or location. It does not, of itself, include such matters as administration, discipline, internal organization, and unit training. Also called OPCOM (JCS Pub 1-02).

operations security
The protection of military operations and activities resulting from the identification and subsequent elimination or control of intelligence indicators (vulnerabilities) which are susceptible to hostile exploitation. The principal elements of an OPSEC program are physical security, information security, signal security, and military deception.

paramilitary forces
Forces or groups which are distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission (JCS Pub 1-02).

peacekeeping operations
Military operations conducted in support of diplomatic efforts to achieve, restore, or maintain peace in areas of potential or actual conflict (TRADOC Pam 525-44).

peacetime contingency operations
Politically sensitive military operations normally characterized by the short term rapid projection or employment of forces in conditions short of conventional war, for example, strike, raid, rescue, recovery, demonstration, show of force, unconventional warfare, and intelligence operations (TRADOC Pam 525-44).

propaganda
Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly (JCS Pub 1-02).

psychological operations
Planned psychological activities in peace and war directed to enemy, friendly, and neutral audiences in order to influence attitudes and behavior affecting the achievement of political and military objectives. They include strategic psychological activities, consolidation, psychological operations and battlefield psychological activities (JCS Pub 1-02).

sabotage
An actor acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises, or utilities, to include human and natural resources (JCS Pub 1-02).

security assistance
Group of programs authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended, or other related statutes by which the United States provides defense articles, military training, and other defense-related services by grant, credit, or cash sales in furtherance of national policies and objectives (JCS Pub 1-02).

security assistance organization
This term encompasses all DOD elements located in a foreign country with assigned responsibilities for carrying out security assistance management functions. For instance, it includes military assistance advisory groups, military missions and groups, offices of defense/military cooperation, liaison groups, and defense attache personnel designated to perform security assistance functions (TRADOC Pam 525-44).

Seabee
A member of one of the US Navy construction battalions for building naval shore facilities in combat zones.

special reaction team
A specially trained team of military or security personnel armed and equipped to isolate, contain, gather information for, and, if necessary, neutralize a specific threat.

spetsnaz
Soviet special operations forces.

status-of-forces agreement
An international agreement which determines the status of an armed force while serving on the territory of another sovereign country also a party to that agreement, gives these forces a standard legal treatment wherever they happen to be, and solves practically all of the legal problems raised by the presence of foreign forces abroad.

subversive activity
Anyone lending aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of incumbent governments by force and violence is subversive and is engaged in subversive activity. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories

WWW.SURVIVALEBOOKS.COM

of treason, sedition, sabotage, or espionage will be placed in the category of subversive activity (JCS Pub 1-02).

strategic intelligence
Intelligence that is required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application but also vary in terms of scope and detail (JCS Pub 1-02).

tactical intelligence
Intelligence which is required for the planning and conduct of tactical operations. Tactical intelligence and strategic intelligence differ primarily in level of application but may also vary in terms of scope and detail (JCS Pub 1-02).

terrorism
The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious or ideological objectives (approved definition for JCS Pub 1-02).

unconventional warfare
A broad spectrum of military and paramilitary operations conducted in enemy-held, enemy-controlled, or politically sensitive territory. Unconventional warfare includes, but is not limited to, the interrelated fields of guerrilla warfare, evasion and escape, subversion, sabotage, and other operations of a low visibility, covert, or clandestine nature. These interrelated aspects of unconventional warfare may be prosecuted singly or collectively by predominantly indigenous personnel, usually supported and directed in varying degrees by (an) external source(s) during all conditions of war or peace (JCS Pub 1-02).

United States country team
The senior, in-country, United States coordinating and supervising body, headed by the chief of the United States diplomatic mission, usually an ambassador, and composed of the senior member of each represented United States department or agency (JCS Pub 1-02).

WWW.SURVIVALEBOOKS.COM

REFERENCES

ARMY PUBLICATIONS

Armored and Mechanized Division Operations. FM 71-100. 20 September 1978.

Camouflage. FM 5-20, 20 May 1968.

Civil Disturbances. FM 19-15. 25 November 1985.

Counterguerrilla Operations. FM 90-8. 29 August 1986.

Countering Terrorism on US Army Installations, TC 19-16. 25 April 1983.

Guard Duty. FM 22-6. 17 September 1971.

An Infantryman's Guide to Urban Combat. FM 90-10-1. 30 September 1982.

The Infantry Platoon and Squad. FM 7-8. 31 December 1980.

The Infantry Rifle Company. FM 7-10. 8 January 1982.

Joint Operational Concept for Air Base Ground Defense. DA Pam 525-14. 15 July 1986.

Larger Unit Operations. FM 100-15. 15 March 1974.

Legal Guide for Commanders. FM 27-10. 12 June 1987.

Low-Intensity Conflict. FM 100-20. 16 January 1981.

Military Operations on Urbanized Terrain (MOUT). FM 90-10. 15 August 1979.

Military Police Support for the AirLand Battle. FM 19-1. 23 May 1988.

Operations. FM 100-5. 5 May 1986.

Physical Security. FM 19-30.1 March 1979.

Rear Battle. FM 90-14. 10 June 1985.

Survivability. FM 5-103. 10 June 1985.

Terrorism Counteraction. FM 100-37. 24 July 1987.

Treaties Governing Land Warfare. DA Pam 27-1. 7 December 1956.

US Army Formal Schools Catalog. DA Pam 351-4. 23 October 1987.

US Army Operational Concept for Low-Intensity Conflict. TRADOC Pam 525-44. 10 February 1986.

MARINE CORPS PUBLICATIONS

Advanced Naval Base Defense. FMFM 8-3. 5 December 1978.

Counterinsurgency Operations. FMFM 8-2. January 1980.

Marine Rifle Company/Platoon. FMFM 6-4. February 1978.

Terrorism Counteraction. OH 7-14. November 1985.

NAVY PUBLICATIONS

Ammunition Allowance for Naval Ships, Ship-to-Shore Rotational Units in Shore Stations. NAVSEAINST 8011.2. 11 July 1985.

Physicsl Security and Loss Prevention Manual. OPNAVINST 5530. 14 Series. 16 September 1985.

WWW.SURVIVALEBOOKS.COM

Protection of Department of Navy Personnel and Resources Against Terrorist Attacks. OPNAVINST 3850.4 Series. 23 March 1984.

Small Arms Service Ammunition Allowance for Civilian and Military Security and Police Guards, Couriers, and Agents. NAVSEAINST C8011.3A. 27 April 1984.

AIR FORCE PUBLICATIONS

Air Base Camouflage Techniques. AFSC, AD/YQ. November 1984.

Emergency Service Team Operations. AFM 125-7. October 1987.

Executive Handbook on Terrorism, Security, Survival. November 1987. May be ordered from HQ, USAF, Office of Special Investigations, Boiling AFB, Washington DC 20332.

Ground Defense of Main Operating Bases, Installations, and Activities. Volume 1. AFR 206-2. September 1983.

Installation Resources Protection Program. AFM 125-37. October 1987.

Operations- Tactical Deception Program. AFR 55-49. September 1987.

Security Police Handbook. AFR 125-3. January 1988.

USAF Antiterrorism Program. AFR 208-1. January 1986.

JOINT AND MULTI-SERVICE PUBLICATIONS

Department of Defense Dictionary of Military and Associated Terms. JCS Pub 1-02. 1 January 1986.

Joint Doctrine for Air Defense. JCS Pub 3-01.3. 23 May 1964.

Joint Doctrine for Theater Counterair Operations. JCS Pub 3-01.2. 1 April 1986.

Tactical Force Protection in LIC Operational Conflict. Center for Low Intensity Conflict. 1 June 1988.

10 United States Code, Uniform Code of Military Justice.

Unified Action Armed Forces (UNAAF). JCS Pub 0-2. 1 December 1986.

WWW.SURVIVALEBOOKS.COM

INDEX

AC-130 gunship, 2-8

adjacent bases, 3-8

agreements
- host-nation support, 3-8
- international, 3-8
- law of war, 3-8
- security assistance organization, 3-8
- stationing, 3-8
- status-of-forces, 3-7 — 3-8

air defense measures
- establishment of, 2-9
- for port and harbor facilities, 2-14

air force elements, 3-6

alarms, 2-11

alternate base defense operations center, 3-5

ambassadors
- responsibilities of, 3-1
- and relationships with commanders in chief, 3-3

ambushes, B-4

antiarmor teams, 2-6

antiarmor weapons. 2-7

antipersonnel mines. *See* mines

antitank mines. *See* mines.

antivehicle mines. *See* mines.

area command, 3-4

area commander, 3-8

area damage control, 2-9 — 2-10, B-6

Army Training and Evaluation Program mission training plan. *See* training

attacks, responding to, B-4

avenues of approach, 2-2

aviation assets, 2-4 — 2-5, 2-8

base
- establishment of, 2-1
- physical layout, 2-10

base cluster, 2-7, 3-4, 3-8

base commander. *See* commander of the base

base communications officer, 4-4

base construction, 2-1

base defense
- definition of, 1-1
- fundamentals of, 1-3

base defense forces, 3-5. *See also* screening forces, main defense forces, close defense forces, *and* mobile reserve

base defense operations center. *See also* alternate base defense operations center
- as the focal point for base defense, 2-7
- mission of, 2-3
- responsibilities of, 3-4 — 3-5

base defense plan, sample, A-1 — A-15

base engineer forces, 3-7

base headquarters, 3-4

base service forces, 3-7

BDOC. *See* base defense operations center

belligerents, treatment of, 3-9

billeting, protection of, B-7

body search. *See* searches, personnel

bombings, terrorist, B-4

booby traps, B-3 — B-4

Bromacil, defoliant, 2-11

C^3. *See* command, control, and communications

chief, security assistance organization, 3-3

civil affairs, 3-7, 5-3. *See also* public affairs

civilians, protection of, B-6

close defense area
- mobile patrols in, 2-6
- perimeter, 2-6

close defense force
- on naval installations, 2-6
- responsibilities of, 2-6, 3-6
- as a security response force, 2-6

CMT. *See* crisis management team

combat service support considerations, B-5

WWW.SURVIVALEBOOKS.COM

command relationships, 3-1 — 3-8, B-6
command, control, and communications, 3-5
commander of the base, 2-3, 2-9, 2-12, 3-2, 3-4 — 3-7, 4-0, 5-3
commander of the joint base, 2-9, 5-3
commander in chief, 3-3
commanders of base elements, 3-6
communications
  at base defense operations center, 3-5
  capabilities, 4-4
  considerations, 4-3
  construction of facilities, 4-3
  for convoys, B-2
  duress signal, 4-4
  at guard locations, 2-11
  links, 3-8
  net, 4-2 — 4-3
  planning considerations, 4-3
  for security forces, 2-13
  system, 4-2
  wire lines, 4-4
concertina wire, 2-11
concrete barriers, 2-11
convoy order, format of, B-3
convoys, defending, B-2
counterattack plan, development of, 2-9
counterinsurgency operations, 3-9
counterintelligence, 4-1
country team
  relationships, 3-3
  responsibilities of, 3-1 — 3-2
cover and concealment
  as protection, 2-1 — 2-2
  for antiarmor weapons, 2-7
crisis management team, 2-10, D-7
crowd control, B-4
currents, study of, 2-13

deep operations, 1-1
defense, evaluation of, 2-3
defense analysis
  enemy, 2-0
  mission, 2-0
  terrain, 2-1
defense force commander, 3-6
defense forces, establishment of, 2-3
defense measures, for perimeter, 2-11
defense plan
  development of, 2-3
  active and passive measures, 2-0
defense training. *See* training
defensive rings, 2-3. *See also* close defense area, main defense area, *and* screening force area.
defoliant. *See* Bromacil
deployment
  advance parties, B-7
  defense considerations, 2-12
  and transit to deployment area, B-7
  and transit within deployment area, B-7
detailed body search. *See* searches, personnel
disaster control forces, 3-7
dogs. *See also* explosives
  for explosive detection, 2-11, B-3
  as sentries, B-2

EEFI. *See* essential elements of friendly information
emergency operations center, 2-10, 3-5, D-6
engineer equipment. *See* equipment, engineer
entrances
  rail and highway, 2-14
  security of, 2-11 — 2-12
EOC. *See* emergency operations center
equipment
  engineer, B-6, C-2
  general, C-1
  placement of, 2-10
  for ports, C-2
  for roadblocks and gates, C-1 — C-2
  for searches, C-2
  protection of, 2-12
essential elements of friendly information, B-9
explosives. *See also* dogs
  checks for, 2-13 — 2-14
  security procedures for, B-4

fire support coordination measures, 2-7 — 2-8
fire support planning, 2-5, 2-7

WWW.SURVIVALEBOOKS.COM

FLIR. *See* forward-looking infrared radar
foreign policy, 3-1
forward-looking infrared radar, 2-8
friendly response force. *See* tactical combat force
frisk. *See* searches, personnel
funding requirements, B-6

ground surveillance radar, 2-10
GSR. *See* ground surveillance radar

hard targeting. *See* targeting, hard
heavy weapons teams, 2-6
high ground, identification of, 2-12
host-nation forces
  in close defense area, 2-6
  as main defense force, 2-6, 3-7
  as mobile reserve, 2-6, 3-7
  responsibilities of, 3-7
  as screening force, 2-4, 3-7
host-nation laws, 3-9
host-nation support
  air traffic control, 5-2
  base security, 5-2
  command and control, 5-2
  convoy scheduling, 5-2
  facilities and systems, 5-1
  personnel, 5-2
  planning factors, 5-1
  rail operations, 5-2
  status-of-forces agreements, 5-2
HUMINT. *See* intelligence, human

identification, friend or foe procedures, 2-9
IMINT. *See* intelligence, imagery
indirect fire, 2-7
inspections, checkpoints for, 2-14
insurgents, treatment of, 3-9
intelligence
  in base defense operations center, 3-5
  collection methods, 4-1
  and combined operations, 5-2
  criminal information, 4-2
  dissemination of, 5-2
  exchange of information, 4-2
  governing directives, 4-0
  human, 4-1, 5-2, B-9
  imagery, 4-1, B-9
  local human, 4-2
  officer, 4-0
  open-source information, 4-2
  priority intelligence requirements, 4-1, B-5, B-7
  representative, 4-0
  services, 4-1
  signal, 4-1, B-9
  specialized equipment, 4-1
  staff, 4-0
  storing, 4-1
internal and external territories, protection of, 2-12
international agreements. *See* agreements
interrogation, 4-1
intruder drills, 2-10
intrusion detection, 2-10

joint base
  definition of, 1-1
  establishment of, 1-1 — 1-2
  organization of, 3-2
joint base command, 3-4
joint base commander. *See* commander of the joint base
joint base defense objectives, 1-1
Joint Chiefs of Staff, 3-3
joint force, 1-2
joint task force commander, 3-4

language translation, 4-1
leave, B-7
legal constraints, 3-8
liaison personnel, 3-8
liberty, B-7
LIC. *See* low-intensity conflict
lighting. *See* port and harbor facilities
listening posts, 2-8
living areas, protection of, 2-12

WWW.SURVIVALEBOOKS.COM

low-intensity conflict
considerations, 1-2
definition of, 1-2
missions, 1-2
political enviroment, 1-2
security measures, 1-3

machine gun teams, 2-6
main defense area, 2-4
main defense force
responsibilities of, 2-4 — 2-6, 3-6
as part of the screening force, 2-4
materiel. *See* equipment
medical facilities, 2-12, B-6
mid- and high-intensity conflicts
deep operations, 1-1
recon and sabotage, 1-2
military police, B-6
minefields, for use in tactical deception, 2-14
mines
antipersonnel, 2-8, 2-10
antitank, 2-8
antivehicle, 2-10
mission analysis, B-5
mission-oriented protective posture. *See* nuclear, biological, chemical
mob violence. *See* crowd control
mobile reserve, 2-3 — 2-4
to assist sentries, B-2
as a blocking force, 2-6
employment of, 2-6
launching counterattacks, 2-6
reinforcing a forward main defense area, 2-6
responsibilities of, 3-6
as a screening force, 2-6
mock attacks, 2-10
MOPP. *See* nuclear, biological, chemical
mortars, employment of, 2-7
MP. *See* military police

national command authority, 3-3
National Security Council, 3-1
naval forces, 3-6
NBC. *See* nuclear, biological, chemical
North Korean commando-rangers. *See* special purpose forces
nuclear, biological, chemical
defense measures, 2-9 — 2-10
defense of HN personnel, 5-2
mission-oriented protective posture, 2-9

observation posts, 2-1, 2-8, 2-10 — 2-11
obstacles
as protection, 2-1 — 2-2
snow and ice, 2-2
to slow the enemy, 2-8
operational contingencies, B-7
operations section, of base defense operations center, 3-5
operations security, 2-9, B-7 — B-10
intelligence indicators, B-9
measures, B-9
objectives, B-9
planning, B-6
program, B-8
OPSEC. *See* operations security
order of battle factors, 4-1
overwatch, using aircraft for, 2-1

pass, B-7
patrol boats, to guard port and harbor facilities, 2-13
patrols
as active security measures, 2-8
foot, B-0
security, B-0 — B-1
vehicle, B-0 — B-1
perimeter, sectors of operation, 2-5
personnel, protction of, 2-12
personnel exchange. *See* language translation
pier clearance, 2-13
planning considerations
air defense, 2-9
antiarmor weapons, 2-7
area damage control, 2-9 — 2-10
aviation assets, 2-7
counterattacks, 2-9
defense forces, 2-3 — 2-6

WWW.SURVIVALEBOOKS.COM

indirect fire, 2-7
mines and obstacles, 2-7
mobile reserve, 2-6 — 2-7
NBC defense. *See* nuclear, biological, chemical
physical layout of base, 2-10 — 2-12
security measures, 2-8
work priorities, 2-8

port and harbor facilities
deployment checks, 2-13
lighting of, 2-13
port checks, 2-14
predeployment checks, 2-13
protection of, 2-12 — 2-14

predeployment, 2-13, B-5

priorities, work. *See* planning considerations

priority intelligence requirements. *See* intelligence

prisoners, treatment of, 3-9

psychological operations forces, 3-7, 5-3

public affairs, 5-3 — 5-4. *See also* civil affairs

quick-body search. *See* searches, personnel

recon and sabotage, 1-2

redeployment
advance parties, B-8
after-action report, B-8
public affairs policy, B-8
reverse deployment, B-8
trainer's debriefing, B-8

remote sensors, 2-1

response forces, 2-7

return-to-force, 2-9

riot control. *See* crowd control

road blocks, B-1

road movement. *See* convoys, defending

rules of engagement, 3-8 — 3-10

screening force, 2-4

screening force area
listening posts, 2-4
observation posts, 2-4
outer defensive ring, 2-4

searches
buildings, B-3
personnel, B-2 — B-3
vehicles, B-1

secretary of state, responsibilities of, 3-1

sectors of operation, 2-5

security
degradation of, B-7
during movements, B-6
enhancement of, B-8
of entrances, 2-11 — 2-12
planning, B-6
for predeployment, B-5
tactical, B-0 — B-5

security measures
active, 2-8
establishment of, 2-8
for individual vessels, 2-14
passive, 2-8

security police, 3-7, B-6

sentries, B-1 — B-2

SIGINT. *See* intelligence, signal

signal intelligence. *See* intelligence, signal

sonic simulators, 2-14

Soviet
doctrine, 1-1 — 1-2
spetsnaz, 1-2

special equipment, maintenance of, B-6

special purpose forces
North Korean commando-rangers, 1-2
Soviet *spetsnaz*, 1-2

stand-to alerts, 2-8

status-of-forces agreements. *See* agreements

storage and distribution areas, protection of, B-5

surveillance, 2-11

TACP. *See* tactical air control parties

tactical air control parties, 2-7

tactical combat force, 2-2
commander's responsibilities, 2-3
to counter Level II and III threats, 2-7
responsibilities of, 3-8

tactical deception, 2-14

WWW.SURVIVALEBOOKS.COM

targeting, hard, B-0
terrain
  canalizing, 2-2
  decisive, 2-2
  key, 2-2
  obstructing, 2-2
  open, 2-2
  and site selection, 2-1
terrorism, D-1 — D-10
  alert notification process, D-9
  contingency plan for, 2-10
  countering, B-6, D-10
  definition of, D-1
  indicators, D-3
  response to, D-6
  unit vunerability, D-1
terrorist skills. *See* terrorism, countering
terrorist teams. *See* terrorism, countering
theater command, 3-1
theater commander, 4-3
theater of operations, 3-1
threat
  assessment, D-2 — D-3, B-5, B-7
  briefings, 4-1
  decision model, D-8
  defending against, 2-2 — 2-3
  levels, 1-2 — 1-3, D-2 — D-4
  susceptibility factors, D-1 — D-2
threat conditions, 3-5, D-2, D-4 — D-6
threat management force, 2-10, D-7 — D-8
THREATCONs. *See* threat conditions
tides, 2-13
TMF. *See* threat management force
training
  Army Training and Evaluation Program mission training plan, B-6
  collective, B-6
  defense, 2-10
  in host-nation support functions, 5-2
  individual, B-6
  institutional, B-6
  Marine Corps Combat and Readiness Evaluation System, B-6
  support, B-6
  tactical exercises without troops, B-6
  tapes, B-6
  threat awareness, B-6
  war games, B-6
  weapon familiarization, B-6
transient forces, 3-7 — 3-8

unexploded devices. *See* explosives
unit vunerabilities, B-5, B-9
United States laws, 3-8 — 3-9
urban defense, B-1 — B-2

vehicle control points, at port and harbor facilities, 2-13

war games. *See* training
warning devices. *See* intrusion detection
water, clarity and depth, 2-13
work priorities. *See* planning considerations
working areas, protection of, 2-12

☆U.S. G.P.O. 1989-627-027:00103