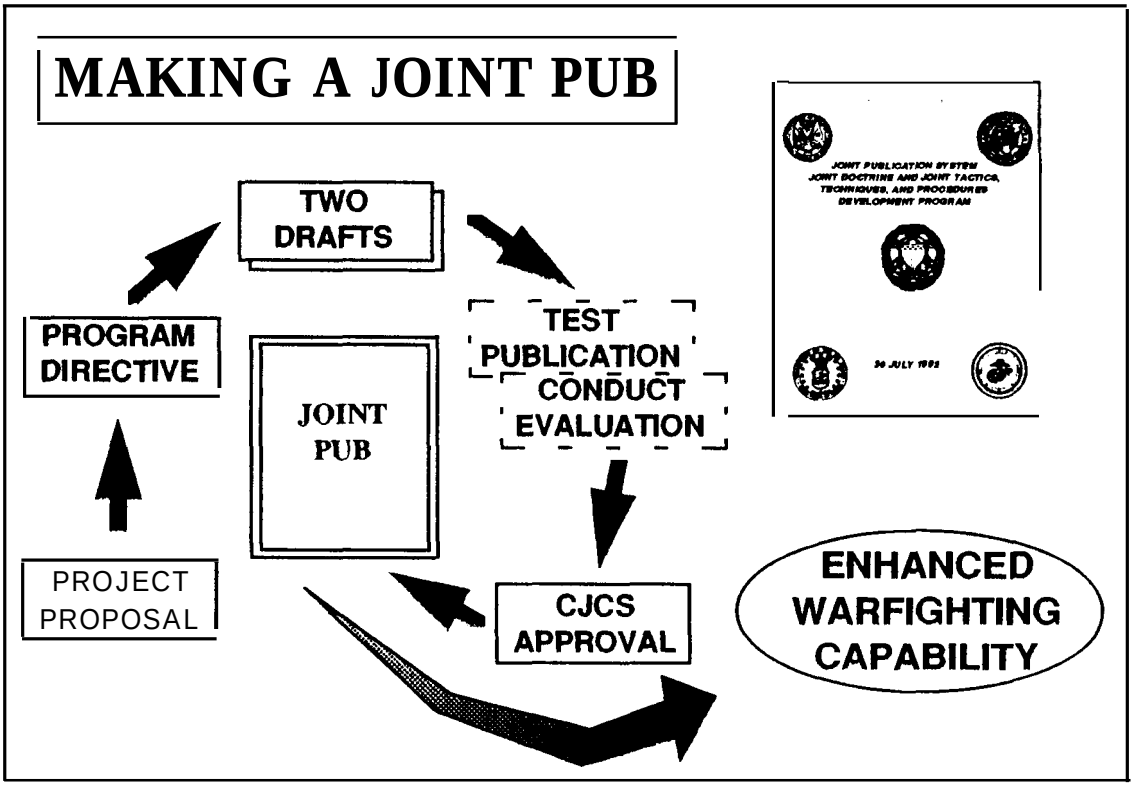
JOINT PUB 3-10.1

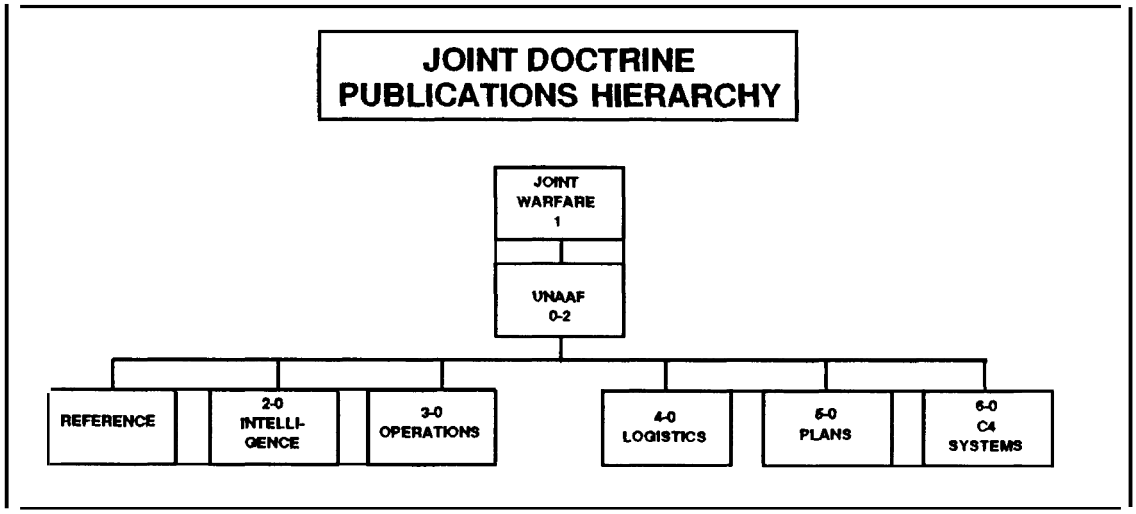
JOINT TACTICS, TECHNIQUES, AND PROCEDURES (JTTP) FOR BASE DEFENSE

15 MARCH 1993

A large body of joint doctrine (and its supporting tactics, techniques, and procedures) has been and is being developed by the US Armed Forces through the combined efforts of the Joint Staff, Services, and combatant commands. The following chart displays an overview of the development process for these publications.



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy. Joint Pub 3–04 .1 is located in the operations series of joint publications .



Joint Pub 1–01, "Joint Publication System, " provides a detailed list of all joint publications. Joint pubs are also available on CD–ROM through the Joint Electronic Library (JEL) . For information, contact : Joint Doctrine Division, J-7, 7000 Joint Staff Pentagon Washington, D. C. 20318–7000 .

Reply ZIP Code: Joint Pub 3-10.1
20318-0400

MEMORANDUM FOR: Distribution List

Subject: Joint Pub 3-10.1, "Joint Tactics, Techniques, and Procedures (JTTP) for Base Defense"

1. This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth principles, doctrine, and military guidance to govern the joint activities and performance of the Armed Forces of the United States.

2. Recommendations for changes to this publication should be submitted to the Director for Operational Plans and Interoperability (J-7), Joint Staff, Washington, D.C. 20318-7000.

3. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal.

4. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

5. Additional copies of this publication can be obtained through Service publication centers.

6. Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

7. The lead agent for this publication is the US Army.

8. The Joint Staff doctrine sponsor for this publication is the Director, J-7.

For the Chairman of the Joint Chiefs of Staff:

H. L. SHEFFIELD
Captain, USN
Secretary, Joint Staff

Enclosure

Distribution:

By Secretary, Joint Staff:

Joint Staff	OSD	NSA	CIA	JWC	USELMNORAD
FEMA	DISA	DIA	DLA	DMA	DNA
NDU	MCCDC	JEWC	AFSC	JDC	DISA-JIEO
CIO					

Additional copies may be obtained from the Secretary, Joint Staff (Documents Division).

Five copies each to: Offices of CSA, CNO, CSAF, CMC, USCG

Copies each to:

USLANTCOM (25)	USCENTCOM (25)	USEUCOM (25)	FORSCOM (25)
USPACOM (25)	USSOUTHCOM (25)	USSPACECOM (25)	
USSOCOM (25)	USSTRATCOM (25)	USTRANSCOM (1)	

Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army: US Army AG Publication Center,
2800 Eastern Boulevard, Baltimore, MD 21220-2898.

Air Force: Air Force Publications Distribution Center,
2800 Eastern Boulevard,
Baltimore, MD 21220-2896.

Navy: CO, Navy Aviation Supply Office,
Distribution Division (Code 03443)
5801 Tabor Ave, Philadelphia, PA 19120-5000.

Marine Corps: Marine Corps Logistics Base,
Albany, GA 31704-5000.

(INTENTIONALLY BLANK)

JOINT TACTICS, TECHNIQUES, AND PROCEDURES FOR BASE DEFENSE

RECORD OF CHANGES

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

In accordance with the procedures contained in Joint Pub 1-01, change recommendations to this publication will be forwarded to:

Urgent: TO: CSA WASHINGTON DC//DAMO-FDQ//
INFO: JOINT STAFF WASHINGTON DC//J7-JDD//

Routine: Operational Plans and Interoperability
Directorate, J-7, JDD
Joint Staff
Washington, D.C. 20318-7000

LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of your document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
i thru viii	O	D-1 thru D-4	O
I-1 thru I-8	O	E-1 thru E-8	O
II-1 thru II-12	O	F-1 thru F-14	O
III-1 thru III-4	O	G-1 thru G-4	O
IV-1 thru IV-18	O	H-1 thru H-4	O
V-1 thru V-4	O	J-1 thru J-6	O
A-1 thru A-6	O	K-1 thru K-10	O
B-1 thru B-4	O	GL-1 thru GL-8	O
C-1 thru C-4	O		

Deleted pages: None.

JOINT TACTICS, TECHNIQUES, AND PROCEDURES FOR BASE DEFENSE

PREFACE

1. Purpose. This publication sets forth the joint tactics, techniques, and procedures (JTTP) necessary for the defense of joint and single-Service bases outside the continental United States (CONUS) and outside the states of Alaska and Hawaii. It expands upon the doctrine set forth in Joint Pub 3-10, "Doctrine for Joint Rear Area Operations." It recognizes that effective defense may require careful integration of air and surface forces, because it is likely that the threat will consist of integrated enemy air and surface operations. The focus is on establishing and maintaining security of joint and single-Service bases in a joint rear area and providing guidelines for base commanders for coordinating and integrating security and defense of their bases with their other responsibilities. This publication should be supplemented with Service manuals that provide more detail on the measures necessary to secure and defend bases. This publication:

   a. Prescribes the command and control arrangements between bases, base clusters, and their higher headquarters.

   b. Describes the responsibilities of base and base cluster commanders and commanders of units and activities within such bases.

   c. Sets forth procedures for base defense and security from the standpoints of operational concepts, analysis, planning, command and control, intelligence, communications, and host nation support (HNS).

2. Application

   a. Tactics, techniques, and procedures established in this publication apply to the commanders of combatant commands, subordinate unified commands, joint task forces, and subordinate component commands. These measures also may apply when significant forces of one Service are attached to forces of another Service, or when significant forces of one Service support forces of another Service.

   b. In applying the tactics, techniques, and procedures set forth in this publication, care must be taken to distinguish between distinct but related responsibilities in the two channels of authority to forces assigned to

combatant commands. The Military Departments and Services recruit, organize, train, equip, and provide forces for assignment to combatant commands and administer and support those forces. Commanders of the unified and specified commands exercise combatant command (command authority) over these assigned forces. Service component commanders are responsible both to joint commanders in the operational chain of command and to the Military Departments and Services in the chain of command for matters for which the joint commander has not been assigned authority.

c. The tactics, techniques, and procedures in this publication are authoritative but not directive. Commanders should exercise their best judgment in its application. This doctrine should be followed, except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in consultation with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance.

3. Scope. This publication describes tactics, techniques, and procedures for the security and defense of bases and base clusters outside the United States in the joint rear area under all threat conditions. It is written for:

a. Commanders and staff officers responsible for planning and conducting joint rear area (JRA) security and defense operations and organizing the forces for security and defense.

b. Commanders, staff officers, and subordinates responsible for the defense of bases and base clusters.

c. Those responsible for the training of base defense forces.

d. Those preparing and presenting instructional material in the military education system.

4. Basis

a. Joint Pub 0-1 (in development), "Basic National Military Doctrine."

b. Joint Pub 0-2, 1 December 1986, "Unified Action Armed Forces (UNAAF)."

c. Joint Pub 1-01, 30 July 1992, "Joint Publication System Joint Doctrine and Joint Tactics, Techniques and Procedures Development Program."

d. Joint Pub 1-02, 1 December 1989, "DOD Dictionary of Military and Associated Terms."

e. Joint Pub 3-0 (Test Pub), 10 January 1990, "Doctrine for Joint Operations."

f. Joint Pub 3-10 (Test Pub), 30 October 1991, "Doctrine for Joint Rear Area Operations."

g. Joint Pub 4-0, 25 September 1992, "Doctrine for Logistic Support of Joint Operations."

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

APPENDIX

CHAPTER I

JOINT REAR AREA CONCEPTS

1. General

a. This chapter describes the joint rear area (JRA) in terms of its geography and functions. It discusses the levels of threat as they affect rear area operations and base defense, and recognizes that effective defense may require careful integration of air and surface forces because the threat will probably consist of integrated air and surface operations. The JRA concept is applicable across the operational continuum. This chapter also sets forth the legal aspects that base commanders must consider.

b. The rear area of a joint force may be vulnerable to attacks by modern enemy forces with sophisticated surveillance devices, accurate weapon systems, and transport assets capable of inserting forces behind friendly combat formations. Rear area installations also may be the targets for indigenous elements capable of the full spectrum of unconventional operations ranging from crime, sabotage, and terrorism to large-scale raids. The JRA contains units and facilities from all components that are critical to the theater or area of operations (AO). These units and facilities are organized into bases to enhance their effectiveness and security.

2. Background

a. Introduction. A JRA is a specific land area within a joint force commander's (JFC's) AO designated to facilitate protection and operation of installations and forces supporting the joint force.

b. Location and Configuration of JRA

(1) This publication concentrates on bases in the JRA. The tactics, techniques, and procedures set forth also can apply to bases established in the combat zone.

(2) The JRA does not normally include a naval AO. When a naval AO and a JRA meet along a coastline, the high water mark will normally designate the boundary between the two. Ports and harbors, though not the built-up areas around them, are normally included in the naval AO. Ports and harbors on the coastline of a JRA may interface with bases necessary for the simultaneous support of land, air, and maritime operations. See Appendix A, Maritime-Land Interface.

(3) The JRA is organized into tactical areas of responsibility (TAORs), which may, in turn, be subdivided into smaller TAORs to facilitate control of the defense. Each base has a corresponding TAOR, which includes the base itself. To facilitate the span of control for area commanders, bases may be grouped into base clusters. Each base cluster's TAOR encompasses those bases included in the cluster.

c. Evolution of JRA

(1) In the early stages of theater development, rear area bases can be highly vulnerable. From the outset, base tactical areas of responsibility (TAORs) must be clearly defined, and rear area security forces must be available. The availability and effectiveness of host nation (HN) contributions to base defense must be assessed. Based on this assessment, the JFC may be required to adjust the concept of operations, sequencing, and unit missions.

(2) The development of base defense procedures during theater development should be directed toward the establishment of a stable JRA supporting the JFC's concept of operations.

d. JRA Operations. The implementation of JRA doctrine and the JTTP for base defense protects the JRA or supports the unified or joint force. The broad functions of activities assigned to bases in the JRA include but are not limited to:

(1) Force Projection. Particularly where air assets are involved, the most important missions of some rear area bases may be to project combat power in support of the JFC's objective.

(2) Security. Designated rear area units contribute to the security of the entire joint force. Bases may contain, for example, aircraft or missiles capable of performing defensive counterair missions, radars, and other equipment critical to air defense or units conducting counterintelligence (CI), executing electronic counter-countermeasures (ECCM), or guarding enemy prisoners of war (EPWs).

(3) Command, Control, Communications, and Computers (C4). Bases containing headquarters and signal centers at all levels may be among the largest and most critical installations in the JRA.

(4) Intelligence. Bases in the JRA may contain intelligence centers and electronic facilities designed to interface with forward-based, airborne, or space-based sensors.

(5) Sustainment. The fighting forces depend upon the combat service support forces, material, and resources to sustain operations on the bases throughout the JRA.

(6) Movements. Joint movement centers (JMCs), rail terminals, and seaports and aerial ports of debarkation (SPODs, APODs) occupy bases in the JRA. Lines of communications (LOCs) between bases and from the JRA to combat forces also must be secured.

(7) Medical Support. Medical facilities in the JRA are special sustainment bases, that should be situated away from all legitimate military targets to avoid endangerment. The Geneva Conventions prescribe the security and defensive measures, as well as the protections, applicable to medical facilities and their personnel.

(8) Infrastructure Development and Area Management. Construction sites and facilities of construction units involved in base development must be considered as bases for defense purposes. All units and facilities in the JRA must be properly positioned and adequately protected to maximize their effectiveness.

(9) Host Nation Support. The HN, in accordance with negotiated agreements, will assist in performing defense functions within the JRA. US forces may also, in coordination with the HN, be responsible for the defense of HN facilities on US bases. Civilian agencies of the US Government, such as the Drug Enforcement Administration and Agency for International Development, located in the HN, may also occupy US or HN bases in the JRA.

e. Combined Considerations

(1) Host Nation Territorial Organization. The JRA normally will be in sovereign territory presided over

by viable and capable HN governments. These governments, represented by their forces and law enforcement agencies, generally will have responsibility for many rear area functions. The JFC will coordinate US HNS requirements with HN commands.

(2) Third Country Allies. When the forces of allied nations share base facilities with the United States and the HN, unity of effort must be achieved by cooperative measures. The presence of allied forces and facilities in the JRA will have its impact on virtually every aspect of base defense, including command and control arrangements, communications, fire support planning and integration, location of various national units, rules of engagement (ROE), establishment of a tactical combat force (TCF), liaison, and the establishment of the bases and base clusters themselves. Combined considerations are discussed in Joint Pub 3-10.

3. Levels of Response. Threats to bases in the rear area are categorized by the levels of defense required to counter them. Each level, or all levels simultaneously, may exist in the JRA. Emphasis on specific base defense and security measures may depend on the anticipated threat level. Responsibilities for dealing with threats at each level are discussed in Chapter II. See Table I-1. The threat levels that follow also are discussed in detail in Joint Pub 3-10.

a. Level I threats can be defeated by base or base cluster self-defense measures.

b. Level II threats are beyond base or base cluster self-defense capabilities but can be defeated by response forces, normally military police (MP) units assigned to area commands with supporting fires.

c. Level III threats necessitate the command decision to commit a TCF. Level III threats, in addition to major ground attacks, include major attacks by aircraft and theater missiles armed with conventional weapons or nuclear, biological, and chemical (NBC) weapons. Appendix B, NBC, and Appendix C, Air and Missile Defense, contain special considerations for the defense of bases against NBC and air threats.

Table I-1. Threat Level Matrix

Threat Level	Examples	Response
I	Agents, saboteurs, sympathizers, terrorists	Unit, base, and base cluster self-defense measures
II	Small tactical units, unconventional warfare forces, guerrillas	Self-defense measures and response force(s) with supporting fires
III	Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations	May require timely commitment of tactical combat force

4. Legal Constraints. Commanders' intent must not be in conflict with legal constraints. Commanders at all levels must be well-informed on the legal aspects of the use of force. The types of guidance relevant to the use of force include international law, US law, HN law, law of war, ROE, and UN sanctions (as applicable). Together, these laws and rules regulate the status and activities of the forces in all states of the operational continuum.

a. International Agreements. International agreements are the most important source 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 may regulate, to some extent, the relationship between the opposing parties in internal conflicts. The US Armed Forces are committed to conducting defense operations according to the applicable provisions of the law of war,

including those of the Hague and Geneva Conventions. The four relevant categories are those concerning:

(1) Law of war.

(2) Security assistance agreements.

(3) Status of forces agreements (SOFA).

(4) HNS agreements.

b. US Laws. US forces overseas follow US law as expressed in statutes, Executive orders, DOD directives and instructions, and military regulations. Directives issued by the theater combatant commander and by the component command commanders are subject to applicable SOFAs or similar agreements. Publications containing applicable US laws and SOFAs should be on file at the security assistance office (SAO) or with the command legal adviser. Some SOFAs and similar agreements are classified.

c. Host Nation Laws. Sovereign HN laws apply to all US forces stationed in that country to the extent provided for by international agreements. Neither US nor HN laws have priority over the law of war; for example, commanders are responsible for the humane care of EPWs regardless of HN policies. Such laws emanate from the various levels of government and from the agencies functioning at each echelon. US advisers, commanders, staff officers, and Service members must understand critical HN laws, and the provisions of DOD and Service policies concerning HNS.

d. Law of War. The law of war (also called the law of armed conflict) and the obligations of the US Government under that law govern the conduct of US forces. US commanders will ensure that the DOD Law of War Program is implemented in accordance with directives and procedures.

(1) Treatment of Combatants. During a war, the treatment of combatants is governed by the law of war, the 1949 Geneva Conventions, and relevant HN and US domestic laws.

(2) Treatment of Insurgents. For insurgents held in US military custody, US policy requires and directs humane care and treatment from the moment they are detained until they are released or repatriated. This policy also applies to all detained or interned

personnel. In combating an insurgency, defenders must accord humane treatment to any civilians involved and scrupulously observe the law to demonstrate US Government concern for individuals.

(3) Treatment of Prisoners. The treatment of EPWs is governed by the 1949 Geneva Conventions. Whether captives are entitled to EPW status will be determined in accordance with the rules and procedures of the Geneva Conventions.

(4) Protection of Noncombatants. These responsibilities under the law of war are especially applicable in or near bases in the rear area. In addition to taking measures to avoid civilian casualties during combat operations, commanders have a special responsibility to safeguard the US and HN civilians employed in support of base missions. Civilian protection from enemy threats must take a high priority in base defense and security plans.

e. Rules of Engagement. ROE are directives issued by competent military authority that delineate the circumstances under which US forces will initiate or continue combat engagement with other forces. Theater combatant commanders establish ROE based upon guidance provided by the National Command Authorities (NCA) through the Chairman of the Joint Chiefs of Staff.

5. Public Affairs. The public affairs (PA) objective for the base is to gain public support and understanding, especially from those on or near the base. The base commander should encourage a strong and active command information program to ensure fullest dissemination of security requirements, safety precautions, and other essential matters. Flexible public information and community relations programs should be established to provide maximum disclosure of information within the constraints imposed by safety and security requirements. Close coordination with civil affairs (CA) personnel is also encouraged to better meet external information requirements. PA activities must be coordinated with other staff agencies to ensure that all actions are complementary.

(INTENTIONALLY BLANK)

CHAPTER II

COMMAND AND CONTROL

1. General. Unity of effort is as essential for the forces in the JRA as it is for the combat forces. Clear-cut procedures for authority and responsibility must be established for the successful execution of missions by the units and activities in the JRA and for the security and survival of the bases housing those units and activities. This chapter sets forth the responsibilities, facilities, geographic organization, and liaison requirements necessary to command, coordinate, and synchronize the defense of bases within the JRA.

2. Responsibilities

a. Theater Combatant Commander. A theater combatant commander (CINC), as commander of a unified command, is ultimately responsible for all JRA operations conducted in the theater. Joint Pub 0-2 provides a listing of CINC responsibilities.

(1) A theater CINC maintains the security of the command and protects US possessions and bases against attack or hostile incursions.

(2) A theater CINC assigns responsibility for defense of the JRA and establishes the method of command or coordination to be exercised or delegates that authority to a subordinate JFC.

(3) A theater CINC ensures that appropriate command relationships between subordinate area and local base defense commanders are established and that local defense areas are delineated, or a theater CINC delegates that authority to a subordinate JFC.

(4) A theater CINC determines the classification of bases in the theater, unless determined by higher authority. A base may be:

(a) A single-Service base.

(b) A joint base. A joint base may be either:

1. One in which one Service component has primary interest.

2. One in which two or more Service components have coequal interest.

b. Joint Force Commander. A JFC (who may be a theater CINC) may form subordinate joint commands whose commanders will be subordinate JFCs. Subordinate JFCs may organize by Service component or function. In the case of a unified command, the JFC may command through a subordinate unified command when it is authorized through the Chairman of the Joint Chiefs of Staff. The term "JFC" will be used throughout the remainder of this publication to identify the commander of a joint force, except where specific responsibilities or functions are vested solely in the theater combatant commander's authority.

c. Supporting Combatant Commanders. Elements of unified commands providing support to the theater, such as US Transportation Command (USTRANSCOM) and US Space Command (USSPACECOM), may establish facilities or occupy bases within the theater. The JFC must ensure that these facilities or bases are adequately defended. Command and coordination relationships between those elements and the area or base commanders subordinate to the JFC will be defined by orders or memorandums of agreement. Coordination must include sharing of intelligence information, because supporting CINC operations are often planned outside the theater.

d. Joint Rear Area Coordinator. The JFC may designate a subordinate commander or a member of the joint force headquarters as the joint rear area coordinator (JRAC). The JFC considers mission requirements, force capabilities, the nature of the JRA, and the threat in making the selection. The JRAC is responsible for coordinating the overall security of the JRA in accordance with JFC directives and priorities. The JRAC coordinates with appropriate JRA commanders to ensure that they maintain the security of their AOs to facilitate sustainment, HNS, infrastructure development, and movements of the joint force. The JRAC also ensures that commanders establish reliable intelligence support and practice area management within their AOs with due consideration of security requirements. The JRAC establishes secure and survivable communications with all forces and commands operating in or transiting the JRA. The JRAC is also responsible for ensuring that the surface area security requirements and priorities for the JRA are integrated in the overall security requirements of the joint force and are coordinated with the area air defense commander (AADC). However, in cases of level III threat or other emergencies, the JFC may assign a

subordinate commander the responsibility to counter the threat and restore JRA security. In this case, the assigned subordinate commander would assume the JRAC's responsibilities and be tasked to restore JRA security. The JRAC will support any requirements requested by the assigned subordinate commander. This option would be exercised for the duration of the threat or as directed by the JFC. The AADC is responsible for the security of the airspace above the JRA. Joint Pub 3-10 includes a detailed discussion of JRAC responsibilities. Figure II-1 depicts notional JRA command and control (C2) networks, with options for the selection of the JRAC.

e. Component Commanders. The JFC may exercise command through Service component or functional component commanders. Although this publication is based on a Service component framework, the principles can be applied within a functional structure. Component commanders may be given responsibility for overall defense of designated areas and bases within the JRA. Joint Pub 3-10 describes component relationships in the JRA.

f. Area Commanders. Service component commanders with area responsibilities subdivide their areas into TAORs for which subordinate commanders are responsible. Land areas in the JRA are normally assigned to Army or Marine components. Although the responsibilities of area commanders do not vary, differences between Army and Marine organizations may dictate some differences in JRA organization. Figure II-2 shows a notional geographic organization for a JRA.

(1) Army forces (ARFOR) in the JRA can constitute a theater army, whose commander, if designated the JRAC, is responsible for the surface security of the entire JRA. The Commander, Army Forces (COMARFOR), organizes by assigning to one or more theater army area commands (TAACOMs) the defense and security responsibilities for appropriate subdivisions of the JRA. TAACOM AORs will be further subdivided and assigned to area support groups (ASGs). ASG commanders plan, coordinate, control, and execute rear security operations through rear area operations centers (RAOCs) or rear tactical operations centers (RTOCs) (see subparagraph 3b).

(2) The JRA, or a part of the JRA, may be the responsibility of the Commander, Marine Forces,

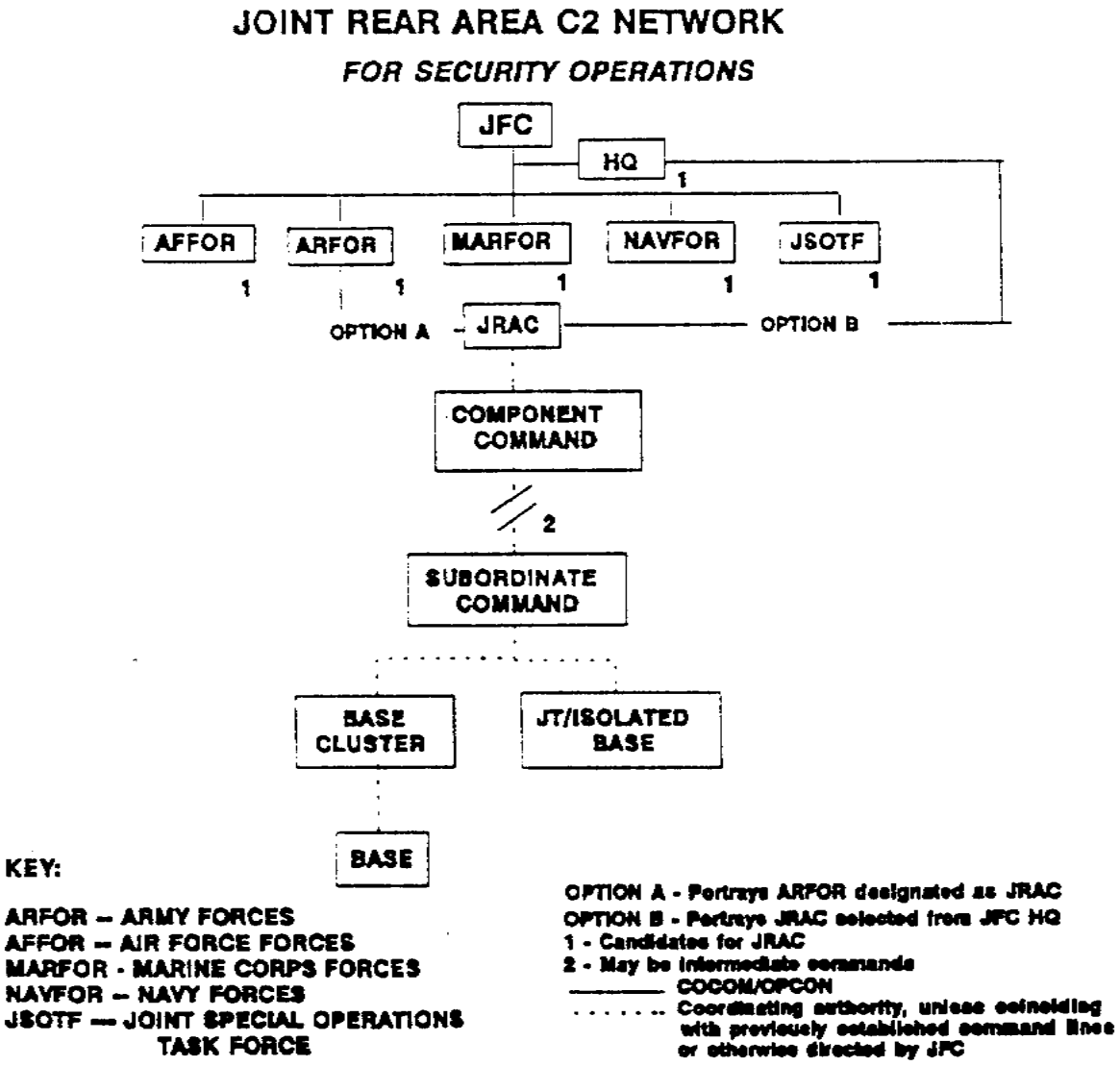


Figure II-1. Joint Rear Area C2 Network.

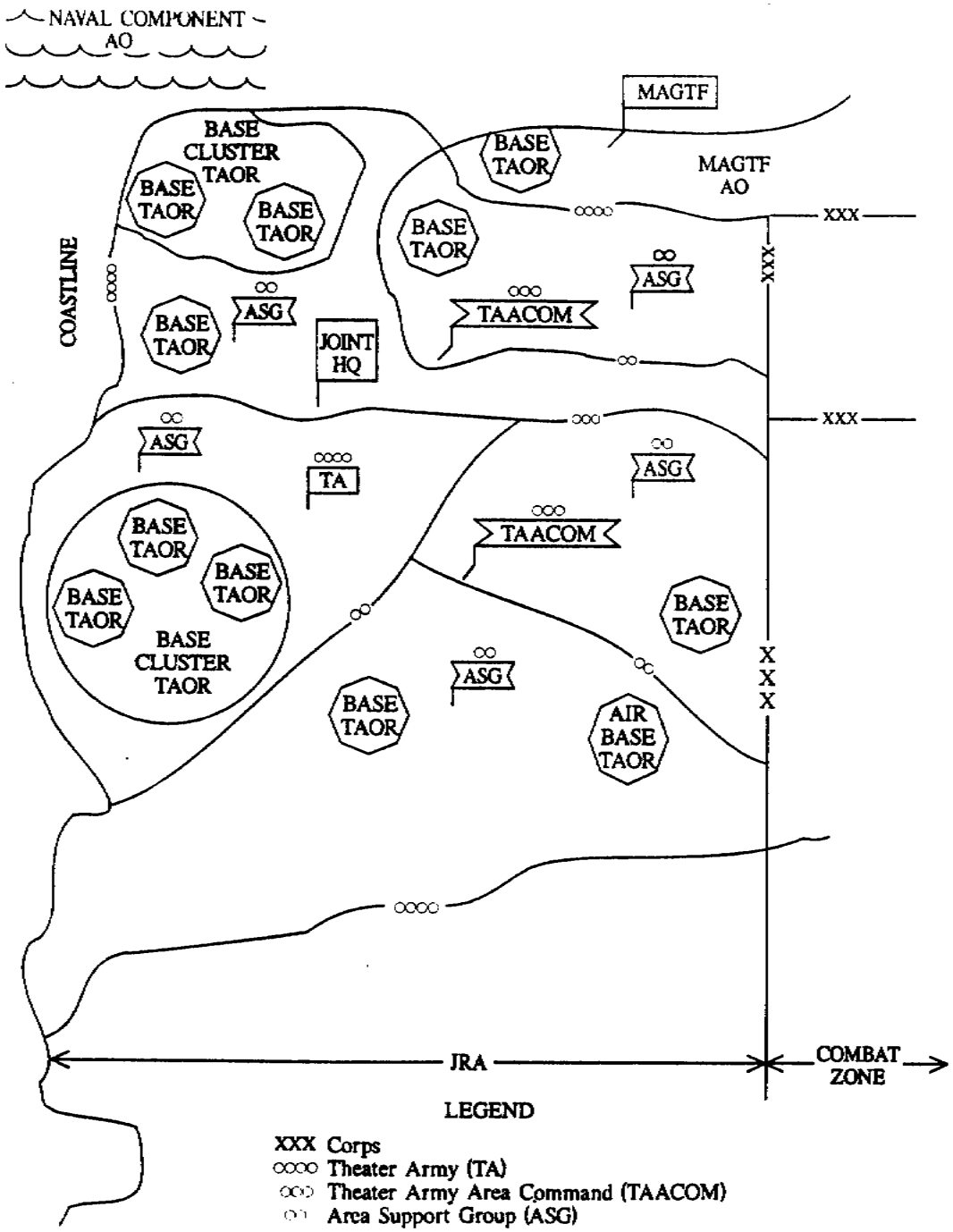


Figure II-2. Notional Geographic Organization -- Joint Rear Area

Figure II-2. Notional Geographic Organization - Joint Rear Area

(COMMARFOR). The COMMARFOR may designate to the commander of the Marine air-ground task force (MAGTF) the mission of Marine rear area operations, including the defense of logistic and air bases. The MAGTF commander may, in turn, choose to designate the MAGTF combat service support commander this mission.

g. Base Cluster Commanders. The base cluster commander (base community commander assumes this responsibility in selected theaters), when designated, is responsible for coordinating the defense of bases within the base cluster and integrating base defense plans into both a base cluster defense plan and the area defense plan. Specific responsibilities for base cluster defense include:

(1) Establishing a base cluster operations center (BCOC) from available base or cluster assets to serve as the focal point for security operations in the base cluster area of operations and integrate execution of local base defense plans with the next echelon RAOC or RTOC. See subparagraph 3c.

(2) Providing appropriate facilities and housing for necessary liaison personnel from bases within the cluster.

h. Base Commanders. Base commanders (or senior installation commander) are responsible for the defense of their bases. The forces of other Service components, assigned to the base for base defense, will be under the base commander's operational control (OPCON). Forces of other Service components assigned or attached to the base for purposes other than base defense will support the base defense effort during an attack or threat of an attack. The base commander's specific responsibilities for defense of the base include:

(1) Establishing a base defense operations center (BDOC) and an alternate BDOC to serve as the focal point for security operations in the base defense area of operations and integrate execution of local base defense plans with the next echelon RAOC or RTOC. See subparagraph 3d.

(2) Planning for employment of transient forces by ensuring that base defense plans include provisions for augmenting the regularly assigned base defense forces during an attack or when the base is threatened with attack. In an emergency, the base commander will be considered to be an area

commander. As such, the commander will have the authority to require support from transient forces for base defense. Principles governing support provided by a transient force during an emergency, and the responsibilities of the commanders concerned, are fully addressed in Joint Pub 0-2.

(3) Maintaining liaison with adjacent bases, base clusters and supporting HN security agencies.

(4) Developing base defense plans that incorporate tenant units.

(5) Disseminating air, ground, and missile attack warnings using established warning alarms.

(6) Maintaining communications with the designated reinforcing and tactical combat forces.

(7) Integrating area security plans with the RAOC and RTOC.

(8) Maintaining communications with supporting emergency ordnance disposal unit.

(9) Developing and requesting information requirements to support area defense operations.

i. Tenant Unit Commanders. The commanders of tenant forces at a base are responsible for the following:

(1) Participating in the preparation of base defense plans.

(2) Providing, staffing, and operating base defense facilities in accordance with base defense plans.

(3) Conducting individual and unit training to ensure readiness for assigned defense tasks.

(4) Providing their share of facilities, equipment, and personnel for the BDOC and, when appropriate, for the BCOC.

(5) Advising the base commander on defense matters peculiar to their units.

(6) Providing for their own internal security.

(7) Sustaining and administering their own forces.

(8) Providing their requirements for common-user communications systems to the base commander's communications element.

(9) Providing organic communications to support their own command's requirements.

j. Response Force Commanders. The response force is a mobile force designated, usually by the area commander, to deal with Level II threats. Response force commanders may be put under the tactical control (TACON) of commanders of threatened bases. They may be assigned their own TAORs, where they will coordinate with base defense forces within the TAOR under a common superior. Every opportunity should be taken to plan and rehearse response force operations within the TAOR.

k. Tactical Combat Force Commanders. The TCF commander is designated by the JFC. The command relationships between the TCF and the JRAC or commanders in the JRA will be determined by the JFC. The TCF is a combat unit, with appropriate combat support and combat service support assets, which is assigned the mission of defeating Level III threats. The threat requiring the commitment of a TCF is usually of such magnitude that several bases or base clusters are threatened. The TCF commander may be directly subordinate to the JFC or to a component commander. Once committed, the TCF is given an TAOR in which to accomplish its assigned mission. Plans for the employment of the TCF should be coordinated with component commanders, area commanders, base cluster commanders, base commanders and with the HN. The TCF and base defense forces should conduct training exercises and rehearsals to ensure that C2 procedures are effective. Joint Pub 3-10 discusses TCFs in detail.

3. Operations Centers

a. Joint Rear Tactical Operations Center. The JRAC will establish a joint rear tactical operations center (JRTOC), using joint force staff elements and representatives from components operating in the JRA, to assist in meeting JRA security responsibilities. Component and staff representation will vary in accordance with mission, forces, and area requirements, and should support the planning, coordination, and execution of JRA operations. The JRAC will ensure that component representation, and representation from the JRAC staff, is sufficient to support assigned mission

responsibilities. The JRTOC should be collocated with a RAOC or RTOC where possible. The JRTOC serves as the JRAC's centralized planning, coordinating, monitoring, advising, and directing agency for JRA operations. It coordinates with other elements on the JRAC staff, with higher, lower, and adjacent command staffs, and with HN and allied command staffs.

b. Rear Area Operations Centers and Rear Tactical Operations Centers. Army and Marine area and subarea commanders usually have RAOCs and RTOCs to assist in accomplishing their base defense missions. These C2 facilities serve as the area and subarea commanders' planning, coordinating, monitoring, advising, and directing agencies for area security operations.

c. Base Cluster Operations Centers. The base cluster commander establishes a BCOC from available base or cluster assets to serve as the focal point for defense operations. Its functions are similar to those of individual BDOCs, and it also may serve as the BDOC for the base on which it is located.

d. Base Defense Operations Centers. The commander of the base establishes a BDOC from available base assets. It serves as the focal point for base security and defense. The BDOC frees the base staff to concentrate on primary support missions. The BDOC may be composed of elements of the base commander's headquarters, elements from tenant units, or a combination of both. The BDOC plans, directs, integrates, coordinates, and controls all base defense efforts and coordinates and integrates into area security operations with the RAOC and RTOC. For the purposes of this publication, the BDOC performs three critical functions: operations, intelligence (including CI), and communications. Some functions, especially on Air Force installations, may be performed by other base command facilities. Appendix D sets forth the organization of a notional BDOC, and a discussion of Air Force base organization.

(1) Operations. The operations section is primarily concerned with planning and coordinating current and potential defense operations. It prepares and implements base security and defense plans and serves as the central point of contact for coordination with:

(a) Higher echelon area defense counterparts.

(b) Other bases.

(c) Area MP forces.

(d) Tactical combat forces (TCFs) and response forces.

(e) HNS forces.

(f) Area damage control (ADC) teams.

(g) Fire support units.

(h) Close air support units.

(2) Intelligence and Counterintelligence. The intelligence section is the base commander's focal point for receipt and transmission of intelligence information. It develops or requests information from:

(a) Supporting HN and US civil or military intelligence and security agencies and units.

(b) Area security patrols.

(c) Convoys.

(d) Adjacent bases.

(e) Communications sites.

(f) Higher echelon sources.

(g) Movement control assets.

(h) Medical evacuation assets.

(i) Defector and EPW interrogators.

(3) Communications. Dedicated communications assets should link all base defense activities and interface with higher echelons. The communications system should have antijam characteristics, provide transmission security, and be robust, redundant, and reliable. It should interface with the communication systems of HN and US response forces. See Chapter III, Communications.

e. Alternate BDOCs and BCOCs. For reliable, survivable C2, base commanders should set up alternate BDOCs and BCOCs if possible. If bases do not have the resources to support this requirement, headquarters elements of units OPCON to bases for defense may be designated for this purpose. C3 connectivity should be the main factors in selecting locations of the alternate BDOCs and BCOCs.

4. Areas of Responsibility. The TAOR concept is key to the C2 of JRA defense. Just as boundaries and other control measures in the combat zone identify the zones and sectors that are the responsibilities of tactical commanders, TAORs in the JRA both fix and limit the geographical defense authority for commanders in the JRA. The JRAC should provide recommended TAORs to the JFC for component and area commanders whose boundaries include all critical areas in the JRA. Component and area commanders, in turn, must ensure that TAORs assigned to base and base cluster commanders encompass all territory necessary to conduct effective defense operations. Special attention must be paid by all commanders to TAOR boundaries. Command arrangements within each TAOR must be clearly established for all anticipated situations, especially when forces of different joint force components and nations occupy the same TAOR.

5. Liaison. Intelligence and operations liaison within and between bases and base clusters, and with higher headquarters, is essential in developing defense plans and executing defensive operations. Early and continuous liaison with HN and allied organizations, and with established response forces, must be conducted to ensure effective and coordinated actions when required.

6. Nonmilitary Agencies. Commanders must establish C2 measures to integrate the defensive capabilities and defense requirements of civilian agencies of the US and HN governments. Private contractors also may require security. Defense-related resources of these agencies may include police, fire departments, and private security guards, observers, and mechanical or electrical security systems. Integration may be accomplished by memorandums of understanding or similar instruments that set forth the requirements and capabilities of all participating organizations.

(INTENTIONALLY BLANK)

CHAPTER III

COMMUNICATIONS

1. General. Effective communications for joint base defense present numerous challenges. All component communications systems, both secure and unsecure, on the base must be compatible to facilitate effective C2 of defense and security operations. The BDOC, as the focal point for base defense C2, is normally the hub for the base defense communications system.

2. Planning and Construction Considerations. Base communications facilities for both defense and primary missions must be planned, coordinated, and established. Considerations include:

a. Organization and integration of capabilities and resources.

b. Specific procedures for transitioning from a no-threat operating environment to a threat environment.

c. Communication system redundancy or equivalent backup systems.

d. Compatibility of equipment and systems.

e. Selection, preparation, and hardening of communications installations.

f. Determination of requirements for on-call augmentation from off-base communications assets.

g. Requirements for control of air support and fire support.

h. Ability to operate in an electronic warfare (EW) environment.

i. Secure voice and data communications.

j. Transmission security and communications deception.

k. Development of signal operating instructions (SOI) or communications plans (COMPLANs) and dissemination to tenant, supporting, and augmentee units.

l. Coordination with HN, TCF, and transient units.

3. Capabilities

a. Existing base communications facilities are used to the maximum extent possible for base defense. However, if such use would divert communications resources from support of the primary base mission, a separate communications system may be necessary. Wire is the normal means of internal base communications between fixed sites like sentry posts, checkpoints, and the BDOC. When dealing with Level II and level III threats, radio will become the primary carrier for tactical traffic.

b. Plans should be developed to provide for alternate means of communications. Planners should also consider the possibility of using community communications systems, such as base cable, armed forces, or civilian-owned radio broadcast stations and television.

c. The base mission operations center and BDOC should net with theater warning systems so that timely action may be taken against NBC, air, missile, and ground attacks. Alarms using loudspeakers, sirens, pyrotechnics, or other established methods (metal banging metal) should be used to sound warnings of those threats. Complete knowledge of the alarm system by all base personnel and rehearsals of required actions are critical to the system's effectiveness.

4. Base Defense Communications System. A secure, robust, redundant, reliable communications system is required between defense units, staff elements, headquarters, and operations centers. A communications system can be enhanced by using automated systems, voice combat nets, and trunked land mobile radios. It should include, if equipment permits:

a. Secure voice and data communications.

b. Immediate access to the BDOC communications net by sector command posts, mobile reserve, patrols, and critical defense positions.

c. Continuous access by the BDOC to the base mission operations center, RAOC, RTOC, and HN forces.

d. Use of formatted messages to reduce message preparation time.

e. Access by supporting CI and intelligence units.

f. Access by supporting fire support and air defense assets.

5. Base Defense Communications Nets. Figure III-1 is a notional structure for base defense communications. The following units or facilities should operate stations in the base defense net:

a. Base Operations Center (BOC) and other C2 facilities such as those found on Air Force installations.

b. BDOC.

c. Fire support element (FSE) or Fire Support Coordination Center (FSCC).

d. Defensive sector command post (CP).

e. Base observation posts (OPs), listening posts (LPs), and patrols.

f. Base mobile reserve.

g. Survival Recovery Center (SRC).

h. TACS.

i. BCOC.

j. Air defense and missile warning.

k. Maritime and offshore defense forces.

l. RAOC and RTOC.

m. RF and TCF.

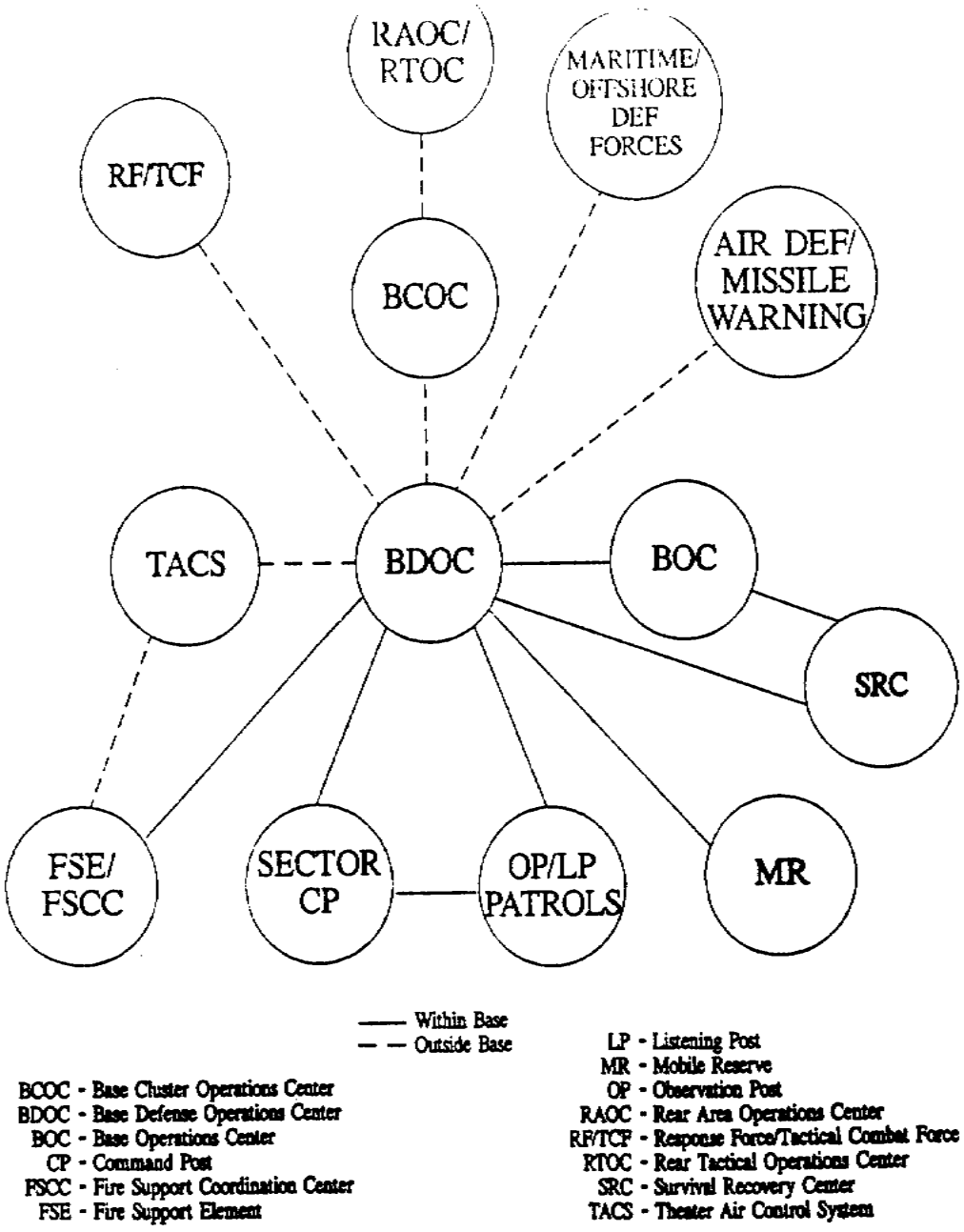


Figure III-1. Notional Base Defense Communications Links

Figure III-1. Notional Base Defense Communications Links

CHAPTER IV

BASE DEFENSE OPERATIONS

1. General. The base commander organizes and controls all forces assigned to the base to capitalize on their capabilities. These forces must be trained, organized, and equipped to contribute to the defense of the base. This chapter sets forth the factors that the base commander must consider in preparing and executing defense plans. A format for a sample base defense plan is at Appendix E.

2. The Fundamentals of Base Defense. The general characteristics of defensive operations are discussed in detail in Service doctrinal publications. Defensive fundamentals, as they pertain to the defense of bases, are as follows:

a. Understand the Enemy. Defenders must be familiar with the capabilities and limitations of enemy forces, weapons, equipment, and tactics. The base commander also must have access to the latest intelligence concerning probable enemy intent.

b. See the Battlefield. Intelligence operations are key to assembling an accurate picture of the battlefield. The intelligence preparation of the battlefield (IPB) provides the commander a continuous, integrated, and comprehensive analysis of the effects of enemy capabilities, terrain, and weather on operations. It helps the commander anticipate battlefield events and develop the priority intelligence requirements (PIR) and information requirements tied to those battlefield events. Intelligence and multidiscipline CI estimates are prepared, continuously updated, and integrated into the base commander's staff decisionmaking process.

c. Use of the Defenders' Advantages. Defenders' advantages may permit a numerically inferior force to defeat a much larger one. Some of these advantages are:

(1) The ability to fight from cover.

(2) More detailed knowledge of local terrain and environment.

(3) The ability to prepare positions, routes between them, obstacles, and fields of fire in advance.

(4) The ability to plan communications, control measures, indirect fires, and logistic support to fit any predictable situation.

(5) The ability to deceive enemy forces about friendly defensive capabilities, dispositions, and execution of operations.

d. Concentrate at Critical Times and Places. Defense of a base is normally conducted along interior lines, permitting the timely and secure movement of forces to engage the most critical threats. The commander must mass enough combat power at points of decision by economizing in some areas, employing a reserve, and maneuvering to gain local superiority at critical points.

e. Conduct Counterreconnaissance and Counterattacks. Fixed bases having well-established perimeters usually have limited depth. Counterreconnaissance and counterattack add depth to the battle, outside the perimeter, allowing the base to continue its primary mission with minimal interference.

f. Coordinate Critical Defense Assets. Synchronization of indirect fires, air and missile defense resources, tactical aircraft, engineers, dismounted troops, armored vehicles, naval surface fire support, and helicopters can produce a combined arms effect. Synchronizing forces and fires produces a synergy capable of defeating a larger enemy force. This synergy results from making enemy movement difficult or impossible and by causing a reaction that may make enemy forces more vulnerable to other friendly capabilities.

g. Balance Base Security With Political and Legal Constraints. Base security may have to be designed around numerous political constraints.

h. Know the Law of War and Rules of Engagement. Base commanders and their subordinates must comply with ROE. They should ensure that inconsistencies among Service component ROE are reconciled.

3. Defensive Factors. The remainder of this chapter deals with base defense against action by organized military or paramilitary units. Considerations for day-to-day security of the base and for combatting terrorism are contained in Appendixes F and G. Base defense should be governed by considering the factors of mission, enemy, terrain and weather, troops and support available, and time available

(METT-T) (including all friendly forces). Additionally, careful consideration should be given to the protection of any key strategic or operational assets located at a base.

a. Mission. The primary mission of the base is to support joint force objectives. Inherent in this mission is the subsidiary mission of defending itself.

(1) The stated defense plan should specify the following essential elements:

(a) Who will defend the base.

(b) Where each unit will defend.

(c) When and for how long the unit must be prepared to defend.

(d) Why the unit will defend.

(e) What the unit will defend.

(2) Essential actions of the defense force are:

(a) Detect. Enemy attempts to reconnoiter or attack the base or interfere with the performance of base functions must be detected at the earliest stage possible.

(b) Warn. The base must be warned that an attack is imminent or under way.

(c) Deny. Defense forces must prevent the enemy from access to the base and from degrading the base's primary function.

(d) Destroy. If possible, defense forces must eliminate the attacking enemy's capability to threaten the base.

(e) Delay. If base forces lack the combat power to defeat the attacking enemy, defense forces must disrupt the attack and attempt to create the conditions for response forces or tactical combat forces to react and destroy the enemy force or to remove or deny base resources to the enemy.

b. Enemy. Every intelligence and counterintelligence resource available to the base commander should be used

to determine enemy capabilities and intentions. The intelligence cycle and intelligence support to joint operations are discussed in Joint Pub 2-0.

(1) PIR are the means by which the commander provides direction for intelligence operations. The answers to questions raised by PIR will indicate or confirm particular enemy courses of action. PIR may include:

(a) The enemy's tactical, operational, and strategic objectives and intentions.

(b) Organization, size, and composition of forces, and locations of their strongholds.

(c) Movement of personnel and equipment.

(d) Religious, political, or ethnic affiliation.

(e) Enemy intelligence capabilities.

(f) Tactics, operational procedures, and patterns of operations.

(g) Special skills (e.g., sniping, demolitions, sabotage).

(h) Motivation, morale, discipline, and fanaticism.

(i) International support.

(j) Support among HN population.

(k) Identities and psychological characteristics of leaders.

(l) Logistic capabilities and patterns of activities to prepare for operations.

(m) Medical capabilities and evacuation support.

(2) Information requirements deal with information about an enemy and the environment that needs to be collected and processed in order to meet the intelligence requirements of the commander.

(3) The intelligence effort should be directed toward collection, exploitation, analysis, and

dissemination of intelligence that will permit the development of friendly capabilities to:

(a) Identify and counter enemy operations security (OPSEC) measures, deceptions, and attacks.

(b) Counter enemy firepower, mobility, EW, imagery, and human intelligence (HUMINT) capabilities.

(c) Destroy, exploit, and/or neutralize enemy strengths.

(d) Exploit enemy vulnerabilities.

(e) Identify and defend against enemy security and counterintelligence capabilities.

c. Terrain and Weather. Sites for bases are usually selected in order to accomplish assigned primary missions. Although defensive considerations are frequently secondary, they must not be ignored. The nature of air bases, for example, precludes establishment of a tight perimeter with extensive cover and concealment for defenders. However, the location of an air base could be chosen to make defense easier by making an unobserved enemy approach more difficult. Likewise, the best ports are located in or adjacent to urban areas. Nonetheless, the base commander must make the best use of the terrain within the commander's TAOR. Commanders analyzing terrain must consider all its military aspects, from the standpoints of both defenders and the enemy. These include observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach (OCOKA). Additionally, commanders must analyze the effects of weather on both defender and enemy weapons systems and tactics. Weather and visibility conditions can have significant effects on ground, air, and maritime operations. Commanders should minimize their own vulnerabilities to adverse weather conditions and exploit any advantages over enemy vulnerabilities.

d. Troops Available for Base Defense. There may be some units on a base whose missions are defense and security, such as MPs at a large headquarters, security police (SPs) on an air base, and air defense forces. However, most of the personnel available for defense (augmentees and selectively armed personnel) will be obtained from the units devoted to the accomplishment of the base's

primary mission. These personnel will not have the same degree of combat skills as dedicated security forces and, therefore, must receive regular training in marksmanship, tactics, and basic ground combat skills. Their contribution to a successful base defense will require close supervision and leadership. Service doctrinal and training publications discuss the needed skills and standards to be attained. The task organization of the base defense plan should take into account the personnel available and the weapons and equipment organic to their units, so that all available combat power on the base may be brought to bear in the event of hostile action. An analysis of the threat may show the necessity of tasking combat forces for a rear area mission when attack in the rear area seems probable.

(1) Defending Against Level I Threats. At this level, available base assets should be able to detect and defeat enemy activities. Day-to-day security activities are conducted by the forces assigned to the base, usually as tasks in addition to their primary duties. At Level I, base defense forces must be trained and exercised to permit smooth transitions to Level II and Level III.

(2) Defending Against Level II and Level III Threats. After transition from a Level I posture to a posture able to engage Level II and Level III threats, base defense forces must be able to disrupt or delay hostile action until response forces or TCF can be committed.

(3) Evaluating the Defense. Commanders of bases must evaluate and plan to:

(a) Use indirect fires to maximum advantage.

(b) Use organic and supporting direct fire weapons to maximum advantage.

(c) Patrol the base TAOR.

(d) Use available air and missile defense capabilities.

(e) Use the mobility of its own combat and combat support elements.

(f) Use engineers in countermobility and survivability roles.

(g) Constitute a reserve, plan for its use, and rehearse its employment in reinforcement, blocking, and counterattacks.

(h) Sustain the defense forces themselves and continue the support of the larger force.

(i) Avoid, detect, protect from, react to, and recover from NBC attacks.

(j) Employ OPSEC measures and deceptions.

(k) Maintain surveillance of beaches, concealed water approaches (e.g., bayous and swamps), and rivers.

(l) Maximize rail and highway entrance security.

e. Time Available. Base commanders will set priorities of work to make best use of the time available to plan, prepare, train for, and evaluate the defense.

4. Base Commander's Intelligence Responsibilities. The base commander is responsible for ensuring that the following intelligence functions are performed in a timely manner:

a. Provision of information and intelligence to the defense force and maintaining current threat data bases.

b. Establishment of intelligence liaison with applicable area, subarea, higher, and adjacent commands, including the joint force Joint Intelligence Center (JIC), HN and third-country military intelligence facilities, and US and HN civilian organizations.

c. Direction of the reconnaissance and observation effort of the base defense force, and arrangement for reconnaissance and observation to be conducted by commands supporting the base defense force. Deconfliction of these intelligence collection efforts is an ongoing process in which the base commander and the intelligence staff must take part.

d. Collection of target information and the dissemination of this information to base cluster or other higher headquarters, the FSE or FSCC (if provided) and any units providing fire support to the base.

e. Procurement of nonstandard maps, charts, and imagery.

f. Development and implementation of local CI measures.

g. Request for augmentation or support by intelligence specialists.

h. Establishment and maintenance of contact with local HN police and intelligence agencies.

5. Planning. Base commanders develop defense plans (Appendix E) to use in organizing base defenses.

a. Forces in Base Defense Areas. Successful defense depends on integrated aggressive, all-around, in-depth measures. Drawing from the units assigned to the base, base commanders organize defense forces within their TAORs, using existing chains of command.

(1) Tactical Area of Responsibility. Areas within the base should be assigned to cover all likely avenues of approach and other key terrain. Boundaries between sectors assigned to subordinate units should be well-defined, with coordinating points, contact points, and fire control measures. Fire support coordination measures are essential for subordinate tenant units to perform their TAOR security missions. These measures decrease the likelihood of fratricide, prevent noncombatant casualties, and minimize damage to the property of friendly civilians.

(2) Defense in Depth

(a) A security area from the defense force's primary defense positions outward to the limits of the base TAOR may contain OPs, LPs, and mounted and dismounted patrols. Defense forces in this area should be equipped with sensors and devices for periods of limited visibility, as well as reliable mobile communications. Aviation support may be requested to augment the capabilities of base security forces. Contact points will be established on or near base TAOR boundaries, where the patrols and security forces of the area commander, HN, or adjacent bases can contact base defense forces.

(b) Boundary areas of various base defense forces must be clearly defined, and that information be disseminated to defending forces. Contact and identification procedures

must be standardized and clearly understood by all defending forces. This can be especially critical when HN and Third World country forces whose primary language is not English and US forces come into contact with each other, or when base defense forces are acting only as augmentation forces.

(c) Defense forces in the base's primary defense positions must be prepared to prevent hostile forces from penetrating the base and interfering with its primary mission. If not capable of defeating enemy threats, the primary defense forces must fix or delay the enemy until commitment of response forces or the TCF or the removal or denial of critical resources to the enemy.

(d) Some forces (augmentees and selectively armed personnel) may be directed to secure areas or facilities within the base vital to performance of the base's mission. Examples are the BDOC, ammunition storage areas, and aircraft revetments. Defensive forces deployed inside the base perimeter require careful fire control to prevent fratricide.

(3) Relationship With Other JRA Defense Forces. Upon notification by a base or base cluster commander through the BDOC or BCOC that a threat exceeds a base's defense capabilities, the area commander, through the RAOC, commits the response forces available or requests the commitment of a TCF. The situation will dictate the C2 relationship between the response force or TCF and the base defense force and whether planned arrangements should be modified.

(a) If base defense forces are already engaging threat forces, the area commander normally passes TACON of the response force to the base commander until the threat is defeated (see Figure IV-1).

(b) When response forces are committed before to the base defense forces are engaged, the area commander normally assigns the response force a TAOR close to or contiguous to the base TAOR (see Figure IV-2). The base commander may place selected base defense forces under TACON of the response force commander.

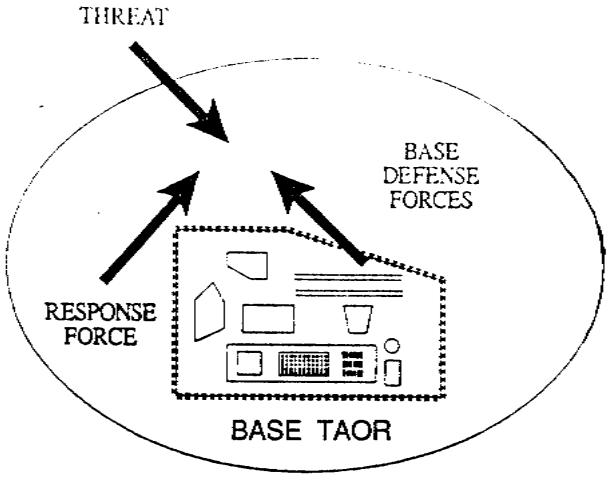


Figure IV-1. Response Force TACON to Base Commander (Response Force Committed While Base Defense Forces Are Engaged With a Threat)

Figure IV-1. Response Force TACON to Base Commander (Response Force Committed While Base Defense Forces Are Engaged With a Threat)

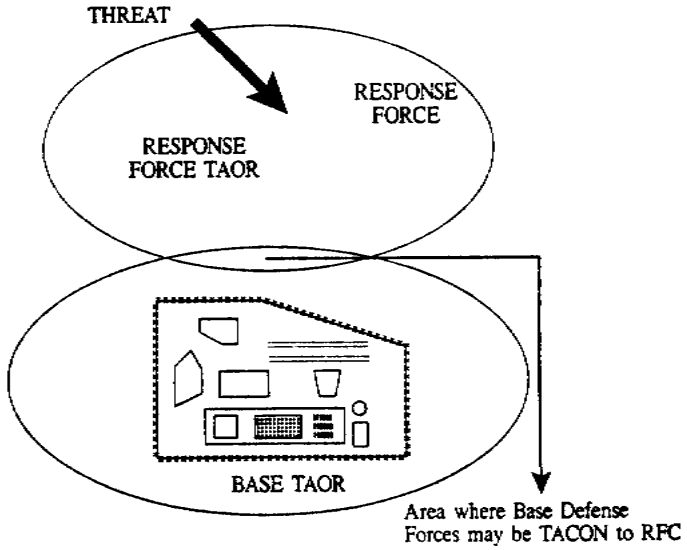
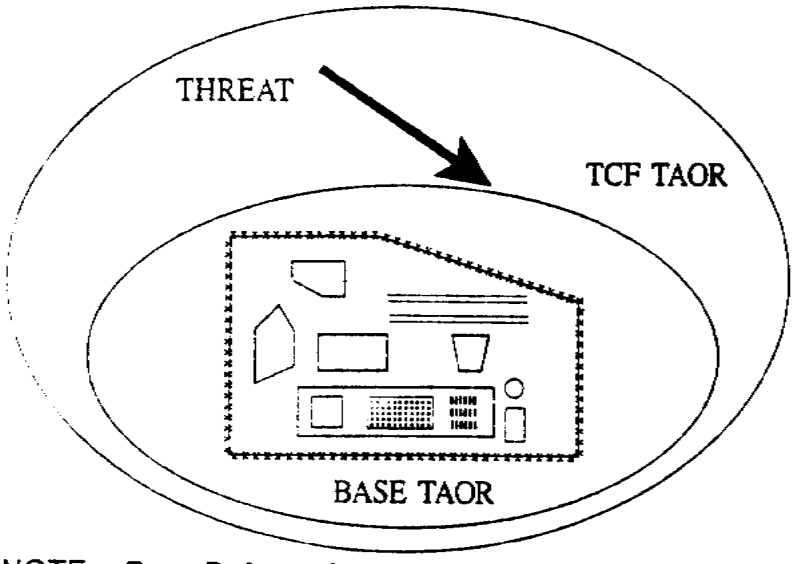


Figure IV-2. Selected Base Defense Force TACON to Response Force Commander (Response Force Committed Prior to Base Defense Forces Engaging the Threat)

Figure IV-2. Selected Base Defense Force TACON to Response Force Commander (Response Force Committed Prior to Base Defense Forces Engaging the Threat)

(c) When a TCF is committed, the situation is serious enough to assign to the TCF commander a TAOR that encompasses a large portion of the rear area. During level III operations, the TCF commander will normally have OPCON over most base or base cluster defense forces and response forces in the assigned TAOR, excluding air defense forces, which remain under OPCON of the AADC. Some base defense forces necessary for the protection of critical base assets may remain under the control of the base commander. BDOCs and/or BCOCs will establish and maintain contact with the tactical operations center (TOC) of the TCF (see Figure IV-3).



NOTE: Base Defense forces necessary for protection of critical base assets remain under the control of base commander.

Figure IV-3. Base Defense Force OPCON to the TCF Commander During Level III Operations

Figure IV-3. Base Defense Force OPCON to the TCF Commander During Level III Operations

b. Mobile Reserve. The base's mobile reserve may be used to reinforce threatened areas of the base perimeter, to block enemy penetrations of primary defense positions, or to counterattack in order to regain lost defense positions or destroy the hostile attacking force. It should be vehicle-mounted, in armored vehicles if available. On large bases or base clusters, the reserve may be airmobile if helicopters are available.

c. Antiarmor Weapons. Rear area forces generally have few organic antiarmor weapons. Antiarmor weapons, including tanks, available to base defense forces will be positioned to cover the most likely high-speed avenues of enemy vehicular approach in mutually supporting positions. Crews must select primary, alternate and supplementary positions, with covered and concealed routes between positions to maximize weapons effectiveness and survivability. Augmentation forces possessing antiarmor weapons should also select positions in anticipation of being committed to defend the base.

d. Indirect Fire Systems. The fires of mortars, field artillery, and naval guns can support the base defense effort.

(1) Fire Support Planning. The FSE or FSCC of the BDOC is the focal point for the planning of fires for base defense. If the base is too small to have its own FSE or FSCC, its BDOC operations personnel must coordinate with fire support personnel at the FSE or FSCC at the BCOC or the appropriate RAOC. Preplanned targets should include probable landing zones (LZs) and drop zones (DZs), avenues of approach, key terrain, obstacles, final protective fires for defensive positions, and obscuration to facilitate movement of counterattack forces. The targets should be planned to minimize collateral damage and civilian casualties. Copies of fire plans and target lists must be provided to the headquarters controlling the fire support assets. Targets may be planned outside the base AOR after coordination with the headquarters responsible for the area concerned.

(2) Fire Support Coordination Measures. Fire support coordination measures permit or restrict fires in and around bases. Careful coordination must take place in planning these measures, especially with the HN. No-fire areas may be required to protect civilians or to prevent disruption of rear area missions by friendly fire.

(3) Observers. Fire support units normally will not furnish observers to bases in the rear area. Observers with appropriate training should be identified on each base to adjust supporting fires and control close air support.

(4) Joint Pub 3-09. Joint aspects of fire support are discussed in Joint Pub 3-09. Service publications provide additional information on fire support planning and fire support coordination measures.

(5) Aviation Fire Support. The base FSE or FSCC will maintain contact with the appropriate air control system to request and control air support for surface base defense efforts, excluding air and missile defense. When available, fixed- and rotary-wing aircraft may be used to extend the range of observation and provide immediate combat response to threats. Some aircraft, like the AC-130 gunship, are particularly well equipped to support base defense. Also, forward-deployed aircraft carriers can often provide a considerably effective and rapid aviation response force.

e. Other Aviation Support. The BDOC and BCOC, with other command and control centers, coordinate other aspects of aviation support. Examples include coordinating air-ground communications frequencies and procedures; coordinating time-on-target (TOT) and pickup points for medical evacuation and air movement of base defense, response force, and TCF elements; and managing air support priorities and diversions for emergency resupply, personnel augmentation, and evacuation.

f. Obstacles and Mines. Careful consideration should be given to the use of antitank and antipersonnel mines in the rear area. However, prior to emplacement of mines or obstacles, permission must be obtained from the commander having authority over the TAOR in which the base is located. Often, the best avenues of enemy approach are the routes that must be used to perform base primary missions. The enemy may also transit areas of high civilian population density. Fire support plans may include the delivery of scatterable mines when enemy attack is imminent. Obstacles must be kept under observation and covered by direct and indirect fires to be effective. Some obstacles may be useful only for certain threat levels. For example, chain-link fencing may constitute a useful obstacle against Level I threats if well-patrolled but not against higher level threats.

g. Communications Countermeasures. The base commander should, when capable, maintain an electronic countermeasures (ECM) and communications jamming capability to disrupt the attacking force's C2.

h. Security Measures. See Appendix F.

i. Work Priorities. The commander must set priorities for the many tasks involved in base defense. Work may occur on several concurrent tasks. Prioritizing might include:

(1) Identifying critical resources and preparing a base defense plan.

(2) Establishing initial base security, including observation posts and patrols outside the perimeter.

(3) Positioning crew-served weapons and troops and assigning fields of fire.

(4) Preparing and emplacing unit NBC detection equipment.

(5) Clearing fields of fire and preparing range cards.

(6) Preparing fighting positions.

(7) Installing and hardening communications.

(8) Emplacing obstacles and mines.

(9) Hardening primary fighting positions, including overhead cover.

(10) Preparing alternate and supplementary positions.

(11) Stockpiling and hardening the locations of ammunition, food, water, and medical supplies.

(12) Preparing routes and trenches between positions.

(13) Developing a counterattack plan.

(14) Conducting rehearsals, including rehearsals of movements to supplementary and alternate positions.

j. Counterattack Plans. The base mobile reserve normally conducts counterattacks, with the objective of sealing a penetration or regaining positions lost to the attacker.

k. Area Damage Control Measures. ADC includes the measures taken before, during, and after hostile action or natural or accidental disasters to reduce the probability of damage and minimize its effects. Engineers perform most of these tasks. Other forces and assets contributing to ADC include ordnance, MPs, NBC, CA, maintenance, medical, signal, supply, transportation, and transiting units, including HN units.

l. Air and Missile Defense Measures. Air and missile defense nullifies or reduces the effectiveness of attack or surveillance by hostile aircraft or attack by missiles after they are airborne. Air and missile defense assets on or near a base will be integrated into the overall air and missile defense plan for the theater or area of operations. The base commander should establish communications links with the air defense net for early warning of impending air attack. If the base is also an air base, local air defense units and the air base operations center must coordinate identification, friend or foe (IFF) procedures. A base defense zone (BDZ) may be established around air bases with specific entry, exit, and IFF procedures. See Appendix C, Air and Missile Defense, and Joint Pubs 3-01.2 and 3-01.5.

m. NBC Defense Measures. See Appendix B, NBC.

n. Threat Response Contingency Plan. The threat response contingency plan outlines specific duties and responsibilities to combat terrorism. See Appendix G, Terrorism, and Joint Pub 3-07.2.

o. Physical Facilities. Commanders must stress continuous upgrading for base physical security. Activities occupying permanent fixed bases will have opportunities for installing sophisticated security equipment not available to units in mobile bases. 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. Plans for base construction must consider ADC. Defenders must use fire-fighting equipment and practice procedures often to maintain proficiency. Where peacetime considerations prevent construction of defensive positions, fields of fire, and obstacles, detailed plans for their construction should be made by appropriately trained personnel. See Appendix H, Specialized Equipment and Materiel.

(1) Intrusion Detection. Defenders can emplace sensors on likely avenues of approach, locating them at the limits of the TAOR, or outside the TAOR if coordinated with adjacent commands. Directed ground surveillance radar (GSR) and airborne forward-looking infrared (FLIR) systems, if available, can improve the chances of detecting intrusions early. Remotely monitored sensors, trip flares, binoculars, night vision devices and other nonlethal warning devices can also be useful. Depending on the threat situation and ROE, antipersonnel and antivehicle mines also may be emplaced, and noncombatant use of the area restricted. Dummy sensors at observation posts, and concealed surveillance resources also should be considered.

(2) Observation. To improve observation, defenders should clear the ground to the front of positions and from near perimeter fences by cutting foliage or applying defoliant. Because total defoliation can expose the base to aerial observation, a balance must be struck between the needs of ground defense and defense against air attack. See Joint Pub 3-11 for a discussion of US policy on the use of herbicides. Perimeter roads on either side of the fence improve observation. A combination of concrete barriers, concertina wire, lighting, surveillance cameras, and intrusion sensors enhances base security. Figure IV-4 displays security facilities available on fixed permanent bases. Observation sites in guard towers or atop buildings can increase the surveillance capabilities of perimeter guards.

(3) Communications. Defenders should install a reliable, secure, and redundant communications system at all guard locations.

(4) Entrances. The base should have as few entrances as possible. Other measures to enhance entrance security can be found at Appendixes E and F. Appendix H contains a listing of associated security equipment.

(5) Working and Living Areas. Buildings housing personnel and sensitive equipment should be out of grenade-throwing range from exterior fences. Shelters with reinforced and sandbagged roofs should be near all working and living areas, to serve both as shelters and fighting positions.

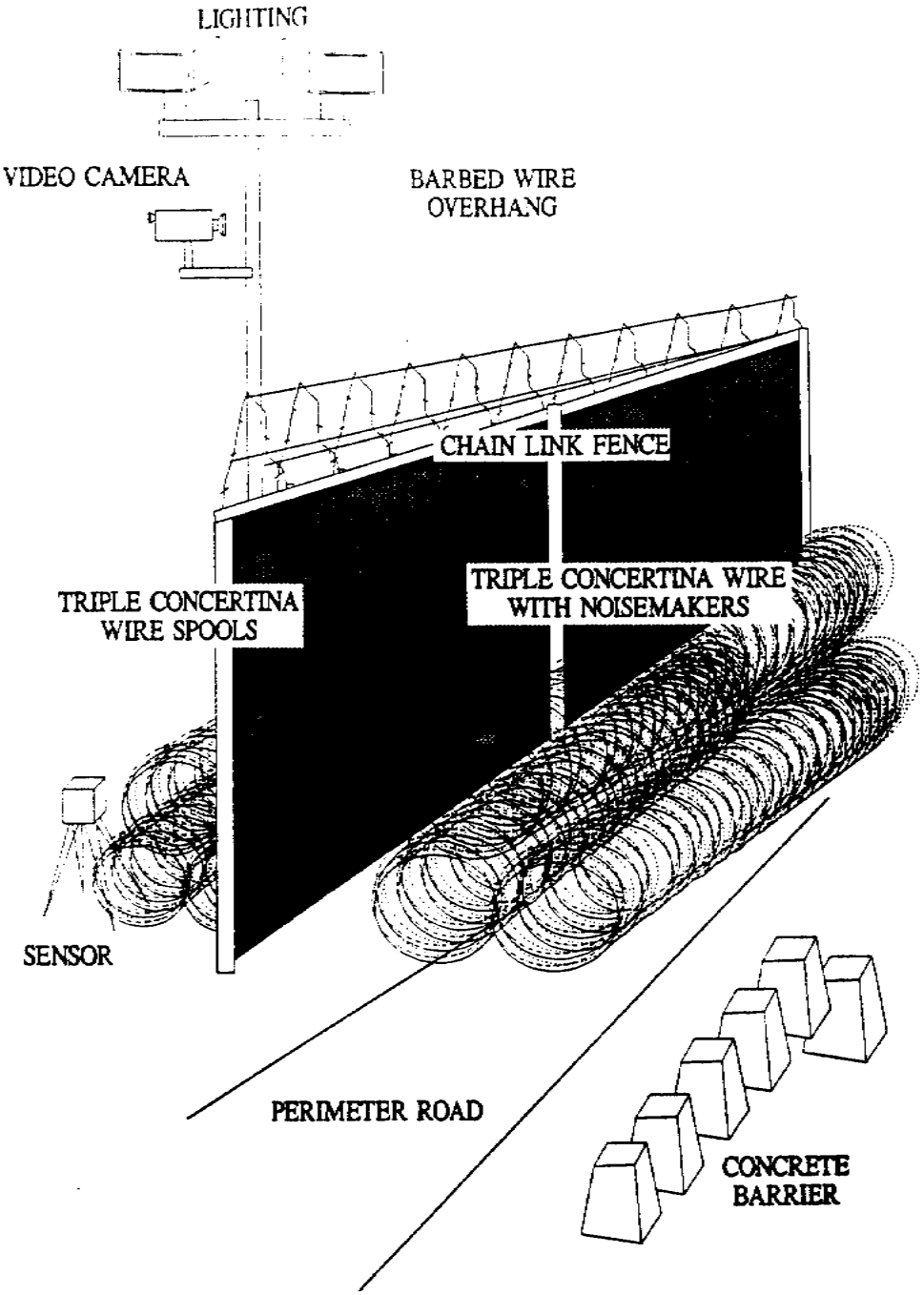


Figure IV-4. Physical Perimeter Defense Measures

Figure IV-4. Physical Perimeter Defense Measures

(6) 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 the local population.

(7) Medical Facilities. Medical facilities should be well-marked if the tactical commander so directs and placed away from possible lucrative targets. They must be able to augment security forces, have backup energy sources, and rely on additional personnel for security if needed.

p. OPSEC Measures and Tactical Deception. OPSEC measures and deception actions should include visual, sonic, olfactory, and electronic measures. The measures should be mutually supporting and credible. Planned patterns of physical security, reaction force operations, and other such matters should be systematically avoided.

6. Evacuation. In extreme situations, it may be necessary to evacuate a base or part of a base, or to move essential base activities elsewhere in the JRA to perform their functions with less enemy interference. Plans should include the identification of bases most at risk, the advantages and disadvantages of evacuation, and the conduct of evacuation operations.

CHAPTER V

HOST NATION SUPPORT

1. General. HNS is based on bilateral diplomatic agreements that commit the HN to provide specific support under prescribed conditions. In the majority of cases, US bases are located in friendly HNs. Once a base is established in an HN, close cooperation with the HN and special consideration for its people, culture, and territory are vital in attaining US goals.

2. Planning for HNS of Base Defense. HNS enhances the abilities of US forces to perform their missions. HNS can reduce requirements for US personnel, materiel and services, allowing more flexibility in assigning forces. HNS is essential when political agreements limit the numbers of US personnel on bases. US forces should expect HNS when the HN has total sovereignty and is acting in concert with US forces to achieve strategic and operational objectives. Factors to consider when planning HNS include:

a. Capability, willingness, and reliability of the HN to provide and sustain resources.

b. Economies in US forces, equipment, and facilities made possible by using HNS.

c. Effects on security, including OPSEC. US and HN CI and security agencies must develop a system to screen the backgrounds and loyalties of HN personnel employed on the base. There must be a detailed agreement on levels of security cooperation.

d. Capability of US forces to coordinate HNS and integrate HN resources into base mission performance and defense.

e. Finance support requirements for HNS. Finance representatives should participate in planning HNS. Finance elements will be required to provide contractor payments, commercial vendor services, and perform other finance tasks related to HNS.

3. Base Defense Coordination. When the forces of the United States, HN, and third-country allies occupy bases together, special consideration must be given to the synchronization of C2 and the defense capabilities from every available source. Commanders should address the considerations set forth in Chapter IV, Base Defense Operations, and Appendix F, Security, from a combined perspective. Base defense plans

must integrate the special capabilities and procedures for maneuver, fire support, C2, intelligence, air and missile defense, mobility and survivability, and combat service support of the units and activities of each nation represented. Plans should provide for intense combined training programs. The defense of bases must be consistent with combined arrangements for operations in the entire JRA, which are discussed in Joint Pub 3-10.

4. 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 fighters, and border patrols may be available as well. US forces also may use HN facilities for hospitals, headquarters, billets, warehouses, and maintenance shops. However, plans for HNS must consider how to use HN resources that are available in relative abundance without imposing a burden on resources the HN needs for its own development.

5. Supplies, Services, and Equipment

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

b. Bases may need local support personnel, such as laborers, stevedores, truck drivers, supply handlers, equipment operators, mechanics, linguists, medical aides, computer operators, and managers. Many will be available from the HN labor pool. When available, HN military or paramilitary units may support US forces by performing functions such as traffic control, convoy escort, base security, and cargo and troop transport.

c. HNS may be provided for special functions, such as rail operations assistance, convoy scheduling, air traffic control, and harbor pilot services. Local purchase or procurement of supplies and services, when permitted by HN agreements, may reduce the theater or AO logistic requirements.

6. Command and Control. US and HN commanders retain command their respective units, with US forces being granted support authority in order to work in fullest cooperation with HN personnel.

a. The degree of C2 that US forces exercise over HNS depends on the type of HNS involved, the location, tactical situation, political environment, and HNS agreements.

b. When possible, the United States coordinates its control of HN resources through local officials. CA personnel provide an interface with HN authorities.

c. The HN may provide all security to US bases or may share the responsibility for base security with US forces. Both situations require close coordination, common communications, and a detailed base defense plan.

7. NBC Defense. When required, HN and third-country military, paramilitary, and civilians providing support are equipped and trained to operate in an NBC environment. Training and equipping are normally national responsibilities. See Appendix B, NBC.

8. Training. US personnel at all levels should receive training in dealing with HN personnel, both on and off duty. Training in the use of HN communications (telephone) systems may be appropriate. Orientation should include HN government regulations, business practices, social customs, military procedures, religious customs, and language familiarity. Frequent training in security awareness, base defense procedures, and safety should be provided to those HN units charged with support of the defense effort.

9. Intelligence. Specific provisions for combined intelligence operations and the sharing of intelligence gained from national systems are usually arranged at the highest levels. Base commanders must ensure that their intelligence elements link with the JFC and other joint force intelligence staffs. HN agencies are normally excellent HUMINT and CI sources. Therefore, effective CI links should be maintained with local HN police, military, and paramilitary agencies for timely information concerning direct threats to the base.

10. Civil Affairs. Base commanders can expect to conduct CA activities and should use CA-trained personnel, if available, to monitor those activities and assist in communicating information concerning appropriate aspects of base operations to the HN. CA personnel efforts can enhance the success of US and HN interface efforts. See Joint Pub 3-57.

11. Psychological Operations. Base commanders should conduct dynamic and continuous psychological operations (PSYOP), assisted by trained PSYOP personnel, to promote HN employee loyalty to the base, promote acceptance and support for base personnel among the surrounding population, and enhance the collection of indicators and warning intelligence. See Joint Pub 3-53.

APPENDIX A

MARITIME-LAND INTERFACE

1. Joint Base on a Shoreline. The establishment of a base on a shoreline in the JRA presents special advantages and challenges to those responsible for the functions inherent in the base's mission and for its defense. The advantages include the availability of the assets of more than one Service component for use by commanders in fulfilling their responsibilities. The special challenges may include the fact that facilities like ports and harbors are usually located in heavily populated areas. Command arrangements may be complicated by diverse purposes when multiple Service components use the same facilities. For example, the following installations may be in close geographical proximity:

   a. Army common-user water terminal.

   b. Support base for a MAGTF.

   c. Naval base supporting and sustaining fleet operations and/or naval coastal warfare operations, naval advanced logistic support site (ALSS), and naval forward logistic site (FLS).

   d. Air Force base operating an aerial port of debarkation.

2. Command and Control

   a. The JFC designates the base commander, usually from the Service component with the dominant force on the installation.

   b. The JFC must designate the chain of command for security and defense, which may differ from the mission chain of command. In the case of multi-Service operations, each Service component facility may be designated a separate base as part of a base cluster commanded by the designated predominant Service commander. The base or base cluster may be directly subordinate to the joint headquarters, to a component commander, or to an area or functional commander. Examples of these area or functional commanders are:

      (1) Marine force service support group commander.

      (2) Army transportation command commander, TAACOM commander, and ASG commander.

(3) Naval coastal warfare commander, ALSS commander, and FLS commander.

(4) Air Force component commander.

3. Defense Planning

a. Potential Threats

(1) Land-Based Attacks. Land threats to the base include all levels of threat discussed in Chapter I. Procedures for defense of land approaches are discussed in Chapter IV.

(2) Air and Missile Attacks. Appendix C discusses the defense of the base from air and missile attacks.

(3) Waterborne Attacks. Friendly naval forces are the primary defense against waterborne threats and should achieve naval superiority in the waters adjacent to the base. However, even if overall superiority is achieved, small enemy units may seek to interfere with base operations from seaward approaches.

(a) Amphibious Raids. The enemy may attempt amphibious raids using watercraft and/or aircraft. Likely beaches, LZs, and insertion areas should be outposted, obstacles should be emplaced, and the mobile reserve employed to counter such raids.

(b) Sea Mining. Enemy mining of the seaward approaches to the base can be conducted from surface vessels, by air, or clandestinely by submarines. Detection of such activity should be a priority effort for surveillance systems, patrol boats, and aircraft guarding the seaward approaches to the base.

(c) Maritime Special Operations Forces. Determined, specially trained, organized, and equipped individuals or units can infiltrate ports, harbors, and bases near shore by swimming, scuba diving, high-speed surface craft, indigenous small boats, or miniature submersibles. They can damage vessels, port facilities, and base resources. Security forces, both seaward and ashore, and their

supporting surveillance systems, must be prepared to locate and counter such threats.

b. Approaches to the Base. Appropriate security and surveillance forces, backed up by capable mobile reserve forces, must be designated to cover every possible avenue of approach. These approaches include:

(1) Beaches.

(2) Concealed water approaches (fjords, bayous).

(3) Rivers.

(4) DZs and LZs.

(5) Land approaches.

(6) Urban terrain and infrastructure (including underground water and sewage systems).

(7) Piers, docks, and waterfront facilities.

c. Defense Forces

(1) Ground Defense Forces. Normally, the units operating the base facilities are the most common source of personnel and equipment to form a ground defense force. For especially critical facilities, dedicated defense forces such as Marine Corps security forces, Air Force security police, Army military police, or Marine Corps military police units may form the core of the ground defense effort.

(2) Air and Missile Defense. See Appendix C.

(3) Navy and Coast Guard Organizations. The naval coastal warfare commander (NCWC) may form a port security and harbor defense group (PSHDGRU) to support defense efforts. The harbor defense commander (HDC) sets the boundaries for harbor defense for the PSHDGRU. Defense of the harbor is the responsibility of the harbor defense commander (HDC), and inland defense is the responsibility of the appropriate area or component commander designated by the JFC. Close coordination on mission priorities must be accomplished for naval coastal warfare (NCW) units between the NCWC and base commander to avoid conflicts. On a larger scale, under the direction of the NCWC, the PSHDGRU may have

OPCON of forces providing port security and harbor defense in more than one port and/or harbor. This may be particularly true along a coastline that has multiple ports in geographic proximity to each other. In this situation, the multiple ports may be designated a base cluster. The PSHDGRU will, through the NCWC, coordinate security operations with the appropriate area or functional commander. The PSHDGRU may possess some or all of the following capabilities:

(a) Mobile Inshore Undersea Warfare Unit (MIUWU). A mobile surveillance and detection unit that possesses surface radar, subsurface sonobuoy, swimmer detection and neutralization, and naval communications capabilities.

(b) Naval Explosive Ordnance Disposal (EOD) Detachment. This detachment provides ordnance handling and evaluation, special weapons and/or ammunition support, and mine detection and neutralization capabilities. This detachment also identifies mine and/or ordnance beaching areas for the port or harbor.

(c) Port Security Unit (PSU). This unit is provided by the US Coast Guard and is integrated into the Navy component in wartime or as allowed by law. The PSU has missions of port safety and port security. The port safety officer serves in an advisory role to the port commander for the handling of explosives, firefighting, fuel transfer, and hazardous materials handling. The port security mission includes patrolling harbors and anchorages, interdiction, surveillance, and the enforcement of exclusionary zones.

(d) Mine Countermeasures (MCM) Elements. These elements detect and destroy enemy mines in harbors, approaches, and sea lanes, using mine countermeasure aircraft and vessels. Because of the small number of MCM forces, control of these assets is normally determined by the naval component commander.

(e) Mobile Diving and Salvage Unit (MDSU). The MDSU has the missions of underwater hull search and repair, channel clearance, vessel salvage, and pier and piling inspection and repair. The

PSHDGRU commander can request this unit's support of base defense efforts from the NCWC when required.

(f) Naval Special Boat Unit (SBU) Detachments. SBU detachments are organized to conduct or support joint special operations and coastal patrol and interdiction (CP&I) with coastal and riverine craft. SBU detachments consist of various high-speed small craft up to the 175-foot ships of the Cyclone (PC-1) class. Most craft can mount crew-served weapons. When available and pending other priorities, the detachments can be requested to support base defense.

4. Planning Considerations. The following factors should be considered when planning the defense of a base on a shoreline:

a. Protection for sea approach chokepoints.

b. Tides and currents.

c. Water clarity and depth.

d. Pier clearance.

e. Lighting.

f. Use of patrol boats.

g. Communications.

h. Rail and highway entrances security.

i. Air and missile defense measures.

j. Security for individual vessels.

k. Area damage control.

(INTENTIONALLY BLANK)

APPENDIX B

NUCLEAR, BIOLOGICAL, CHEMICAL DEFENSE

1. General. Every base commander integrates NBC defense measures designed to detect, defeat, and minimize the effects of NBC attacks. Units occupying bases in the JRA must plan and train to perform their missions in an NBC environment if necessary. Joint Pub 3-11, (in development), "Joint Doctrine for Nuclear, Biological, and Chemical (NBC) Defense" provides guidance for joint NBC defense.

2. Fundamentals. There are three fundamentals of NBC defense: contamination avoidance, protection, and decontamination.

a. Contamination Avoidance. This fundamental is the most difficult to implement on bases in the JRA because of the immobility of bases. However, some effects may be avoided or minimized by taking the following measures:

(1) Take passive measures to prevent the enemy from selecting the base as a target, such as using camouflage, concealment, deception, and dispersion. Smoke may be used to enhance concealment measures.

(2) Detect and identify hazards. Monitor for contamination, reconnoiter, and survey specific areas to determine contamination status.

(3) Use the NBC warning and reporting system. When a hazard is detected, pass the alarm locally and then warn others by using the standard warning and reporting systems. If detailed surveys are conducted later to determine the actual extent of contamination, the results of these surveys also should be disseminated using the standard reporting formats.

(4) Limit contamination spread. Cover equipment vital to mission accomplishment before attack to prevent unnecessary contamination; use only mission-essential equipment when contamination is present; and restrict personnel movement in the contaminated area.

(5) Move from the contaminated area when the mission permits. However, avoid spreading or carrying the contamination during movement.

(6) If required, evacuate biological and unknown chemical agent samples through intelligence channels to a laboratory for identification.

b. Protection. Protection is required when contamination cannot be avoided. Doctrinal manuals discuss NBC protection in detail. Protection is divided into three broad areas: force protection, individual protection, and collective protection.

(1) Force protection involves actions taken by a commander to reduce force vulnerability to NBC attack. On small bases, this will require that the unit conduct a procedure called mission-oriented protective posture (MOPP) analysis. However, several other decisions concerning alarm placement, automatic masking, etc., will be required as part of the analysis. Forces on large bases or base clusters will conduct a process called vulnerability assessment and risk reduction. The vulnerability assessment is an estimate of the probable impact on the force of an enemy NBC attack. It occurs both before and after initiation of NBC warfare.

(2) Individual protection involves those measures each person must take to survive and continue the mission. It includes the specific actions required for maximum protection against NBC hazards with minimum loss of efficiency. Members of base units must be equipped with individual protective clothing and equipment. All must be proficient in protective measures to take before, during, and after an NBC attack. Mission-essential US and HN civilians working on the base must be trained and equipped to ensure their survival. Crews of naval and merchant vessels in ports also must be prepared for NBC attacks.

(3) Collective protection should be an integral part of NBC countermeasures. Collective protection provides selected contamination-free working environments and allows personnel relief from continuous wear of NBC protective clothing. Collective protection is required in accordance with individual Service directives. Examples of areas normally requiring collective protection are:

(a) Command posts and communications centers.

(b) Fire direction centers.

(c) Missile control complexes.

(d) Combat vehicles.

(e) First-aid stations and hospitals.

(f) Rest and relief stations.

(g) Fixed-site logistic facilities.

c. Decontamination. Decontamination is the reduction of the contamination hazard by removal or neutralization of hazardous levels of NBC contamination on personnel and materiel. The primary purposes of decontamination are to stop erosion of combat power and reduce casualties that may result from inadvertent exposure or failure of protection. Initial decontamination may be performed by base personnel. Detailed decontamination may require requesting assistance from chemical units assigned to support area commanders, in accordance with JRAC priorities. Service manuals discuss decontamination in detail. Decontamination sites should be established in the base area and decontamination supplies should be prestaged before an anticipated NBC attack. Some planning considerations are:

(1) Identify hasty and deliberate decontamination sites.

(2) Designate decontamination teams and ensure that they have the necessary equipment and command and control assets.

(3) Plan for treatment of contaminated casualties.

(4) Plan for the marking and reporting of contaminated areas and terrain decontamination.

(5) Plan for employment of detection alarms.

(6) Conduct necessary NBC training.

(7) Plan for disposal of the waste products of decontamination operations.

3. Other NBC Considerations

a. Obscurants. Employ obscurants to improve survivability during windows of increased vulnerability, such as

imminent air attacks, command post displacements, or critical operations like fast refueling or main supply route repair. Employ deceiving smoke in conjunction with electronic and physical deception measures to mislead the enemy. Use smoke to disrupt enemy surveillance and target acquisition means.

b. Flame Weapons. Incorporate flame weapons, if available, into barrier plans. Use flame weapons to destroy and demoralize enemy forces and illuminate the battlefield.

(INTENTIONALLY BLANK)

APPENDIX C

AIR AND MISSILE DEFENSE

1. Active Air and Missile Defense. Some bases in the JRA have limited capability to engage and destroy incoming enemy aircraft and missiles; therefore, commanders must be aware of the assets that they do possess and use them to maximum effect.

a. Integration With Other Air Defense Assets of the Joint Force. Some bases, by their nature, possess special capabilities for active air and missile defense. Bases with air defense missile units and counterair and antiair warfare aircraft play important roles in the overall theater air defense. These units are subject to the weapon control procedures of the AADC. For details concerning the integration of air defense efforts in the JRA see Joint Pub 3-10 and Joint Pub 3-52.

b. Air and Missile Defense Weapons Organic to Base Units. More pertinent to the close-in defense of the base are the weapons possessed by base units. Many ground units are equipped with shoulder-fired missiles, like the STINGER, and heavy machineguns that may be assigned air defense roles. Forward area air defense weapons, like the CHAPARRAL, STINGER, AVENGER, or VULCAN may be assigned to bases in the JRA for point defense of critical installations. Naval antiair warfare assets on ships in harbors or offshore, such as standard missiles and close-in weapon systems, may be available to augment the base air and missile defense posture. The base commander must ensure that all base air and missile defense assets are coordinated with appropriate airspace control authorities, often by the establishment of BDZs and short-range air defense engagement zones (SHORADEZs) in coordination with the AADC. The training of weapon crews in ROE is essential to prevent fratricide.

2. Passive Air and Missile Defense Measures. The objective of passive air and missile defense is to degrade the enemy's ability to target US and HN or allied forces and facilities, reduce vulnerability to attack, and provide for reconstitution and recovery of forces.

a. Warning. Attack warning is a trigger event for passive defense measures by non-air-defense assets. Air defense warnings are normally issued by the AADC and are categorized as red (hostile attack imminent), yellow (probable), or white (improbable). Air defense assets will initiate engagements sequences to counter aircraft

and missiles threats in accordance with established air defense control measures, ROE and specific directives issued by the AADC.

b. Reducing Targeting Effectiveness

(1) Operations Security. Such OPSEC measures as transmission security, signature reduction, smoke, dummies, and pattern painting deny enemy sensor and reconnaissance assets accurate and timely acquisition, and identification of friendly targets. Signature reduction measures include camouflage, commonality of vehicle appearance, emission control programs for infrared and electromagnetic emissions, and cover and concealment. Local unit security is an important element in denying accurate targeting data to enemy special operations forces or other enemy agents.

(2) Military Deception. Military deception shapes the enemy's intelligence by conveying or denying data to their intelligence system. The intent is to influence their actions to our advantage, or to guard the secrecy of our actions. Deception normally will be employed as OPSEC measures.

(3) Mobility. Mobility, especially when combined with concealment, deception, and dispersal, can create uncertainty for the enemy as to whether they have found a key asset or a decoy. Mobility also creates uncertainty whether that asset will still be there when the enemy attacks it.

c. Reducing Vulnerability

(1) Hardening. Hardening reduces the effect of attack on aircraft, base support equipment and facilities, nuclear delivery systems and storage areas, C2 nodes, and other facilities. Hardening measures should commence before hostilities if possible. Field expedients should be replaced by permanent fortifications as time and resources permit.

(2) Dispersal. Dispersal reduces target vulnerability by increasing the distance between friendly assets. However, dispersal also will increase the difficulty of defending from a ground attack and frequently will reduce the efficiency of base operations.

(3) Training Civilian Authorities. Local authorities should be trained to organize and instruct their populations to protect themselves from air and missile attack. Effective training of this nature will reduce the physical and emotional impact of such attacks.

d. Reconstitution and Recovery. Following an attack, units must be restored to a desired level of combat effectiveness commensurate with mission requirements and available resources. Reconstitution may include reestablishing or reinforcing C2, reallocating or replacing personnel, supplies, and equipment, conducting essential training, reestablishing unit cohesion, and repairing damage.

(INTENTIONALLY BLANK)

APPENDIX D

BASE DEFENSE OPERATIONS CENTER

1. The Base Defense Operations Center

a. There is no standard organization for a BDOC. Just as the size, type, and classification of bases vary, so does the organization of the BDOC.

b. The base commander must form the BDOC from available base assets. There are several options regarding the location and status of the BDOC:

(1) A base mission operations center also performs BDOC function. This option is possible when the function of the base can be interrupted in order to conduct defensive operations. The base staff becomes the base defense staff.

(2) BDOC is adjacent to the base mission operations center. Base defense operations are conducted while the base's primary mission continues. The defense function is separate from the mission, but proximity permits a high degree of coordination and possible sharing of physical facilities, such as communications and messing.

(3) BDOC is separate from the base mission operations center. This option may be forced by the necessity to occupy separate facilities or may be selected to ensure that the two functions do not mutually interfere.

c. Support

(1) During low-threat periods the BDOC may be able to function with austere support. Only sufficient personnel and equipment to supervise security efforts and process long-range intelligence may be necessary. Most base personnel can then concentrate their efforts on the base's primary mission, although all personnel should rehearse base defense procedures.

(2) As the threat to the base is perceived to increase, more base units and personnel are diverted from mission tasks to their defense responsibilities. As a result, the BDOC evolves, as planned, into an operations center capable of controlling a full-scale defense of the base.

2. Notional BDOC. When fully augmented for controlling the defense of the base against full-scale attacks, the BDOC should be structured with the following functional elements. Numbers of personnel in each element depend on base size and the requirements for 24-hour operations. Some functions may be performed by other C2 activities on the base. Paragraph 3 discusses base defense facilities on an Air Force installation.

a. Operations Element

(1) BDOC chief (Commander, Base Defense Force).

(2) Operations personnel.

(3) NBC personnel.

(4) Engineer representative.

(5) MP or SP representative.

(6) Legal personnel.

b. Intelligence Element

(1) Intelligence personnel.

(2) CI personnel.

c. Fire Support Element and Fire Support Coordination Center. If attached, Air Force, Navy, Marine air, Army air defense, and naval gunfire liaison personnel will join the FSE/FSCC to form a fire support cell. Normally, a BDOC will not be provided an FSE/FSCC, in which case the function will be performed by the BDOC operations element.

d. ADC Element

e. Civil-Military Operations (CMO) Element

f. Communications Element

g. Liaison Teams

(1) RAOC/RTOC liaison officer (LNO).

(2) HN representative.

(3) Tactical combat force LNO.

(4) Intelligence and CI liaison personnel.

h. Medical Element

3. Air Force Base Defense

a. The base commander, operations personnel, NBC personnel, engineer representatives and CI personnel from Air Force Office of Special Investigations (AFOSI) are located at the SRC.

b. Damage control and EOD personnel are located at the Damage Control Center (DCC).

c. The BDOC on Air Force installations consists of security personnel, fire support representatives (including naval gunfire support if available), and HN representatives.

d. The SP chief works for the senior installation commander and acts as the commander's executive agent for ground defense (ground defense force commander) operating the BDOC. Personnel from AFOSI and wing intelligence functions or sections provide their information to the BDOC intelligence section.

4. Level I Threat Considerations. In the level I threat environment, the BDOC may take the form of a regional coordination center, including civilian advisers. BDOC can coordinate US and HN military and civilian activities and coordinate the politico-military battle.

(INTENTIONALLY BLANK)

APPENDIX E

SAMPLE BASE DEFENSE PLAN

(In Joint Operations Order (OPORD) Format)

SECURITY CLASSIFICATION

Copy No. _____
Issuing Headquarters
Place of Issue
Message Reference Number

Type and Serial Number of Operations Order.

References:

a. Maps or Charts

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

Task Organization. (List this information here, in paragraph 3, or in an annex, if voluminous. The organization for defense should clearly specify the base units providing the forces for each defense element. Attached or transient units and the names of commanders should be included. The defense requirements of US and HN civilian organizations quartered on the base also should be identified. Their capabilities to assist in the defense must be determined and integrated into the base defense plan.)

1. Situation. (Under the following headings, describe the environment in which defense of the base will be conducted, in sufficient detail for subordinate commanders to grasp the way in which their tasks support the larger mission.)

a. Enemy Forces. (Describe the threat to the base, to include the composition, disposition, location, movements, estimated strengths, and identification and capabilities of hostile forces, including terrorist organizations.)

b. Friendly Forces. (List information on friendly forces not covered by this operation order, to include the mission of the next higher headquarters and adjacent bases, and units not under base command whose actions will affect or assist the defense of the base. These units may include MP or Air Force SP response forces, fire support, naval coastal warfare forces, engineers, NBC decontamination or smoke units, EOD, or HN military or police organizations, and public and private civilian organizations of both the United States and HN.)

c. Attachments or Detachments. (When not listed in the Task Organization, list elements attached to or detached from base units and the effective times.)

2. Mission. (Give a clear, concise statement of the commander's defense mission.)

3. Concept of the Operation. (Under the following headings, describe the commander's envisioned concept of the operation.)

a. Commander's Intent. (The commander discusses how the development of the defense is envisioned and establishes overall command priorities. This subparagraph should provide subordinates sufficient guidance to act upon if contact is lost or disrupted.)

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

(1) Phasing. (Set forth, if necessary, the phases of the operation as they are anticipated by the commander.)

(2) Maneuver. (Describe the organization of the ground defense forces, the assignment of elements to the security area to primary, alternate, and supplementary defensive positions, and to the base rear area. Describe the purpose of counterattacks and set work priorities.)

(3) Fires. (State plans for employing supporting fires, such as mortars and other indirect fire assets, smoke, and aviation support.)

c. Tasks for Subordinate Elements. (If not previously described, this and succeeding subparagraphs should set forth the specific tasks for each subordinate defense element listed in the Task Organization.)

d. Reserve. (The next-to-last subparagraph of paragraph 3 contains instructions to the base's mobile reserve.)

e. Coordinating Instructions. (Always the last subparagraph of paragraph 3. Contains those instructions applicable to two or more elements or to the command as a whole.)

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

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

(b) Materiel Control Procedures

1. Incoming

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

b. (List special controls on delivery of supplies to restricted areas.)

2. Outgoing

a. (List required documentation.)

b. (List special controls on delivery of supplies from restricted areas.)

c. (List classified shipments.)

(c) Vehicle Control

1. (State policy on registration of vehicles.)

2. (State policy on search of vehicles.)

3. (State policy on parking.)

4. (State policy on abandoned vehicles.)

5. (List controls for entering restricted areas.)

(d) Train Control

1. (State policy on search of railcars.)

2. (State policy on securing railcars.)

3. (State policy on entry and exit of trains.)

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

(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.

d. Protective lighting system. (Use and control, inspection, direction, actions during power failures, emergency lighting.)

(b) Intrusion Detection System

1. Security classification.

2. Inspection and maintenance.

3. Use and monitoring.

4. Action upon alarms.

5. Logs and registers.

6. Sensitivity.

7. Fail-safe and tamper-proof provisions.

8. Monitor panel location.

(c) 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 that procedures include randomness.)

(a) Composition and organization. (NOTE: In a low-intensity conflict environment, the interior guard may be a contracted civilian security force.)

(b) Tour of duty.

(c) Essential posts and routes.

(d) Weapons and equipment.

(e) Training.

(f) Military working dogs.

(g) Method of challenge.

(h) Alert force.

1. Composition.

2. Mission.

3. Weapons and equipment.

4. Location.

5. Deployment concept.

(4) Rules of Engagement. (Coordinate and control the use of force to prevent fratricide.)

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

(a) Individual actions.

(b) Alert force actions.

(6) Security Alert Status

(7) Air Surveillance

(8) Noncombatant Evacuation Order (NEO) Plans

(9) Coordination With HN or Adjacent Base Plans

(10) Measures for Coordination With Response Force and Tactical Combat Forces

(11) Procedures for update of this OPORD. (If the OPORD is not effective upon receipt, indicate when it will become effective.)

4. Administration and Logistics. (This paragraph sets forth the manner of logistic support for base defense. State the administrative and logistic arrangements applicable to the

operation. If the arrangements are lengthy, include them in an annex or a separate Administrative and Logistics Order. Include enough information in the body of the order to describe the support concept.)

a. Concept of Combat Service Support. (Include a brief summary of the base defense concept from the combat service support point of view.)

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

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

d. Damage Control. (List plans for firefighting, clearing debris, and emergency construction.)

e. Personnel. (List procedures for strength reporting, replacements, and other procedures pertinent to base defense, including handling civilians and prisoners of war.)

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

5. Command and Signal

a. Communications. (Give information about pertinent communications nets, operating frequencies, codes and code words, recognition and identification procedures, and electronic emission constraints. Reference may be made to an annex or to a SOI.)

b. Command

(1) Joint and combined relationships. (Command relationships must be spelled out clearly, to include command succession. Shifts in relationships as the defense progresses, as when a response force is committed, must be specified. These relationships may be presented in chart form as an annex.)

(2) Command posts and alternate command posts. (List locations of the BDOC, BCOC, and their alternate sites, along with the times of their activation and deactivation.)

6. Acknowledgment Instructions

Annexes:

A. Task Organization
B. Intelligence
C. Operations
D. Logistics
E. Personnel
F. Public Affairs
G. Civil Affairs
H. Engineer Support
J. Command Relationships
K. Command, Control, and Communications
L. Force Protection
M. Host Nation Support
N. NBC Defense

Distribution:

Authentication:

APPENDIX F

SECURITY

Security is the primary concern under threat Level I, especially if the base is located in an urban area.

SECTION A
TACTICAL SECURITY

1. Patrols. Patrolling is necessary outside the physical base, but within the TAOR, to provide additional base security. Patrolling urban areas involves different risks and considerations than patrolling open or cleared uninhabited areas. Patrolling may require the use of military working dogs. A patrol is tasked to collect information; confirm or deny accuracy of previously gained information; provide security; and harass, destroy, or capture the enemy. The two categories of patrol are reconnaissance and combat. Patrols can be conducted dismounted or mounted.

a. Dismounted Patrols. A patrol may be a fire team, squad, platoon, or company. Patrol members must be able to interact with local inhabitants but still should be ready to conduct combat operations. Multiple units maintain mutual support for each other as they move and operate.

b. Mounted Patrols. Mounted patrols are especially useful in an economy of force mission where the unit has a large sector to cover and few personnel to patrol. Mounted patrols can be used to cover gaps between units in the defense, provide flank security and coordination, patrol forward of the base perimeter to provide early warning, and assist in reconnaissance when a large sector must be covered in a relatively short time.

(1) Organization and Preparation. The leaders of the patrol must analyze the mission, determine what elements are needed, and decide how to accomplish the mission.

(a) The patrol leader must consider route selection, linkup procedures, resupply, signal plan, departure from and reentry to base defense positions, and other friendly units in the area. Recognition signals must be firmly established to provide early and immediate identification by friendly forces.

(b) A map, ground, or aerial reconnaissance by the leader will help balance the size of the area, the time constraints of the mission, and the patrol's security requirements.

(2) Fundamentals of Movement. Inherent in all mounted patrol operations is the command and control of movement. Communications and maintenance are vital because they support movement.

(a) Competent navigation and aggressive leadership are vital ingredients to movement. Movement techniques must be understood at all levels of command. An important requirement for a mounted patrol is for the patrol to see the enemy first. The global positioning system should be used, if available.

(b) Once the enemy is sighted or encountered, the patrol moves to accomplish its task.

(c) While moving, a patrol must maximize cover and concealment using the terrain. The leader must weigh the degree of security allowable against the required speed of execution to minimize the risk to the patrol.

(d) A mounted patrol should never enter a major cross compartment without first establishing security and visually inspecting the area. Mounted patrols should make maximum use of dominating overwatch positions that offer good observation and fields of fire. Elements occupying overwatch positions must do the following:

1. Visually check the security of the position and be prepared to dismount to secure the area.

2. Occupy covered or concealed positions.

3. Cover the areas for observation and fire assigned by the element leader.

4. Orient weapons on likely or suspected enemy positions.

5. Search for and be alert for enemy activity.

(3) A mounted patrol must:

(a) Be alert for unusual people, vehicles, or incidents close to the beginning and end of the patrol route.

(b) Avoid the same daily routes and times.

(c) Avoid isolated routes and stops.

(d) Lock vehicle doors when appropriate.

(e) Stop short of unusual objects or incidents.

(f) Detour around suspicious obstacles.

(g) Continually check to the rear.

(h) Be aware of vehicles' capabilities.

(i) Use and practice movement techniques, such as traveling overwatch and bounding overwatch.

2. Roadblocks and Checkpoints. A roadblock is used to limit the movement of vehicles along a route or to close access to certain areas or roads. Checkpoints are manned locations used to control movement. A roadblock is used with a checkpoint to channel vehicles and personnel to the search area. Roadblocks may be set up on a temporary or surprise basis or may be semipermanent in nature.

a. Roadblocks are used to:

(1) Maintain a continuous check on road movement, apprehend suspects, and prevent smuggling of controlled items.

(2) Prevent infiltration of unauthorized civilians into or through a controlled area.

(3) Check vehicles for explosive devices.

(4) Ensure proper use of routes by both civilian and military vehicles.

b. Because roadblocks cause considerable inconvenience and even fear, ensure that the civilian population understands that the roadblocks are preventive and not punitive measures.

c. Roadblocks and checkpoints may be either deliberate or hasty. The deliberate roadblock or checkpoint is a relatively fixed position on the base, in a town, or in the open country, often on a main road. It acts as a useful deterrent to unlawful movement. The hasty roadblock or checkpoint is highly mobile and is quickly positioned on the base, in a town, or in the open country. Its actual location is designed to achieve surprise.

d. Conceal the roadblock or checkpoint, when appropriate. The location should make it difficult for a person to turn back or reverse a vehicle without being observed. Positions beyond sharp curves have the advantage that drivers do not see the checkpoint in sufficient time to avoid inspection. However, the checkpoint should be positioned so that drivers can stop safely.

e. A roadblock or checkpoint requires adequate personnel to provide security. A security force is concealed an appropriate distance from the roadblock or checkpoint to prevent the escape of any vehicle or person attempting to turn back upon sighting the checkpoint. The vehicle, driver, and passengers are searched. If possible, the area designated for searching vehicles is below ground level to deflect an explosive blast upward.

f. For a roadblock or checkpoint to be effective, special measures are required:

(1) Signs. Portable signs in the native language and in English must be available. Signs should denote the speed limit of approach, vehicle search area, vehicle parking area, male and female search areas, and dismount point.

(2) Lights. Adequate lighting is essential for the search area at night.

(3) Communications. Radio or land line communication is required among the various locations supporting the checkpoint operation. These include the security position, the search area, and the BDOC.

(4) Barriers. Obstacles across the road and around the search area should be provided. Obstacles must be strong and big enough to prevent motorists from driving through or around them.

(5) Firepower. Security personnel must have adequate firepower to withstand an attack or halt a vehicle attempting to flee or crash through the checkpoint.

(6) Linguists. Personnel familiar with the native language are essential at all roadblocks and checkpoints.

g. Establishment of Roadblocks and Checkpoints. Each roadblock and checkpoint is established by placing two parallel obstacles across the road. In addition to having barriers large enough to prevent someone from running over or through them, barriers should have gaps negotiable only by slowly moving vehicles.

(1) The separation between obstacles depends on the amount of traffic to be held in the search area. The blocked section of road can be used as the search area. If possible, there should be a place adjacent to the road where large vehicles can be searched without delaying the flow of traffic.

(2) Areas are required for searching suspects of both sexes and for detaining persons for further interrogation. Personnel manning a checkpoint should include a member of the local police, a fluent interpreter, EOD personnel, and trained females for searching other females. When a vehicle is being searched, the occupants should stand clear of the vehicle and be searched concurrently. The vehicle searcher should use an assistant to watch the occupants and provide additional security. If available, explosive detectors and dogs may be used to aid the search. Politeness and consideration should be shown to the extent consistent with a thorough search, and roadblock or checkpoint personnel should be thoroughly familiar with the limits of their legal authority.

3. 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.

a. Security Precautions. When employed in urban areas, commanders must estimate the threat and plan for the

defense. In addition, they should consider the following security precautions:

(1) Wire fences or barriers for additional protection.

(2) 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-charge explosive devices.

(3) Canopies of chain-link, weld mesh, or corrugated iron. These will protect roofs if they are placed at least 1 meter above the roofs. Sandbags placed directly on roofs will absorb shrapnel.

(4) Obstacles in the approaches will slow or stop vehicles and personnel approaching the defended area. However, the entrance gate 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.

(5) 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:

(a) Entrances, to check entry permits.

(b) Observation posts or rooftops, to observe all avenues of approach and dominate buildings and grounds.

(c) Perimeter sites.

b. Employment of Sentries. Sentries must be properly trained and equipped. Some security operations may require the use of military working dogs. Sentries must be briefed on the ROE and appropriate use of force. They must be able to call on the base mobile reserve for assistance. Sentries employed in urban areas must:

(1) Detect and deter anyone seeking to gain unauthorized access to the secured area.

(2) Prevent damage, arson, and looting within the secured area.

(3) Ensure the maintenance of essential services.

(4) Be briefed on friendly forces operating in the area such as patrols, OPs and LPs, and other adjacent unit activities.

4. Convoy Defense. Convoys on large bases or between bases are arranged for control and protection using armored vehicles, military police escort, or aerial 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 combat units is not available. Each convoy is organized into an advance party, main body, and trail party. The convoy commander estimates the situation and develops a plan, to include a briefing for all convoy members. The briefing should include:

a. Enemy situation and capabilities, terrain, and weather.

b. Composition and order of march.

c. Chain of command and location of leaders.

d. General security posture.

e. Communications and signals.

f. Objectives.

g. Routes, schedules, and other control measures.

h. Emergency actions, actions on contact, and actions at halts.

5. Searches

a. Personnel. Personnel searches may be required to maintain the safety and security of the command. Quick body searches or detailed body searches may be conducted, consistent with the security environment and respect for the individual being searched. Metal detection systems should be used if available.

b. Buildings

(1) 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 ECM constraints.

(2) Assume that any unoccupied house or building is booby-trapped. Position supporting fire elements (machineguns, mortars) to cover the roofs and adjacent buildings. Begin search from roof if possible. Mark cleared room windows with sheets or blankets. Arm search teams with grenades, shotguns, and light machineguns. 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 obvious entryways and, if possible, use holes in walls and roofs. Check doors and windows for booby-traps before entering. Clearly mark with white tape the routes through the building that have been cleared. Once the building is cleared of traps, the team leader will allocate teams of searchers to make detailed room searches. If possible, avoid all radio transmissions from within buildings being searched.

(3) Military working dogs, if available, can be used to search for arms, ammunition, explosive caches in buildings, open areas, and routes to be cleared.

(4) Local officials should accompany search teams. If the building is occupied, an occupant should accompany the team.

6. Ambushes. Planned ambushes are surprise attacks by fire from concealed positions on a moving or temporarily halted enemy. However, in urban areas, ambushes are often designed to apprehend wanted persons, not necessarily to kill them. Urban ambushes should be planned to avoid harm to civilians and should be coordinated with HN forces. Sites for ambushes should be carefully planned considering the latest intelligence about hostile groups or persons.

7. Responses to Attacks. When responding to an attack from an urban area, defenders must try to kill or capture assailants while keeping the base secure. Defenders also must consider:

a. Returning fire according to ROE.

b. Submitting a contact report, including the location, numbers of casualties, and estimated opposition.

c. Dispatching sufficient force to engage the enemy.

d. Estimating the civilian situation.

e. Establishing roadblocks on likely escape routes.

f. Deploying cordon sentries, as necessary.

g. Alerting local authorities.

h. Recovering and aiding hostages.

i. Securing the scene for collection of evidence.

8. Crowd Control

a. 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 minimum force, and return control to civilian authorities. HN police agencies should assume principal responsibility 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.

b. The best way to disperse rioters is to make key arrests and simultaneously demonstrate the ability to disrupt the activities of the remaining rioters. Separation from leaders combined with the likelihood of apprehension and the denial of unrestricted actions can have a debilitating effect on mob activities. 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 troops to the assembly or base area. Try not to escalate the violence by misuse of force. The use of riot control agents must follow stated national policy and HN agreements. Close coordination with legal counsel and US diplomatic missions may be necessary.

SECTION B
UNIT SECURITY

9. Planning

a. Mission Analysis. To perform a mission analysis, ask the following questions:

(1) How can the mission be adversely affected by an attack?

(2) What are the security aspects of both specified and implied tasks?

b. Threat Assessment. Coordinate with intelligence and CI personnel to 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. Identify insurgent and terrorist groups operating in the deployment area. Develop a list of PIR, including:

(1) Methods of operation.

(2) Attack methodology.

(3) Preattack indicators.

c. Support Considerations. To implement unit security, the following areas should be considered:

(1) Supply. Procure special security equipment, such as detectors, portable barriers, and intrusion detection devices. Protect storage and distribution areas.

(2) Maintenance. Maintain special equipment and provide security to maintenance units.

(3) Transportation. Provide security during movement and in staging areas and provide liaison with security agencies such as area MP organizations supporting movements.

(4) Engineer. Provide security and ADC measures and special engineer equipment.

(5) Base Military or Security Police. Check, inspect, and improve unit physical security. Provide liaison with local police and security personnel. Screen US and HN civilian employees.

(6) Health Services Support. Ensure security of medical facilities, secure medical supplies and equipment, and safeguard patients.

10. Operational Considerations

a. Factors That Degrade Security

(1) An established routine or pattern of events.

(2) Inability to restrict access.

(3) Inability to choose unit location based on security considerations.

(4) Restrictions on the employment of security forces.

(5) Required presence of nonunit personnel.

(6) Inadequate coordination or liaison.

b. Measures That Enhance Security

(1) Continuous reassessment of the mission, policies, threat, and attitude of local inhabitants.

(2) Using organic and special equipment, such as closed circuit TV, intrusion detection devices, sensors, lighting, barriers, and barricades.

(3) Assigning physical security responsibilities to trained physical security officers.

(4) Ensuring that security personnel are aware of guard orders, ROE, local restrictions, and other regulations and policies.

(5) Maintaining and conducting an aggressive training program, with frequent realistic exercises involving US and HN forces.

(6) Preparing good defensive positions, barrier plans, and dispersion procedures for vehicles and high-value facilities.

(7) Maintaining a low off-base personnel profile.

(8) Restricting access of visitors to the unit location.

SECTION C
OPERATIONS SECURITY

11. Objectives. The OPSEC program is designed to deny access to intelligence and information that the threat can use to learn about plans and operations. The BDOC operations element normally will be the responsible agency for OPSEC, supported by the CI element. OPSEC objectives are to:

a. Avoid stereotyped operations.
b. Understand methods used by the threat to collect intelligence.
c. Deny intelligence and information to the enemy.
d. Integrate OPSEC into physical and personnel security programs.

12. Measures. Defenders must:

a. Develop essential elements of friendly information (EEFI) on those items and activities of planning and operations that hostile forces can use.
b. Vary locations, routes, and schedules of key activities.
c. Use protective barriers.
d. Check personnel identification at critical entrances.
e. Use additional measures at critical installations, such as communications centers, command posts, and high-density troop areas.
f. Control schedules of VIPs.

3. Intelligence Indicators of Friendly Activity. Activities of base units and personnel may be useful to enemy intelligence agencies.

a. Operational Indicators

(1) Troop restrictions before an operation.
(2) Increased friendly patrolling and air reconnaissance.
(3) The complete cessation of friendly patrolling.
(4) Increased friendly troop movements.
(5) Special requests for rations, transport, or ammunition.

b. HUMINT Indicators

(1) Media coverage.
(2) Visits by VIPs.
(3) Special religious services.
(4) Bulletins or other notices announcing changes to normal procedures.

c. Communications Indicators

(1) Nonroutine changes to call signs and frequencies.
(2) Changes in antennas or facilities.
(3) Increased electronic signature.

(INTENTIONALLY BLANK)

APPENDIX G

TERRORISM

1. General. Terrorism is 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. Terrorism involves a criminal act that is often symbolic and intended to influence an audience beyond the immediate victims. Terrorist tactics include assassination, arson, bombing, hostage-taking, kidnaping, hijacking and skyjacking, seizure, raids or attacks on facilities, sabotage, hoaxes, potential use of special weapons, and environmental destruction. Combatting terrorism consists of actions, including antiterrorism (defense 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.

2. Unit Vulnerability. Commanders should evaluate how vulnerable their units are to terrorist attack, including consideration of the HN political environment. Vulnerability changes as units change locations, activities, and quarters, and as reinforcements are available or VIPs conduct visits. Commanders need to update their evaluations continually.

3. Threat Conditions and Responses. Warnings of terrorist activity against US bases normally will come from US intelligence or security authorities or through the security agencies of the HN. Warnings also may come from local police or even from terrorist organizations themselves. In combatting terrorism, bases should use common terrorist threat conditions (THREATCONs), each with its specific security measures and required responses.

a. Threat Assessment. Threat assessments will be used to determine threat levels, to implement security decisions, and to establish awareness and resident training requirements. Threat levels are determined by an assessment of the situation using the following six terrorist threat factors:

(1) Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

(2) Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

(3) Intentions. Recent demonstrated anti-US terrorist activity, or stated or assessed intent to conduct such activity.

(4) History. Demonstrated terrorist activity over time.

(5) Targeting. Current credible information on activity indicative of preparations for specific terrorist operations.

(6) Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to implement their intentions.

b. Threat Levels. The severity of the terrorist threat is indicated by the designated threat level, assigned through analysis of the above threat assessment factors. Threat levels, and associated factors, are:

(1) Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history and intentions must be present.

(3) Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and/or capability may or may not be present.

c. THREATCON. The terrorist threat level is one of several factors used in the determination of terrorist THREATCON. Factors that enter into the decision to assign a particular THREATCON and its associated measures include threat, target vulnerability, criticality of assets, security resource availability, impact on operations and morale, damage control, recovery procedures, international regulations, and planned US Government actions that could trigger a terrorist response. The terrorist THREATCON system provides a common framework to facilitate inter-Service

coordination, support US military antiterrorist (AT) activities, and enhance overall DOD implementation of US Government AT policy. THREATCONs are described below. Measures and required actions are listed in Joint Pub 3-07.2.

(1) THREATCON NORMAL. Applies when a general threat of possible terrorist activity exists, but the threat warrants a routine security posture.

(2) THREATCON ALPHA. Applies when there is a general threat of terrorist activity against personnel and installations, the exact nature and extent of which are unpredictable and circumstances do not justify full implementation of THREATCON BRAVO measures. However, base defense forces may have to implement selected measures from higher THREATCONs based on intelligence received. Base defense forces must be able to maintain the measures in this THREATCON indefinitely.

(3) THREATCON BRAVO. Applies when an increased and more predictable threat of terrorist activity exists. Base defense forces must be able to maintain the measures of this THREATCON for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

(4) THREATCON CHARLIE. Applies when an incident occurs or when intelligence indicates an imminent terrorist action against US bases and personnel. Implementation of measures in the THREATCON for more than a short period probably will create hardship and affect peacetime activities of the unit and its personnel. Sustaining this posture for an extended period probably will require augmentation.

(5) THREATCON DELTA. Applied in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

4. Base Terrorism Response. The commander of the base is responsible for preventive and protective security measures to protect units and individual Service members and their ability to accomplish their missions. These measures are described in Appendix F. Joint Pub 3-07.2 also describes such measures, as well as techniques for the preparation of a base AT plan.

(INTENTIONALLY BLANK)

APPENDIX H

SPECIALIZED EQUIPMENT AND MATERIAL

The following tables listing equipment and materiel specific to joint base defense are not all-inclusive. Base mission, threat, and environment may dictate other requirements. Commanders must ensure that all base defense personnel are properly trained and qualified to use equipment and weapons, as appropriate. SOPs for using equipment and weapons should be developed and implemented.

Table H-l. Equipment and Material for General Use

Pyrotechnic pistols	Telescopes and tripods	Loudspeakers
Riot guns	Infrared devices	Fire extinguishers
Tear gas launchers	Listening devices	Cameras with flash attachments and tripods
Tear gas grenades	Protective masks	Telescopic sights
Hand-held flashlights	Marshaling wands	Photographic filters
Riot helmets	Whistles	Polaroid cameras
Shields	Grass-cutting equipment	Hand-held radios
Police batons	Defoliant	Tactical deception equipment (camouflage nets, false structures and equipment, false fencing)
Handcuffs and flexicuffs	Binoculars	High-pressure hoses and equipment
Body armor	Fire-fighting equipment	Closed circuit television (CCTV) camera
Leg armor	Medical equipment and supplies	Low-light-level CCTV camera
Vehicle intrusion alarms	Tactical maps--1:50,000 if available out to 35 km	Infrared spotlights and goggles
Manuals on local people and customs	Ground surveillance equipment	
Manuals on threat and personal protection	FLIR on aircraft	
Trip flares		
Night vision devices		

Table H-2. Equipment and Material for Roadblocks and Gates

Portable lamps, lights	Marker lights	Tire puncture chains
Traffic signs	Visor sleeves	Portable and stationary metal detectors
Lightweight barriers	Mirrors	City street maps (1:25000 or 1:15000)
Steel cable	Badge system at all entry points	
Concertina wire	Traffic cones	

Table H-3. Equipment and Material for Searches

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

Table H-4. Equipment and Material for Specialists

Explosive detectors	Concrete mixers	EOD equipment
Remote light units	Portable compressors	Military working dogs
Remote-controlled EOD devices	Hydraulic platform	NBC detection devices
Video periscopes	Engineer tractors	Command destruct munitions (thermite grenades)
Endoscopes	Engineer heavy equipment	
Platform hoists		

Table H-5. Equipment and Material for Static Defense

Portable sensors	Wire netting	Duress signal systems at guard stations (doorbell, radio)
Portable alarms	Corrugated steel	
Portable lighting systems	Fencing	Call to arms system (alarm, loudspeakers)
Barriers (drop arm, swing arm, and counterbalance)	Steel girders	Sandbags
Roadblock equipment for exit and entry control	Scaffolding	Telephone system and switch backup generators
CCTV	Mines (antivehicle, antipersonnel)	Water purification system
Shot direction indicator	Piping for personnel turnstiles	Armor plate glass
Wire (barbed, concertina)	Perforated steel planking (PSP) matting	

Table H-6. Equipment and Material for Ports

Minesweeping equipment	Percussion grenades	Sonar buoys
Diving equipment	Patrol boats	Antisubmarine nets
Underwater demolition equipment	Underwater salvage equipment	Antiswimmer nets
Minehunting equipment		Mines

(INTENTIONALLY BLANK)

APPENDIX J

REFERENCES

JOINT PUBLICATIONS

1. Joint Pub 0-2, 1 December 1986, "Unified Action Armed Forces (UNAAF)"

2. Joint Pub 1-01, 30 July 1992, "Joint Publication System (Joint Doctrine and JTTP Development Program)"

3. Joint Pub 1-02, 1 December 1989, "DOD Dictionary of Military and Associated Terms"

4. Joint Pub 2-0 (Test Pub), 30 June 1991, "Doctrine for Intelligence Support to Joint Operations"

5. Joint Pub 3-0 (Test Pub), 10 January 1990, "Doctrine for Joint Operations"

6. Joint Pub 3-01.2, 1 April 1986, "Joint Doctrine for Theater Counterair Operations"

7. Joint Pub 3-01.5 (in development), "Doctrine for Joint Theater Missile Defense"

8. Joint Pub 3-07 (Test Pub), 18 October 1990, "Doctrine for Joint Operations in Low-Intensity Conflict"

9. Joint Pub 3-07.2 (in development), "JTTP for Antiterrorism"

10. Joint Pub 3-09 (in development), "Doctrine for Joint Fire Support"

11. Joint Pub 3-10 (Test Pub), 30 October 1991, "Doctrine for Joint Rear Area Operations"

12. Joint Pub 3-11, (in development), "Joint Doctrine for Nuclear, Biological, and Chemical (NBC) Defense"

13. Joint Pub 3-15 (in development), "Joint Doctrine for Barriers, Obstacles, and Mines"

14. Joint Pub 3-52 (Test Pub), 15 August 1991, "Doctrine for Joint Airspace Control in the Combat Zone"

15. Joint Pub 3-53, February 1987, "Joint Psychological Operations Doctrine"

16. Joint Pub 3-54, 15 December 1982, "Joint Doctrine for Operations Security"

17. Joint Pub 3-57 (Test Pub), 25 October 1991, "Doctrine for Joint Civil Affairs"

18. Joint Pub 4-0, 25 September 1992, "Doctrine for Logistics Support of Joint Operations"

19. Joint Pub 4-01.6, 22 August 1991, "JTTP for Logistics Over the Shore (JLOTS)"

MULTI-SERVICE PUBLICATIONS

1. FM 19-6/AFM 3-3 (Draft), 25 April 1991, "Army-Air Force Air Base Ground Defense"

2. FM 90-12/FMFRP 2-73/TACP 50-50/PACAFP 50-50/USAFEP 50-50/AACP 50-50, 2 October 1989, "Base Defense: Multi-Service Procedures for Defense of a Joint Base"

3. FM 90-23/TACP 50-49/USAFEP 50-49/PACAFP 50-49/AACP 50-49, 14 November 1989, "Rear Security Operations: Army-Tactical Air Forces Procedures for Rear Security Operations at Echelons Above Corps"

4. FM 100-20/USAF Pamphlet 3-20, 5 December 1990, "Military Operations in Low Intensity Conflict"

5. DA Pamphlet 525-14/USAF Pamphlet 206-4, 15 July 1986, "Joint Operational Concept for Air Base Ground Defense"

ARMY PUBLICATIONS

1. AR 381-10, 1 July 1984, "US Army Intelligence Activities"

2. AR 381-12, 1 July 1981, "Subversion and Espionage Directed Against the US Army (SAEDA)"

3. AR 381-19, 16 February 1988, "Intelligence Dissemination and Production Support"

4. AR 381-20, 26 September 1986, "US Army Counterintelligence Activities"

5. AR 525-13, "The Army Combating Terrorism Program"

6. AR 530-1, 1 May 1991, "Operations Security"

7. FM 1-103, 30 December 1981, "Airspace Management and Army Air Traffic Control in a Combat Zone"

8. FM 3-4, 21 October 1985, "NBC Protection"

9. FM 3-5, 24 June 1985, "NBC Decontamination"

10. FM 3-100, 23 May 1991, "NBC Defense, Chemical Weapons, Smoke and Flame Operations"

11. FM 5-34, 14 September 1987, "Engineer Field Data"

12. FM 5-116, 7 March 1989, "Engineer Operations: Echelons Above Corps"

13. FM 6-20, 17 May 1988, "Fire Support in the AirLand Battle"

14. FM 6-20-30, 18 October 1989, "Fire Support for Corps and Division Operations"

15. FM 6-30, 16 July 1991, "Tactics, Techniques and Procedures for Observed Fire"

16. FM 7-8, 31 December 1980, "The Infantry Platoon and Squad (Infantry, Airborne, Air Assault, Ranger)"

17. FM 7-10, 14 December 1990, "The Infantry Rifle Company (Infantry, Airborne, Air Assault, Ranger)"

18. FM 7-20, 28 December 1984, "The Infantry Battalion (Infantry, Airborne and Air Assault)"

19. FM 7-30, 17 February 1989, "Infantry, Airborne, and Air Assault Brigade Operations"

20. FM 11-23 (Draft), September 1987, "Theater Communications Command"

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

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

23. FM 33-1, 31 July 1987, "Psychological Operations"

24. FM 34-1, 2 July 1987, "Intelligence and Electronic Warfare Operations"

25. FM 34-2, 14 November 1986, "Collection Management"

26. FM 34-3, 15 March 1990, "Intelligence Analysis"

27. FM 34-37, 30 September 1987, "Echelons Above Corps (EAC) Intelligence and Electronic Warfare Operations"

28. FM 34-52, 8 May 1987, "Intelligence Interrogation"

29. FM 34-60, 5 February 1990, "Counterintelligence"

30. FM 34-130, 23 May 1989, "Intelligence Preparation of the Battlefield"

31. FM 41-10, 17 December 1985, "Civil Affairs Operations"

32. FM 44-18, 30 September 1981, "ADA Employment, Stinger"

33. FM 54-40, 29 July 1987, "Area Support Group"

34. FM 63-4, 24 September 1984, "Combat Service Support Operations: Theater Army Area Command"

35. FM 71-100, 16 June 1990, "Division Operations"

36. FM 90-14, June 1985, "Rear Battle"

37. FM 100-5, 5 May 1986, "Operations"

38. FM 100-15, 13 September 1989, "Corps Operations"

39. FM 100-16, 16 April 1985, "Support Operations: Echelons Above Corps"

40. FM 101-5, 25 May 1984, "Staff Organization and Operations"

AIR FORCE PUBLICATIONS

1. Air Force Manual 2-11, 1 January 1992, "Air Force Foreign Internal Defense Operations"

2. Air Force Pamphlet 31-302, "Air Base Ground Defense and Contingency Operations"

3. Air Force Pamphlet 360-2, 28 September 1987, "Wing Commander's Air Base Operability (ABO) Planning Considerations Guide"

4. Air Force Instruction 31-301, "Air Base Ground Defense Tactical Doctrine"

5. Air Force Regulation 355-1, 17 November 1986, "Disaster Preparedness Planning and Operations"

6. Air Force Regulation 355-3, 5 September 1989, "Air Force Personnel Shelter Program"

7. Air Force Regulation 355-8, 31 August 1990, "Mission Oriented Protective Postures"

8. Air Force Regulation 360-1, 31 December 1986, "Air Base Operability -- Planning and Operations"

NAVY PUBLICATIONS

1. NWP 8, "Command and Control"

2. NWP 15-2, September 1981, "Special Boat Squadrons in Naval Special Warfare"

3. NWP 39, June 1988, "Naval Coastal Warfare Doctrine"

4. NWP 40, "Inshore Undersea Warfare"

MARINE CORPS PUBLICATIONS

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

2. OH 2-6, 7 August 1986, "MAGTF Rear Area Security"

(INTENTIONALLY BLANK)

APPENDIX K

USERS EVALUATION REPORT ON JOINT PUB 3-10.1

1. Users in the field are highly encouraged to submit comments on this pub. Please fill out the following: Users' POC, unit address, and phone (DSN) number.

2. Content

   a. Does the pub provide a conceptual framework for the topic?

   b. Is the information provided accurate? What needs to be updated?

   c. Is the information provided useful? If not, how can it be improved?

   d. Is this pub consistent with other joint pubs?

   e. Can this pub be better organized for the best understanding of the doctrine and/or JTTP? How?

3. Writing and Appearance

   a. Where does the pub need some revision to make the writing clear and concise? What words would you use?

   b. Are the charts and figures clear and understandable? How would you revise them?

4. Recommended urgent change(s) (if any).

5. Other

6. Please fold and mail comments to the Joint Doctrine Center (additional pages may be attached if desired) or FAX to DSN 564-3990 or COMM (804) 444-3990.

(FOLD)

FROM:

THE JOINT STAFF, J-7
ATTN: JOINT DOCTRINE CENTER
NORFOLK NAVAL AIR STATION
NORFOLK, VA 23511-5380

(FOLD)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

AADC	area air defense commander
ADC	area damage control
AFFOR	Air Force forces
AFOSI	Air Force Office of Special Investigations
ALSS	naval advanced logistic support site
AO	area of operations
AOR	area of responsibility
APOD	aerial port of debarkation
ARFOR	Army forces
ASG	area support group
AT	antiterrorism
BCOC	Base Cluster Operations Center
BDOC	Base Defense Operations Center
BDZ	base defense zone
BOC	Base Operations Center
C2	command and control
C3	command, control, and communications
C4	command, control, communications, and computers
CA	civil affairs
CCTV	closed circuit television
CI	counterintelligence
CINC	commander of a unified or specified command; commander in chief
CMO	civil-military operations
COCOM	combatant command (command authority)
COMARFOR	Commander, Army Forces
COMMARFOR	Commander, Marine Forces
COMMZ	communications zone
COMPLAN	communications plan
CONUS	continental United States
CP	command post
CP&I	coastal patrol and interdiction
DCC	Damage Control Center
DSN	Defense Switched Network
DZ	drop zone
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
EEFI	essential elements of friendly information
EOD	explosive ordnance disposal
EPW	enemy prisoner of war
EW	electronic warfare

FLIR	forward-looking infrared
FLS	naval forward logistic site
FSCC	Fire Support Coordination Center
FSE	fire support element
GSR	ground surveillance radar
HDC	harbor defense commander
HN	host nation
HNS	host nation support
HQ	headquarters
HUMINT	human intelligence
IFF	identification, friend or foe
IPB	intelligence preparation of the battlefield
IR	infrared; information requirement
JFACC	joint force air component commander
JFC	joint force commander
JIC	Joint Intelligence Center
JMC	Joint Movement Center
JRA	joint rear area
JRAC	joint rear area coordinator
JRTOC	Joint Rear Tactical Operations Center
JSOTF	joint special operations task force
JTTP	joint tactics, techniques, and procedures
LNO	liaison officer
LOC	lines of communications
LP	listening post
LZ	landing zone
MAGTF	Marine air-ground task force
MARFOR	Marine forces
MCM	mine countermeasures
MDSU	mobile diving and salvage unit
METT-T	mission, enemy, terrain and weather, troops and support available, time available
MIUWU	mobile inshore undersea warfare unit
MOPP	mission-oriented protective posture
MP	military police
MR	mobile reserve
MTMC	Military Traffic Management Command
NAVFOR	Navy forces
NBC	nuclear, biological, and chemical
NCA	National Command Authorities
NCW	naval coastal warfare
NCWC	naval coastal warfare commander
NEO	noncombatant evacuation order

OCOKA	observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach
OP	observation post
OPCON	operational control
OPORD	operation order
OPSEC	operations security
PA	public affairs
PIR	priority intelligence requirements
PSHDGRU	port security and harbor defense group
PSP	perforated steel planking
PSU	port security unit
PSYOP	psychological operations
RAOC	rear area operations center
RFC	response force commander
RF	response force
ROE	rules of engagement
RTOC	Rear Tactical Operations Center
SAO	security assistance office/officer
SBU	special boat unit
SEAL	sea-air-land team
SHORAD	short-range air defense
SHORADEZ	short-range air defense engagement zone
SOFA	status of forces agreement
SOI	signal operating instructions
SOP	standing operating procedure
SP	security police
SPOD	seaport of debarkation
SRC	Survival Recovery Center
TAACOM	theater army area command
TACON	tactical control
TACS	Theater Air Control System
TAOR	tactical area of responsibility
TCF	tactical combat force
THREATCON	threat condition
TOC	Tactical Operations Center
TOT	time-on-target
TPFDL	time-phased force and deployment list
UN	United Nations
UNAAF	Unified Action Armed Forces
USSPACECOM	US Space Command
USTRANSCOM	US Transportation Command
VIP	very important person

area damage control. Measures taken before, during or after hostile action or natural or man-made disasters, to reduce the probability of damage and minimize its effects. (Joint Pub 1-02)

area of responsibility

1. A defined area of land in which responsibility is specifically assigned to the commander of the area for the development and maintenance of installations, control of movement, and the conduct of tactical operations involving troops under his control along with parallel authority to exercise these functions.

2. In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation. (Joint Pub 1-02)

base

1. A locality from which operations are projected or supported.

2. An area or locality containing installations which provide logistic or other support.

3. Home airfield or home carrier. (Joint Pub 1-02)

base cluster. In base defense operations, a collection of bases, geographically grouped for mutual protection and ease of command and control. (Joint Pub 1-02)

base cluster commander. In base defense operations, the senior officer in the base cluster (excluding medical officers, chaplains, and commanders of transient units), with responsibility for coordinating the defense of bases within the base cluster, and for integrating base defense plans of bases into a base cluster defense plan. (Joint Pub 1-02)

base cluster operations center.** A command and control facility that serves as the base cluster commander's focal point for defense and security of the base cluster.

base commander. In base defense operations, the officer assigned to command a base. (Joint Pub 1-02)

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

base defense forces.** Troops assigned or attached to a base for the primary purpose of base defense and security, and augmentees and selectively armed personnel available to the base commander for base defense from units performing primary missions other than base defense.

base defense operations center.** A command and control facility established by the base commander to serve as the focal point for base security and defense. It plans, directs, integrates, coordinates, and controls all base defense efforts, and coordinates and integrates into area security operations with the rear area operations center/rear tactical operations center.

base defense zone.** An air defense zone established around an air base and limited to the engagement envelope of short-range air defense weapons systems defending that base. Base defense zones have specific entry, exit, and identification, friend or foe procedures established. Also called BDZ.

civil affairs. The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. (Joint Pub 1-02)

coastal sea control. The employment of forces to ensure the unimpeded use of an offshore coastal area by friendly forces and, as appropriate, to deny the use of the area to enemy forces. (Joint Pub 1-02.)

host nation support. Civil and/or military assistance rendered by a nation to foreign forces within its territory during peacetime, times of crisis/emergencies, or war based upon agreements mutually concluded between nations. (Joint Pub 1-02)

joint base. For purposes of base defense operations, 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. (Joint Pub 1-02)

joint rear area. A specific land area within a joint force commander's area of operations designated to facilitate protection and operation of installations and forces supporting the joint force. (Joint Pub 1-02)

joint rear area coordinator. The officer with responsibility for coordinating the overall security of the joint rear area in accordance with joint force commander directives and priorities in order to assist in providing a secure environment to facilitate sustainment, host nation support, infrastructure development, and movements of the joint force. The joint rear area coordinator also coordinates intelligence support and ensures that area management is practiced with due consideration for security requirements. Also called JRAC. (Joint Pub 1-02)

joint rear area operations. Those operations in the unified and joint rear area that facilitate protection or support of the joint force. (Joint Pub 1-02)

joint rear tactical operations center. A joint operations cell tailored to assist the joint rear area coordinator in meeting mission responsibilities. Also called JRTOC. (Joint Pub 1-02)

naval coastal warfare commander. An officer designated to conduct naval coastal warfare missions within a designated naval coastal geographic area. Also called NCWC. (Joint Pub 1-02)

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

rear area operations center/rear tactical operations center.** A command and control facility that serves as an

area/subarea commander's planning, coordinating, monitoring, advising, and directing agency for area security operations.

response force.** A mobile force with appropriate fire support designated, usually by the area commander, to deal with Level II threats in the rear area.

short range air defense engagement zone. See weapon engagement zone. (Joint Pub 1-02)

status of forces agreement. An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. To the extent that agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements. (This definition is provided for information and is proposed for inclusion into Joint Pub 1-02 by Joint Pub 3-52 (Test Pub)).

tactical area of responsibility. A defined area of land for which responsibility is specifically assigned to the commander of the area as a measure for control of assigned forces and coordination of support. Commonly referred to as TAOR. (Joint Pub 1-02).

tactical combat force.** A combat unit, with appropriate combat support and combat service assets, that is assigned the mission of defeating Level III threats.

weapon engagement zone. In air defense, airspace of defined dimensions within which the responsibility for engagement normally rests with a particular weapon system.

a. fighter engagement zone. Fighter engagement zones will be established in those areas where no effective friendly or enemy surface-to-air capability is deployed. Also called FEZ.

b. high altitude missile engagement zone. Normally applied to long-range surface-to-air missiles, a high altitude missile engagement zone will limit the volume of airspace within which these weapons may conduct

engagements without specific direction of the area air defense commander. Also called HIMEZ.

c. low altitude missile engagement zone. Volume of airspace established for control of low- to medium-altitude surface-to-air missile engagements. A low altitude missile engagement zone will limit the volume of airspace within which these weapons may conduct engagements without specific direction of the area air defense commander Subject to weapon system capabilities, the low altitude missile engagement zone will normally extend beyond the forward edge of the battle area. Also called LOMEZ.

d. short range air defense engagement zone. Areas of short range air defense (SHORAD) deployment may fall within a low altitude engagement zone or high altitude engagement zone. Some areas might be solely defended by SHORAD assets. A SHORAD engagement zone can be established to define the airspace within which these assets will operate. Because centralized control over the SHORAD weapons may not be possible, these areas must be clearly defined and disseminated so friendly aircraft can avoid them. Also called SHORADEZ. (This definition is provided for information and is proposed for inclusion into Joint Pub 1-02 by Joint Pub 3-52 (Test Pub)).

** Upon approval of this publication, this term and definition will be included in Joint Pub 1-02.