

Joint Publication 3-10



Joint Security Operations in Theater



13 November 2014



PREFACE

1. Scope

This publication provides doctrine for the planning and execution of joint security operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for interagency coordination and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations, education, and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, sub-unified commands, joint task forces, subordinate components of these commands, the Services, and combat support agencies.

b. The guidance in this publication is authoritative; as such, this doctrine will 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 unless the CJCS, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:



DAVID L. GOLDFEIN, Lt Gen, USAF
Director, Joint Staff

Intentionally Blank

**SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-10
DATED 3 FEBRUARY 2010**

- **Revised the discussion on levels of threat to include insider threats.**
- **Added discussions on force protection detachments, cyberspace and information security, air-land interface, personnel recovery, private security contractors, security managers, protection of classified materials.**
- **Added discussion on location and marking of medical facilities in accordance with (IAW) the Geneva Conventions.**
- **Updated figures in Chapter II, “Fundamentals, Relationships, and Duties,” on command and coordinating relationship to better align with the text.**
- **Added a discussion of identity intelligence as it relates to enemy capabilities and security access.**
- **Revised counterintelligence planning consideration sections to clarify mission and to include insider threats.**
- **Revised the discussion on the treatment of detainees IAW United States laws and policy.**
- **Revised the discussion of Department of Defense civilian and contractor employees.**
- **Combined Chapters IV and V to reduce redundancy.**
- **Revised the discussion on nonlethal weapons.**
- **Revised the discussion on insider threats as it relates to working with host-nation security forces.**
- **Revised the discussion of air base defense considerations, aircraft vulnerabilities, and man-portable air-defense systems.**
- **Added Appendix C, “Integration of Protection and Security in Theater.”**
- **Eliminated outdated terms and definitions, including base commander, base defense forces, joint electromagnetic spectrum management program, rear-area operations center/rear tactical operations center, and response force.**
- **Modified and updated the following terms and definitions: base defense operations center, mobile security force, and tactical combat force.**
- **Updated references and eliminated redundancies.**

Intentionally Blank

TABLE OF CONTENTS

| | PAGE |
|--|--------|
| EXECUTIVE SUMMARY | vii |
| CHAPTER I | |
| OVERVIEW | |
| • Introduction | I-1 |
| • Joint Security Environment | I-1 |
| • Joint Security Framework | I-4 |
| • Base Functions and Nodes | I-6 |
| CHAPTER II | |
| FUNDAMENTALS, RELATIONSHIPS, AND DUTIES | |
| • Introduction | II-1 |
| • Joint Security Operations Command and Control | II-1 |
| • Roles and Responsibilities | II-3 |
| • Establishment of Base and Base Cluster Command Relationships | II-11 |
| • Operations Centers | II-12 |
| CHAPTER III | |
| PLANNING | |
| • Introduction | III-1 |
| • The Fundamentals of Planning Joint Security Operations | III-1 |
| • Joint Security Operations Planning Overview | III-3 |
| • Major Planning Considerations | III-7 |
| • Other Planning Considerations | III-21 |
| CHAPTER IV | |
| JOINT SECURITY OF BASES AND LINES OF COMMUNICATIONS | |
| • Introduction | IV-1 |
| • Tenets for Joint Security Operations | IV-1 |
| • Base and Base Cluster Operations Overview | IV-1 |
| • Base Security in Level I and Level II Threat Environments | IV-4 |
| • Countering Level III Threats | IV-13 |
| • Air Base Defense Considerations | IV-17 |
| • Seaport Facility Defense Considerations | IV-20 |
| • Lines of Communications Considerations | IV-20 |
| APPENDIX | |
| A Joint Security Operations Centers | A-1 |
| B Sample Base Defense Plan | B-1 |
| C Integration of Protection and Security in Theater | C-1 |

Table of Contents

D References D-1
E Administrative Instructions E-1

GLOSSARY

Part I Abbreviations and Acronyms GL-1
Part II Terms and Definitions GL-4

FIGURE

I-1 Levels of Threat I-3
I-2 Notional Structure for Joint Security Areas I-5
I-3 Key Joint Security Area Related Functions/Nodes I-6
II-1 Joint Security Coordinator Relationships II-6
II-2 Army Component Designated as the Joint Security Coordinator II-7
II-3 Tenant Unit Commanders' Responsibilities II-11
III-1 Fundamentals of Joint Security Operations Planning III-1
III-2 Levels of Threat Troop Capability Requirements III-6
III-3 Positioning Considerations III-19
III-4 Objectives of Civil-Military Operations in Joint Security Operations.. III-26
III-5 Base Security Considerations: Use of Non-United States
Contractor Personnel III-28
IV-1 Tenets for Successful Joint Security Operations IV-2
IV-2 Base Boundary Considerations IV-3
IV-3 Base Security Work Priorities IV-4
IV-4 Fundamentals of Lines of Communications Security IV-21
IV-5 Joint Line of Communications Security Board IV-22

EXECUTIVE SUMMARY COMMANDER'S OVERVIEW

- **Provides guidelines to plan and execute operations to protect a joint security area outside the continental United States.**
- **Discusses the joint security environment.**
- **Describes levels of threat, to include insider threats.**
- **Outlines the joint security framework, with a discussion of base functions and nodes.**
- **Provides the fundamentals of planning joint security operations.**
- **Provides an overview of base and base cluster operations.**
- **Discusses security considerations in Level I and II threats and for countering Level III threats.**
- **Explains line of communications (LOC) security operations and the integration of LOC security actions with joint movement control operations.**

Overview

Base and line of communications (LOC) security must be properly planned and executed to prevent or mitigate hostile actions against US personnel, resources, facilities, equipment, and information.

Joint security operations (JSO) provide for the defense of, and facilitate force protection (FP) actions for, designated bases, base clusters, lines of communications (LOCs), and other designated areas. They provide for unity of effort and efficient use of limited resources to maintain a relatively secure environment allowing the joint force commander (JFC) and component commanders to focus on their primary mission. JSO may include the participation of host nation (HN) forces, to include various police or security forces.

Joint Security Environment

Joint security areas (JSAs) may be small or may span national boundaries, each with a distinct security environment and different policies and resources to address threats. They will normally contain units, surface LOCs, and facilities from all elements of the joint force, supporting commands, other US Government departments and agencies,

intergovernmental organizations (IGOs), nongovernmental organizations (NGOs), as well as important HN infrastructure. JSAs may contain the units and facilities of one or more multinational partners organized into bases and base clusters to enhance their effectiveness and security. Vital sea and air LOCs, through which the bulk of logistic support flows, have their greatest vulnerability where they converge, often times at the aerial ports of debarkation or seaports of debarkation.

Levels of Threat

There are three levels of threat. Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, assassination, and subversion. These include a potential for insider attacks by elements or individuals of HN partners and security forces, often characterized as green-on-blue. Level II threats include small-scale forces conducting irregular warfare that can pose serious threats to military forces and civilians. Attacks by Level II threats can cause significant disruptions to military operations and the orderly conduct of local government and services. Level III threats may be encountered when a threat force has the capability of projecting combat power by air, land, sea, or anywhere into the operational area (OA).

Security Forces

Various types of security forces will be assigned to secure the JSA and LOCs. These will include dedicated and cluster base forces, LOC security forces, mobile security forces (MSFs), and tactical combat forces (TCFs).

Joint Security Framework

A JSA is a specific surface area designated by the JFC to facilitate protection of joint bases and their connecting LOCs that support joint operations. Regional political considerations and sensitivities will influence whether a JSA is established. The JSA may be used in both linear and nonlinear operations.

Base Functions and Nodes

Base functions include joint force projection, movement control, sustainment, and command and control (C2). Base nodes include air bases, airfields, forward arming, refueling points, sea ports, and sea bases.

Fundamentals, Relationships, and Duties

Joint Security Operations (JSO) Command and Control (C2) The JFC will normally designate JSAs to provide the security of base, base clusters, and LOCs. The JFC establishes C2 relationships within the OA, but may delegate certain authority to subordinate commanders in order to facilitate effective C2 and decentralized execution of security operations.

Roles and Responsibilities

Geographic combatant commanders (GCCs) establish area of responsibility (AOR)-wide FP measures, procedures, and policies for joint forces, family members, Department of Defense (DOD) civilian work force, and designated government contractor employees who are assigned, attached, in-transit, or otherwise physically located within their AORs. In addition, the GCCs may be tasked to provide support for interagency, IGO, NGO, and HN activities to enhance security for US forces, US citizens, and HN citizens. These responsibilities include protecting the command and protecting bases, LOCs, and critical HN infrastructure against attack during ongoing military operations. GCCs must ensure that subordinate staffs and/or commands are formally delegated the authority to conduct JSO.

Elements of functional combatant commands (FCCs) providing support to the OA, such as United States Transportation Command and United States Special Operations Command may establish facilities or occupy bases within the OA. The FCC coordinates with the applicable GCC and/or subordinate JFC to ensure that these facilities or bases are adequately secured.

Subordinate JFCs provide security of all military bases and LOCs within their joint operations area.

The JFC dedicates assets for JSO in proportion to the severity of the threat to conserve resources and prevent degradation of support. This function is normally vested in the JFC's staff or with a component commander with the capability to perform the function. **In high-threat environments, the JFC normally designates a joint security coordinator (JSC) to provide a dedicated focus on JSO within the JSAs.**

Component commanders with area responsibilities provide for the defense of their areas of operations (AOs), the overall defense of bases located in their AOs, and for LOCs within their AOs.

When an AO is not established, commanders must provide for the defense of those bases critical to their component responsibilities.

Service component commanders with area responsibilities establish base and base clusters within their AOs and delegate the authority to provide security to those subordinate commanders.

The JFC may designate a senior base commander as a base cluster commander. A base cluster is a collection of bases, geographically grouped for mutual protection and ease of C2. The base cluster commander coordinates the defense of bases within the base cluster and integrates defense plans of bases into a base cluster defense plan.

The JFC normally designates the commander of the primary activity of a base as the base commander. The base commander is responsible for all base security operations within the base boundary and will closely coordinate operations with all occupants.

Tenant unit commanders are commanders of units that reside and operate on, but do not fall under, the direct command of the base commander. Tenant unit commanders must actively participate in the preparation of base security and defense plans.

In operations where there is the possibility of a Level III threat, the JFC may elect to establish a dedicated joint security combat force called a TCF. The command relationships between the TCF and subordinate commanders will be determined by the JFC.

Planning

The Fundamentals of Planning JSO

The fundamentals of JSO planning are:

- Establish Clear Joint Security Related C2 Relationships.

- Establish Joint Security Related Responsibilities.
- Understand the Enemy.
- Understand the Operational Environment.
- Use the Defenders' Advantages.
- Mitigate Defenders' Disadvantages.
- Balance Security Actions with Civil and Political Considerations.

Major Planning Considerations

- **FP.** Antiterrorism measures will be a large part of the base security plan and consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces.
- **Intelligence.** The JSC coordinates the intelligence and counterintelligence requirements of organizations with JSO responsibilities with the intelligence directorate of a joint staff.
- **Communications.** The JSC must have an interoperable, secure, reliable, flexible, and survivable communications network to accomplish the mission.
- **Cyberspace and Information Security.** JFCs should establish an integrated, multidisciplinary security program that implements information, personnel, contracted services, physical security operations, and cyber security considerations in the JSA.
- **Chemical, Biological, Radiological, and Nuclear (CBRN) Defense.** Many adversaries can employ CBRN weapons to attack bases, other critical facilities, and LOCs. All US forces in the OA should prepare to plan and execute CBRN defense operations.
- **Air and Missile Defense.** Since most units operating on base and surface LOCs in the OA

have limited capability to engage and destroy incoming enemy air and missile threats, commanders must be aware of the capabilities and limitations of joint force defensive counterair operations for their areas. The JSC's focus is protection for the JSAs. Dependent upon the size and scope of the JFC's mission, the joint force may establish an integrated air defense system to conduct defensive counterair operations.

- **Threat Early Warning and Alert Notification System.** Threat early warning is essential to the protection of joint forces operating throughout the OA and should be linked through the JSC and the joint security coordination center (if established) down through designated base cluster operations center and base defense operations center.
- **Land Force Component and Joint Security.** Joint security on the land includes bases, mission-essential assets, LOCs, and convoy security.
- **Maritime-Land Interface.** Bases established on a shoreline can present special advantages and challenges to those responsible for the functions inherent in the base's mission and for its defense. Challenges may include ports and harbors usually located in heavily populated areas.
- **Air-Land Interface.** The threats to an active airfield may extend far beyond the surface area designated as a base boundary. To address these threats, the air component uses the planning construct of the base security zone to ensure that those ground threats and hazards that could impact operations are considered and planned for accordingly.
- **Terrain Management and Infrastructure Development.** Infrastructure development focuses on facility security modification and damage repair in order to reduce the efforts that joint forces must make to heighten their base

and LOC security posture. Additionally, use of HN manpower, medical support, equipment, and materiel should be maximized.

- **Area damage control (ADC).** ADC includes the measures taken before, during, and after hostile action or natural or manmade 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 combat support units, logistic units, tenant units, transient units, and HN units.
- **Integration of Joint Security and Logistic Operations.** Joint logistics integrates strategic, operational, and tactical level logistic operations. JSO are built on movement control, open LOCs, secure reception points, transshipment points, logistic bases, and obtaining host-nation support.
- **Detainee Operations.** Commanders at all levels must plan for and anticipate the capture of detainees. Commanders must ensure that all detainees are treated humanely and in accordance with US law, the law of war, and applicable US policy.
- **Personnel Recovery (PR).** When JFCs and their staffs conduct mission analysis, PR should be considered as one of the means to mitigate risks. When the chief of mission (COM) is responsible, PR will have to be planned and executed within HN sovereignty and COM authorities.

Other Planning Considerations

The JSC coordinates the security of bases and LOCs through the integration and synchronization of host-nation support, multinational operations, civil-military operations, and interagency coordination. The JSC also considers the role of the DOD civilian work force and contractor employees, laws, agreements, and other legal constraints.

Joint Security of Bases and Lines of Communications

Tenets for JSO

The tenets for JSO include knowledge of the enemy, unity of command, economy of force, and responsiveness.

Base and Base Cluster Operations

A base is a locality from which operations are projected or supported. At the base level, the component in command of the base has overall responsibility for the security of everything within the base boundary. Tenant units normally secure their own facilities within the base, but also provide select forces for base defense. The base commander normally exercises tactical control (TACON) over those forces.

A base cluster is a collection of bases, geographically grouped for mutual protection and ease of C2. The base cluster commander will be appointed by the JFC or designated representative and may be the next higher tactical C2 headquarters of the base, the senior base commander, or another designated base commander, depending on the situation.

A base security force is a security element established to provide local security to a base. It normally consists of the combined dedicated and on-call forces assigned or attached and those forces from tenant units attached with specification of TACON for base defense or security operations.

C2 Considerations

The area commander, normally a combat arms land force commander, is responsible to provide security support to all bases and base clusters (if designated) within the command's AO. This responsibility will often include bases that are commanded by organizations not part of the area commander's forces. The base cluster commander has direct responsibility for area security within the assigned cluster.

Base Security in Level I and Level II Threat Environments

Successful security depends on an integrated and aggressive plan consisting of on-call base security, dedicated security forces, base or base cluster MSFs, and ADC response services (medical, firefighting, and engineer). Actions against enemy threats and other potential emergencies, to include natural disasters and accidents, must be planned for and adjustments to base or base cluster security plans made. Drawing from the

units available, commanders organize security forces within their bases and base clusters. The base commander integrates the base security plans with those of the base cluster.

Countering Level III Threats

Enemy forces infiltrating or penetrating friendly positions and moving into the friendly OA, or conducting airborne, air assault, or amphibious operations, are some sources of Level III threats. The designated land force commander may establish a TCF to deal with these types of threats, designate another force as the on-order TCF, or accept the risk of not designating a TCF.

The area commander decides the composition of the TCF after weighing the risk of allocating forces to the TCF and thus decreasing the combat power available elsewhere. In large JSAs with dispersed bases and base clusters, the TCF must be capable of moving by air and ground to speed reaction time. A TCF typically consists of infantry, Army or Marine Corps aviation (attack and utility helicopters), augmented with combat engineer and field artillery support.

During Level III operations, the area commander retains overall C2 for security within the JSA. However, in coordination with the base or base cluster commander, the area commander may delegate TACON over selected security forces located in the OA to the TCF commander, excluding air defense forces, which remain under the joint force air component commander or area air defense commander.

Air Base Defense Considerations

Base commanders of any Service who command installations with active airfields must identify threat systems and plan and secure air operations. This should include approach and departure corridors used by the aircraft as well as dispersal plans while on the ground. Base, base cluster, and area commanders must be aware of the nature of these threats and share the responsibility to counter them.

Seaport Facility Defense Considerations

When a seaport or marine terminal is part of a designated base cluster, the base commander will normally be responsible for security within the base boundaries with HN, Army, or Marine Corps forces responsible for shore boundary defense, and Navy and

US Coast Guard forces providing waterside harbor approach security.

LOC Considerations

The greatest risk to joint force operations can be threats to main supply routes from the ports of debarkation forward to the main battle area (in linear operations) or forward operating bases (in nonlinear, noncontiguous operations). Fundamentals of LOC security include:

- LOC security is an operation, not a logistic function.
- LOC security in Level II and III threat conditions will require dedicated security force capabilities.
- LOC security action must be closely synchronized with joint movement control operations.

CONCLUSION

This publication provides doctrine for planning and execution of joint security operations. It outlines the JFC's responsibilities and discusses command and control considerations in various threat environments. It focuses on planning considerations that are designed to secure bases and LOCs in support of joint operations.

CHAPTER I OVERVIEW

“The protection function encompasses a number of tasks, including . . . securing and protecting forces, bases, JSAs [joint security areas], and LOCs [lines of communications].”

Joint Publication 3-0, *Joint Operations*

1. Introduction

a. Deployed military units, forward-based activities, and forward operating bases (FOBs) support the National Security Strategy, National Defense Strategy, and National Military Strategy. These units, activities, and bases protect themselves against threats designed to interrupt, interfere, or impair the effectiveness of joint operations. Base and line of communications (LOC) security must be properly planned and executed to prevent or mitigate hostile actions against US personnel, resources, facilities, equipment, and information.

b. This publication provides **guidelines to plan and execute operations to protect a joint security area (JSA) outside the continental United States. Within this publication, these operations are referred to as joint security operations (JSO).** JSO provide for the defense of, and facilitate force protection (FP) actions for, designated bases, base clusters, LOCs, and other designated areas. They provide for unity of effort and efficient use of limited resources to maintain a relatively secure environment allowing the joint force commander (JFC) and component commanders to focus on their primary mission. JSO may include the participation of host nation (HN) forces, to include various police or security forces. The JFC should establish the operational framework that best addresses the operational environment while providing for maximum flexibility. **The designation of a JSA is normally based on the nature of the threat, type and scope of the mission, and the size of the operational area (OA).**

c. This publication also outlines joint security coordinator (JSC) responsibilities and discusses joint security organizational options and command and control (C2) considerations.

2. Joint Security Environment

a. **General.** A geographic combatant commander (GCC) or a subordinate JFC must be prepared to protect bases, base clusters, airfields, seaports, and LOCs within the OA. Commanders should take a holistic approach to JSO and plan to counter threats through a combination of combat power, antiterrorism (AT), FP, law enforcement, counterintelligence (CI), information security, personnel security, industrial security, operations security (OPSEC), emergency management, and response. This creates an integrated, multidisciplinary all-hazards approach to risk management and supports mission accomplishment. Enemy forces with sophisticated surveillance devices, accurate weapon

systems, and transport assets capable of inserting forces behind friendly combat formations make JSAs increasingly vulnerable. When JSAs are noncontiguous, enemy forces may operate within the OAs of friendly forces. **Standoff weapon threats in the form of improvised explosive devices (IEDs), artillery, mortars, rockets, missiles, unmanned aircraft systems (UASs), and surface-to-air missiles (SAMs) are of particular concern.**

b. **Description.** JSAs may be small or may span national boundaries, each with a distinct security environment and different policies and resources to address threats. They will normally contain units, surface LOCs, and facilities from all elements of the joint force, supporting commands, other United States Government (USG) departments and agencies, intergovernmental organizations (IGOs), nongovernmental organizations (NGOs), as well as important HN infrastructure. JSAs may contain the units and facilities of one or more multinational partners organized into bases and base clusters to enhance their effectiveness and security. Vital sea and air LOCs, through which the bulk of logistic support flows, have their greatest vulnerability where they converge, often times at the aerial ports of debarkation (APODs) or seaports of debarkation (SPODs).

c. **Levels of Threat. There are three levels of threat.** These different levels provide a general description and categorization of threat activities, identify recommended security responses to counter them, and establish a common reference for planning. Figure I-1 lists examples of each of these levels of threat. Each level or any combination of levels may exist in the OA independently or simultaneously. Emphasis on specific base or LOC security measures may depend on the anticipated level of threat. This does not imply that threat activities will occur in a specific sequence or that there is a necessary interrelationship between each level. **Commanders and staff should go beyond size and type of units when determining and describing levels of threat. Threat levels should be based on the activity, capability, and intent of enemy agents or forces. They can be further described by looking at mission impact.** Where a Level I threat may require only a routine response by base security forces and have negligible impact on the mission, a Level III threat could cause mission failure and requires a significant combat force response. While the doctrinal principles and guidelines provided herein are applicable to all threats, their **primary focus is on Level I and II threats.**

(1) **Level I Threats.** Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, assassination, and subversion. These include a potential for insider attacks by elements or individuals of HN partners and security forces, often characterized as green-on-blue. Conducting these attacks or assisting the insurgency falls into four broad categories: co-option, infiltration, impersonation, and personal grievances. Co-option occurs when an existing HN security force member is recruited by various pressures, incentives, or other coercive means. Infiltration transpires when an insurgent joins HN security forces through standard recruitment and is positioned to act immediately or as a sleeper agent. Impersonation occurs when an insurgent or insurgents pose as HN security forces to gain access to restricted areas or to get close enough to a target. Personal grievances, or cultural friction, can lead to attacks by a HN security force member due to a disagreement, actual or perceived personal affront, or frustration. These four types of insider threats are not limited to HN security forces and may also occur with other HN or third country national (TCN) personnel. Activities include individual terrorist attacks,

| Levels of Threat | |
|------------------|--|
| Threat Level | Examples |
| Level I | Agents, saboteurs, sympathizers, terrorists, civil disturbances |
| Level II | Small tactical units; irregular forces may include significant stand-off weapons threats |
| Level III | Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations |

Figure I-1. Levels of Threat

random or directed killing of military and civilian personnel, kidnapping, and/or guiding special-purpose individuals or teams to targets. Level I threat tactics may include hijacking air, land, and sea vehicles for use in direct attacks; the use of improvised weapons (e.g., vehicle-borne IEDs, suicide bombers, roadside bombs), sniping, man-portable air defense systems (MANPADSs), and individual grenade and rocket-propelled grenade attacks. Civilians sympathetic to the enemy may become significant threats to US and multinational operations. They may be the most difficult to counter because they are not normally part of an established enemy agent network and their actions may be random and unpredictable. Countering criminal activities and civil disturbances requires approaches that differ from those used to counter conventional forces. These approaches normally require detailed coordination and training with HN military, security, and police forces. Significant portions of the local population may believe that these activities can disrupt friendly operations. **Countering Level I threats should be part of the day-to-day FP measures implemented by all commanders.** Intelligence support and identifying portions of the local population sympathetic to US or multinational goals is key to countering these threats.

(2) **Level II Threats. Level II threats include small-scale forces conducting irregular warfare that can pose serious threats to military forces and civilians.** Attacks by Level II threats can cause significant disruptions to military operations and the orderly conduct of local government and services. Forces constituting Level II threats are capable of conducting well-coordinated, but small-scale, hit-and-run attacks; improvised weapons attacks with roadside or vehicle-borne IEDs; raids; and ambushes. These forces may employ significant standoff weapons threats such as mortars, rockets, rocket-propelled grenades, and MANPADSs. In addition, Level II threats may include special operations forces that are highly trained in irregular warfare as well as operations typically associated with terrorist attacks. These forces establish and activate espionage networks, collect intelligence, carry out specific sabotage missions, develop target lists, and conduct damage assessments of

targets struck. If the JFC assigns a base boundary to an installation, sufficient joint forces should be tasked to defeat enemy Level II forces.

For more information on counter-IED operations and improvised weapons, refer to Joint Publication (JP) 3-15.1, Counter-Improvised Explosive Device Operations, and the Weapons Technical Intelligence Handbook.

(3) **Level III Threats.** Level III threats may be encountered when a threat force has the capability of projecting combat power by air, land, sea, or anywhere into the OA. Specific examples include airborne, heliborne, and amphibious operations; large combined arms ground force operations; and infiltration operations involving large numbers of individuals or small groups infiltrated into the OA, regrouped at predetermined times and locations, and committed against priority targets. Air and missile threats to bases, base clusters, and LOCs also present imminent threats to joint forces. **Level III threats are beyond the capability of base and base cluster security forces, and can only be effectively countered by a tactical combat force (TCF) or other significant forces.**

(4) **Chemical, Biological, Radiological, and Nuclear (CBRN) Threats.** Commanders and JSCs must be aware that CBRN weapons may be used at any level of threat by terrorists or irregular forces alone or in combination with conventional forces in order to achieve their political or military objectives.

For additional information on CBRN defense considerations, see JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear Environments.

d. **Security Forces.** Various types of security forces will be assigned to secure the JSA and LOCs. These will include dedicated and cluster base forces, LOC security forces, mobile security forces (MSFs), and TCFs. **An MSF is a highly mobile, dedicated security force with the capability to defeat Level I and II threats within a JSA. A TCF is a rapidly deployable, air-ground mobile combat unit capable of defeating Level III threats, to include enemy combined arms. TCFs include combat support and combat service support elements.** Specialized forces may also be employed at air and sea bases as well as in air and missile defense. All of these types of forces, including the MSF and TCF, will be described further in Chapter III, “Planning,” and Chapter IV, “Joint Security of Bases and Lines of Communications.”

3. Joint Security Framework

a. A JSA is a specific surface area designated by the JFC to facilitate protection of joint bases and their connecting LOCs that support joint operations. Regional political considerations and sensitivities will influence whether a JSA is established. The JSA may be used in both linear and nonlinear operations. Figure I-2 depicts a notional structure for JSAs in which all bases are located in a land component commander’s area of operations (AO).

b. Joint planners should be aware that bases, base clusters, and FOBs may be referred to in higher level guidance as contingency locations or contingency bases.

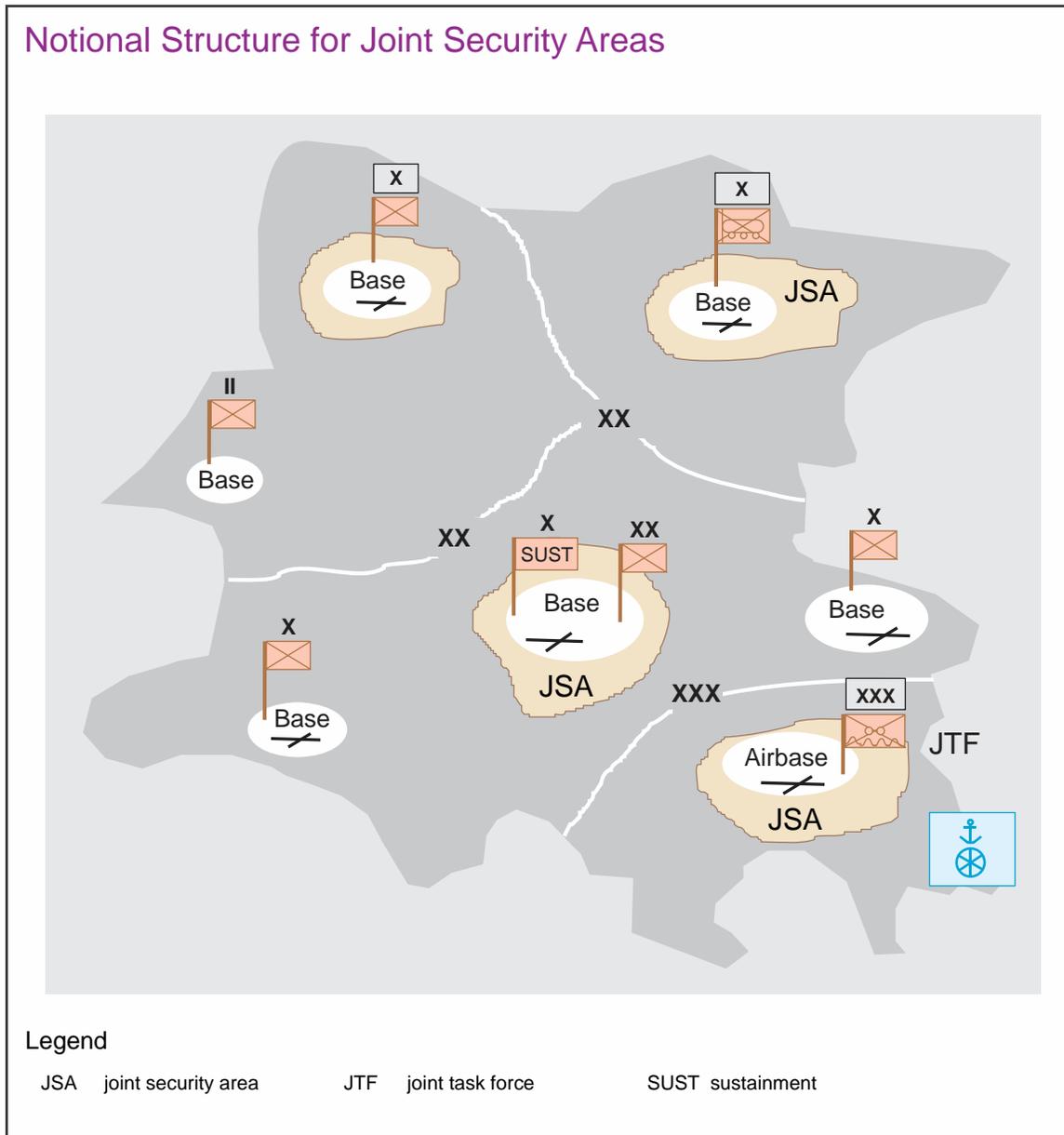


Figure I-2. Notional Structure for Joint Security Areas

For more information on contingency locations and base classification, see Department of Defense Directive (DODD) 3000.10, Contingency Basing Outside the United States.

c. The size of a JSA may vary considerably and is highly dependent on the size of the OA, mission essential assets, logistic support requirements, threat, or scope of the joint operation. In linear operations the JSA may be included in, be separate from, or adjoin the rear areas of the joint force land component commander (JFLCC), joint force maritime component commander (JFMCC), or Service component commanders.

d. **JSA**s may be designated where joint forces are engaged in combat operations or where stability operations are the primary focus. Providing security of units,

activities, bases/base clusters, and LOCs located in noncontiguous areas presents unique challenges based on the location, distance between supporting bases, and the security environment.

e. JSAs may be established in different countries in the GCC’s area of responsibility (AOR). The airspace above the JSA is normally not included in the JSA. This airspace is normally governed by procedures promulgated in JP 3-52, *Joint Airspace Control*. The JSA will typically evolve as the OA changes in accordance with (IAW) requirements to support and defend the joint force. An amphibious objective area may precede a JSA when establishing a lodgment. A lodgment would normally be expanded to an area including existing ports and airfields from which operations could be conducted, and then eventually evolve to areas including multiple countries and sea bases.

4. Base Functions and Nodes

Base functions and nodes include, but are not limited to, the items shown in Figure I-3 and described in the following subparagraphs.

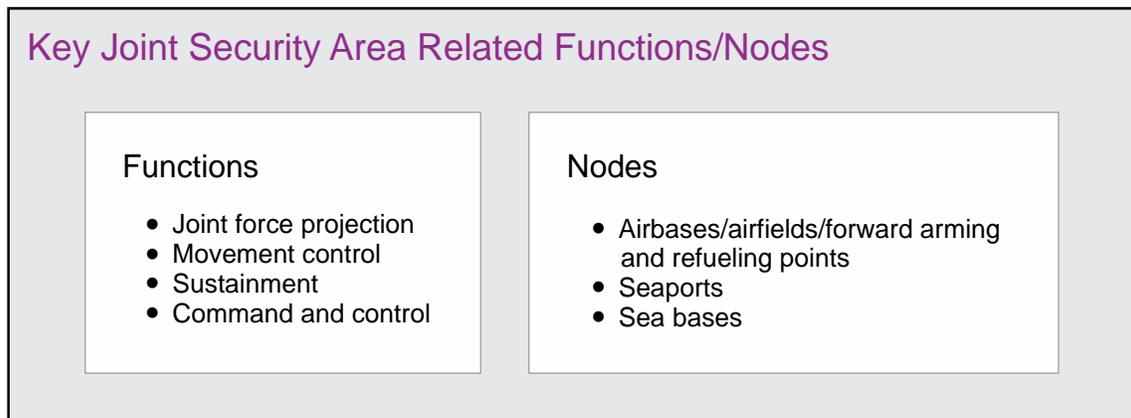


Figure I-3. Key Joint Security Area Related Functions/Nodes

a. **Joint Force Projection.** Joint force projection is the ability to project the military instrument of national power from the US or another theater, in response to requirements for military operations. It allows the JFC to concentrate forces and materiel for mission success. Force projection, enabled by global force management, forward presence, and agile force mobility, is critical to US deterrence and warfighting capabilities. The President or the Secretary of Defense (SecDef) could direct GCCs to resolve a crisis by employing immediately available forces. However, when this response is not sufficient or possible, the rapid deployment of forces from other locations may be necessary. **Force projection involves the mobilization, deployment, employment, sustainment, and redeployment of the joint force.** A secure area is vital for reception of personnel, materiel, and equipment; assembling them into units at designated staging sites; moving newly assembled units to the OA; and integrating them into a mission-ready joint force.

For further information on force projection, see JP 3-35, Deployment and Redeployment Operations.

b. **Movement Control.** Movement control is the planning, routing, scheduling, and control of personnel and cargo movement over LOCs throughout the OA. It includes maintaining in-transit visibility of forces and materiel through the deployment and/or redeployment process. Freedom of movement is critical to the joint force. **Joint movement control must be closely coordinated with the JSO.** A JFC normally designates a joint movement center (JMC) to centralize transportation movement. The JMC controls intratheater force movement, coordinates strategic movements with United States Transportation Command (USTRANSCOM), and oversees the execution of transportation priorities. Rail terminals, SPODs, APODs, and other key transportation nodes may be located in a JSA.

For further information on movement control, see JP 4-09, Distribution Operations.

c. **Sustainment.** The primary mission of many of the forces in a JSA is to sustain joint force operations and forces throughout the OA. These forces may include any number and type of logistic units. They may include contractor provided supply, medical treatment facilities, and logistic capabilities. Medical treatment facilities should be located and marked IAW the provisions of the Geneva Conventions. Medical units must not be used in an attempt to shield military objectives from attack. Where possible, they should be positioned so that attacks against military objectives do not imperil their safety. While the Geneva Conventions prescribe the protections applicable to medical treatment facilities and their personnel, many adversaries such as insurgents and terrorists do not abide by these conventions. As such, commanders should evaluate the OA and balance the desire to separate these facilities with the need to provide security.

For further information on sustainment, see JP 4-0, Joint Logistics, as well as other applicable 4-Series JPs.

d. **C2.** Bases containing C2 capabilities such as major headquarters and signal centers are critical installations in a JSA. The loss of C2 capabilities will have a significant impact on operations.

e. **Air Bases, Airfields, Forward Arming, and Refueling Points.** Airfields are critical nodes, and are therefore lucrative targets. **Aircraft approach and departure corridors and the standoff weapons footprint immediately contiguous to air bases are elements of key terrain from which threats must be deterred and mitigated.**

f. **Seaports.** SPODs, seaports of embarkation, and joint logistics over-the-shore sites are key nodes often located on a vulnerable seam between the JFLCC's and JFMCC's OAs. Therefore, component or subordinate JFCs must ensure advance coordination for security operations planning that entails C2, communications, rules of engagement (ROE), coordination points, and responsibility for security along LOCs and employment of forces. The JFC and subordinate JFCs should clearly delineate port security requirements and assign responsibilities.

g. **Sea Bases.** The JFMCC normally uses the composite warfare commander for defense of seabasing operations with principal warfare commanders establishing preplanned

responses to defend the sea base, as well as sealift, airlift, and connector craft within the assigned OA. Proximity to the littorals, especially airfields, ports, and harbors, and the requirement to respond to threats along boundaries, will be of interest to the JSC and may require close coordination with maritime forces. The relationship between supported and supporting commanders, while similar to those described in Chapter II, “Fundamentals, Relationships, and Duties,” and Chapter IV, “Joint Security of Bases and Lines of Communications,” is complicated by the multiple tasks that may be assigned to the individual ships. Environmental factors and the possibility that the shipping will not remain static may complicate defensive planning.

CHAPTER II FUNDAMENTALS, RELATIONSHIPS, AND DUTIES

“Even in friendly territory a fortified camp should be set up; a general should never have to say: ‘I did not expect it.’”

**The Emperor Maurice
The Strategikon
c. 600 AD**

1. Introduction

Unity of command is fundamental to effective security within the JSA. The JFC designates OAs, selects appropriate command structures, and establishes a C2 network through multinational, subordinate, and adjacent commanders to direct and coordinate the actions of components and supporting organizations or agencies. **C2 authority and responsibilities must be established for the units and activities throughout the OA for the security of the bases and base clusters and their supporting LOCs.** Operations within the JSA will almost always involve interaction with a combination of HN forces, multinational forces (MNFs), contractor employees, US military personnel not assigned to the GCC, US country teams, IGOs, and NGOs. This chapter discusses JSO C2, roles and responsibilities, command relationships, and operations centers.

2. Joint Security Operations Command and Control

a. **The JFC will normally designate JSAs to provide the security of base, base clusters, and LOCs.** The JFC establishes C2 relationships within the OA, but may delegate certain authority to subordinate commanders in order to facilitate effective C2 and decentralized execution of security operations.

b. The JFC may retain control of JSO and may coordinate them through the operations directorate of a joint staff (J-3), or may designate a functional or Service component commander with joint security responsibilities. To facilitate JSO, **commanders should establish a joint security element to coordinate JSO.** The individual who normally leads a joint security element is referred to as the JSC.

c. **The JSC (or staff element) may establish a joint security coordination center (JSCC)** using elements from the JSC’s staff and representatives from all components operating in the OA to assist in meeting joint security requirements. Component and staff representation will vary IAW mission, forces, and security requirements.

See Appendix A, “Joint Security Operations Centers,” for more information on the functions and organization of the JSCC.

SEPTEMBER 2012 CAMP BASTION RAID IN AFGHANISTAN

The attack was described as “the worst loss of US airpower in a single incident since the Vietnam War.” The raid was a complex and coordinated assault by 19 Taliban fighters dressed in United States Army uniforms using several types of weapons, which took place on the eastern side of Camp Bastion near the United States Marine Corps (USMC) aircraft hangars at 22:00 local time. The assault team penetrated the perimeter of the camp, guarded by troops from Tonga, and separated into three teams to carry out the attack. One team engaged a group of USMC mechanics from VMM-161 who were in the area; the same team had attacked the aircraft refueling stations. Another group attacked the aircraft, and the last group was engaged at the base cryogenics compound. The group that attacked the aircraft attached explosive charges to several of the jets, and then fired rocket-propelled grenades (RPGs) at several others.

The attackers were defeated after a four-hour firefight by USMC personnel, civilian security contractors, and No. 51 Squadron RAF (Royal Air Force) Regiment, with helicopter support supplied by a British AH-64 Apache and USMC AH-1W Super Cobras and machine-gun equipped UH-1s, which took off while under fire from the insurgents. The RAF troops, who were located on the opposite side of the base, arrived at the scene approximately 12 minutes after the attack began. Contrary to many news and media reports, the initial reaction force was a group of former US Service-members who were operating under Department of Defense security forces at Camp Leatherneck as private contractors. They held the attack back long enough for heavier armed quick-reaction force and air-to-ground forces to arrive. The Taliban targeted Harriers, their biggest threat, as well as several small fuel and munitions holding areas near the flight-line. Civilian contractors (all prior-service combat veterans) were an integral part of the base defense and voluntarily responded despite being under-equipped compared to a standard infantryman. Civilian contractors who responded from the munitions supply area and from the main base area skirted the north end of the flight-line until contact with the enemy was made. They killed the first group of four insurgents, and suppressed another group of three armed with RPGs until a British AH-64 Apache used its main cannon to eliminate the threat. Marines from VMM-161 killed the second group of five Taliban with small arms fire as they tried to advance down the flight-line area. A third group of five insurgents was flushed out of hiding hours later and shot by USMC and civilian contractor forces in a compound near their entry point. The final group of five insurgents was detected near the flight-line hours later and four were killed by gunfire from hovering helicopters. The final individual insurgent was injured and captured.

Various Sources

d. Bases/base clusters will normally be established to support joint operations and be placed under the control of a base commander or base cluster commander. The base commander is responsible for security within the base boundary and has a direct interest in the security of the area surrounding the base. The area commander will normally establish base boundaries in coordination with (ICW) the base commander or base cluster commander. Base defense is accomplished in a coordinated effort by base security forces providing security within the base boundary and other ground or surface forces executing security tasks outside that boundary. **The base boundary, established based on mission, enemy, terrain and weather, troops and support available-time available, and civil considerations, extends beyond the base perimeter, and includes key terrain that must be secured through active control by security forces or coordination with HN forces.** Base boundaries may be dynamic, requiring ongoing coordination due to changing factors and HN limitations. **These factors are not limiting and other factors may be identified in establishing the base boundary.**

e. The JFC may task the land, air, or maritime component commander to provide TCFs to counter Level III threats. The JFC also assesses the availability and effectiveness of HN contributions to base security. Based on this assessment, the JFC may adjust the concept of operations, sequencing, and unit missions. Transportation nodes (ports, highway networks, waterways, airfields, and railroads), C2, intelligence capabilities, host-nation support (HNS), and civil considerations impact the JSA and operations.

f. **The base commander is responsible for security operations** and will normally exercise tactical control (TACON) over all forces performing base defense missions within the base boundary. This includes both isolated bases and bases with a contiguous joint force area commander. The base and base cluster commander coordinates such operations with the joint security element, HN security forces, or other agencies as appropriate.

3. Roles and Responsibilities

a. US Embassy Representatives

(1) **Chief of Mission (COM).** By statute, the COM directs, coordinates, and supervises all USG executive branch employees in that country (except those under the command of a GCC). Close coordination between each COM and country team in the GCC's AOR is essential in order to support US regional goals and objectives. Each COM has a formal agreement with the GCC to delineate which Department of Defense (DOD) personnel fall under the FP responsibility of each. GCC and COM security memorandums of agreement (MOAs) do not alter established command relationships, nor relieve commanders of responsibility for unit security. The GCC has responsibility for all DOD elements and personnel within that AOR, except those for whom security responsibility has been transferred to the COM via the MOA process.

(2) **Regional Security Officer (RSO).** The RSO is the COM's senior security officer and manages programs to ensure the security functions of all US embassies and consulates in a given country or group of adjacent countries. The RSO works closely with

the senior defense official (SDO)/defense attaché (DATT) to ensure the safety and security of DOD elements and personnel for whom the COM has security responsibility.

(3) **SDO/(DATT)**. The SDO/DATT is the senior US military officer in a foreign country representing SecDef, the Chairman of the Joint Chiefs of Staff, and the GCC. Specific SDO/DATT responsibilities for JSO include, but are not limited to, the following:

(a) Functions as the single point of contact for JSO for all DOD elements not assigned to the GCC that are the security responsibility of the COM.

(b) In designated countries, and IAW GCC/COM security MOAs, exercises FP responsibility for the in-country combatant command forces.

(c) Coordinates with JSC on JSO issues.

(d) Maintains authority over in-country military personnel not assigned to the GCC, in cases of emergency where US national/or DOD interests are involved, and the urgency of the situation precludes referral up the chain of command to the GCC.

(e) Initiates combined JSO planning, ICW the COM and RSO, with the HN and coordinates execution of these operations with the COM, GCC, through the JSC and ICW the JFC.

(f) Performs additional joint security responsibilities and duties as assigned by the GCC.

(4) **Force Protection Detachment (FPD)**. The FPD provides CI support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat. It functions as the DOD focal point for CI support to FP of in-transit DOD personnel and resources in countries where there is no permanent DOD CI presence. FPD members fall under the direction, coordination, and supervision of the COM except when they are under the GCC. The FPD keeps the SDO/DATT informed of its activities. The FPD coordinates those activities with the RSO and security elements of DOD in-transit forces to ensure safety of those for whom the GCC has security responsibility.

b. DOD

(1) **GCC**. The GCC is ultimately responsible for all military JSO conducted in the AOR. The GCC, through the JSCC or similar organization, coordinates JSO through the SDO/DATT with the COM as appropriate. **GCCs establish AOR-wide FP measures, procedures, and policies for joint forces, family members, DOD civilian workforce, and designated government contractor employees who are assigned, attached, in-transit, or otherwise physically located within their AORs.** In addition, the GCCs may be tasked to provide support for interagency, IGO, NGO, and HN activities to enhance security for US forces, US citizens, and HN citizens. These responsibilities include protecting the command and protecting bases, LOCs, and critical HN infrastructure against attack during ongoing military operations. GCCs must ensure that subordinate staffs and/or commands are formally delegated the authority to conduct JSO.

(2) **Functional Combatant Commanders (FCCs).** Elements of functional combatant commands providing support to the OA, such as USTRANSCOM and United States Special Operations Command, may establish facilities or occupy bases within the OA. **The FCC coordinates with the applicable GCC and/or subordinate JFC to ensure that these facilities or bases are adequately secured.** Command and coordination relationships between those elements and the area or base commanders subordinate to the JFC will be defined by orders or MOA. Coordination must include sharing of intelligence information, because supporting operations of FCCs are often planned outside the OA.

(3) **Subordinate JFC.** Subordinate JFCs include the commanders of subordinate unified commands and joint task forces. Subordinate JFCs have the authority to organize forces to best accomplish the assigned mission based on their concept of operations. Subordinate JFCs provide security of all military bases and LOCs within their joint operations area (JOA). The subordinate JFC conducts joint security planning, risk assessment, and force allocation; assigns AOs; and designates LOCs. They do this by either ensuring that the joint security coordination authority duties are clearly assigned to a formally designated JSC or by embedding the authority in the J-3 staff.

(4) **JSC.** The JSC is the officer with responsibility for coordinating the overall security of the OA IAW JFC directives and priorities. Establishing and maintaining JSO throughout the OA, although vital to the survivability and success of the joint force, **is an economy of force mission.** The JFC dedicates assets for JSO in proportion to the severity of the threat to conserve resources and prevent degradation of support. This function is normally vested in the JFC's staff or with a component commander with the capability to perform the function. In a low-threat environment, the JFC will normally designate JSC responsibilities within the joint staff (e.g., J-3). In this environment, the inherent defensive capabilities of bases, units, or HN forces are generally adequate to deter the threat. **In high-threat environments, the JFC normally designates a JSC to provide a dedicated focus on JSO within the JSA(s).** Under these circumstances, the JFC normally designates a component commander with the joint staff (e.g., J-3). In this environment, the inherent defensive capabilities of bases, units, or HN forces are generally adequate to deter the threat. **In high-threat environments, the JFC normally designates a JSC to provide a dedicated focus on JSO within the JSA(s).** Under these the JFC normally designates a component commander with the appropriate capabilities and force structure to perform this function. The JFC considers mission requirements, force capabilities, the nature of the operating environment, and the threat in making the designation. Figures II-1 and II-2 depict notional OA C2 networks, with options for the selection of the JSC.

(a) The JSC coordinates the overall security of the JSA(s) IAW JFC directives and priorities. The JSC coordinates with appropriate commanders on security issues to facilitate sustainment, HNS, and infrastructure development and protection, in addition to movements of the joint force. The JSC's overall coordination responsibility for security of the JSA(s) does not lessen the responsibility that component elements residing or operating in the OA have for their own security. The JSC also assists commanders in establishing reliable intelligence support and practicing terrain management within their OA with due consideration of security requirements. The JSC establishes secure and survivable communications with all forces and commands operating in or transiting the JSA(s). The

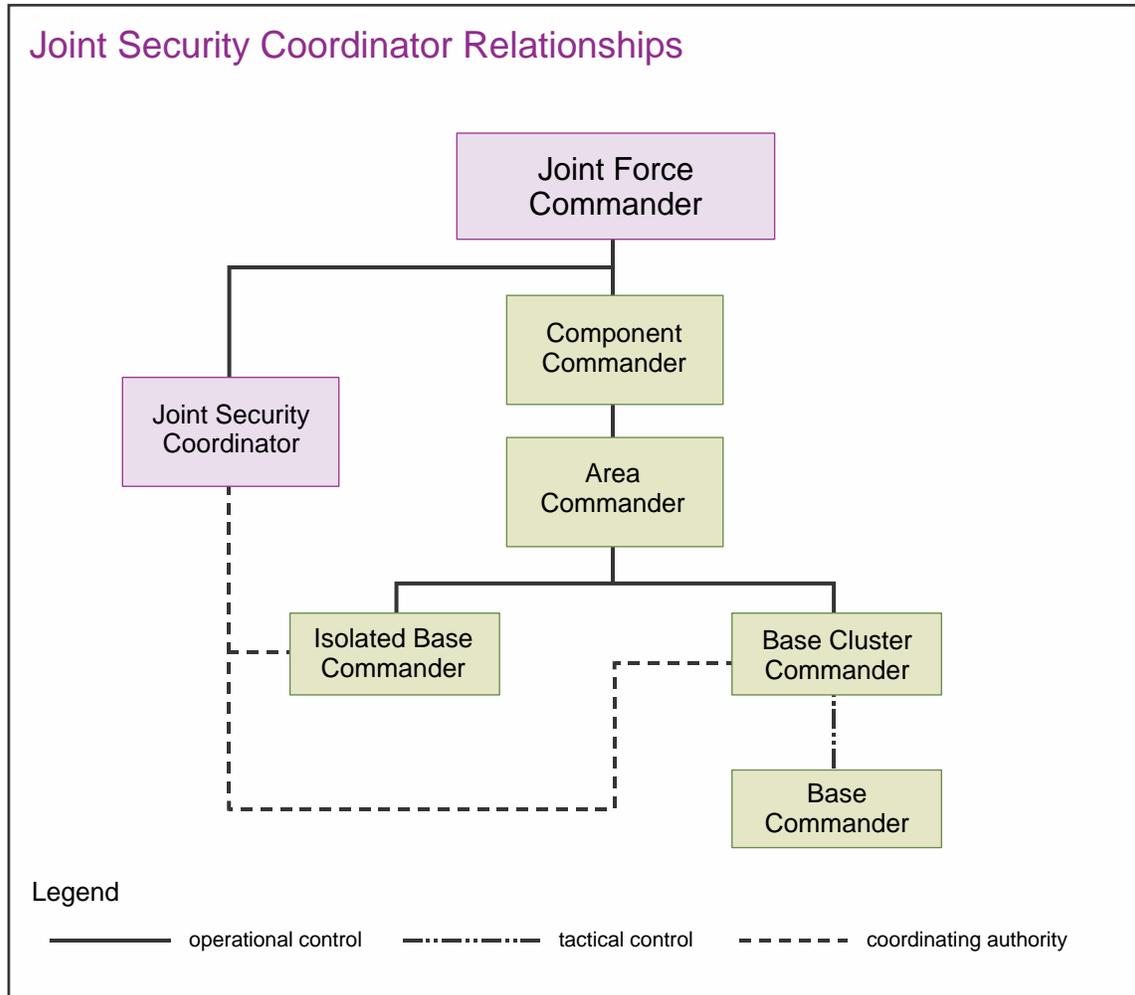


Figure II-1. Joint Security Coordinator Relationships

JSC normally coordinates security requirements and priorities with the joint force air component commander (JFACC)/area air defense commander (AADC).

(b) In cases of Level III threats or other emergencies, the JFC may delegate a subordinate commander the authority to counter the threat and restore JSA security. The JSC will support requests by the assigned commanders.

(c) Specific joint security coordination during military operations includes coordinating with appropriate commanders and staff to ensure that the following applies:

1. The base and LOC construction and security posture in JSA supports the JFC's concept of operations and is adaptable to support future operations.

2. The overall base and LOC security plan is developed and coordinated with appropriate US forces, MNFs, other USG departments and agencies, military personnel not assigned to the GCC under the COM and SDO/DATT, and HN commands.

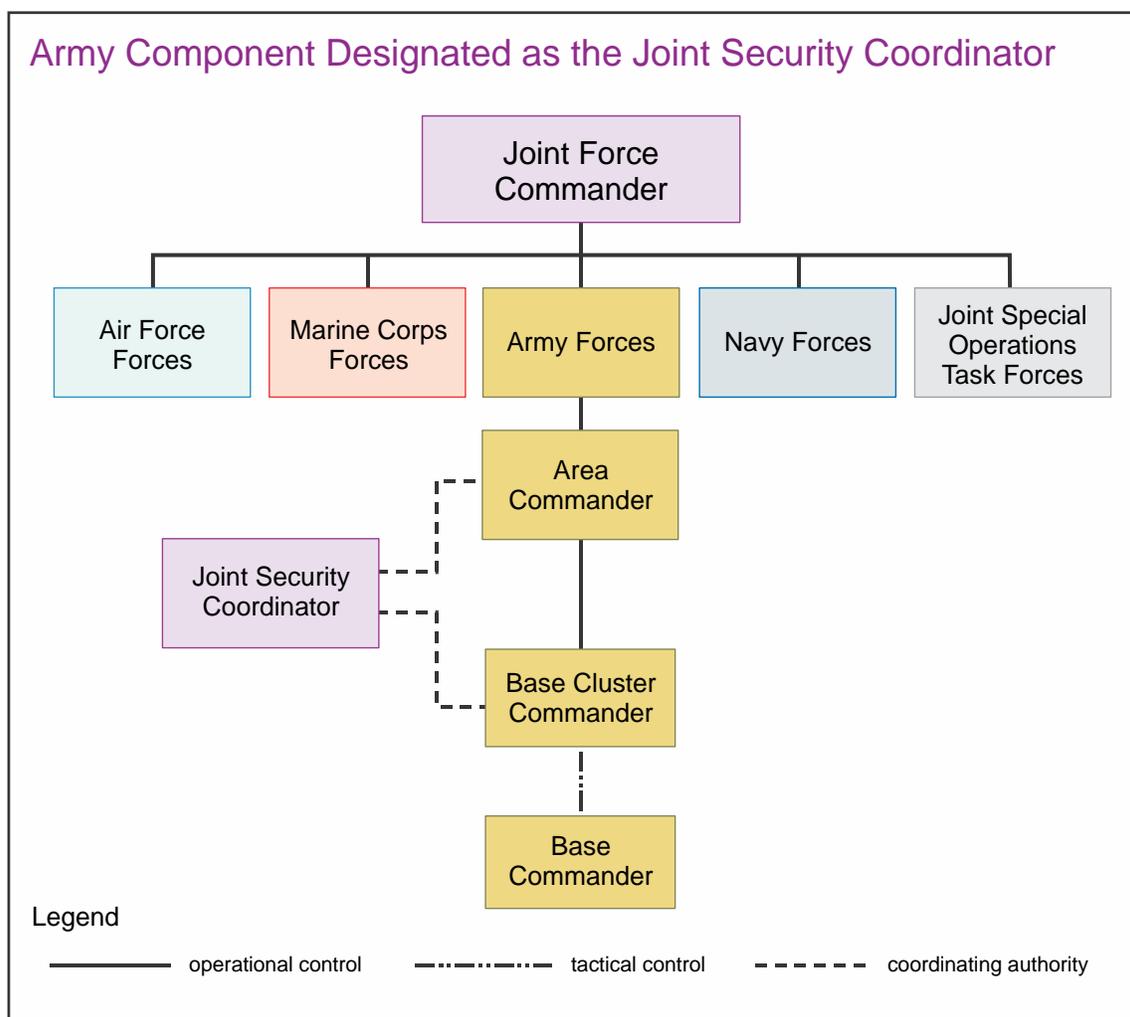


Figure II-2. Army Component Designated as the Joint Security Coordinator

3. The chain of command established by the JFC and the degree of authority granted to the JSC are adequate for the mutual protection and security of all US personnel and assets in the OA.

4. Intelligence and law enforcement are responsive to the needs of base commanders and LOC security forces operating in the JSA.

5. Objective criteria are developed and shared to assess the criticality and vulnerability of bases, base clusters, LOCs, and key infrastructure, both internal and external to the OA, to prioritize security improvements and position MSFs and TCFs, as required.

6. Coordination with the AADC has been completed to ensure that air and missile defense requirements for the JSA(s) are integrated into US, multinational, and/or HN air defense plans IAW JFC priorities and concept of operations.

7. Base and LOC defense plans incorporate adequate provisions and procedures for the CBRN warning and reporting system.

8. Appropriate liaison is established with multinational and HN commands for coordination of JSO.

9. All relevant international and domestic (US and HN) legal guidelines impacting security within the JSA (i.e., relevant US, HN, and international law including the law of war, HN agreements, status-of-forces agreements [SOFAs], and ROE) are disseminated and shared to appropriate command levels.

(5) **Component Commanders.** The JFC normally exercises command through Service or functional component commanders and designates command responsibilities based on the operational mission.

(a) **Security Responsibilities**

1. Component commanders with area responsibilities provide for the defense of their AOs, the overall defense of bases located in their AOs, and for LOCs within their AOs.

2. Within established AOs, other component commanders must ensure and provide for the defense of their assets and/or bases critical to their component responsibilities. A component commander with unique security requirements (e.g., those related to the MANPADS footprint around a joint operating base) should expect to provide the majority of forces for the defense of those assets/bases.

3. When an AO is not established, commanders must provide for the defense of those bases critical to their component responsibilities. Accordingly, that component should expect to provide the majority of forces to conduct these security operations.

(b) Joint security responsibilities are usually modified by HN agreements when operating in the sovereign territory of multinational partners who normally retain responsibility for the overall security of an OA. In these circumstances, the component commanders would continue to execute their security authority as directed by the JFC through other appropriate commanders and **ICW the JSC**, to:

1. Organize appropriate component bases into base clusters and designate base and base cluster commanders. Organize the defense of bases within their OA.

2. Coordinate the local security of bases and base clusters, LOCs, and key infrastructure to include establishing priorities for security and area damage control (ADC) IAW JFC directives.

3. Establish a C2 network linking bases and base clusters, and ensure that adequate coordination is established with MNFs and HN activities within or bordering their security zones.

4. Ensure that base and base cluster defense plans are adequate, coordinated, and complementary to applicable HN security plans.

5. Serve as the single point of contact to coordinate JSO within their AO with the HN (if so designated by the JFC).

6. Identify, train, and position base or LOC MSFs as well as other area security units IAW JFC directives and priorities.

7. Perform other security responsibilities as directed by the JFC through the JSC.

(c) Service and functional component commanders may also establish bases IAW JFC guidance to meet the JFC's objectives. In this case, component commanders delegate authority to provide security and defense of those bases to the base commander and coordinate security and defense issues with Service or functional components with area responsibilities, as appropriate.

(6) Area Commanders. Service component commanders with area responsibilities establish base and base clusters within their AOs and delegate the authority to provide security to those subordinate commanders.

(a) **Component commanders with a JSA in their AO may be designated as the JSC and be delegated the authority to conduct security operations.** In lower-level threat environments, the commander, Army forces, may delegate joint security coordination responsibilities to a subordinate Army unit, normally a maneuver enhancement brigade (MEB). The MEB is designed to provide C2 of forces from multiple branches, but especially those that conduct support area and maneuver support operations for the force. The MEB's capability to conduct support area operations in the assigned echelon support area provides added security and defense for other units and enhances the freedom of mobility for the supported echelon. The MEB would subdivide and assign specific security areas to appropriate Army units. If assigned, Army MEBs plan, coordinate, control, and execute JSO within the JSA.

(b) The JSA or a designated part of the OA may be the responsibility of the commander, Marine Corps forces, who may designate the commander of the Marine air-ground task force (MAGTF) the JSO mission, including the defense of logistic and air bases within the JSA. The MAGTF commander may, in turn, choose to designate the MAGTF logistics combat element commander for this mission. Tasks may include joint security responsibilities (e.g., ADC, convoy security, movement control) that will be conducted by Marine Corps forces in the JSA.

(7) **Base Cluster Commander.** When necessary, the JFC may designate a senior base commander as a base cluster commander. A base cluster is a collection of bases, geographically grouped for mutual protection and ease of C2. The base cluster commander coordinates the defense of bases within the base cluster and integrates defense plans of bases into a base cluster defense plan. The base cluster commander normally has **TACON of forces assigned to the base primarily for the purpose of local base defense. The authority the base cluster commander will exercise over other forces residing on the base for primary purposes other than local base defense must be established by the JFC**

and be explicitly detailed in order that appropriate JSO may occur as part of the overall base defense plan.

(8) **Base Commander.** The JFC normally designates the commander of the primary activity of a base as the base commander. The base commander is responsible for all base security operations within the base boundary and will closely coordinate operations with all occupants. A base commander provides and **exercises base defense C2 through a base defense operations center (BDOC).** The base commander establishes a BDOC to serve as the focal point for FP, security, and defense within the base boundary. Through the BDOC, the base commander plans, directs, integrates, coordinates, and controls all base defense efforts, and coordinates and integrates security operations with the base cluster operations center (BCOC) as appropriate. This normally involves **TACON over forces assigned or attached to the base primarily for the purpose of local base defense.** The base commander may also exercise TACON over **other forces residing on the base for primary purposes other than local base defense** when these forces are called on to perform functions related to base defense or local security missions as part of the overall base defense plan. Commanders of units residing on the base that are not explicitly detailed by the JFC for base defense should coordinate with the base commander for participation in the base defense plan. The base commander provides for base terrain management and the location of all mission-essential assets. **The base commander is determined by the JFC based on the classification of the base and by the functions and unique security requirements of the individual Services. The Service designated with base command responsibilities provides the C2 structure for FP, security, and defense operations within the base boundary.**

(9) **Tenant Unit Commanders.** Tenant unit commanders are commanders of units that reside and operate on, but do not fall under, the direct command of the base commander. **Tenant unit commanders must actively participate in the preparation of base security and defense plans.** They will normally be required to provide security of their own forces and mission-essential assets, provide individuals to perform perimeter/gate security, and will often be assigned battle positions IAW base security plans. These forces, when provided, will generally be under the TACON of the base commander for the purpose of base defense. Most importantly, **they are required to ensure that all personnel are properly trained to support and participate in base security in the event of attack.** Tenant joint special operations task forces, because of low personnel densities, must coordinate the above requirements with the base commander (see Figure II-3).

(10) **TCF Commanders.** In operations where there is the possibility of a Level III threat, the JFC may elect to establish a dedicated joint security combat force called a TCF. **The command relationships between the TCF and subordinate commanders will be determined by the JFC.** The TCF is normally commanded by a designated land component commander or subordinate commander. The TCF is a combat unit with appropriate combat support and combat service support assets to defeat Level III threats. The threat requiring the commitment of a TCF is usually of such magnitude that several bases or base clusters are threatened. Once committed, the TCF is given an OA by the appropriate commander in which to accomplish its assigned mission. With this OA, the TCF commander is the supported commander for the integration and synchronization of maneuver, fires, and

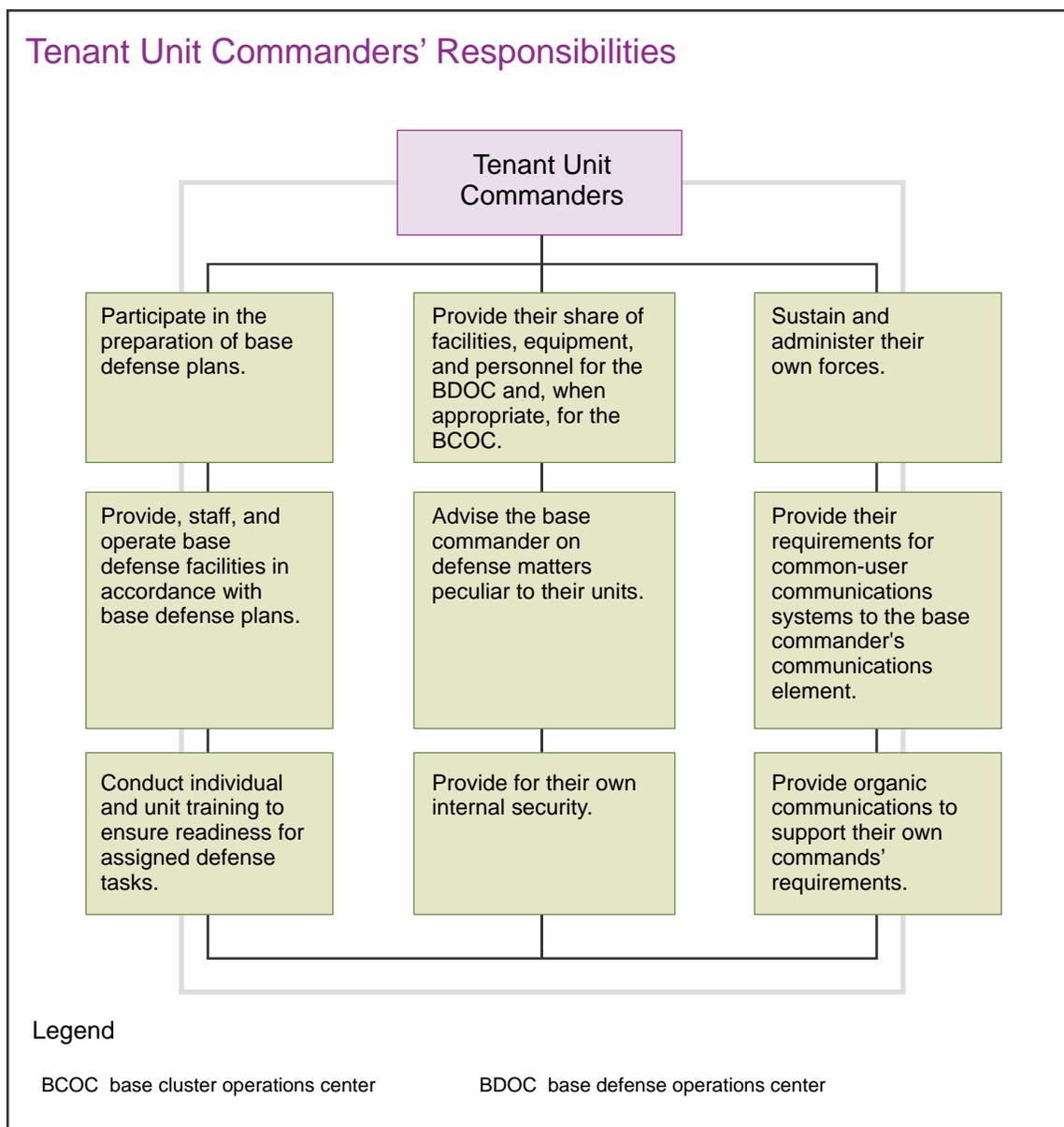


Figure II-3. Tenant Unit Commanders' Responsibilities

interdiction. This may require the rearrangement of boundaries within an OA. Plans for the employment of the TCF should be coordinated and rehearsed with area commanders, base cluster commanders, base commanders, and with the HN.

4. Establishment of Base and Base Cluster Command Relationships

a. **Command Relationships in JSO.** The JFC, normally through a designated JSC, ensures that appropriate command relationships among subordinate area, base, and base cluster commanders are established and understood by all affected commands. Command relationships determine the interrelated responsibilities between commanders as well as the authority of commanders in the chain of command. **The typical command relationships established in support of JSO should be TACON between the base or base cluster**

commander and the dedicated security force, when the attached force is from a different component command.

b. **Base Classification.** Unless determined by higher authority, the JFC will determine the classification of bases IAW established policies. A base may be either a single Service base or a joint base.

(1) **Single Service Base.** A single Service base contains forces primarily from one Service and where the base's primary mission is under the control of that same Service. Base commanders of these bases are normally designated by the Service component commander.

(2) **Joint Base.** A joint base has two or more Service units where no Service has a majority of forces or primacy of mission responsibility. The JFC assigns command authority of this base to a Service component and that component will then designate the base commander. When a joint base is designated, **it is critically important that the JFC, normally through the JSC, delegate the authority to conduct JSO within the base boundary to a single commander.** However, other Services have security forces that contribute to or can accept command of base or base cluster security (e.g., elements of the Navy Expeditionary Combat Command and United States Coast Guard [USCG] port security units [PSUs]).

5. Operations Centers

a. **JSCC.** A JFC may elect to establish a JSCC using the designated JSC staff elements and representatives from the components operating within the OA. Component and staff representation will vary IAW mission, forces, and security zone requirements, and should support the planning, coordination, and execution of all joint security-related operations. The JSC will ensure that component representation and representation from the JSC staff is sufficient to support assigned mission responsibilities. **The JSCC is the JSC's full-time organization to centrally plan, coordinate, monitor, advise, and direct all base security operations in the JSO.** It coordinates with other elements on the JSC staff, with higher, lower, and adjacent command staffs, and with HN and allied command staffs. The JSCC is manned with full-time staff for key personnel and additional personnel with subject matter expertise as required.

See Appendix A, "Joint Security Operations Centers," for more information on the functions and organization of the JSCC.

b. **BCOC.** A BCOC is a C2 facility established by the base cluster commander to serve as the focal point for the security of the bases within the base cluster. It plans, directs, integrates, coordinates, and controls all base cluster security efforts. The BCOC personnel keep the base cluster commander informed of the situation and resources available to cope with security-related requirements. They coordinate all BDOC efforts, and integrate JSO with other designated higher-level staff as designated by the JFC. The nature of the BCOC depends on the combination of forces involved and may include other sister Services, multinational HN, and/or other personnel of US agencies. **The BCOC is similar in many**

respects to the land force unit’s tactical operations center, and, in some cases, may be one and the same. Representatives from intelligence, maneuver, and fire support staff the BCOC. The base cluster commander provides other functional staff representatives to augment base commanders as necessary. Multi-Service, other agency, HN, and/or multinational representation should be part of the BCOC when elements of their armed forces, police, or paramilitary forces are directly involved in the overall base defense effort or they are a major tenant organization to the base.

See Appendix A, “Joint Security Operations Centers,” for more information on the functions and organization of the BCOC.

c. **BDOC.** A BDOC is a C2 facility established by the base commander as the focal point for FP, security, and defense within the base boundary. Through the BDOC, the base commander plans, directs, integrates, coordinates, and controls all base security efforts, and coordinates and integrates area security operations with the BCOC, if established, or other designated higher-level staff as designated by the JSC. The nature of the BDOC depends on the combination of forces involved and may include sister Services, multinational HN, and/or personnel of other US agencies, depending on the combination of forces located at each base. Multi-Service, other agency, HN, and/or multinational representation should be part of the BDOC when elements of their armed forces, police, or paramilitary forces are directly involved in the overall base defense effort, or they are a major tenant organization to the base. The center normally consists of three primary sections—command, intelligence, and operations—with additional sections as necessary. These additional sections could include a logistic section to plan the provision of services and support to the base, and an ADC section that provides inspection, planning, and control of the base’s emergency response/ADC resources. The BDOC is manned full time with key personnel and augmented with subject matter expertise as required. The joint defense operations center is used in some theaters to refer to a BDOC.

See Appendix A, “Joint Security Operations Centers,” for more information on the functions and organization of the BDOC.

Intentionally Blank

CHAPTER III PLANNING

“Never break the neutrality of any port or place, but never consider as neutral any place from whence an attack is allowed to be made.”

**Vice-Admiral Horatio Nelson (Royal Navy)
Letter of Instruction
1804**

1. Introduction

The JSC, through the joint force subordinate commanders, base cluster commanders and base commanders, monitors and coordinates the overall organization and control of forces responsible for base and LOC security and advises the JFC on all issues associated with JSO. These forces must be trained, organized, and equipped to properly execute JSO. This chapter sets forth joint force security planning considerations along with the discussion on special considerations relevant to JSO.

2. The Fundamentals of Planning Joint Security Operations

Understanding the planning fundamentals of JSO is key to the proper execution of this mission. Commanders should ensure security operations are being planned and executed as part of normal operations. The fundamentals of JSO planning are listed in Figure III-1.

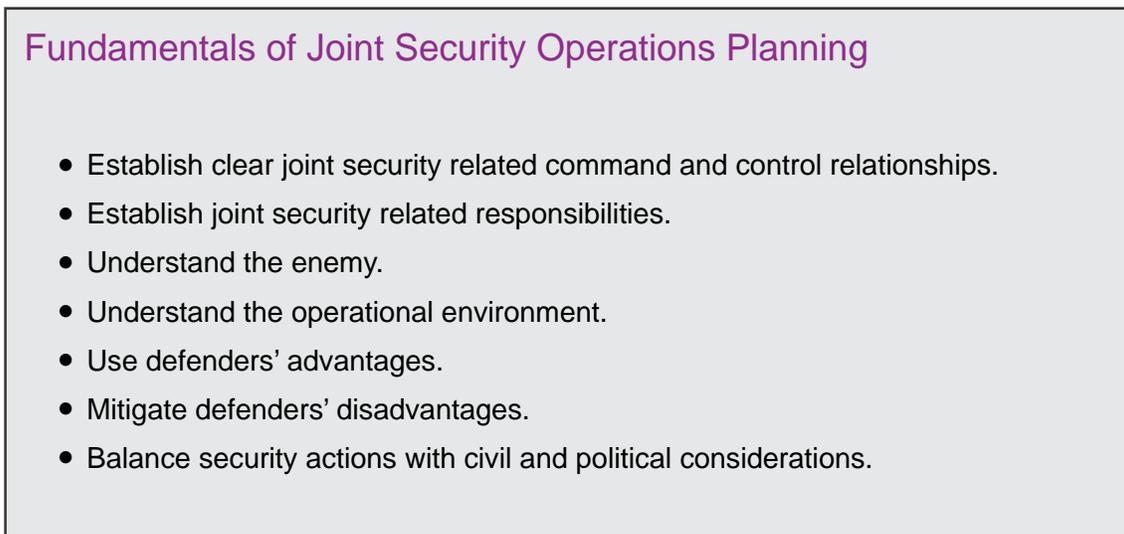


Figure III-1. Fundamentals of Joint Security Operations Planning

a. **Establish Clear Joint Security Related C2 Relationships.** The JFC or the designated representative establishes clear and well-understood C2 relationships to enable joint security planning, coordination, and execution.

b. **Establish Joint Security Related Responsibilities.** The JFC, normally assisted by a designated JSC, must ensure that base, base cluster, and LOC security responsibilities are established early in the decision-making process.

c. **Understand the Enemy.** Joint forces must be familiar with the capabilities of enemy forces; weapons; equipment; tactics; and political, ideological, cultural, economic, and/or other motivational factors. The status of the civilian populace as related to previous enemy activity may also play a significant role. Commanders and their staffs should be kept apprised of the latest intelligence on probable enemy intent.

d. **Understand the Operational Environment.** Joint intelligence preparation of the operational environment (JIPOE) provides the commander a continuous, integrated, and comprehensive analysis of enemy capabilities, the anticipated impact on friendly operations and civilian populace, terrain, weather, and any other characteristics of the operational environment that may influence the JSC's decision. It helps the commander anticipate events, develop priority intelligence requirements (PIRs) and information requirements tied to those events, and develop effective counters to those events. Everyone from the base commander through the JFC must have access to the latest intelligence concerning relevant actors, local and transnational threat networks operating within the operational environment, and their probable objectives and intentions.

For more information on the JIPOE process, see JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

e. **Use the Defenders' Advantages.** There is strength in the defense and commanders and planners should take these advantages into account as they prepare and execute JSO. Key advantages to the defense include:

- (1) The ability to fight from cover and concealment.
- (2) Detailed knowledge of local waterways, 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, close air and logistic support to fit any predictable situation.
- (5) The ability to conduct rehearsals of contingency response plans on the terrain they will be executed on.

f. **Mitigate Defenders' Disadvantages. Military bases and surface LOCs are fixed, often valuable targets with limited depth for maneuver.** Mitigating the disadvantages of securing fixed facilities and LOCs is critical to the success of JSO. Key methods and techniques to mitigate these disadvantages include:

- (1) Establish strongly defended boundaries with well-controlled access points.

- (2) Integrate MSFs into base and LOC security plans.
- (3) Apply aggressive countermeasures to include patrolling, observation posts (OPs), listening posts, and biometrics screening throughout the operational environment.
- (4) Harden facilities and critical resources.
- (5) Synchronize fires with base defense and LOC security actions.
- (6) Conduct execution rehearsals.
- (7) Develop, maintain, and execute CBRN emergency response measures.
- (8) Integrate intelligence collection assets and other early detection assets to see beyond the base perimeter.

g. **Balance Security Actions with Civil and Political Considerations.** Base and LOC security will have to be planned and executed IAW the standing ROE and other higher headquarters orders, which may include numerous constraints and restraints. All commanders and staff officers responsible for planning, coordinating, and executing JSO must take these factors into account. Failure to do so may have significant, possibly negative, strategic-level impact. Base commanders and their subordinates must comply with established ROE and should ensure that inconsistencies among Service components, multinational partners, and possibly even contractor personnel ROE are reconciled. Discrepancies need to be resolved at the JFC's level to ensure all bases and Services are operating with the same guidance. In areas with US country teams, commanders must liaise closely with the COM through the SDO during planning efforts to account for all political considerations.

3. Joint Security Operations Planning Overview

Base and LOC security may be governed by the factors explained in the following subparagraphs (not an exhaustive list).

a. **Mission. The primary mission of the base is to support joint force objectives.** Inherent in this mission is the subsidiary mission of securing these bases and LOCs from enemy action. The stated security plan should specify the following essential elements:

- (1) Who will secure the base?
- (2) Where is each unit positioned?
- (3) When and for how long must the unit(s) be prepared to provide security?
- (4) What are the control and coordinating measures?
- (5) What specifically will the unit(s) secure? Careful consideration should be given to the protection of any mission-essential assets within a given base or LOC-related assets.

For more detailed guidance on planning, see JP 5-0, Joint Operation Planning.

b. **Enemy.** Every intelligence resource available to the base commander should be used to identify the enemy and **determine their capabilities and intentions as they relate to base and LOC security considerations.** CI resources will be used to detect, identify, exploit, disrupt, and neutralize enemy intelligence and terrorist threats.

The intelligence process and intelligence support to joint operations are discussed in JP 2-01, Joint and National Intelligence Support to Military Operations.

(1) **The JFC should provide commander's critical information requirements (CCIRs) to the staff and components.** CCIRs comprise a comprehensive list of information requirements identified by the commander as being critical in facilitating a timely decision-making process that effects successful mission accomplishment. In the course of mission analysis, the intelligence planner identifies the intelligence required to answer the CCIRs. Mission analysis leads to the development of intelligence requirements (general or specific subjects upon which there is a need for the collection of information or the production of intelligence). CCIRs include both friendly forces information requirements and PIRs. **Those intelligence requirements deemed most important to mission accomplishment are identified by the commander as PIRs.** Based on the command's intelligence requirements, the intelligence staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). JP 3-07.2, *Antiterrorism*, provides the template for a threat information organization matrix, which may be of value when developing information requirements. Specific joint security related PIRs may include:

(a) The enemy's tactical, operational, and strategic objectives and intentions as they relate to attacks on bases and LOCs.

(b) Organization, size, and composition of forces, and locations of strongholds that threaten bases and LOCs.

(c) Movement of enemy personnel and equipment.

(d) Enemy intelligence capabilities, to include use of local hire base workers and infiltrators.

(e) Enemy capabilities and tactics (special consideration should be given to standoff capabilities such as mortars, missiles, SAMs, and CBRN weapons).

(f) Local support for enemy causes.

(g) Proximity of enemies to LOC choke points.

(2) **Information requirements** deal with necessary information about the enemy, environment, and other factors that need to be collected and processed to meet the intelligence and other requirements of the commanders responsible for JSO. The intelligence effort should be directed toward planning and direction, collection, processing

and exploitation, analysis and production, and dissemination and integration of intelligence that will permit the development of friendly capabilities to:

- (a) Prevent and disrupt enemy attacks on bases and LOCs.
- (b) Counter enemy fires, mobility, electronic warfare, imagery, and human intelligence (HUMINT) capabilities.
- (c) Identify and defend against enemy intelligence collection efforts.
- (d) Use identity intelligence (I2) efforts to help build a biometrically-enabled watchlist.
 1. Identification and associations of known or suspected insurgents, terrorists, or criminals.
 2. Identification of suspected or known locations of buildings and facilities used by insurgents, terrorists, and criminals.

c. Terrain and Weather. Bases and surface LOCs are usually selected in order to accomplish missions related to their use. Although defensive considerations are frequently secondary, they should not be ignored. The nature of air bases, for example, precludes establishment of tight boundaries with extensive cover and concealment for defenders. However, the defense of an air base can be enhanced if the location does not allow the enemy to approach unobserved. Likewise, ports are located in or adjacent to urban areas. **Nonetheless, the base commander should make the best use of the terrain within the OA.** Commanders analyzing terrain should consider all its military aspects, from the standpoints of base and LOC function as well as security considerations from both a defender's and enemy's perspective. Security considerations include observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach. Additionally, commanders should analyze how the weather affects both defender and enemy weapons systems and tactics. **Weather and visibility conditions can have a significant impact on land, air, and maritime operations.** Additionally, prevailing winds can determine the effectiveness of enemy employment of CBRN weapons and/or the release of toxic industrial materials (TIMs) from nearby industrial facilities. Commanders should minimize their own vulnerabilities to adverse weather conditions (i.e., flash flooding, high winds) and exploit any advantages over enemy vulnerabilities.

d. Troops and Support Available for JSO. There may be some units on a base whose primary missions are defense and security, such as Army and USMC military police (MP) units at a large headquarters, Air Force security forces on an air base, and air and missile defense forces. In some cases, the JFC or subordinate commander may determine that land combat forces, usually platoon to battalion task force level, may also be assigned as dedicated base, surface LOC, and/or area security forces. **In other cases, particularly bases where there are limited combat forces, security forces may be formed from logistic, transiting, or other support units.** In these situations, support in the form of special training and equipment will be required. This support is essential in ensuring that such forces are capable of performing the required security missions and

tasks. **Most on-call personnel made available for joint security related missions will be obtained from the units whose primary mission is not security related.** In many cases, these personnel will not have the same degree of combat skills as dedicated security forces and therefore must receive additional training in marksmanship, tactics, and basic ground combat skills. Integration of these forces into successful JSO requires close supervision and leadership. Dedicated resources, normally from within the base, will be required to provide the needed support to ensure forces are at the requisite level to respond effectively. Figure III-2 shows troop capability requirements for each threat level. Any incorporation of contractors authorized to accompany the force (CAAF) and private security contractors into the JSO plan will be IAW US, HN, and international law, and relevant SOFAs or other international agreements, as well as the contract and associated documents. Legal advice should be sought prior to the inclusion of CAAF and private security contractors in JSO.

| Levels of Threat Troop Capability Requirements | |
|--|--|
| Threat Level | Capability Requirement |
| Level I | Base and line of communications security force defense capability. May require military police (or Service equivalent) presence. |
| Level II | Level I with additional mobile security force or area security force with specified base and line of communications security related mission requirements. |
| Level III | Level II plus may require the employment of a tactical combat force. |

Figure III-2. Levels of Threat Troop Capability Requirements

(1) **Level I Threat Troop Requirements.** Level I threats involve day-to-day security measures that must be maintained by all military forces. At this level, **available assets should be able to detect and defeat enemy activities. Level I security activities are conducted primarily by the forces assigned to the mission, usually as tasks in addition to their primary duties.** Early in the process of planning for any joint security operation, the JSC and unit commanders will determine which units and/or individuals will be exempt from security duties and ensure that those assigned security duties have the requisite ground combat skills to accomplish the mission. The JSC normally establishes a dedicated security force and determines its size and composition by striking a balance between economy of force requirements weighed against the enemy threat and the size and importance of the base or LOC.

(2) **Level II Threat Troop Requirements.** Level II threats include threats that will often require, in addition to the standard base and LOC security forces, a dedicated MSF or area command combat force specifically focused on JSO. The MSF would normally be, at a minimum, an MP platoon or Air Force security force flight, but could also be a land force combat arms unit. Key capabilities of this force normally would include:

- (a) Armored mobility (armored wheeled or combat-tracked vehicles).
- (b) Larger caliber direct-fire weapons (heavy machine guns, automatic grenade launchers, and/or direct fire cannons).
- (c) Organic or on-call indirect-fire capability (medium mortars at a minimum).

(3) **Level III Threat Troop Requirements.** Level III threats require the same forces as level II threats and normally include a TCF. A TCF is an on-call mobile force capable of responding to larger-scale conventional or counterinsurgency threats in the JSA. A TCF normally consists of a combined arms task force with organic combat and combat support elements and ability to call for fires (indirect and air delivered).

e. **Time Available.** Commanders assess the time available to plan, prepare, and execute the mission. This includes the time required to assemble, deploy, and maneuver units in relationship to the enemy and conditions. Commanders consider how friendly or adversary forces use time and the possible results, as it can fundamentally alter the situation. Time available is normally in terms of the mission and tasks assigned and bounded by adversary capabilities. At all levels, commanders should use the time available effectively and provide subordinates with time to plan and prepare their own operations. Commanders monitor the time available, and as events occur, assess its impact on mission timelines.

f. **Civil and Political Considerations.** JFC and subordinate planners should give significant consideration to the civil and political impact of joint security measures and actions. For example, closing key surface LOCs (military use highways, pipelines, railways, waterways) to civilian use may be desirable from a security perspective, but the potential impact on the local population and on relief and reconstruction programs could greatly outweigh the advantages of such measures.

4. Major Planning Considerations

a. **FP.** Countering level I threats **is considered to be a part of the day-to-day FP measures for bases.** AT measures will be a large part of the base security plan and consist of defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces. An integrated and comprehensive AT program (physical security, construction standards, CBRN passive defense, OPSEC, CI, I2, biometrics and forensics screening, etc.) should be developed, implemented, and updated in order to effectively detect, defend, and respond to a terrorist threat.

For more specific guidance on AT planning and operations requirements, see JP 3-07.2, Antiterrorism, as well as the applicable GCC's FP and AT directives or operation orders (OPORDs).

b. **Intelligence.** Effective intelligence support, including CI and law enforcement agency information, is essential to conducting successful JSO. Current intelligence and CI estimates should be focused on joint security challenges and should incorporate intelligence from all US, multinational, and HN sources. **JSO should be completely and deliberately linked to the overall JFC's JIPOE and component intelligence preparation of the battlespace processes.**

(1) **Responsibilities.** The JSC coordinates the intelligence and CI requirements of organizations with JSO responsibilities with the intelligence directorate of a joint staff (J-2). The J-2, through the joint intelligence operations center (JIOC) and/or the joint intelligence support element (JISE), is responsible for ensuring that the appropriate resources and operations are allocated to support these requirements. Where appropriate, the J-2 should leverage intelligence reachback from other intelligence organizations to enhance intelligence capabilities.

JOINT INTELLIGENCE SUPPORT ELEMENT ESTABLISHMENT AT JOINT BASE BALAD DURING OPERATION IRAQI FREEDOM

Early in the war, Joint Base Balad suffered the highest level of indirect fire attacks among forward operating bases in Iraq. Casualties were few, and damage not severe, but threats posed by the continued attacks forced the Air Force to consider reducing flight operations at a time when strike aircraft provided the preponderance of fire support for ground forces throughout the theater, and tactical airlift was expanding operations in order to reduce over-the-road convoys. Preventing the denial of air operations required the use of controlling activities not only within the air base perimeter but also in the surrounding area where indirect fire attacks were launched and adversary support networks were located. Previous doctrine was premised on the expectation that air bases would be located in a rear area where the threat would be greatly reduced. In reality, the fence surrounding Joint Base Balad represented the line of contact with the enemy. Insurgents and irregular fighters hid within the population surrounding the base and launched indirect fire attacks day and night. A myriad of joint, coalition, and host nation ground forces provided security beyond the installation perimeter.

At Joint Base Balad the most effective base defense operations were not established until an aggressive intelligence support effort was undertaken, most notably by the Joint Intelligence Support Element. Informed by intelligence professionals, uniquely knowledgeable on air base operations, the Joint Defense Operations Center (JDOC) was able to integrate joint intelligence reporting for Air Force and Army ground forces to exploit areas of interest and disrupt insurgent operations before airfield damage could be inflicted. These actions drove the enemy toward hasty, inaccurate, and small numbers of shots in their attacks. The weakened efforts of the adversary, coupled with JDOC's timely warnings of imminent attacks and condensed airfield recovery actions, greatly reduced times of airfield closure, and minimized enemy impacts on airfield operations.

Various Sources

(2) **Intelligence Considerations.** The JSC requires timely and accurate all-source intelligence to coordinate appropriate joint security related actions. However, intelligence will typically come from supporting organizations operating throughout the OA, and the supporting JIOC and/or JISE may provide surveillance video, geospatial intelligence, signals intelligence, CI, and HUMINT, as required. Logistic units are also a valuable source of information regarding potential unconventional, subversive, IED, CBRN, guerrilla, and terrorist threats. This information is usually reported through intelligence and operational channels simultaneously. The JSC, in conjunction with the command counterintelligence coordinating authority (CCICA) or joint task force CI coordination authority, will coordinate with appropriate commanders and staff to ensure that:

(a) Reporting means and procedures are established and used for the timely reporting of suspicious activities or incidents to the JSC.

(b) Adequate liaison is established with HN military commands and government agencies in the OA to collect valuable information from those sources.

(c) Chains of command are used to convey essential information and intelligence to support all forces engaged in JSO.

(d) Separate or transient forces that may have been diverted from other tasks, and which may not otherwise have access to critical information, receive effective intelligence support.

(e) Biometric collection devices loaded with the current biometrically-enabled watchlist are provided.

(3) **CI.** An effective CI process is one of the most important ways that commanders and the JSC can contribute to maintaining adequate joint security. The CI process includes the complementary functions of investigations; operations; collection, reporting, analysis and production, and dissemination. CI is particularly effective in assisting commanders, the JSC, and staffs in identifying the espionage, sabotage, assassination, subversion, and terrorist threats posed by conventional, unconventional, and insider threats.

(a) **CI Plan.** The J-2, through the CCICA and in conjunction with the CI organizations, should plan for collection requirements, conduct liaison operations with HN intelligence and security services, provide for incident investigations, and obtain analytical support, particularly to the JSC staff and the JSC force protection working group (FPWG) (if established). CI planning should include an assessment of all foreign intelligence entities. CI can provide commands and staffs with identification and analysis of threats from unconventional forces, terrorists, partisans, and civilian groups sympathetic to the enemy.

(b) **CCICA.** The CCICA provides the commander with current CI estimates that include analysis of adversary or other foreign intelligence capabilities and other threats as appropriate. The CCICA establishes effective communications networks and liaison with HNs, allies, joint forces, and law enforcement agencies and ensures that this information is reported in a timely and consolidated manner to the components that plan and execute JSO.

(c) **Insider Threat.** CI is one of the pillars to support theater operations to counter the insider threat. To effectively counter the insider threat problem, CI must coordinate and share information with security, cybersecurity, law enforcement, JSC, and other appropriate personnel and staffs. In order to support JSC, the CI staff will validate and integrate insider threat reporting requirements into the intelligence collection plan; establish and implement CI activities to identify and counter these threats; and identify CI triggers indicative of a CI insider threat.

(4) **I2.** I2 results from the fusion of identity attributes (biologic, biographic, behavioral, and reputational information related to individuals) and other information and intelligence associated with those attributes collected across all intelligence disciplines. I2 utilizes enabling intelligence activities, like biometrics-enabled intelligence, forensics-enabled intelligence, and document and media exploitation, to discover the existence of unknown potential threat actors by connecting individuals to other persons, places, events, or materials, analyzing patterns of life, and characterizing their level of potential threats to US interests.

More information on intelligence operations can be found in JP 2-0, Joint Intelligence, JP 2-01, Joint and National Intelligence Support to Military Operations, and JP 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations.

c. Communications

(1) **General.** The JSC must have an interoperable, secure, reliable, flexible, and survivable communications network in order to accomplish the mission. Existing military or commercial communications systems should be used based on security, redundancy, and reliability to the maximum extent possible. However, additional communications systems (e.g., Joint Worldwide Intelligence Communications System) may be required to reconfigure or expand the network.

(2) **Communications System Support Responsibilities.** The communications system directorate of a joint staff, ICW the JSC, provides overall management of organic communications systems (e.g., single-channel radios and internal switching or terminal equipment supporting the JSC staff) and coordinates with the appropriate system manager for nonorganic communications system support. The JSC will designate units to establish HN connectivity as required. (NOTE: The JSC will establish necessary liaison with the communications system directorate of a joint staff to ensure that all communications requirements for the JSA are met.)

(3) **Individual Component Responsibilities.** Each component command will establish communications with the JSC and lateral organizations. Deficiencies in communications assets should be identified and resolved through the JFC.

(4) **Joint Movement Control Communications.** Communications to support LOC security operations should be coordinated with, and will often use, the joint movement control communications structure. This is especially true when LOC security operations are

limited to internal convoy defense capabilities. See Chapter IV, “Joint Security of Bases and Lines of Communications,” for more information.

(5) **Inter-Service and Multinational and Contractor Communications System Challenges.** Often, tenant units, the program managers for contractors deploying with the force, or even MSF organizations will be operating with noncompatible communications equipment. The JSC and subordinate commanders responsible for planning and executing JSO must ensure that specific base, base cluster, and LOC security communications measures are planned for and tested to ensure compatibility. This includes planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures as part of joint electromagnetic spectrum management operations. If communications compatibility is identified as an issue, then proper corrective actions should be taken by the appropriate commander.

Further discussion of communications systems can be found in JP 6-0, Joint Communications System, and JP 6-01, Joint Electromagnetic Spectrum Management Operations, specifically for joint electromagnetic spectrum management operations.

d. **Cyberspace and Information Security.** JFCs should establish an integrated, multidisciplinary security program that implements information, personnel, contracted services, physical security operations, and cyber security considerations in the JSA.

Further discussion of this area is covered in JP 3-12, Cyberspace Operations, JP 3-13, Information Operations, and JP 3-13.3, Operations Security.

e. **CBRN Defense.** CBRN defense operations must be incorporated into JSO plans and procedures. Many adversaries can employ CBRN weapons to attack bases, other critical facilities, and LOCs. All US forces in the OA should prepare to plan and execute CBRN defense operations.

(1) **Responsibilities of the JSC.** The JSC coordinates with component commanders and other appropriate commanders and staffs to ensure that CBRN defense planning, exercises, equipment, personnel, avoidance, protection, decontamination, and preventive measures are incorporated in security planning and operations. This includes positioning friendly CBRN defense assets to support mission requirements and future operations.

(2) **Responsibilities of Component Commanders.** Component commanders incorporate CBRN defense planning, exercises, equipment, personnel, avoidance, protection, decontamination, and preventive measures into area and base or base cluster security plans. They also position friendly CBRN defense personnel and assets to support current mission requirements and facilitate future operations, IAW JFC directives and priorities.

(3) **Base Commander and Base Cluster Commander.** Every base and base cluster commander integrates operational fundamentals designed to prepare for, protect against, prevent, respond, and recover from CBRN threats and hazards.

For further information on CBRN defense operations, see JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear Environments.

f. **Air and Missile Defense.** Since most units operating on base and surface LOCs in the OA have limited capability to engage and destroy incoming enemy air and missile threats, commanders must be aware of the capabilities and limitations of joint force defensive counterair operations for their areas. The JSC's focus is protection for the JSAs. Dependent upon the size and scope of the JFC's mission, **the joint force may establish an integrated air defense system (IADS) to conduct defensive counterair operations.** The IADS is not a formal system in itself but the aggregate of component air defense systems operating in the OA. The focal point of the IADS normally is the joint air operations center. The JSC should establish effective liaison with the JFACC and AADC at the joint air operations center during development of the critical and defended lists to ensure that defensive counterair coverage is coordinated and maintained throughout the OA to reduce or mitigate the effectiveness of the air and missile threat. That JSC liaison serves as the JSC's eyes and ears as well as their representative on matters of Service capabilities and limitations. This integrated and coordinated air and missile defense planning should include detailed plans to disseminate timely air and missile warning and cueing information to components, forces, multinational partners, and civil authorities. Air and missile warning and cueing information for JSAs must be planned for and executed at the JSCC and down to each BDOC/BCOC. Special consideration must be given to the critical asset list.

For more information on joint air and missile defense in general, see JP 3-01, Countering Air and Missile Threats, Navy Warfare Publication 3-01.01, Fleet Air Defense, Marine Corps Warfighting Publication (MCWP) 3-22, Antiair Warfare, Air Force Doctrine Annex 3-01, Counterair Operations, and Field Manual (FM) 44-100, US Army Air and Missile Defense Operations.

g. **Threat Early Warning and Alert Notification System.** Threat early warning is essential to the protection of joint forces operating throughout the OA and should be linked through the JSC and JSCC (if established) down through designated BCOCs and BDOCs. Alert notification systems are divided into two general categories:

(1) **Air Warning.** The air and missile defense warning system is a critical link in the OA air early warning system. Early warning and identification of enemy air threats, enemy air- and surface-to-surface missiles, and airborne and air assault operations are provided by several types of forward collection methods, including forward-deployed reconnaissance units, air defense systems, and the theater air ground system. A JFC's tactical warning requirements are supported by national and theater intelligence systems.

(2) **Surface, Subsurface, and Land Warning.** Information about potential surface, subsurface, and land threats are provided by various air, land, sea, and space intelligence, surveillance, and target acquisition systems. The JIOC/JISE will provide fused intelligence early warning of surface, subsurface, or land threats to the bases and LOCs.

(3) The JSC coordinates with appropriate commanders and staffs to ensure that a reliable, responsive, and redundant air, land, and sea early warning system is established

from the joint force level down to the base level throughout the OA. The JSC will ensure that a standardized alert system is implemented throughout the JSA to ensure warning and uniform response to threats. Training should be conducted to ensure that all joint forces understand the correct responses to the various and sometimes confusing early warning alert notification systems.

(4) Land and maritime component commanders are responsible for ensuring that adequate early warning systems are established in their AO IAW JFC directives.

h. Land Force Component and Joint Security. Joint security on the land includes bases, mission-essential assets, LOCs, and convoy security. Challenges include logistic facilities that may be located in heavily populated areas that are often linked by long and vulnerable surface LOCs.

(1) In a JSA, multiple Service components may be using the same facilities within a base complex such as:

- (a) Army intermediate staging bases, tactical assembly areas, or FOBs.
- (b) Army common-user water terminals.
- (c) MAGTF support bases.
- (d) Air Force air bases and airfields for APODs and close air support (CAS).
- (e) Naval bases supporting and sustaining fleet operations.

(2) Joint Security and Protection

(a) JSO requires fixing responsibility for protecting the joint force. A senior land commander will normally be designated with responsibility for JSO.

(b) When the commander, Army forces, is designated as the JFLCC, this responsibility is exercised through the designated protection cell. When designated as the JSC and responsible for the JSA, the Army headquarters protection cell (with augmented joint, interagency, and multinational personnel) provides the nucleus of the JSCC. The protection cell:

1. Integrates and synchronizes protection tasks and systems in the operations process.

2. Advises commanders on the priorities for protection and coordinates the implementation and sustainment of protective measures to protect assets according to the commander's priorities.

3. Provides input to the commander's plan by integrating the threat and hazard assessment to minimize vulnerability and provides vulnerability mitigation measures to help reduce risks.

(3) In support of the JFC's concept of operations, the JFLCC plans and conducts security operations to ensure protection of US and multinational mission-essential assets and the support areas required for sustainment of land operations. The JFLCC will normally assign an Army MEB for security of defined OAs, to serve as its operational protection headquarters, and to assist the supported headquarters in retaining the freedom of action not assigned to maneuver units.

(a) Area security may be the predominant method of protecting support areas that are necessary to facilitate the positioning, employment, and protection of resources required to sustain, enable, and control tactical forces. Area security operations are often emphasized in noncontiguous AOs to compensate for the lack of protection integrity that large or distant, unoccupied areas often create. Area security operations are often an effective method to provide civil security and control during some stability operations. Forces engaged in area security operations can saturate an area or position on key terrain to provide protection through early warning, reconnaissance, or surveillance and guard against unexpected enemy attack with an active response.

(b) Base and base cluster defense are essential to joint land operations. Land forces may contribute to the protection of multiple FOBs within their AOs.

(c) The security and protection of LOCs are critical to joint land operations because most support traffic moves along these routes. The security of LOCs (rail, pipeline, highway, and waterway) presents one of the greatest security problems in an OA. Route security operations are defensive in nature and are terrain-oriented. A route security force may prevent an enemy force from impeding, harassing, or destroying traffic along a route or portions of a route by establishing a movement corridor. Units conduct synchronized operations (reconnaissance, security, mobility) within the movement corridor. A movement corridor may be established in a high-risk area to facilitate the movement of a single element, or it may be an enduring operation.

(d) Critical infrastructure protection programs support the identification and mitigation of vulnerabilities to defense critical infrastructure, which includes DOD and non-DOD domestic and foreign infrastructures essential to plan, mobilize, deploy, execute, and sustain US military operations on a global basis. Coordination between DOD entities and other USG departments and agencies, state and local governments, the private sector, and equivalent foreign entities, is key in effective protection of critical assets controlled both by DOD and private entities. Vulnerabilities found in defense critical infrastructure shall be remediated and/or mitigated based on risk-management decisions made by responsible authorities. These vulnerability-mitigation decisions should be made using all available program areas, including AT, physical security, CBRN, FP, military deception (MILDEC), and OPSEC. While these programs are normally utilized as part of US homeland defense, they can also be utilized in long-term contingency operations. Not only can establishing a critical infrastructure program help to secure essential services for land forces and the civilian populations in early operational phases, it can also help with the transition to the HN.

(4) US Army theater security organizations. The US Army has several organizations specifically designed and equipped to conduct security functions.

(a) Among the Army's modular support brigades, the MEB performs maneuver support and joint security and protection tasks. MEBs are designed to provide protection capabilities and other support to the joint force to include:

1. Engineer.
2. MP.
3. CBRN.
4. Civil affairs (CA).
5. Air defense artillery.
6. Explosive ordnance disposal (EOD).
7. TCFs.

For more information, see FM 3-81, Maneuver Enhancement Brigade.

(b) Regional Support Groups. Army units specifically designed to serve as base headquarters and provide C2, to include oversight of security for temporary bases.

(c) Rear operations centers (area) may provide augmentation for base C2 and security management for critical bases and facilities.

For more information, see Army Doctrine Reference Publication (ADRP) 3-37, Protection.

i. **Maritime-Land Interface.** Bases established on a shoreline can present special advantages and challenges to those responsible for the functions inherent in the base's mission and for its defense. Challenges may include ports and harbors usually located in heavily populated areas.

(1) 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) Air Force base operating an APOD.

(d) Naval base supporting and sustaining fleet operations and/or maritime expeditionary security force operations, naval advanced logistic support site, and naval forward logistic site.

(2) **Coastal Riverine Force (CRF)**

(a) In support of the JFC's concept of operations in time of war or contingency, the CRF plans and conducts operations to provide strategic mobility and safe haven for US and MNFs in littoral areas and for sustainment of land operations. Additional CRF operations include port security, harbor defense, high-value asset security, intelligence-collection support, reconnaissance, and surveillance.

(b) **The JFC is responsible for maritime security.** This responsibility is exercised through the JFMCC, who will normally assign a harbor defense commander (HDC) to be in charge of maritime security forces for a defined operations area.

(c) The JFMCC may assign a coastal riverine squadron (CRS) commanding officer as sub-area operational commander as needed to support operations at a port or harbor. The CRS commanding officer may be assigned TACON of other Navy or USCG forces to support operations. These can include USCG PSUs, EOD detachments, and mobile diving and salvage units (MDSUs). This is particularly true along a coastline that has multiple ports in geographic proximity to one another. In this situation, the multiple ports may be designated a base cluster. The CRS commanding officer will coordinate security operations with the appropriate area or functional commander.

(3) **Defense Planning.** Friendly naval forces are the primary defense against waterborne threats and should achieve maritime 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 Operations.** The enemy may attempt amphibious operations using watercraft and/or aircraft. Likely beaches, landing zones, and insertion areas should be guarded, obstacles should be placed, and the mobile reserve employed to counter such operations.

(b) **Sea Mining.** Enemy mining of the seaward approaches to the base can be conducted from surface vessels, by air, or 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.** 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 should be prepared to locate and counter such threats.

(4) **Approaches to the Base.** Appropriate security and surveillance forces, backed up by capable MSFs, should be designated to cover every possible avenue of approach. These approaches include:

- (a) Beaches.
- (b) Concealed water approaches (fjords, bayous).
- (c) Rivers.
- (d) Drop zones and landing zones.
- (e) Land approaches.
- (f) Urban terrain and infrastructure (including underground water and sewage systems).
- (g) Piers, docks, and waterfront facilities.

(5) **Navy and USCG Organizations.** A HDC defends the harbor while inland defense is the responsibility of the appropriate area or component commander designated by the JFC. Close coordination should be conducted between the CRS commander and the seaport/marine terminal commander to avoid conflicts. The CRF may possess some or all of the following capabilities:

(a) **PSUs.** Rapidly deployable USCG units organized for sustained operations. They often operate under the Navy Expeditionary Combat Command and are embedded within the Navy's CRF. These units operate six-armed, 32-foot transportable port security boats. PSUs provide waterborne security, harbor surface interdiction response and point defense operations for strategic shipping and critical port facilities, and includes a shore-side security force for maritime infrastructure and FP. PSUs primarily support the naval coastal warfare mission of harbor defense/port security operations.

(b) **Naval 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) **Mine Countermeasures (MCM) Elements.** These elements detect and destroy enemy mines in harbors, approaches, and sea lanes, using MCM aircraft and vessels. Because of the small number of MCM forces, control of these assets is normally determined by the JFMCC.

(d) **MDSU.** The MDSU has the missions of underwater hull search and repair, channel clearance, vessel salvage, and pier and piling inspection and repair. The CRF commander can request this unit's support of base defense efforts from the JFMCC commander, when required.

(e) **Riverine Company.** The riverine company is the standard unit of action for the CRF. Companies are deployable, self-sustaining units that may operate independently or ICW other forces. Each company has two platoons with personnel assigned for boat operations, a security team capable of conducting visit, board, and search-and-seizure

missions, and an intelligence surveillance reconnaissance team capable of operating unmanned vehicles and squadron-level communications equipment. Each company is equipped with four green-water capable patrol boats and four riverine/harbor security boats.

(6) Factors that should be considered when planning the defense of a base on a shoreline include the type and nature of the threat as well as protection for sea approach chokepoints, tides and currents, water clarity and depth, pier clearance, lighting, use of patrol boats, communications, rail and highway entrances security, air and missile defense measures, security for individual vessels, and ADC.

j. **Air-Land Interface.** The threats to an active airfield may extend far beyond the surface area designated as a base boundary. To address these threats, the air component uses the planning construct of the base security zone to ensure that those ground threats and hazards that could impact operations are considered and planned for accordingly.

k. **Terrain Management and Infrastructure Development.** Effective terrain management and infrastructure development is critical to the success of JSO. The joint force must take advantage of security enhancement capabilities by using and enhancing available fixed and permanent installations, facilities, and fabrications. Infrastructure development focuses on facility security modification and damage repair in order to reduce the efforts that joint forces must make to heighten their base and LOC security posture. Additionally, use of HN manpower, medical support, equipment, and materiel should be maximized.

(1) **Terrain Management Responsibilities**

(a) The JFC has overall responsibility for terrain management in the OA and may assign specific terrain management responsibilities to subordinate commanders.

(b) **The JSC coordinates terrain management with component capabilities.** The JSC's primary terrain management responsibility is to advise commanders on the stationing of units and facilities in the JSA.

(c) **Component Commanders.** The JFLCC and JFMCC are responsible for terrain management within their AOs. They consider security when they position bases and station units and facilities.

(2) **Positioning Considerations**

(a) **Unit Positioning.** Factors affecting base and unit positioning include threats, the suitability and survivability of available facilities, and the subordinate unit's mission requirements. Component commanders and their staffs should use these factors and their own risk assessments to determine whether units should be dispersed or grouped for mutual support.

(b) **Facility and Supply Positioning.** Factors affecting the positioning of facilities and supplies include current threats and the requirements of the units operating or using the facility and supplies, the impact of the facility or supplies on the joint force mission and concept of operation, LOCs, and accessibility. Considerations include those described in Figure III-3.

Positioning Considerations

Clustering

Clustering of support activities reduces vulnerability to ground attack but can increase vulnerability to air, missile, and/or chemical, biological, radiological, and nuclear attack.

Location

Locating key facilities away from high-speed routes minimizes vulnerability to enemy ground penetrations but may also reduce accessibility to units requiring support.

Dispersal

Dispersal of critical supplies such as fuel, ammunition, and spare parts reduces the risk of loss but also reduces the ease and speed of distribution.

Figure III-3. Positioning Considerations

(3) **Infrastructure Development Responsibilities.** Joint forces deployed to developed areas should be able to use established infrastructure and existing facilities. Joint forces deployed to less-developed areas must rely more on austere new construction or temporary facilities IAW established base development criteria. HNS should be sought in both developed and undeveloped areas.

(a) **GCC.** The GCC is responsible for identifying the wartime facility and construction requirements for US forces. These requirements are coordinated with the Department of State and other USG partners, HN organizations, multinational partners, and relevant NGOs. During hostilities, the GCC specifies theater construction policy through the engineering support plan appendix for each operation plan.

(b) **JSC.** The JSC implements construction policy with due consideration to security concerns and requirements.

(c) **Commanders.** Commanders implement construction policy IAW JFC directives and guidelines to enable mission success and secure people, equipment, and facilities.

More information on base construction can be found in JP 3-34, Joint Engineer Operations.

1. **ADC.** ADC includes the measures taken before, during, and after hostile action or natural or manmade 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 combat support units, logistic units, tenant units, transient units, and HN units. **When an attack or natural disaster occurs, the objective is to continue regular operations by quickly restoring control, evacuating casualties, isolating dangerous areas, and replacing personnel and materiel losses.**

(1) **General.** Effective planning, clear delineation of responsibilities, and efficient use of assets help prevent and contain damage and rapidly restore operations.

(2) **Responsibilities**

(a) **JSC.** The JSC may advise commanders and staffs on ADC operations.

(b) **Area and Base Commanders.** Commanders are responsible for planning, prioritizing, coordinating, and executing ADC.

(c) **HN**

1. **Authority.** The HN, depending on applicable agreements, may have overall responsibility for ADC within its territorial boundaries. In these circumstances, US forces will retain responsibility for ADC within US base boundaries and be prepared to assist the HN with ADC operations outside US base boundaries.

2. **Assistance.** HNS agreements frequently address HN assistance for ADC operations. Commanders are usually single points of contact to coordinate ADC operations and should plan, coordinate, prioritize, and execute HNS for ADC IAW the JFC's priorities and concept of operations.

(3) **ADC Planning Requirements**

(a) **General.** ADC is executed at the lowest level. Base and base cluster security plans may have ADC annexes identifying responsibilities, priorities, requirements, and procedures for conducting ADC operations. These plans will be coordinated and integrated at the component and subordinate command levels to ensure rapid response and efficient use of limited ADC assets.

(b) **Specific Planning Responsibilities.** Base and base cluster ADC annexes should identify responsibilities and procedures required before, during, and after an incident. Plans should also include responsibilities for all units occupying the base or located in the base cluster that can make contributions to ADC. Examples include, but are not limited to, security forces, engineers, ordnance, EOD, CBRN contamination avoidance through reconnaissance, decontamination, CA, maintenance, medical support, communications systems, supply, and transportation.

m. **Integration of Joint Security and Logistic Operations.** Joint logistics integrates strategic, operational, and tactical level logistic operations. JSO are built on movement control, open LOCs, secure reception points, transshipment points, logistic bases, and obtaining HNS.

(1) **Responsibilities.** The JSC coordinates the overall security in the JSA and seeks joint security support of the joint force logistic concept of operations. **The JSC must coordinate with the JMC (if established) or other movement control agency on employment and joint security of all movements within the JSA.**

(2) Other Considerations

(a) **Medical Operations.** Enemy operations that interdict LOCs and disrupt sustainment activities could restrict medical support personnel capacity to retrieve and evacuate wounded, sick, and injured personnel and provide timely medical care.

(b) The JFC should employ a joint movement control agency, center, or cell to conduct joint movement control planning, coordinate actions and resolve issues, especially with the HN, and act as the lead for joint movement control functions. The JSC should establish liaison with the JMC through the JSCC to monitor movements in the OA.

For more information on joint movements and movement control, see JP 4-09, Distribution Operations.

n. **Detainee Operations.** Detainee operations can be critical to security. The JSC should consider detainee-related issues and develop plans and procedures to respond to these issues. Commanders at all levels must plan for and anticipate the capture of detainees. Commanders must ensure that all detainees are treated humanely and IAW US law, the law of war, and applicable US policy.

For additional information, see JP 3-63, Detainee Operations, and DODD 2310.01E, The Department of Defense Detainee Program.

o. **Personnel Recovery (PR).** PR is the sum of military, diplomatic, and civil efforts to prepare for and execute the recovery and reintegration of isolated personnel. PR is a system in which the objectives are to return the isolated personnel to duty, sustain morale, increase operation performance, and deny adversaries the opportunity to influence our military strategy and national will by exploiting the intelligence and propaganda value of isolated personnel. When JFCs and their staffs conduct mission analysis, PR should be considered as one of the means for mitigating risks. When the COM is responsible, PR will have to be planned and executed within HN sovereignty and COM authorities. Developing relationships and plans with the HN ICW COM increases the probability of the successful recovery of isolated personnel.

For more specific guidance on PR planning and operations requirements, see JP 3-50, Personnel Recovery.

5. Other Planning Considerations

The integration of US military capabilities, often with forces from other nations, other USG departments and agencies, NGOs, HN civil authorities, and HN security forces, requires effective and efficient JSO planning. **The JSC coordinates the security of bases and LOCs through the integration and synchronization of HNS, multinational operations, civil-military operations (CMO), and interagency coordination.** The JSC also considers the role of the DOD civilian work force and contractor employees, laws, agreements, and other legal constraints. The goal is to maximize the effectiveness of the base and LOC security forces through the proper employment of all security assets.

a. **HNS**

(1) The effective use of HNS enhances the capability of US forces to achieve success during military operations. Many HNs can provide valuable support to security operations. **The JSC and appropriate subordinate commanders must consider HN capabilities when planning and conducting security operations.** HN personnel and organizations can frequently perform many functions efficiently because of their familiarity with language, local customs, terrain, transportation and communications networks, facilities, and equipment. Much of this support may be provided by local organizations or personnel, secured through local procurement. HNS can be limited by the availability of resources and equipment. HNS can also be constrained by lack of interoperability with joint force equipment, insufficient HN capabilities, HN political issues and concerns, HN legal constraints (which can be similar to US Posse Comitatus Act restrictions), and lack of US and HN agreements concerning HNS.

(2) **Responsibilities**

(a) **JSC.** The JSC coordinates with commanders and the HN lead staff (if designated) to ensure that HN security assets enhance security of military forces and support the JFC's concept of operations.

(b) **Component Commanders.** Component commanders employ HNS IAW JFC directions and guidelines. When HNS security assets are available, component commanders should ensure that:

1. HN security assets dedicated to US forces are used and positioned to help defend bases, LOCs, and facilities and can support the JFC's current and future concept of operations.

2. US base and base cluster defense plans are coordinated with and complement HN security plans.

3. HN commands are advised of US forces' priorities for security.

(3) **Considerations. HNS is normally based on an HN agreement to provide specific support in prescribed conditions.** Agreements are made at various levels, including national, theater, subordinate joint force command, functional component command (e.g., JFLCC), Service component command, and the local unit. In general, HNS is highly situational and heavily dependent on both the operational capabilities of the HN and its support for US policies.

(a) **C2.** The degree of coordination between US and HN forces and activities depends on the type of HNS involved, the location, tactical situation, the political environment, and existing agreements. In some instances, forces from one command may be placed under TACON of the other. The USG coordinates its control of HN resources through local officials or HN territorial commands and defines control with treaties or HNS agreements. When an established US military structure is absent, the SDO assigned to the

US embassy country team will normally be the point of contact for US forces' coordination of HNS requirements.

(b) **Training.** US personnel at all levels should be trained to build relations with HN personnel, both on and off duty. Orientation should include HN government regulations, business practices, social customs, military procedures, religious customs, and language familiarity. HN units that help defend joint forces, bases, and LOCs should be kept safe and trained in security awareness, base security plans, and LOC security. Safety should be provided to those HN units charged with support of the defense effort.

(c) **HN Security Support.** Many HNs can and do provide extensive support for security-related activities. Specific types of HN security support are:

1. **Civilian Guard and Labor Service Units.** These units are usually in place during peacetime or developed after the commencement of hostilities. The use of civilian guards after hostilities commence will be on a case-by-case basis as directed by the GCC.

2. **Special Military Units.** These units perform specific wartime missions, such as guarding detainees and securing valuable facilities, materiel, or ammunition. Included in this group are HN MP units, which provide support but are not necessarily assigned or totally dedicated to US forces.

3. **Individual Military Personnel Units.** These HN personnel may be used as fillers for selected HN units that support security, or are directly integrated with US units, such as the Korean augmentation to the US Army in Korea.

4. **Paramilitary Units.** Some nations' police are paramilitary in nature, such as Belgium's Gendarmerie, and function in both civilian and military roles. They have significantly more utility for HNS in a hostile environment than normal civilian police.

5. **Light Infantry and Security Units.** Many HNs use these types of units as their primary security forces. They are frequently given both area and point security missions.

6. **Civilian Police.** These organizations frequently assist US MP and security forces during peacetime, but have significantly less capability during wartime.

7. **Intelligence Units and Agencies.** HNS intelligence organizations may help provide essential elements of information to the JFC's base and LOC security plan. Base commanders should ensure HN intelligence elements link with the JFC and other joint force intelligence staffs. HN agencies can be excellent HUMINT and CI sources. HN organizations can provide tactical intelligence on enemy ground, naval, and air forces, CI on foreign intelligence and security service threats, terrorist intentions and collection capabilities, and interrogation and debriefing reports from detainees, refugees, other returning dislocated civilians, and enemy sympathizers. HN intelligence personnel can add local and national cultural insight to intelligence assessments and data.

For more information on HNS see JP 3-57, Civil-Military Operations.

(d) **HNS in CBRN Environments.** When required, HN military, paramilitary, and selected civilians providing support are equipped and trained to operate in a CBRN environment. Training and equipping are normally national responsibilities. In the event of a CBRN incident, many types of HNS may be needed. The need of HNS may be due to limited CBRN defense supplies and/or CBRN units. Some of the types of HNS that can be requested are decontaminants, water, water transportation assets, CBRN detection devices, engineer digging equipment or units, and decontamination equipment or units.

For further information on CBRN defense measures, see JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear Environments.

b. Multinational Operations

(1) **Integrating MNFs into JSO.** The JFC coordinates with MNF and HN commands IAW existing agreements. In some instances or contingencies, the JFC will have access to the US ambassador and the country team for help in the coordination process. Intelligence and operations liaison between bases, base clusters, and higher headquarters is essential to develop security plans and execute defensive operations. Early and continuous liaison with MNF and HN and allied organizations, and with established MSFs, enables effective and coordinated action.

UNITED STATES AFRICA COMMAND SECURITY COOPERATION

Ghana Armed Forces along with US Army Africa concluded Western Accord 13 with a command post exercise June 24, 2013, at the Kofi Annan International Peacekeeping Center, Accra, Ghana. Western Accord 13 was a two part exercise that included academics and a command post exercise. In part one, participants received classes focused on collective tasks, functional and staff procedures in support of command and control of a peacekeeping operation based on real-world events. In part two, a brigade headquarters staff prepared and then executed its plan to move forces into a contested area, defeat terrorists, and restore basic essential services and the rule of law while setting the stage for national reconciliation. The command post exercise was the scenario-based portion of the exercise designed for the Economic Community of West African States (ECOWAS) to conduct peacekeeping and stability operations. Each staff member was led by a member of the ECOWAS to facilitate and demonstrate the unity between nations. In the scenario, the Armed Forces in Support of Mali Task Force received an operation order to assume responsibility for the eastern sector's unstable area in order to conduct security and stability operations. Scenarios were interjected to force the staff to communicate to solve problems. Approximately 13 countries and more than 200 personnel from ECOWAS and the United States, and observers from several neighboring countries, participated in the exercise.

SOURCE: United States Africa Command

(2) **C2 of US Forces in Multinational Operations.** The President of the United States always retains direct command authority over US forces. This includes the authority and responsibility for effectively using available resources and for planning, organizing, directing, coordinating, controlling, and protecting military forces for the accomplishment of assigned missions. It is sometimes prudent or advantageous, however, to place appropriate US forces under the operational control or TACON of a foreign commander to achieve specified joint security related military objectives. In making the determination to place US forces under the operational control or TACON of non-US commanders, the President must carefully consider such factors as the mission, size of the proposed US force, risks involved, anticipated duration, and ROE.

(3) **HN and MNF.** HN and MNF governments, represented by their military forces and law enforcement agencies, generally will have responsibility for many base and LOC security functions. The JFC will coordinate US MNF and HNS requirements with MNF and HN commands.

See JP 3-16, Multinational Operations, for more information on multinational operations.

c. **CMO.** CMO are the activities of a commander performed by designated CA or other military forces that establish, maintain, influence, or exploit relationships between military forces and indigenous populations and institutions by directly supporting the attainment of objectives relating to the reestablishment or maintenance of stability within a region or HN. These relationships facilitate military operations in support of US objectives. **CMO enhances HN civil authority and legitimacy and helps the local population understand and comply with military security measures.** CMO may help mitigate negative effects of JSO on the local population and minimize civilian interference with JSO. CMO may be applicable in all military operations and is particularly important during long-term stability operations. JSO impact on the local population should be addressed in planning. The JSC coordinates with the component commanders to ensure that they incorporate CMO procedures into all JSO. CMO should be planned and coordinated with multinational and HN forces, HN and local government officials, and the IGO and NGO community IAW the JFC's directives. This coordination facilitates unity of effort and conservation of resources while working toward accomplishment of the JSC mission. CA forces are trained to plan and conduct CMO and CA operations. CA can support the JSC through the establishment of a CMO center to coordinate with indigenous populations and institutions. The CA force plans operations to support a commander's CMO by identifying and mitigating civil vulnerabilities that may lead to instability and to prevent interference with JSO. It can provide interface and coordination directly with indigenous populations and institutions to facilitate the objectives shown in Figure III-4.

Additional information on CMO can be found in JP 3-57, Civil-Military Operations.

Objectives of Civil-Military Operations in Joint Security Operations

- Enhance base and line of communications security measures.
- Reduce civil interference with joint security operations.
- Reduce impact of joint security operations on the civilian population.
- Assist in the integration of civil security and defense assets.
- Facilitate humanitarian relief operations.
- Contribute to military information support operations development with information about individuals and groups in the operational environment, conditions affecting their behavior, and other factors by engagement with the local population.

Figure III-4. Objectives of Civil-Military Operations in Joint Security Operations

d. Interagency, IGO, and NGO Coordination

(1) Interagency coordination occurs between USG departments and agencies, including DOD, to accomplish objectives. Similarly, IGO and NGO coordination is between elements of DOD and IGOs or NGOs to achieve an objective. All levels of joint operations integrate US political and military objectives into unified action.

(2) The JSC, with the assistance of joint force CMO assets and reachback to the geographic combatant command joint interagency coordination group, integrates JSO with the activities of other USG departments and agencies, NGOs, IGOs, regional organizations, and the operations of HN forces and activities of various HN agencies conducting security operations in the GCC's AOR and/or the JOA. By understanding the interagency coordination process, the JSC will be better able to appreciate how the skills and resources of the various USG departments and agencies interact with NGOs, IGOs, and regional organizations to assist in the overall security posture of the joint force.

(3) **NGOs.** Where long-term problems precede a deepening crisis, NGOs are frequently on scene before the US military and are often willing to operate in high-risk areas. They will often remain long after military forces have departed. NGOs, who respond quickly and effectively to crises, can decrease the resources that a JFC would otherwise devote to an operation. NGOs range in size and experience from those with multimillion dollar budgets and decades of global experience in developmental and humanitarian relief to newly created small organizations dedicated to a particular emergency or disaster. The joint force may provide security for NGOs. This relationship is beneficial as NGOs often share common goals with joint operations.

For further information on interagency, IGO, and NGO coordination, see JP 3-08, Interorganizational Coordination During Joint Operations.

e. **DOD Civilian Work Force and DOD Contractor Employees**

(1) **General.** US forces often deploy for contingency operations with a significant number of supporting DOD civilians and contractor personnel. Their contributions to the force are critical to the success of today's joint operations. **The management, control, and security of the DOD civilian work force and contingency contractor personnel are a unique and significant challenge for the JFC, subordinate JFCs, and Service component commanders.**

(2) **DOD Civilian Work force.** The DOD civilian work force is made up of US citizens or foreign nationals hired directly or indirectly to work for the DOD, paid from appropriated or nonappropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent, or on-call positions. The DOD civilian work force should be prepared to respond rapidly, efficiently, and effectively to meet mission requirements for all contingencies and emergencies.

(a) Each DOD component should develop plans, programs, contingency and emergency manpower requirements, and a state of readiness, including organization infrastructure.

(b) **The DOD civilian work force will follow joint security policies and operational direction when deployed in support of military operations.** They should be processed and supported in the same manner as military personnel of their employing component, as permissible by law and existing SOFAs.

(c) **Responsibilities**

1. The JFC and DOD components should develop, maintain, and exercise civilian contingency and emergency plans and procedures to implement DOD planning guidance and policy, to prepare the DOD civilian work force for employment and deployment, to support all contingencies and emergencies rapidly, efficiently, and effectively. The GCC will establish DOD civilian work force accountability procedures to include names, numbers, locations, and status of deployed individuals. The GCC should also issue theater-specific admission requirements for DOD civilians and include summaries of civilian work force status in situational reports. GCC reports must comply with all requirements of DODD 1400.31, *DOD Civilian Work Force Contingency and Emergency Planning and Execution*.

2. The JSC should monitor DOD component and GCC compliance with all DOD civilian work force contingency and emergency plans and procedures to ensure that the proper level of security is provided to the DOD civilian work force.

(3) **Contingency contractor personnel** will provide support to US military forces during military operations. They include all DOD contract personnel and their subcontractor personnel, including US citizens, TCNs, and local national personnel who are hired by, and provide support to, US military forces in contingency operations under such contracts. **DOD contingency contractor personnel are separate and distinct from contractor employees working for the Department of State or other USG**

departments and agencies, even when their contracts are administered by a US military contracting agency. The JFC may have limited responsibility for the security of other USG department and agency personnel to include their contractors.

(a) DOD contingency contractor personnel include **system support, external support, and theater support** personnel. System support contractors and many external support contractor personnel deploy with the force and are referred to as CAAF. CAAF personnel often have a habitual relation with, reside with, and provide direct support to US military units. **CAAF personnel, for the most part, are treated similarly to DOD civilians in relation to joint security, AT, and FP programs.** They are, IAW their contract, required to abide by JFC and component AT and FP as well as other joint security related directives and policies.

(b) Non-CAAF personnel include theater support and some external support contractors, local nationals, and TCNs. These locally hired personnel often reside off base and will, in general, be provided incidental security support when they are working on a military base or in close proximity to US forces. Use of local national or TCN employees must be carefully considered from the base security perspective. **In some operational situations, the use of non-US citizen personnel can carry significant security, and even medical, risks. Commanders and the JSC coordinate vetting and access standards for HN and TCNs at all levels. In the absence of a SOFA, GCC specify vetting procedures for base access (biometrics and forensic screening, etc.) and requirements for unclassified network access by country.** Figure III-5 provides considerations related to the use of local national and TCN contract employees to support base operations.

**Base Security Considerations:
Use of Non-United States Contractor Personnel**

- Will these contractor personnel reside on base or live off base?
- If they live off base, what base access control measures are required?
- How will access be controlled to specific areas within the base?
- Is there a vetting and badging process in place? If so, who will enforce it and how?
- Will these contractor personnel be physically screened and/or searched in order to enter the base?
- Will armed escorts be required? If so, who will do this? How will this requirement be resourced?

Figure III-5. Base Security Considerations: Use of Non-United States Contractor Personnel

(c) **Responsibilities.** GCCs, subordinate JFCs, Service components, and DOD agencies:

1. Ensure that operational specific contractor policies and requirements are identified in appropriate plans and orders. This integrated planning includes the Service components and DOD agencies coordinating any proposed contractor support arrangements that may impact the operation plan or OPORD.

2. Ensure that the contract clearly and accurately specifies the terms and conditions under which the contractor is to perform, describes the specific support relationship between the contractor and the DOD, and contains standardized clauses to ensure efficient deployment/redeployment, management, protection, authorized roles of health service and other support, and sustainment.

3. Plan for security of contingency contractor personnel in locations where there is not sufficient protection. In appropriate cases, the GCC may provide security through military means, commensurate with the level of security provided to DOD civilians.

4. Monitor component compliance with contractor personnel contingency and emergency plans and procedures to ensure that the proper level of security is accorded.

(d) Security Considerations for Contractors

1. Area commanders, base commanders, and supported unit commanders are responsible for individual AT and FP support, and may have security responsibility for contractor personnel. To accomplish this task, area commanders should have oversight of all supporting contingency contractor personnel in their AO.

2. Contractors must comply with oversight organization policies stated in their contract and ensure that their employees follow all individual FP and PR security requirements. Contractors are expected to take passive FP measures for their safety and security. Also, contractors should require their deployed employees to take measures for self-defense, such as driving classes, carrying cell phones, and following procedures to report suspicious incidents.

3. Contingency contractor personnel may be armed for self-defense subject to US law and pursuant to DOD policy, HN, and international law, including SOFAs and international agreements. All requests for permission to arm contingency contractor personnel must be reviewed by the appropriate GCC's staff judge advocate (SJA).

4. Security contractors should not be used to protect US or coalition military forces, facilities, and supply routes in areas where major combat operations are ongoing or imminent, except as specifically authorized by the GCC. Security contractors may be employed to protect selected military assets in areas where major combat is not imminent or ongoing, if consistent with applicable US, HN, and international law, and relevant SOFAs or other international agreements.

5. The use of force by contingency contractor personnel is strictly limited by law and generally is not protected by SOFA provisions. The combatant command SJA must ensure that any use of contracted security forces to protect US military forces, facilities, and supplies is done IAW applicable US, international, and HN law.

6. CAAF and selected other contingency contractor personnel should, as a minimum, receive information on local and security procedures, be issued CBRN and other protection equipment (along with the requisite training), and travel and movement security support. Such training and equipment should be designated in the contract and be given before deployment at the designated deployment center. The JFC and component commanders or DOD agencies determine and execute operationally specific FP and general security training requirements for non-CAAF personnel.

7. The use of private security contractors (PSCs) has become common in contingency operations. During the planning process, guidance and procedures should be produced to include selection, training, accountability, equipping, and procedures for PSCs. PSC C2, ROE, and their roles and responsibilities should be addressed by the GCC in each individual theater, the terms of the contract, and the appropriate Service regulations. The J-3 has the responsibility to coordinate PSC planning across the staff and across all Service components. Additionally, the J-3 may have a subordinate element that has a coordinating role with JSO as it pertains to armed contractor oversight.

For more information, see Department of Defense Instruction (DODI) 3020.50, Private Security Contractors (PSCs) Operating in Contingency Operations, Humanitarian or Peace Operations, or Other Military Operations or Exercises, DODI 3020.41, Operational Contract Support (OCS), and JP 4-10, Operational Contract Support.

f. **Laws, Agreements, and Other Legal Constraints**

(1) Commanders at all levels should have access to professional legal advice with regard to the legal aspects of the use of force in security operations. Such legal advice normally comes from an SJA who observes the requirements of international law, US law, US policy, and HN law, all of which may regulate the status and activities of US forces during military operations. This section provides a very basic summary of principal legal topics that may impact JSO in theater.

(2) **Responsibilities**

(a) The **GCC, assisted by the SJA**, coordinates with commanders and staffs to ensure that JSO comply with the law of war, established ROE, US law, international agreements, and HN laws.

(b) **Component and Base Commanders.** Component and base commanders, assisted by their SJAs, are to disseminate JFC ROE to all members of the joint force in or passing through their AO or base. They disseminate laws, regulations, and procedures regarding treatment of detainees to appropriate US forces, and ensure that liaison is established with HN authorities to coordinate these actions. They ensure that legal representatives are available to assist US forces and to coordinate with HN authorities on such matters as HN logistic support to US forces, processing and detention of detainees, HN law enforcement capacity, and responsibility for ADC.

(c) The JFC may operate in a noncooperative HN, or have no HNS. Therefore, the JFC should be prepared to execute all JSA functions with or without HNS.

(3) **ROE.** ROE are directives, issued by competent military authority, that delineate the circumstances and limitations under which US forces will initiate or continue combat engagement with other forces encountered.

For more information on ROE, see Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.

(4) **US Law.** US forces, regardless of location, follow US law. US law is expressed in statutes and executive orders. DOD directives and instructions; Service regulations; and geographic combatant and component command directives, OPORDs and regulations; are all promulgated pursuant to these laws. US law also includes some international agreements to which the USG is a party. Persons serving with or accompanying the US Armed Forces in the field, including US citizens, USG civilian employees, and contractors, may be prosecuted for violations of US law under either Article 2 of the Uniform Code of Military Justice (during a time of declared war or contingency operation), or under the Military Extraterritorial Jurisdiction Act of 2000 if certain requirements are met. Joint force security directives issued by the GCC and by the component commanders are subject to applicable SOFAs or similar agreements. For specific publications, containing applicable US laws and SOFAs, contact the US embassy SDO or the GCC's legal adviser. Some SOFAs and similar agreements are classified.

(5) **International Agreements.** The Armed Forces of the United States are committed to conducting joint operations according to the applicable provisions of the law of war, including those of The Hague and Geneva Conventions. International agreements are the primary source of rules of international law applicable to US, multinational, and HN forces. One type of international agreement, and the most comprehensive, is a SOFA, which generally establishes the framework under which US military personnel operate in a foreign country, addressing how the domestic laws of the foreign jurisdiction shall be applied towards US personnel while in that country. However, these may be modified or become inapplicable in time of armed conflict. They proscribe most of the reciprocal rights, powers, duties, privileges, and immunities of the US forces to include DOD civilians and contractor personnel stationed abroad and of the governments of the host and allied/coalition nations and their respective armed forces. Other important types of international agreements concern security assistance and HN support agreements. For specific information on HN support agreements (e.g., acquisition and cross-servicing agreements) and international agreements (e.g., defense cooperation agreements), contact the US embassy military SDO or GCC's legal advisor.

(6) **HN Laws.** HN laws apply to individual members of US forces in the HN, unless those laws are specifically modified or made not applicable to US forces by the terms of an international agreement, such as a SOFA. US commanders, legal advisers, staff officers, DOD civilians, and Service members must understand the applicability of HN laws to personnel and operations, as well as the relationship between HN laws and US laws, policies, and regulations.

Intentionally Blank

CHAPTER IV JOINT SECURITY OF BASES AND LINES OF COMMUNICATIONS

“Rear guards are the safety of armies and often they carry victory with them.”

**Frederick the Great
Instructions to his Generals
1747**

1. Introduction

The JFC, with or without a formally designated JSC, assigns and controls forces that are responsible for executing base and LOC security operations. **A proactive security posture is essential to JSO.** Security forces must be trained, organized, and equipped to execute base and LOC security against Level I and II threats, and be prepared to engage Level III threats. This chapter provides guidance for base and base cluster security operations, discusses defensive considerations against Level III threats, and explains LOC security operations and the integration of LOC security actions with joint movement control operations.

2. Tenets for Joint Security Operations

The tenets for JSO include knowledge of the enemy, unity of command, economy of force, and responsiveness. These tenets are discussed in Figure IV-1. Well-trained forces to provide a timely and often immediate response to threats are equally important.

3. Base and Base Cluster Operations Overview

The JSC coordinates with the base and base cluster commanders to capitalize on Service or functional components combined capabilities and to minimize collective vulnerabilities.

a. **Base.** A base is a locality from which operations are projected or supported. **At the base level, the component in command of the base has overall responsibility for the security of everything within the base boundary.** Tenant units normally secure their own facilities within the base, but also provide select forces for base defense. The base commander normally exercises TACON over those forces.

b. **Base Cluster.** A base cluster is a collection of bases, geographically grouped for mutual protection and ease of C2. The base cluster commander will be appointed by the JFC or designated representative and may be the next higher tactical C2 headquarters of the base, the senior base commander, or another designated base commander, depending on the situation. There is no fixed number of bases in a base cluster, but typically a base cluster contains two to seven bases. **The JFC, normally through the JSC, designates each base cluster.**

c. **Base Security Forces.** A base security force **is a security element established to provide local security to a base.** It normally consists of the combined dedicated and on-call forces assigned or attached and those forces from tenant units attached with specification of

Tenets for Successful Joint Security Operations

Knowledge of the Enemy

Knowledge of the enemy's identity, capabilities, vulnerabilities, and likely intentions is essential to prepare for combat operations, prevent surprise, and protect the joint security area.

Unity of Command

Unity of command is the cornerstone for uninterrupted support of the main effort and the protection of the joint security area. It requires coordination and cooperation toward the common goals with the joint security area. It may be achieved by the joint force commander through the joint security coordinator, area commanders, base cluster commanders, and base commanders.

A tactical combat force, if required, is normally employed by a component commander or another commander as directed by higher authority. The tactical combat force will normally operate in a specified operational area within the joint security area.

Economy of Force

Defense of the joint security area should not significantly detract from the overall joint force mission.

Consequently, only the minimum means necessary to accomplish the joint security area defense should be committed.

Responsiveness

Responsiveness requires immediate reaction and rapid deployment of sufficient combat power to destroy the enemy and area damage control resources to minimize damage.

Responsiveness is enhanced by timely intelligence and reliable communications.

Figure IV-1. Tenets for Successful Joint Security Operations

TACON for base defense or security operations. It may also include an MSF consisting of MP, Air Force security forces, or combat arms units. The mission of the base security force is to counter Level I and II threats. **The base commander normally appoints a base security force commander to execute FP, security, and defense functions within the base boundary. This individual will plan and execute all base security IAW the base commander's guidance. The base commander tasks units located within the base to provide personnel, equipment, and materiel to form or augment the base security force.**

d. **C2 Considerations.** The area commander, normally a combat arms land force commander, is responsible to provide security support to all bases and base clusters (if designated) within the command's AO. This responsibility will often include bases that are commanded by organizations not part of the area commander's forces. The base cluster commander has direct responsibility for area security within the assigned cluster. In cases

where the isolated base commander has no dedicated land combat arms forces, the base commander, ICW the JSC, should normally form an MSF capable of conducting area security operations needed to protect the base. This may entail operations outside the base boundary. In all cases, command arrangements and joint security operation directives, orders, and policies must be clearly established for all anticipated situations. The following diagrams in Figure IV-2

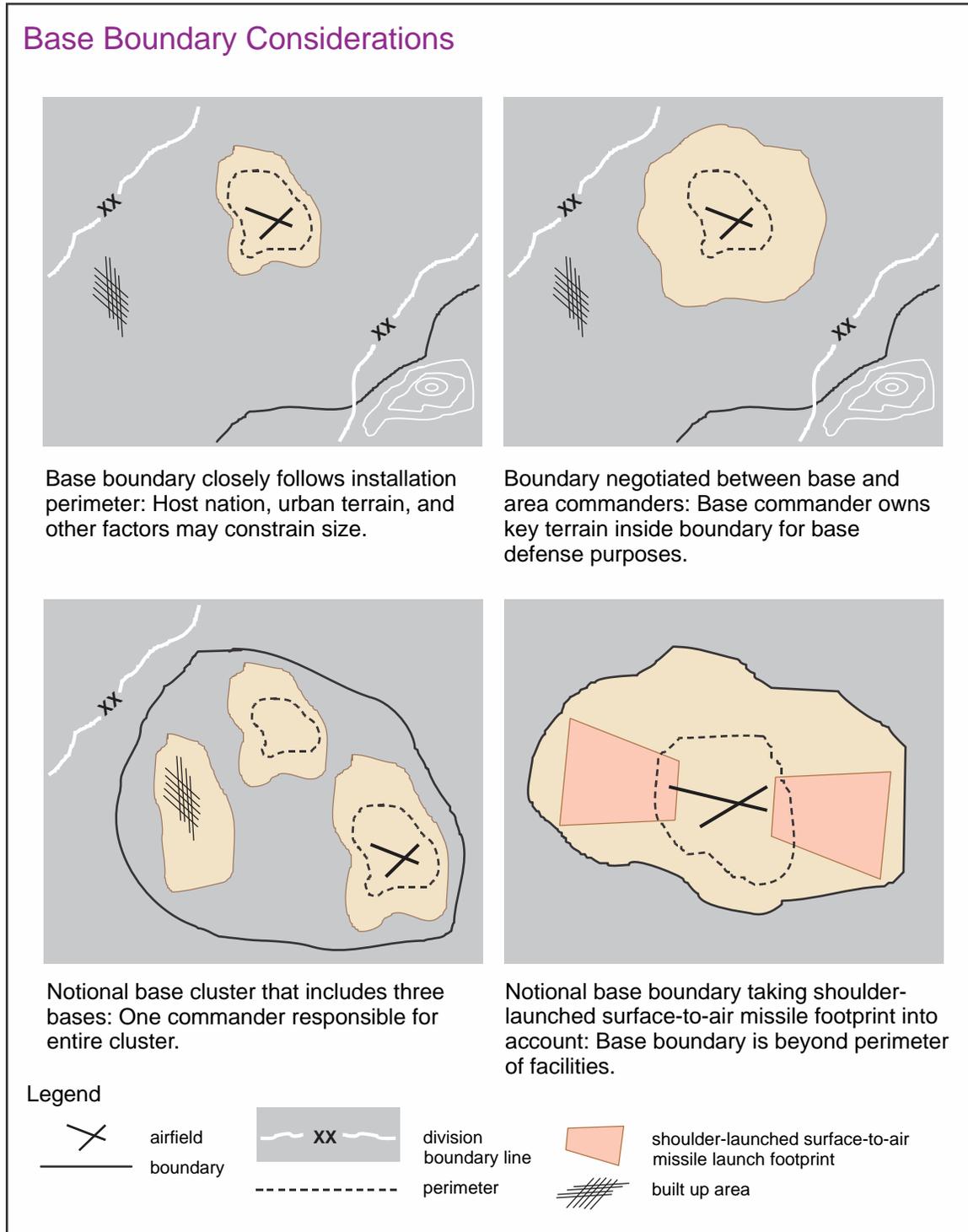


Figure IV-2. Base Boundary Considerations

illustrate a number of considerations for establishing the base boundary. When HN, urban terrain, and other factors constrain the size of the base boundary, the base commander must coordinate/integrate proactive security operations with the area commander or HN to counter the threat of standoff attacks or assume the risk.

e. **Work Priorities.** Base and base cluster commanders must set priorities for tasks involved in base security. Work may occur on several concurrent tasks. Figure IV-3 reflects some key base security work priorities.

Base Security Work Priorities

- Prepare a base security plan.
- Establish appropriate perimeter standoff, based on threat and host nation situation.
- Establish vehicle and personnel entry points and search areas.
- Establish access control processes, badges, and local national labor and visitor control procedures.
- Construct personnel survivability shelters in vicinity of work centers, living areas, and recreation facilities.
- Establish attack warning systems (including alarms, codes, actions, and means of population education).
- Integrate host nation or coalition forces as required.
- Establish mass casualty procedures and capabilities.
- Develop a joint coordinated fire plan.
- Conduct rehearsals.
- Establish/coordinate active security patrols within the base boundary to deny the enemy freedom of action.
- When defending airbases, establish man-portable air defense system suppression patrols and response capabilities to deny the enemy terrain from which to engage aircraft landing/taking off. This will be done within the base boundary or in coordination with the area commander.
- Establish procedures for 100 percent personnel accountability and subsequent reporting of personnel missing or unaccounted for.

Figure IV-3. Base Security Work Priorities

4. Base Security in Level I and Level II Threat Environments

a. **General.** Base and base cluster commanders develop security plans to organize base security operations. **Successful security depends on an integrated and aggressive plan consisting of on-call base security,** dedicated security forces, base or base cluster MSFs, and ADC response services (medical, firefighting, and engineer). Actions against enemy

threats and other potential emergencies, to include natural disasters and accidents, must be planned for and adjustments to base or base cluster security plans made. Drawing from the units available, commanders organize security forces within their bases and base clusters. The base commander integrates the base security plans with those of the base cluster.

(1) Base security forces should be able to conduct escalation of force from warning, to nonlethal capability, to a high degree of direct-fire lethality to cope with potential threats. This may include a mixture of nonlethal weapons, small arms, automatic weapons, and antitank systems. The MSF should be able to coordinate for indirect fire support, have a high degree of tactical mobility, and a reasonable span of C2. A base security force should be able to:

(a) Conduct reconnaissance patrols to detect and report the location, strength, and capabilities of enemy forces located near the base, and both landward and seaward if base is at a seaport.

(b) Develop fighting positions within the base from which enemy advances can be stopped or destroyed.

(c) Plan and conduct patrols to deny the enemy key terrain from which to conduct standoff attacks.

(d) Utilize intelligence products to assist in the planning, coordinating, and executing of proactive combat operations.

(e) Use the MSF to attack small enemy units threatening the base from within the base boundary.

(f) Provide internal security for critical capabilities and mission-essential assets located on the base.

(g) Understand established fire control measures to prevent friendly fire incidents within the base and between the bases and base clusters, as well as with other forces operating outside the base perimeter, to include the TCF, MSF, and HN security forces. In addition, the likelihood of civilians and infrastructure in the area around the base should be properly considered when deciding upon courses of action.

(2) The MSF commander must have the most up-to-date copy of the base defense plan and, when applicable, base cluster defense plan to effectively coordinate between the base and MSF operations. This coordination occurs through the BDOC and BCOC, if established. The MSF commander coordinates with the base to ensure that he understands the base defense plan, to include methods of contacting the BDOC or BCOC, including call signs and frequencies. Base defense plans and layouts should include the following:

(a) Positions of mission-essential internal assets, external coordination points, and no-fire areas.

(b) Locations of any obstacles or mines near the base.

- (c) Locations and directions of fire of crew-served weapons.
- (d) Locations of target reference points and preplanned fires.
- (e) Locations of OPs employed by the base.
- (f) Signal for final protective fires.
- (g) Procedures to obtain fire support and clearance of fires.
- (h) Sensor and patrol plans.
- (i) Closest medical treatment facility.
- (j) Location of CBRN collective protection facilities and decontamination sites.
- (k) Location of ammunition supply point.
- (l) Procedures to obtain aviation units tasked to respond to incidents.
- (m) Communications plan.
- (n) Integration of nonlethal weapons to support the use of force policy.
- (o) Plan for PR.

(3) The composition and size of a MSF will vary. The nature and size of the threatening enemy force influences the size and number of MP, security forces, or land force combat arms elements that make up the MSFs. Base and base cluster commanders, ICW the JSC, consider the following:

- (a) The priority of ongoing operations.
- (b) The criticality of the base under attack.
- (c) The amount of time needed for friendly elements to consolidate.

(4) The base commander, ICW the area commander, continuously assesses the situation and, if appropriate, requests commitment of more MSF assets to handle the threat.

b. **Control Measures.** Control measures in base and base cluster security operations are the same as those used in defensive operations. The JFC designates bases and base clusters. **The area commanders/base cluster commanders coordinate base boundaries, establish phase lines, contact points, objectives, and checkpoints as necessary to control the base clusters.** These control measures include fire support coordination measures (FSCMs) employed to facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces in and around the base and base clusters. No-fire areas may be required to protect civilians, prevent disruption of sustaining operations, or protect combat

outposts, OPs, and patrols. All control graphics are coordinated with HN agencies to minimize interference, misunderstandings, and collateral damage. The base commander designates target reference points and sectors of fire for organizations located within the base boundary. All fires within the OA will be coordinated among all affected organizations. These measures decrease the likelihood of friendly fire incidents, prevent noncombatant and civilian casualties, and minimize damage to the property of friendly civilians. The area commander normally designates reconnaissance and patrol areas to provide area security outside the base boundaries, as necessary. MSFs should conduct aggressive patrols, and develop and occupy defensive positions in these areas to counter enemy attacks. The objective is to provide the base additional early warning, deter enemy actions, and, if possible, defeat enemy elements operating in the base cluster. MSFs should be assigned to cover all likely avenues of approach, areas likely to be used to launch stand-off weapons, and other key terrain.

c. Base Security Tactics

(1) **Defense Against Penetrating Attacks.** Perimeter primary 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, security forces must delay the enemy until the MSF can respond. The base's MSF may be used to reinforce threatened areas, to block enemy penetrations of primary security positions, or to counterattack to regain lost security positions or destroy the attacking force. The MSF should be mounted in vehicles that provide as much personal protection as possible. Security forces should be equipped with reliable communications and should have sensors and devices to compensate for capability loss during periods of limited visibility. Active and passive security and surveillance sensors and devices include but are not limited to closed circuit television surveillance kits, forward-looking infrared and thermal imaging systems, unattended ground sensors, and intelligence collection assets such as the aerostat (blimp) and UASs. Aviation and naval support may be requested to augment the capabilities of base security forces and enhance reconnaissance and surveillance operations. Sensors and defensive positions are employed on the base boundaries to provide indications and warning or detect and defeat the enemy. Joint fires are planned in detail to ensure the synchronization and integration of joint fire support capabilities, in support of the base defense and MSF. Forces (augmentation and selectively armed personnel) may be directed to secure facilities within the base vital to performance of the base's mission. Examples are the BDOC, ammunition storage areas, and aircraft revetments. Security forces require careful fire control to prevent friendly fire incidents.

(2) **Defense Against Standoff Attacks.** Standoff attackers are a fleeting target. Level I and II threats depend on blending in with the legitimate populace and revealing themselves as combatants only when they engage in a hostile act. It is not feasible to catch every terrorist or guerrilla before they act, so the best practice is to shape the base security environment with robust defense operations within the base boundary.

(a) These proactive combat operations deny the enemy key terrain; disrupt enemy planning, reconnaissance, and organization; detect the enemies as they move into position; and posture forces to quickly neutralize detected forces.

(b) Robust tactical real-time intelligence-collection assets within the base boundary can also act as a force multiplier to cue joint fires and forces. Some of these tactical intelligence-collection assets may also need to be located outside of the base boundary to provide early warning of threats and to request area commander combat power to counter threats.

(c) For imminent threats originating outside the base boundary when the area commander is not able to assist due to competing priorities, the base commander must either use base security combat power to counter the threat with the permission of the area commander, or assume the risk from enemy standoff attacks.

(d) The HN may also limit the base commander's ability to counter standoff attacks. In such cases, the use of joint patrols and/or liaison officers may allow the base commander to affect their battlespace. Inability to adequately defend the base as a result of HN limitations on the base boundary must be communicated up the chain of command to revise existing agreements or accept the risk.

d. Other Base Security Considerations

(1) **Direct Fire Weapons Systems.** The base and/or port security force commanders should try to maximize the effectiveness of all available organic direct fire weapon system capabilities. Heavy direct fire weapons (often limited to heavy machine guns and automatic grenade launchers) must cover the most likely avenues of approach and have sufficient fields of fire to employ the weapons effectively and efficiently. If possible, in-place live-fire training should be conducted. Often, civil considerations may limit the commander's authority to clear fields of fire and to conduct live-fire training, especially if the base is adjacent to a major urban area.

(2) **Antiarmor Weapons.** Forces performing base security actions generally have few organic antiarmor weapons. Antiarmor weapons, including tanks, will be positioned to cover the most likely high-speed avenues of approach in mutually supporting positions. The base defense plan will assign positions for augmentation forces possessing antiarmor weapons.

(3) **Indirect Fire Systems.** Mortars, field artillery, and even naval surface fire can support the base security effort. In Level I and II threat environments, mortars are often the most readily available and most responsive indirect fire weapons systems.

(a) **Fire Support Planning.** The BDOC fire support officer is the focal point for the planning of indirect fires for base security. The BDOC fire support officer coordinates with the supporting fires cell or fire support coordination center (FSCC). Designated or planned targets should include areas likely to be used as locations for standoff weapons and likely enemy avenues of approach. **These targets should be planned to minimize collateral damage and civilian casualties.** Copies of fire support plans and target lists must be provided to the headquarters controlling the fire support assets. Targets may be planned outside the base boundary after coordination with the headquarters

responsible for the area concerned. The BDOC and FSCC will ensure that all fire missions are properly coordinated to prevent the possibility of friendly fire incidents.

(b) **FSCMs.** FSCMs 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 missions by friendly fire.

(c) **Observers.** Joint fires observers should be identified on each base to ensure sufficient fire support coordination.

See JP 3-09, Joint Fire Support, for additional information on fire support planning and FSCMs.

(4) **CAS.** The supporting fires cell or FSCC will maintain contact with the appropriate air control system to request CAS for base security efforts. Effective employment of CAS is dependent on the presence of qualified joint terminal attack controllers within the MSF. When available, fixed- and rotary-wing aircraft and UASs may be used to extend the range of observation and provide immediate combat response to threats. UASs may also be used to provide:

(a) Intelligence, surveillance, and reconnaissance.

(b) Armed surveillance and armed overwatch, to include area security as well as movement support (convoy security, mine, and IED detection).

(c) Targeting: target detection, identification, acquisition, target designation, and battle damage assessment.

(d) Communication support: voice and data communication relay.

(e) Attack, strike, and engagement.

(f) Logistics support: cargo (aerial delivery and recovery).

(g) Support to forces conducting both casualty evacuation and medical evacuation.

For further information on CAS and UAS employment, refer to JP 3-09.3, Close Air Support, JP 3-30, Command and Control for Joint Air Operations, and Army Tactics, Techniques, and Procedures (ATTP) 3-04.15, UAS Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aircraft Systems.

(5) **Other Aviation Support.** The BDOC and BCOC, with other C2 centers, coordinate other aspects of aviation support. Examples include air reconnaissance of the base or base cluster area and air movement of base security. They may also coordinate to manage air support priorities and diversions for emergency resupply, personnel augmentation, and evacuation.

(6) **Coastal and Harbor Security Support.** The supporting CRF commander will maintain contact with the maritime component commander to provide waterborne and shore security for seaports and bases that are adjacent to navigable waters, excluding air and missile security. When available, USCG security resources and Navy CRF may be used to extend the range of observation and provide immediate combat response to waterborne threats.

(7) **Vulnerability to Release of TIMs.** Base security planners must consider the threat of personnel TIM exposure due to TIM attack or accidental TIM release from adjacent industrial facilities such as chemical plants or nuclear power facilities. Establish communications with industrial security forces for these facilities and a process for immediate notification of TIM release.

(8) **Barriers, Obstacles, and Mines.** The commander directs the construction and improvement of perimeter barriers. This includes establishing clear fields of fire and implementing physical security measures such as checkpoints on vehicle and pedestrian routes leading onto the base, and PSUs boarding suspect vessels. Concrete barriers, natural obstacles, and aggressive offensive actions can deny enemy access to the area immediately surrounding the base. Keeping the enemy at a distance degrades their ability to launch damaging attacks against the base. The commander should continue to direct improvement in the base defense, as time and other resources permit, to ensure a stable security system. Obstacles must be kept under observation and covered by direct and indirect fires. 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 will be ineffective against higher-level threats. The use of mines will be very limited, if authorized at all.

See JP 3-15, Barriers, Obstacles, and Mine Warfare for Joint Operations, for more information on barriers, obstacles, and mines.

(9) **Physical Facilities.** Commanders must stress continuous upgrading of base physical security. Activities occupying fixed bases will have opportunities to install sophisticated security equipment not available to units in mobile bases. Hardening of high-value areas within the base must be planned for, resources must be obtained, and actions carried out. Plans for base construction must consider ADC, fortification, survivability, and barrier/obstacles. JP 3-07.2, *Antiterrorism*, provides a discussion and guidance for the development of design basis threats. Design basis threats are the baseline type of threat against which an asset must be protected and upon which the building, structure, or protective system is designed to withstand.

For more information on building standards, see Unified Facilities Criteria (UFC) 4-010-01, DOD Minimum Antiterrorism Standards for Buildings.

(a) **Intrusion Detection.** Defenders can place sensors on likely avenues of approach, locating them at the limits of the defense or outside the defense if coordinated with adjacent commands. Directed ground and sea surveillance radar and airborne forward-looking infrared systems, if available, can improve the detection of intrusions.

Remotely monitored sensors, trip flares, binoculars, night vision devices, UASs, and other nonlethal warning devices can also be useful. Dummy sensors at OPs and concealed surveillance resources also should be considered.

(b) **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. Perimeter roads on either side of the fence improve observation. A combination of concertina wire, lighting, surveillance cameras, and intrusion sensors enhances base security. Observation sites in guard towers or atop buildings can increase the surveillance capabilities of perimeter guards. In urban areas, leveling of adjacent buildings may be required, but these types of measures must be carefully weighed against the potential negative impact that they may have on the local civilian population.

(c) **Entrances.** The base should have as few entrances as possible. These entrances should meet existing JFC guidance and other published FP requirements. Control of the entrances must be balanced against threat and base mission requirements.

(d) **Working and Living Areas.** Buildings housing personnel and sensitive equipment should have adequate standoff from the perimeter as required by combatant command's standards and the UFC. Shelters with reinforced and sandbagged roofs should be near all working and living areas, to serve both as shelters and fighting positions.

For more information on building standards, see UFC 4-010-01, DOD Minimum Antiterrorism Standards for Buildings, and the applicable Corps of Engineers guidance sheets.

(e) **Medical Treatment Facilities.** Medical treatment facilities should be located and marked IAW the provisions of the Geneva Conventions. Medical units must not be used in an attempt to shield military objectives from attack, and, where possible, should be sited so that attacks against military objectives do not imperil their safety. Base or base cluster commanders may direct otherwise only in circumstances dictated by operational imperatives, but must seek authorization through the chain of command. Medical treatment facilities may be guarded by a picket, placed forward to warn/delay/deter, by sentries, or by an escort. However, the guards are to protect patients and medical personnel from marauders and bandits. Medical personnel are noncombatants and therefore shall not be employed in any combatant related duties.

(f) Base physical security plans must ensure adequate protection for mission essential vulnerable areas and task mission-essential assets.

(10) **OPSEC and MILDEC in Support of Security Operations.** OPSEC and MILDEC are integral to plan and execute JSO. OPSEC and MILDEC can cause the enemy to act using misinformation, and lead to tactical, operational, or even strategic errors. Exploitation of those errors can degrade enemy plans and operations, thus improving base or base cluster security. OPSEC countermeasures must be continual and effectively guarded to avoid compromise. Friendly security forces should not establish

observable patterns, unless those patterns are part of a MILDEC plan. MILDEC can provide critical support to JSO, but only if they are credible to the intended audience. Since MILDEC is intended to occur with enemy observation, the commander should design deceptive actions which are both credible and observable.

For more information on OPSEC, see JP 3-13.3, Operations Security. For more information on deception, see JP 3-13.4, Military Deception.

(11) **Riverine Operations.** Rivers and other inland waterways provide significant transportation routes in much of the world. As such, security forces throughout the JSA may be called upon to either secure a river or inland waterway or utilize the waterway to secure the JSA itself. Additionally, riverine forces may be required to provide LOC security.

(12) **Nonlethal Weapons Systems.** Nonlethal weapons provide joint forces with additional escalation-of-force options short of lethal force. These weapons should be fully considered in any base security plan to help minimize civilian casualties and property damage. A variety of nonlethal weapons can help joint forces determine the seriousness of the threat, deny access, and suppress enemy threats by disabling personnel and equipment, particularly in Level 1 threat environments. Nonlethal weapons must always be covered by lethal weapons in case they fail to dissuade the threat. The successful accomplishment of any operation in which nonlethal weapons are employed requires extensive preparation, of which individual and unit training are vital.

(13) **Insider Threat and FP Considerations in Working with HN Security Forces.** In counterinsurgency and stability operations, US forces are often faced with unconventional enemy tactics. Joint forces frequently provided advisers to HN security forces in Operation IRAQI FREEDOM and Operation ENDURING FREEDOM to build HN capacity and enable the drawdown of US and coalition forces. The advisers' close proximity to undisciplined, and often culturally conflicted, HN security personnel left them vulnerable. Even major cooperative operations were exploited by extremists to attack friendly forces. Insider attacks have come within base perimeters, on joint patrols throughout the AO, and inside HN security facilities. In these instances, capabilities like biometrics screening and forensics exploitation of captured insurgent materials and facilities may provide additional defense mechanisms to insider threats. When developing and implementing FP plans and measures, I2 capabilities may be required to counter and deter insider threat strategies and tactics.

AFGHANS IN UNIFORM ATTACKING THEIR COALITION PARTNERS

In 2012, the US Government's Special Inspector General for Afghanistan Reconstruction reported that 15 percent of US casualties from hostile action came in the form of Afghan police and soldiers turning their guns on their allies, commonly referred to as "green-on-blue" attacks. In 2012, 62 coalition deaths were attributed to green-on-blue attacks, with 32 being US personnel. This accounted for more than 11 percent of all US casualties in 2012.

Three green-on-blue incidents occurred within one week of media reporting identifying US Soldiers' disposal of Qurans in a military burn pit in February 2012. These attacks left six US personnel dead, including a US Air Force Lieutenant Colonel and US Army Major shot inside the Afghan Interior Ministry. This incident prompted the North Atlantic Treaty Organization (NATO) Commander to temporarily suspend all non-mission-essential advisory missions, calling into question the entire NATO strategy to transition the Afghan force's lead security.

Although in 2013 the number of these incidents decreased, they have continued to impact the advisory mission and, in turn, the transition to Afghan control. While it is unclear what percentage of these attacks were actually conducted by the Afghan National Security Force, they present a unique challenge to the advisory mission and host nation security cooperation as a whole.

Various Sources

5. Countering Level III Threats

In some operations the JFC must plan for combat operations in the JSA. Area commanders assigned a JSA in their AO will develop TCFs or PSUs to decisively concentrate combat power. Defeating Level III threats in the JSA will enable support bases to sustain operations. Area commanders must also ensure that joint forces take active and passive measures to protect US forces and equipment.

a. **General.** Enemy forces infiltrating or penetrating friendly positions and moving into the friendly OA, or conducting airborne, air assault, or amphibious operations, are some sources of Level III threats. The designated land force commander may establish a TCF to deal with these types of threats, designate another force as the on-order TCF, or accept the risk of not designating a TCF. The commander may establish a number of TCFs IAW the Level III threat and the JFC's guidance. Designating more than one TCF provides greater flexibility to respond to multiple threats. The primary advantage of dedicated, rather than on-order, TCFs is that TCFs can plan and prepare for one mission. Another advantage is that dedicated TCFs build stronger liaison and more consistent communications with supported bases and base cluster BDOCs and BCOCs. It also allows the dedicated TCF to rehearse its plans. When the designated commander assigns a subordinate unit an on-order TCF mission, they establish criteria that trigger the unit's TCF mission. Knowledge of the enemy, unity of command, economy of force, and responsiveness are essential to enable the TCF to counter Level III threats.

b. **TCF.** The area commander may designate a TCF to respond to Level III threats and protect the forces in the JSA. The area commander decides the composition of the TCF after weighing the risk of allocating forces to the TCF and thus decreasing the combat power available elsewhere. In large JSAs with dispersed bases and base clusters, the TCF must be capable of moving by air and ground to speed reaction time. A TCF typically consists of infantry, Army or Marine Corps aviation (attack and utility helicopters), augmented with combat engineer and field artillery support. The commander may also organize a TCF with armored cavalry, armor, mechanized infantry units, naval attack aircraft and boats, and vessels providing naval air and surface fire support. A TCF should have sufficient combat and combat support assets. A TCF may be supported by:

- (1) Military intelligence.
- (2) Field artillery.
- (3) Engineers.
- (4) Army or Marine Corps aviation (e.g., attack, air assault, C2, and special electronic mission aircraft).
- (5) MP/security police.
- (6) CAS/close combat attack.
- (7) Air defense artillery.
- (8) Area signal nodes.
- (9) Navy and USCG vessels and aircraft.

NOTE: These assets are limited and may be engaged in other missions, and not immediately available to the TCF. The force conducting the JSA security mission may also receive support from other US and/or MNFs, including the HN.

c. **Responsibilities of the JFC.** The JFC's combat actions in the JSA are designed to synchronize US, multinational, and HN forces. If a TCF is designated, the JFC (or designated representative) provides guidance to the component or area commander assigned responsibility for TCF employment.

d. **Responsibilities of the commander assigned the JSA within an AO.** The commander responsible for the security of the JSA will normally exercise TACON over the TCF. He ensures the TCF is properly established, trained, and supported. This commander normally will be responsible for coordinating TCF actions with subordinate base cluster and commanders within the JSA.

e. **Responsibilities of the TCF commander.** The TCF will normally be under the C2 of the commander assigned the AO in which it is operating. MSFs designated by the JFC in the designated OA may be placed under the TACON of the TCF commander. The TCF

commander may also receive TACON of transient forces in an emergency, as directed by appropriate higher headquarters and IAW guidance established in JP 1, *Doctrine for the Armed Forces of the United States*. In addition, the TCF commander may receive joint fire support as directed by appropriate higher command.

f. **Base Security in Level III Threat Environments.** Bases are often very difficult to defend against Level III threats. When there is the possibility of a Level III threat against a base, extraordinary action may be required. These actions could include, but are not limited to:

- (1) Significant additions to MSF capabilities.
- (2) Employment of additional barriers and mines outside and around the base boundary.
- (3) Developing extended, in-depth individual defensive positions.
- (4) Increased training and rehearsal of base defense actions, to include rehearsal of MSF and TCF coordination.
- (5) Enhanced fire support.
- (6) Increased port security patrols.
- (7) Improved integrated air and missile defense.

g. **Coordinating Base Defense and TCF Actions.** During Level III operations, the area commander retains overall C2 for security within the JSA. However, ICW the base or base cluster commander, the area commander may delegate TACON over selected security forces located in the OA to the TCF commander, excluding air defense forces, which remain under the JFACC or AADC. These forces are used to delay and disrupt Level III threats, protect the flank of a TCF, or allow a base the time to establish security in greater depth. Some base security forces necessary for the protection of mission-essential base assets may remain under the control of the base commander. MSF units within the base perimeter work closely with the BDOC/BCOC to synchronize the security plan. BDOCs and BCOCs establish and maintain contact with the tactical operations center of the area commander or the TCF, as ordered. Upon notification by a base or base cluster commander through the BDOC or BCOC that a threat exceeds a base's security capabilities, the area commander may commit the TCF. The area commander will determine C2 relations between the security forces or TCF, and the base security force, based on the situation, as well as determining whether other arrangements should be modified.

REAR AREA SECURITY IN RUSSIA 1941-1944

From June 1941 to July 1944, the German army fought on Russian soil. During the entire period, the Germans were faced with the problem of fighting Russian partisans (irregular forces) to hold open their lines of communications [LOCs] and vital base areas. The German anti-partisan warfare went through three phases: (1) The German offensive of summer/fall 1941, (2) The Soviet counteroffensive winter of 1941/42 and following German offensive ending August 1942, (3) German defensive battles from November 1942 to June 1944. Each phase had its counterpart in partisan/anti-partisan warfare.

Phase one saw the birth of the Soviet partisan movement with 30,000 men, consisting of hard-core communists and Red Army stragglers left behind the advancing German front. Hoping to destroy the partisans and secure their LOCs, the Germans employed nine security divisions. Soon, however, the German Army was forced to remove regular front line units (up to Regiment strength) to support the anti-partisan operations. They formed special task forces up to division strength to conduct mop-up and pacification operations. An 8-to-1 superiority was necessary to destroy partisan units by using encirclement tactics.

During the second phase, the partisan strength grew to about 150,000. They had gained the capability to threaten rear area security to the extent that operations of field armies and whole army groups were affected. The Germans were forced to counter the threat by resorting to large-scale operations. Some of these operations required several German divisions and were then only successful due to superior training, mobility, and firepower.

The third phase saw partisan strength at a quarter million men supported by the local population and with large areas under partisan control. Some partisan units were equipped with heavy weapons, artillery, and even tanks. The Germans streamlined their anti-partisan organization, strengthened their security forces, and adopted aggressive counter-measures. The most effective were large-scale encirclement operations. In these operations the Germans engaged with as many as six combat divisions reinforced by tanks, artillery, and aircraft. However, none of these later operations were fully successful because they lacked the numbers to have tight encirclement rings completely around partisan areas. By the end, the Germans had 250,000 troops dedicated to security mission and 10 training and reserve divisions had to be moved from the interior to Russia. Augmented by regular forces from the front for months at a time, conservative estimates place manpower for anti-partisan security actions at 400,000.

SOURCE: US Army Center of Military History

6. Air Base Defense Considerations

Aircraft are especially vulnerable during take-off and landing operations, as well as when parked on the airfield. Base commanders of any Service who command installations with active airfields must identify threat systems and plan and secure air operations. This should include approach and departure corridors used by the aircraft as well as dispersal plans while on the ground. They must also determine the best tactics, techniques, and procedures to counter and neutralize these threats, and identify seams within the joint force as they relate to securing aircraft arrivals and departures against MANPADSs, indirect and direct fire attacks, and laser pointers and illuminators that can temporarily blind aircrew. Threats to aircraft may be launched a considerable distance from the air base. Ideally, the base commander has sufficient forces and a large enough base boundary to counter these threats. Base, base cluster, and area commanders must be aware of the nature of these threats and share the responsibility to counter them. Base commanders must also consider that air base defense is not merely the protection of air assets but the ability to generate air power. The occurrence of direct/indirect fire at any location on the base can disrupt air power generation without causing damage.

a. **Planning.** Planning air base security requires the integration of air operations into the theater air plan, plotting MANPADS footprints, defining approach and departure corridor security procedures, and identifying indirect fire and direct fire ranges (footprints). Air base commanders typically coordinate base boundaries with the area commander to ensure such boundaries provide appropriate protection for aircraft and support materials using MANPADSs and direct/indirect fire footprints. Depending on the air base capabilities, these areas may or may not be within the base boundaries and the security provided by the base commander. Additional coordination should be made with other forces to provide security where the MANPADS or direct/indirect fire footprints are outside the airbase boundary.

b. **Threats to Air Bases.** Air base security and local area assessments should be conducted to identify the area of vulnerability to direct fire, indirect fire, and MANPADS threats (in terms of possible launch sites), to include the air base arrival and departure corridors. A thorough assessment should include the capabilities of security forces, intelligence, CI, and operational personnel as well as local and HN authorities.

(1) Criteria to identify possible direct fire, indirect fire, and MANPADS launch sites include, but are not limited to:

(a) Cover and concealment—an object's capacity to conceal adversary forces and equipment and prevent detection by friendly forces, and to provide protection for the adversary from return fire.

(b) Line of sight providing unobstructed view of the target.

(c) Exposure time—the amount of time the intended target is vulnerable to an operational attack.

(d) Distance to target and the range of the adversary's weapons systems as well as target recognition for the adversary to positively identify the intended target. Set-up time for an adversary's fire team to assemble into an attack position.

(e) The amount of time it takes to detect an adversary's fire team once their weapons are exposed.

(2) Base commanders and area commanders must coordinate actions to protect airfields from launch sites outside the base or installation fence line. Actions include delineation of base boundaries, efforts to mitigate direct fire, indirect fire, and MANPADS launch sites, and the allocation of resources to detect, deter, and destroy threats to air base operations and personnel.

(3) The preferred method is to deny an attacker access to potential launch sites. However, that may not always be possible. Base, base cluster, and area commanders, depending on the situation, should develop and exercise contingency plans for responding to an incident of direct fire, indirect fire, or MANPADS attack. Rapid reaction plans will facilitate the immediate engagement of an adversary attack or post attack, to deter/prevent future attacks and ease concern for air travel safety by the public at large.

c. **Direct and Indirect Fire Threats.** When locations that support direct and indirect fire threats are identified, those areas can be isolated by expanding the base boundary or airfield area of control and reducing areas of vulnerability. The following mitigation measures may require coordination with local/HN authorities:

(1) Increased physical presence at prime launch sites. Visual observation of security teams is a strong deterrent.

(2) Focused and random patrols of potential engagement/launch sites. Incorporate random patrols into the base defense plan.

(3) Employment of technical equipment (counter-fire radar) to detect and respond to the various threats.

(4) Employment of a counter fire base defense scheme.

(5) Dispersal of stationary aircraft to reduce damage from direct or indirect fire attacks.

(6) Barriers/screens to mitigate direct fire threats.

(7) MSFs to neutralize enemy forces and minimize time of disruption for sortie generation.

d. **MANPADS Threats**

(1) Most GCCs have designated their respective JIOCs as the office of primary responsibility to maintain a database with current intelligence and operations information on

select countries and air bases, to include MANPADS target acquisition. For example, Air Mobility Command, Air Force Central Command, and United States Air Forces in Europe maintain databases and policy matrices that describe the MANPADS threats for countries or in the vicinity of specific airfields, the requirement for defensive systems, and policy on permitting non-defensive system-equipped aircraft to operate in MANPADS threat locations. This information can assist the JFACC in making policy decisions for aircraft operations at those same locations.

(2) Commanders should employ mitigation measures to counter the MANPADS threat in air base defense and in reducing aircraft in-flight susceptibility.

(a) When developing base defense plans, considerations for air base defense and the MANPADS threat include:

1. After analysis of possible launch sites, isolating prime MANPADS launch sites and vulnerable areas by expanding the air base area of control to reduce vulnerability. The following mitigation measures may require coordination with local and HN authorities:

a. Increased physical presence at prime launch sites. Visual observation of security teams is a strong deterrent.

b. Focused and random patrols of potential launch sites, to include preplanned targeting. Incorporate random patrols into the base defense plan.

c. Employment of technical equipment to detect and respond to the threats.

2. Educate personnel on the MANPADS threat (to include component recognition), areas of vulnerability, and reaction plans. Develop and provide MANPADS awareness training for security force personnel and local and HN authorities. Develop a MANPADS awareness program for neighborhood watch groups, local businesses, and installation facilities close to air bases or along flight paths. Ensure pilots and flight crews are familiar with MANPADS threats and counters for each air base. Direct voice communications to the BDOC allow for initial visual assessments of potential threats and their locations by flight crews during departure and approach. The Defense Intelligence Agency Missile and Space Intelligence Center is the organization of expertise for enemy missile systems.

(b) To reduce aircraft in-flight susceptibility to the MANPADS threat, base defense plans should:

1. Establish air base procedures for the use of aircrew tactical countermeasures and tactics. (Development and dissemination may require coordination with local and HN authorities.) Train aircrews to identify MANPADS launches and their effects on aircraft. Ensure mission planners and aircrews review air component threat working group risk assessments and threat mitigation measures before flight.

2. Vary arrival and departure times of aircraft. Stagger the arrival times of normally scheduled missions to make arrival, departure, and ground times harder to predict for the adversary.

3. Randomly change approach and departure routes as a deterrent (IAW current Federal Aviation Administration guidelines).

4. Limit or discontinue use of landing lights in threat zones to reduce heat producing targeting options.

5. In high-threat areas or when intelligence has indicated a high alert status, coordinate, develop, and practice plans for engine-running offloads to minimize ground time.

e. **MSF Actions.** Synchronize MSF operations with air base operations through clear command relations and integrated tactics, techniques, and procedures.

7. Seaport Facility Defense Considerations

When a seaport or marine terminal is part of a designated base cluster, the base commander will normally be responsible for security within the base boundaries with HN, Army, or Marine Corps forces responsible for shore boundary defense, and Navy and USCG forces providing waterside harbor approach security. However, if the seaport or marine terminal is isolated or located outside of a land combat area commander's AO, the designated HDC will normally be given responsibility to secure the seaport or marine terminal, as well as the harbor approaches. In these situations, the HDC may be required to use organic shore security forces to serve as the MSF while other naval personnel provide boundary security. In other more high risk situations, the area commander, ICW the JSC and the HDC, may provide a MSF from another Service for base security, especially if the seaport or marine terminal is isolated. In these situations, the MSF would be placed TACON to the HDC. The HDC should be aware that some arriving cargo ships may be carrying US Navy embarked security teams. These forces remain on the ship during loading and offloading operations, and protect the ship while in port.

8. Lines of Communications Considerations

“Co-equal with the security of flanks, the maintenance and full use of the lines of communications to the rear are of major concern to the commander. It is his responsibility that the incoming supply is equal to the needs of his deployments and that the supporting arms and fires which have been promised him keep their engagements. Or if they do not, he must raise hell about it.”

Brigadier General S.L.A. Marshall
Men Against Fire: The Problem of Battle Command, 1947

Onward movement of personnel, equipment, and materiel through joint reception, staging, onward movement, and integration is vital to joint force operations. **The greatest risk to joint force operations can be threats to main supply routes from the ports of debarkation forward to the main battle area (in linear operations) or FOBs (in nonlinear, noncontiguous operations).** Some guidelines for planning and executing surface LOC security operations in support of joint operations and links between JSC LOC security actions with joint movement control operations are provided.

a. **Fundamentals of LOC Security.** LOC security operations include the protection of ground supply routes, inland waterways, rail lines, and pipelines that are used to support joint force operations in contingency operations (see Figure IV-4). LOC security is especially challenging in major combat operations and in sustained, high-risk combat and follow-on stability operations.

Fundamentals of Lines of Communications Security

- Line of communications security is an operation, not a logistic function.
- Line of communications security in Level II and III threat conditions will require dedicated security force capabilities.
- Line of communications security actions must be closely synchronized with joint movement control operations.

Figure IV-4. Fundamentals of Lines of Communications Security

(1) Security of LOCs that transit unassigned areas requires special consideration, especially in Level II and III threat environments. Even when the JFC designates a JSA, units may not have sufficient combat capabilities to secure them.

(2) **Area commander, JSC, and JFC linkages are key to LOC security.** The area commander is responsible for security. The JSC remains responsible to the JFC for coordination and staff oversight.

b. Joint Movement Control

(1) The GCC has a wide range of options to exercise joint movement control. Subordinate JFCs and Service component commanders may be directed to carry out their own movement, or the GCC may establish a theater-level joint transportation board. In some instances a combination of both may exist. The organization charged with movement control plans, allocates, coordinates, and deconflicts transportation, and establishes and operates an in-transit visibility system to assist in tracking theater movements. It also establishes the location, identity, and communications facilities of nodes in the transportation system and promulgates tasking procedures, cycles, and deadlines. The joint movement control plan integrates the transportation capabilities of the component commands and provides for centralized planning and decentralized execution and is key to an effective movement control system. **A disciplined joint movement control system can enable LOC security to be**

planned and executed. The JSC will work closely with the designated joint movement control organization to plan movements through the most secure routes throughout the OA.

(2) The planning, control, and security of personnel and cargo movement over LOCs throughout the OA are vital to the joint force. Normally, a JMC coordinates strategic movements with USTRANSCOM and ICW the JSC, oversees the execution of joint transportation priorities and controls movement. In major operations, the JMC executes movement control to include coordination of convoys passing through higher-level organizational, cross Service, and MNF boundaries.

(a) JSC links to the JMC enhance LOC security throughout the OA. One technique to link the JSC and JMC planning is to establish a joint line of communications security board (JLSB). Functions and characteristics of a JLSB can be found in Figure IV-5.

(b) The JSC works closely with the JMC to monitor the security of joint movements throughout the OA. The JSC may use assessment teams and recommend adjustment of security forces based on threats to movement security.

(c) A joint deployment and distribution operations center (JDDOC) is designed to synchronize and optimize intertheater and theater deployment, distribution, and sustainment operations within a GCC's AOR. The JDDOC is an integrated operations and fusion center (movement control organization), acting in consonance with the GCC's overall requirements and priorities, and on behalf of the GCC, may direct common user and intratheater distribution operations. The JMC will work closely with the JDDOC.

Joint Line of Communications Security Board

Functions

- Assesses and reports current line of communications security status.
- Assesses and reports line of communications security capability shortfalls.

Make Up

- Joint security coordinator lead (or J-3 if there is no joint security coordinator)
- Joint movement center/joint transportation representative
- J-2 representative
- Provost marshal representative
- Others as required (weather, civil affairs, legal)

Battle Rhythm

- Normally meets on a daily basis or operates full time based on joint force commander guidance.

Legend

J-2 intelligence directorate of a joint staff J-3 operations directorate of a joint staff

Figure IV-5. Joint Line of Communications Security Board

For further information on movement control, see JP 4-0, Joint Logistics, and JP 4-09, Distribution Operations.

c. **Security of LOCs.** The primary threats to movement along ground LOCs in Level I and II threat environments are mines, ambushes, and improvised weapons. Improvised weapons include modified conventional weapons and munitions, IEDs, and improvised chemical, biological, or radiological weapons. Level III threats may include risk of interdiction from air and ground conventional forces. Land LOCs, rail lines, and pipelines may also be vulnerable to demolitions, sniper fire, and indirect fire. Commanders and their staff develop LOC security measures to mitigate risks to LOCs. Logistic personnel should synchronize these measures with JSO. Certain units rely on the supported commander to provide FP.

(1) **Active Security.** Active LOC security techniques include measures to achieve positive control of the LOCs and reduce threats. Active security includes:

- (a) Patrols.
- (b) Snipers.
- (c) Fighting positions along LOCs.
- (d) Check points.
- (e) Route sweeps.

(2) **Cordon Security Operations.** Cordon security operations are **area defense missions that protect a specific route for a designated period during which multiple movements take place.** They establish a security cordon to allow safe passage of personnel, materiel, and units transiting high-risk portions of the OA. Cordon security requires combat arms forces and intelligence resources to observe and secure the designated route. Cordon operations may be used to establish a reserved route for exclusive military, USG, or NGO use. The JFC will consider the resources and possible harm to civil-military relations of each particular LOC security operation.

(a) **Movement Corridors.** Commanders can use a variety of tactics, techniques, and procedures to enhance LOC security operations. One procedure is to establish movement corridors. Movement corridors connect two or more support areas in the OA and complement cordon security operations. Movement corridors help layer and integrate security with LOCs. The width and depth of the movement corridor will be dependent on JFC guidance and mission, enemy, terrain and weather, troops and support available, time available, and civil factors.

(b) Security cordons keep enemy forces more focused on the security force than on engaging vulnerable forces on the LOCs. Cordon security is provided by two or more combat outposts positioned to provide mutual support. The JSC, via the JFC's J-3, normally assigns an area commander this mission. The area commander selects air assault, mechanized, or motorized combat units to man combat outposts at critical locations along the

assigned route. Combat outposts can be composed of mechanized or motorized platoon-size elements equipped with automatic weapons, communications, and sensors, and supported by fire support assets. On waterway LOCs, patrol boats can provide and reinforce security.

(c) One of the primary responsibilities of the cordon commander is to collect and disseminate combat information concerning the assigned route obtained by reconnaissance patrols, UAS overflights, or other collection methods. This information is provided to higher headquarters, the JSC, and all units moving, or scheduled to move, along the designated route. In some cordon operations, the cordon outposts may also serve as communications relay sites.

(d) Combat outposts are located within supporting distance of each other whenever possible. Units assigned to combat outposts provide MSFs to respond to enemy activity in their assigned cordons. Forces at combat outposts conduct random or directed reconnaissance patrols, UAS sorties, and offensive operations on a frequent but irregular schedule to suppress enemy activity in the corridor. Rotary-wing, tiltrotor, and fixed-wing assets can significantly enhance LOC security.

(3) **Passive Security.** Passive LOC security techniques include measures that do not require significant manpower or resources. Passive LOC security techniques include:

(a) Convoy formation and march control conduct movement with security to present the least valuable target.

(b) Security-related driving techniques (speed of march, actions on contact, overwatch positions).

(c) Route variance.

(d) Variations of convoy departure times.

(e) OPSEC countermeasures.

(f) Convoys combined with other operations and tactical movements to enhance security along LOCs. These activities include aircraft traversing the LOC, maintenance, training exercises or troop movements, HN military and police traffic control activities, and HN civilian activities. Passive security supplements active security.

For more information on convoy operations, see FM 4-01.45/Marine Corps Reference Publication (MCRP) 4-11.3H/Navy Tactics, Techniques, and Procedures (NTTP) 4-01.3/Air Force Tactics, Techniques, and Procedures (AFTTP) 3-2.58, Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Operations. See also, JP 3-15.1, Counter-Improvised Explosive Device Operations.

(4) **Reconnaissance and Surveillance.** LOC reconnaissance and surveillance includes main supply routes, pipelines, waterways, and terrain the enemy could use to influence the joint force's movement. LOC reconnaissance and surveillance should be done

at irregular intervals to avoid regular patterns that enemy forces could exploit. Route reconnaissance and surveillance techniques include:

- (a) Manned aircraft or UASs.
- (b) HN military or police physical reconnaissance and traffic control.
- (c) Patrols and other actions on LOCs.
- (d) Waterway patrols.

d. Other Considerations

(1) **Risk Management.** The JFC, normally through a JSC, assesses risk to LOC security. The JSC works closely with the JFC's staff and component representatives, HN, other USG departments and agencies, and MNFs to determine risk to LOC security and measures to defeat or mitigate these risks. The JSC assists commanders and staffs at all levels in identifying and mitigating risks to forces transiting LOCs. The JIPOE process provides essential data for LOC security planning. JIPOE updates should be disseminated as they are identified. The JSC identifies risk, develops courses of action, assesses resource requirements, recommends actions to area commanders, and then monitors the LOC security actions. The steps in the risk-management process are to identify threats, assess threats to determine risk, develop control or security measures, make risk-assessment decisions, implement control and security measures, and review these measures for continued use.

(2) **Civil Considerations.** The JFC, normally through the JSC, will take civil considerations into account when planning LOC security. LOC security will affect the HN civilian population as well as other USG departments and agencies and NGOs in the OA. The JFC may temporarily designate a route for military use only. Restricting routes to military use can adversely affect the local population, as well as other USG and NGO operations. Even partial restrictions can have a negative impact. All LOC security activities should be coordinated with the JFC's CMO staff.

For further information on CMO, see Chapter III, "Planning," and JP 3-57, Civil-Military Operations.

(3) **Communications and Reporting Requirements.** In a joint environment, regulation of transportation and LOC security will mitigate congestion and enable the LOC security plan. Robust communications and reporting requirements are essential to transportation regulation. Often, resources to support LOC security are unreliable or unavailable. The JFC may reallocate communications resources from other operations. Joint transportation planners will recommend which LOCs require joint control and which should be regulated via area commanders. The traffic regulation reporting plan will be coordinated with and support LOC security requirements. Successful movement is linked to robust information and communications systems, orchestrated by the JSC and staff on behalf of the JFC. The communication systems provide timely data to adjust the responses of the terminals and nodes along LOCs. In some cases, a dedicated LOC security frequency may

be designated. The Joint Surveillance Target Attack Radar System may provide C2 of strike resources in support of a ground conflict during LOC security missions.

APPENDIX A JOINT SECURITY OPERATIONS CENTERS

1. Joint Security Coordination Center

a. **JSCC Basic Functions.** The JSCC can conduct 24-hour operations. Its primary responsibilities include:

(1) Coordinate and oversee security operations within the designated OA. Monitor emergency service, FP, AT, physical security, base and base cluster defense plans, and FPWG policies, plans, and operations to align them with operation plans, orders, directives, policies, and regulations.

(2) Review the JFC's operational vulnerability assessment and assistance program (VAAP) for risk mitigation measures to all bases, base clusters, LOCs, APODs, SPODs, and other organizations or facilities located in the AOR and the JOA.

(3) Prepare policy, plans, and guidance on JSO for implementation by subordinates assigned within an AOR and the JOA.

(4) Help the J-3 prepare joint security plans and orders for current operations. Coordinate with the J-3 to deconflict JSO with ongoing and planned operations.

(5) Inform the JSC of all JSO, including enemy, friendly, and civilian activities.

(6) Monitor the status of assigned or attached security forces and other resources, and provide the commander information to aid, allocate, and move forces and materiel.

(7) Ensure that units in the AOR and the JOA conduct active and passive security measures, to include integration of the IADS.

(8) Identify and prioritize allocation of resources to defeat or mitigate vulnerabilities.

(9) Provide for centralized collection and processing of information from intelligence and operational sources, and disseminate intelligence products to area commanders and subordinate units. Intelligence products include joint security base and LOC threat conditions, weather, and hazards.

(10) Provide members to JLSB as required.

b. Unique Positions and Responsibilities Within the JSCC

(1) **JSC.** Principal staff officer responsible for planning and preparing JSO throughout the OA.

(2) **Chief of Staff/Deputy, JSC.** Assistant to the JSC for the planning and preparation of JSO throughout the OA responsible for coordinating actions and directing the JSCC staff for the JSC.

2. Base Defense Operations Center

Basic BDOC Functions. The BDOC can conduct 24-hour operations. Its primary functions include:

- a. Provide C2 organization for coordinated base security operations.
- b. Prepare plans to implement the base commander's base defense guidance.
- c. Plan and execute FP, AT, and physical security operations IAW published guidance.
- d. Conduct FPWG and threat working group.
- e. Monitor assigned, attached, and tenant unit forces and resources and provide the commander information to aid, allocate, and move forces and materiel to meet base defense requirements.
- f. Identify base defense shortfalls and communicate them to the base cluster commander or JSC, as well as Service or applicable functional component command.
- g. Inform the base commander of base security concerns.
- h. Ensure that all units within the base perimeter conduct active and passive security measures. Monitor and direct guard forces.
- i. Assess competing operational demands inherent to multi-Service or multinational environments.
- j. Develop and execute a reconnaissance and surveillance plan to ensure proper security from standoff threats within base boundaries and coordinate with area commander/base cluster commander for the area outside the base boundary.
- k. Establish and maintain connectivity with higher-level staff (BCOC or JSCC).
- l. Coordinate with the area commander or tenant commander to deconflict security activities from combat and stability operations.
- m. Plan and coordinate for base fire support.
- n. Identify and share base emergency response/ADC capabilities, to include medical support, combat engineering, EOD, firefighting, and others, as required.
- o. Evaluate actions to identify operational deficiencies, lessons learned, and best practices, and develop methods to improve combined operational effectiveness to include coordinating training and exercising base security measures.

3. Base Cluster Operations Center

Basic BCOC Functions. The BCOC acts as both a BDOC and BCOC, so it would perform all basic functions and specific BDOC tasks described above. Additional BCOC functions would include, but are not limited to, the following:

- a. Inform the base cluster commander of the current situation within the base cluster, including enemy, friendly, and civilian activities.
- b. Prepare comprehensive plans to implement the base commander's overall base cluster defense and security guidance.
- c. Communicate any base defense shortfalls identified to the JSC, as well as Service component and/or applicable functional component command.
- d. Assess potential conflicting interests and operational demands of base cluster forces inherent when operating in multi-Service or multinational environments.
- e. Provide centralized collection and processing of information from various intelligence and operational sources and share resultant base cluster intelligence products as appropriate. Information would include weather, civil considerations, LOC conditions, CBRN threats, IEDs, or other known hazards.
- f. Provide the essential C2 organization to conduct integrated base defense.
- g. Develop and execute a reconnaissance and surveillance plan to ensure that bases are properly protected from stand-off threats outside their base boundary.
- h. Establish and maintain connectivity with higher level staff (JSCC or JSC).
- i. When necessary, coordinate and deconflict base security, base cluster security, and local combat operations.
- j. Plan and coordinate the base cluster fire support plan.
- k. Identify and share base and base cluster emergency response and ADC capabilities to include medical support, combat engineering, EOD, firefighting, etc.
- l. Evaluate actions to identify operational deficiencies and develop methods to improve combined operational effectiveness to include coordinating training and exercising base defense measures.

4. Common Positions and Key Responsibilities for all Operations Centers

The following positions, when created, normally require personnel to be dual hatted:

- a. **Operations Officer.** The operations officer serves as the principal advisor to the JSC or base commander on all operational matters. Other responsibilities include the following:

- (1) Direct the operations within the center.
- (2) Develop a training, exercise, and certification plan for the JSCC staff, or units and individuals who have been designated as part of the base defense plan.
- (3) Monitor current operations and intelligence in order to help synchronize the efforts and make operational decisions in line with the JSC/base commander's intent. Enforce full participation and support to the FPWG and VAAP.
- (4) Seek guidance from the principal staff on situations that are beyond the operations officer's decision-making authority.
- (5) Notify staff sections on significant operational events and include appropriate staff sections in critical decision making.
- (6) Prepare and submit operational and situational reports as required to the JSC/base commander.
- (7) Monitor outgoing communications and correspondence for completeness, accuracy, and staff coordination.
- (8) Maintain a log of significant events and distribute the guidance from the JSC/base commander or staff officers.
- (9) Coordinate planning with higher headquarters.
- (10) Monitor security status of base(s) and deconflict security operations.
- (11) Assist in developing PIRs and coordinating with appropriate staffs for collection on intelligence requirements.

b. **Intelligence Officer.** The intelligence officer's duties are to:

- (1) Supervise intelligence section personnel.
- (2) Ensure frequent communications with higher-level intelligence organization as directed by the JSC.
- (3) Provide intelligence input on the situation report (SITREP).
- (4) Ensure subordinate commands receive intelligence updates and other information in a timely manner through the most appropriate means.
- (5) Provide daily intelligence update to the operations center and FPWG.
- (6) Coordinate and maintain liaison with HN intelligence agencies.
- (7) Keep the operations officer informed of all significant intelligence and intelligence threats and events.

(8) Conduct pattern and trend analysis for enemy activities to determine future enemy targets, times, and preferred attack methods.

c. **FP Officer.** This officer serves as the principal advisor to the JSC or base commander on all AT, FP, physical security, and emergency services matters. Duties include the following:

(1) Develop, publish, and provide guidance on all FP, AT, physical security, vulnerability assessment, and working group policies and procedures.

(2) Chair the JSC/base commander's FPWG and threat working group.

(3) Assist the operations officer in preparing and submitting operational and situational reports, as required, to the base commander.

(4) Brief the operations officer on FP matters.

(5) Set the standard for the base commander's FPWG, to include ensuring unity of effort on base defense; sharing of information and intelligence; establishing the FPWG's agenda, priorities, and VAAP input; conducting and monitoring the JSC/base commander's risk assessment program; and identifying base defense resources.

(6) Conduct vulnerability assessments and provide to the base commander IAW DOD policy and theater guidance.

d. **Battle Captain.** The battle captain will:

(1) Be responsible for tracking day-to-day operations.

(2) View all incoming messages and distribute appropriate guidance for each.

(3) Act as the operational focal point in coordinating the efforts of the staff.

(4) Ensure the accuracy of map information, mission statement, task organization charts, battle board information, the significant events display, and daily journal.

(5) Provide daily operational update to the FPWG.

(6) Determine which events appear on the significant event display.

(7) Inform other staff sections of significant events.

(8) Monitor the communications network ICW the communications noncommissioned officer (NCO).

(9) Direct or commence the drafting of required operational action messages such as fragmentary orders.

(10) Coordinate the shift change briefings.

(11) Monitor the progress of the base commander's daily SITREP to ensure all required inputs are received in a timely manner to allow the message to be transmitted on time.

e. **Operations NCO.** The operations NCO's primary duties include the following:

(1) Assist the operations officer in the conduct of operations.

(2) Assist with the accuracy of map information, mission statement display, task organization chart, chart data board information, maintaining the journal, and ensuring that the situation map is up to date.

(3) Maintain master files for all incoming and outgoing messages by date time group.

(4) Maintain the significant events log.

(5) Ensure that files, logs, and reports (both computer and hard copy) are maintained, current, and submitted as required.

(6) Supervise information flow procedures.

(7) Supervise the maintenance of incoming and outgoing message files and ensure that message read files are available for the base commander and staff.

(8) Provide direct supervision of the daily journal.

(9) Establish personnel and equipment listings for administrative support.

(10) Be responsible for the routine upkeep and maintenance of the operation center.

(11) Assist in the daily preparation of the SITREP.

(12) Obtain material required by the staff.

(13) Prepare map overlays as required.

f. **Fire Support Officer.** The fire support officer's duties include the following:

(1) Assist the operations officer in developing base fire support plans.

(2) Coordinate fire support related plans, measures, and communications requirements with the appropriate BDOC, BCO, JSCC staff, or area command staff as required.

(3) Conduct assessments of existing fire support plans and coordinate exercise/rehearsals of same.

g. **Communications Officer.** When there is no full-time communications officer, the operations NCO would serve in this position. Key duties include:

- (1) Provide advice on communications matters.
- (2) Ensure adequate secure voice and communications connectivity is maintained with appropriate headquarters.
- (3) Coordinate required communications for the JSCC/BDOC/BCOC.
- (4) Maintain a log of significant communications activities.
- (5) Monitor action on all communications operations.
- (6) Prepare briefings on communications status for the JSC/base commander and provide communications input to the SITREP.
- (7) Maintain the secure telephone system between higher and subordinate command headquarters.
- (8) Maintain current status of all joint communications in support of the operation and available for contingency operations.
- (9) Identify trends that may develop to degrade communications.
- (10) React to requests for additional communications support, or restoration of degraded communications.
- (11) Publish telephone number listing.
- (12) Actively participate in and support the FPWG and VAAP.

h. **Logistics Officer.** The logistics officer's duties include the following:

- (1) Maintain a thorough knowledge and understanding of all logistic plans and actions applicable to base defense requirements.
- (2) Monitor and coordinate the logistic functions and requirements, including general engineering, in support of base defense.
- (3) Prepare logistic input to the SITREP.
- (4) Actively participate and support the FPWG and VAAP.

i. **Engineer Officer.** The engineer officer's duties include:

- (1) Advise and establish JSC/base commander's general engineering policy and guidance.

(2) Provide general engineering and, when applicable, combat engineering and input to JSC/base defense plans.

(3) Coordinate and supervise base defense construction and environmental support actions.

(4) Develop infrastructure criteria IAW the JFC's engineer guidance.

(5) Coordinate for the contract procurement of real property FP equipment (e.g., barriers, guard shacks, lighting).

(6) Actively participate and support the FPWG and VAAP.

(7) Order and distribute maps.

j. **CBRN Officer.** The CBRN officer will:

(1) Act as lead subject matter expert for CBRN defense, response to CBRN incidents, and sensitive site assessment.

(2) Actively participate and support FPWG.

(3) Conduct vulnerability analysis based on the latest intelligence/threat assessments.

(4) Assist operations officer in CBRN defense planning and review CBRN annexes to higher headquarters operation plan and concept plan.

(5) Support the operations center for theater-level CBRN warning and reporting.

(6) Coordinate with medical representative on health service requirements.

(7) Coordinate with logistics officer pertaining to CBRN defense equipment, supplies, maintenance, and transportation of CBRN assets.

(8) Coordinate with HN to determine CBRN response capability and CBRN support requirements.

k. **Security Manager.** The security manager should:

(1) Implement commander's program for the protection of classified information.

(2) Manage personnel security for all DOD employees, military personnel, and DOD contractors.

(3) Report all incidents involving classified information through the system of record.

For further information, see DOD Manual 5200.01, Volumes 1-4, DOD Information Security Program.

1. **Medical Representative.** The medical representative's duties include:

(1) Advise JSC/base commander and staff on health support matters related to base defense.

(2) Plan for and assist in exercising mass casualty treatment.

(3) Plan for and assist in exercising base casualty evacuation procedures.

(4) Actively participate and support the FPWG and VAAP.

m. **Liaison Officer.** The liaison officer represents tenant units, component, and/or activity. Actively participates in all planning and in the FPWG and VAAP, as required.

Intentionally Blank

APPENDIX B SAMPLE BASE DEFENSE PLAN

1. Overview

a. The following format is offered as one method of developing a base defense plan. It is optimized for a base or installation, to include deployed units and can be adapted for use at other facilities. It is meant to help the JSC, as the principal staff officer responsible for planning and preparation of JSO throughout the OA, structure the base defense plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military OPORD (Situation-Mission-Execution-Administration and Logistics-Command and Signal).

b. This format enables the integration of existing programs such as law enforcement, physical security, AT, OPSEC, information security, high-risk personnel protection, and other installation efforts. Base defense plans should be integrated into all plans and separate annexes. Remember that staff interaction is a crucial element of developing a realistic, executable plan.

c. Although this sample is patterned after the military OPORD, it can be used by other DOD agencies and facilities to protect personnel, activities, and materiel under their control.

d. This sample uses supporting annexes, appendices, tabs, and enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

e. The primary reference for plan formats is Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance*. Should a conflict exist between this Appendix and the format found in CJCSM 3130.03, the APEX manual format takes precedence.

2. Sample Format

(In Joint Operation Order Format)
SECURITY CLASSIFICATION
Copy No. ____
Issuing Headquarters Place of Issue
Message Reference Number

Type and Serial Number of Operation 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, HN, and other 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 OPORD, to include the mission of the next higher headquarters and adjacent bases as well as units not under base command whose actions will affect or assist the defense of the base. These units may include MP units, other security forces, fire support, CRF, special operations forces, engineers, CBRN units (to provide decontamination and obscuration support), EOD, HN military or police organizations, and public and private civilian organizations of both the United States and the 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 security forces, the assignment of elements to counter standoff and penetrating attacks to include the base boundary patrol concept of operation and establishment of a defense with primary, alternate, and supplementary defensive positions, as well as reaction force responsibilities. Describe the purpose of counterattacks and set work priorities.)

(3) Fires. (State plans for employing air and missile defense and 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) Base Boundary. (Define and establish the base boundary as coordinated with the area commander. Include a description of plans to cope with enemy standoff attacks.)

(b) 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.)

(c) 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.)

(d) 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.)

(e) 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. Types and locations.
2. Security classifications.
3. Maintenance.
4. Operation.
5. Probability of Detection.

- a. Limitations.
- b. Compensating measures.
- c. Redundant capabilities.

(c) Protection of Classified Information

1. Security containers.
2. Personnel access to areas containing classified material.
3. Vetting and verification of clearance.
4. Classified material handling procedures.
5. Emergency destruction plan.

(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 standing operating procedures as annexes. Ensure that procedures include randomness.)

(a) Composition and organization. (NOTE: In security and support operations 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) MSF.

1. Composition.

2. Mission.

3. Weapons and equipment.

4. Location.

5. Deployment concept.

(4) Rules of Engagement. (Delineate the circumstances and limitations under which US forces will initiate and/or continue combat engagement with other forces encountered.)

(5) Contingency Plans. (Indicate actions in response to various emergency situations. List as annexes any detailed plans, such as combating terrorism, responding to bomb threats, active shooter response, hostage situations, emergency destruction of classified information, natural disasters, and firefighting.)

(a) Individual actions.

(b) MSF actions.

(6) Security Alert Status.

(7) Air Surveillance.

(8) Noncombatant Evacuation Operation Plans.

(9) Coordination with HN or Adjacent Base Plans.

(10) Measures for Coordination with Response Force and Tactical Combat

(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, casualty reporting, and other procedures pertinent to base defense.)

f. CA. (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 signal operating instruction.)

(1) Types.

(a) Primary.

(b) Alternate.

(2) Operation.

(3) Maintenance.

(4) Authentication.

b. Command.

(1) Joint and multinational relationships. (Command relationships must be spelled out clearly, to include command succession. Shifts in relationships as the defense progresses, as when a security 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. Communications
- L. Force Protection
- M. Host-Nation Support
- N. CBRN

Distribution:

Authentication:

APPENDIX C

INTEGRATION OF PROTECTION AND SECURITY IN THEATER

1. **Protection.** The protection function focuses on preserving the joint force's fighting potential in four primary ways. One way uses active defensive measures that protect the joint force, its information, bases, necessary infrastructure, and LOCs from an enemy attack. Another way uses passive defensive measures that make friendly forces, systems, and facilities difficult to locate, strike, and destroy. Equally important is the application of technology and procedures to reduce the risk of friendly fire. Finally, emergency management and response reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters.

2. **Security** is a principle of joint operations.

(1) The purpose of security is to prevent the enemy from acquiring unexpected advantage.

(2) Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise. Security results from the measures taken by commanders to protect their forces. Staff planning and an understanding of enemy strategy, tactics, and doctrine enhance security. Risk is inherent in military operations. Application of this principle includes prudent risk management, not undue caution.

3. **In a JSA**, an integrated approach to security is critical to the protection of joint bases and their connecting LOCs that support joint operations. The integration of multiple security activities is a combination of protective measures, implemented by organizations throughout the joint force, to protect the force. Some essential security activities include:

(1) **Communications security** is the result of all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. *JP 6-0, Joint Communications System, provides additional information on communications security. For additional guidance on communications security, see DOD Manual 5105.21, Volume 1, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.*

(2) **Cybersecurity** employs measures to maintain the availability, integrity, authentication, confidentiality, and nonrepudiation of computers, communications systems, electronic communications services, wire communication, and electronic communication, to include the associated information. LOCs must be protected not only from destruction but also from sabotage and surreptitious access. Proper system configuration and network approval must be obtained to provide adequate protection of communications. Insider threat is of particular concern when dealing with information systems. Proper certification and accreditation of systems will assist with overall security.

For joint doctrine on cybersecurity (previously called information assurance), see JP 3-12, Cyberspace Operations. For additional DOD guidance on cybersecurity, see DODI 8500.01, Cybersecurity.

(3) **Industrial Security** integrates contractor personnel and associated equipment synchronously to provide services in a designated OA in support of the joint force IAW the terms and conditions of the contract. Contractor personnel make up an increasing part of the total force structure supporting US military forces across the full spectrum of military operations. Requirements for allowing contractors access to sensitive and classified information, as well as their participation in operations, are important factors in the joint environment. Commanders should understand the advantages and limitations of utilizing contract support.

For further information see JP 4-10, Operational Contract Support. For additional guidance on the National Intelligence Security Program, see DOD 5220.22-M, National Industrial Security Program.

(4) **Information security** protects information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security encompasses policies, processes and implementation of risk management to prevent the compromise, loss, unauthorized disclosure, or unauthorized destruction of information, regardless of physical form or characteristics. This includes actions to regulate access to both controlled unclassified information and classified information.

For additional guidance on information security, see DOD Manual 5200.01, Volume 1-4, DOD Information Security Program: Overview, Classification, and Declassification.

(5) **OPSEC** is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other associated activities. OPSEC focuses on five security processes: determining critical information, identifying threats or adversaries, detecting vulnerabilities via friendly actions used by an adversary to gain access to critical information; assessment of risk level, and implementing countermeasures to lower the risk. OPSEC measures must be taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

See JP 3-13.3, Operations Security, for relevant joint doctrine. For additional guidance on OPSEC, see Department of Defense Manual (DODM) 5205.02-M, DOD Operations Security (OPSEC) Program Manual.

(6) **Personnel Security** is an interlocking and mutually supporting set of program elements (i.e., need to know, investigation, binding contractual obligations on those granted access, security education and awareness, and individual responsibility) that provides reasonable assurance against the compromise of information.

For additional guidance on Personnel Security, see DODM 5200.02-R, DOD Personnel Security Program.

(7) **Physical security** is concerned with physical measures designed to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. Employment of these measures demonstrates security in depth through a layered security effort to identify, diminish, and/or eliminate the threat. *For additional guidance on physical security, see DOD 5200.08-R, DOD Physical Security Program.*

Intentionally Blank

APPENDIX D REFERENCES

The development of JP 3-10 is based upon the following primary references.

1. Department of Defense Publications

- a. DODD 1400.31, *DOD Civilian Work Force Contingency and Emergency Planning and Execution*.
- b. DODD 3000.03E, *DOD Executive Agent for Non-Lethal Weapons (NLW) and NLW Policy*.
- c. DODD 3000.10, *Contingency Basing Outside the United States*.
- d. DODD 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure*.
- e. DODD 4500.54E, *DOD Foreign Clearance Program (FCP)*.
- f. DODD 5205.75, *Department of Defense Operations at US Embassies*.
- g. DODD 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*.
- h. DODI 1400.32, *DOD Civilian Work Force Contingency and Emergency Planning Guidelines and Procedures*.
- i. DODI 2000.12, *DOD Antiterrorism (AT) Program*.
- j. DODI 2000.16, *DOD Antiterrorism (AT) Standards*.
- k. DODI 3020.41, *Operational Contract Support (OCS)*.
- l. DODI 3020.50, *Private Security Contractors (PSCs) Operating in Contingency Operations, Humanitarian or Peace Operations, or Other Military Operations or Exercises*.
- m. DODI 5210.84, *Security of DOD Personnel at US Missions Abroad*.
- n. DODI 5240.22, *Counterintelligence Support to Force Protection*.
- o. DODI 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*.
- p. DODM 5200.01, *Volumes 1-4, DOD Information Security Program*.
- q. DOD O-2000.12-H, *DOD Antiterrorism Handbook*.
- r. DODD O-5240.02, *Counterintelligence*.

2. Chairman of the Joint Chiefs of Staff Publications

- a. CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*.
- b. CJCSI 5120.02C, *Joint Doctrine Development System*.
- c. CJCSI 5261.01G, *Combating Terrorism Readiness Initiatives Fund*.
- d. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3103.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance*.
- e. CJCSM 3122.01A, *Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures)*.
- f. CJCSM 3122.02D, *Joint Operation Planning and Execution System (JOPES) Volume III (Time-Phased Force and Deployment Data Development and Deployment Execution)*.
- g. CJCSM 3130.06A, *Global Force Management Allocations Policies and Procedures*.
- h. JP 1, *Doctrine for the Armed Forces of the United States*.
- i. JP 2-0, *Joint Intelligence*.
- j. JP 2-01, *Joint and National Intelligence Support to Military Operations*.
- k. JP 2-01.2, *Counterintelligence and Human Intelligence Support to Joint Operations*.
- l. JP 3-0, *Joint Operations*.
- m. JP 3-01, *Countering Air and Missile Threats*.
- n. JP 3-02, *Amphibious Operations*.
- o. JP 3-06, *Joint Urban Operations*.
- p. JP 3-07.2, *Antiterrorism*.
- q. JP 3-07.3, *Peace Operations*.
- r. JP 3-08, *Interorganizational Coordination During Joint Operations*.
- s. JP 3-09, *Joint Fire Support*.
- t. JP 3-09.3, *Close Air Support*.
- u. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*.

- v. JP 3-12, *Cyberspace Operations*.
- w. JP 3-13.3, *Operations Security*.
- x. JP 3-13.4, *Military Deception*.
- y. JP 3-15, *Barriers, Obstacles, and Mine Warfare for Joint Operations*.
- z. JP 3-15.1, *Counter-Improvised Explosive Device Operations*.
- aa. JP 3-16, *Multinational Operations*.
- bb. JP 3-17, *Air Mobility Operations*.
- cc. JP 3-30, *Command and Control for Joint Air Operations*.
- dd. JP 3-31, *Command and Control for Joint Land Operations*.
- ee. JP 3-34, *Joint Engineer Operations*.
- ff. JP 3-35, *Deployment and Redeployment Operations*.
- gg. JP 3-40, *Countering Weapons of Mass Destruction*.
- hh. JP 3-41, *Chemical, Biological, Radiological, and Nuclear Consequence Management*.
- ii. JP 3-52, *Joint Airspace Control*.
- jj. JP 3-63, *Detainee Operations*.
- kk. JP 4-0, *Joint Logistics*.
- ll. JP 4-02, *Health Services*.
- mm. JP 4-09, *Distribution Operations*.
- nn. JP4-10, *Operational Contract Support*.
- oo. JP 6-0, *Joint Communications System*.
- pp. JP 6-01, *Joint Electromagnetic Spectrum Management Operations*.

4. Multi-Service Publications

- a. Army Technical Publication (ATP) 3-11.42/MCWP 3-38.1/NTTP 3-11.36/AFTTP 3-2.83, *Multi-Service Tactics, Techniques, and Procedures for Installation Emergency Management*.

- b. ATTP 3-04.15/MCRP 3-42.1A/NTTP 3-55.14/AFTTP3-2.64, *UAS Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aircraft Systems*.
- c. ATTP 4-32.2/MCRP 3-17.2B/NTTP3-02.4.1/AFTTP 3-2.12, *UXO Multi-Service Tactics, Techniques, and Procedures for Unexploded Ordnance*.
- d. FM 3-07.31/MCWP 3-33.8/ AFTTP 3-2.40, *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations*.
- e. FM 3-09.32/MCRP 3-16.6A/NTTP 3-09.2/AFTTP(I) 3-2.6, *Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower*.
- f. FM 3-11.3/MCRP 3-37.2A/NTTP 3-11.25/AFTTP(I) 3-2.56, *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Contamination Avoidance*.
- g. FM 3-11.5/MCWP 3-37.3/NTTP 3-11.26/AFTTP (I) 3-2.60, *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination*.
- h. FM 3-22.40/MCWP 3-15.8/NTTP 3-07.3.2/AFTTP 3-2.45, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Nonlethal Weapons*.
- i. FM 3-55.6/MCRP 2-24A/NTTP 3-55.13/AFTTP(I) 3-2.2, *Multi-Service Tactics, Techniques, and Procedures for the Joint Surveillance Target Attack Radar System*.
- j. FM 4-01.45/MCRP 4-11.3H/NTTP 4-01.3/AFTTP 3-2.58, *Multi-Service Tactics, Techniques, and Procedures for Tactical Convoy Defense*.

5. Army Publications

- a. Army Regulation 525-13, *Antiterrorism*.
- b. Army Doctrine Publication 3-0, *Unified Land Operations*.
- c. ADRP 3-0, *Unified Land Operations*.
- d. ADRP 3-37, *Protection*.
- e. ATP 4-16, *Movement Control*.
- f. ATP 4-94, *Theater Sustainment Command*.
- g. ATTP 4-10, *Operational Contract Support Tactics, Techniques, and Procedures*.
- h. FM 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*.
- i. FM 3-05.2, *Foreign Internal Defense*.

- j. FM 3-22.90, *Mortars*.
- k. FM 3-24, *Counterinsurgency*.
- l. FM 3-34.210, *Explosive Hazards Operations*.
- m. FM 3-34.400, *General Engineering*.
- n. FM 3-39, *Military Police Operations*.
- o. FM 3-57, *Civil Affairs Operations*.
- p. FM 3-90-1, *Offense and Defense, Volume 1*.
- q. FM 3-90.31, *Maneuver Enhancement Brigade Operations*.
- r. FM 3-93, *Theater Army Operations*.
- s. FM 22-6, *Guard Duty*.
- t. Technical Manual 3-34.85, *Engineer Field Data*.

6. Air Force Publications

- a. Air Force Doctrine Volume 1, *Basic Doctrine*.
- b. Air Force Doctrine Volume 3, *Command*.
- c. Air Force Doctrine Volume 4, *Operations*.
- d. Air Force Doctrine Volume 5, *Support*.
- e. Air Force Doctrine Annex 3-10, *Force Protection*.
- f. Air Force Doctrine Annex 2-0, *Global Integrated Intelligence, Surveillance, and Reconnaissance*.
- g. Air Force Policy Document 31-1, *Integrated Defense*.
- h. Air Force Handbook (AFH) 10-222, *Civil Engineer Base Development*.
- i. AFH 31-109, *Integrated Defense in Expeditionary Environments*.
- j. AFH 31-305, *Security Forces Deployment Planning Handbook*.
- k. Air Force Instruction 31-304, *Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees*.
- l. AFTTP 3-10.2, *Integrated Base Defense Command and Control*.

7. Marine Corps Publications

- a. Marine Corps Doctrine Publication 1-0, *Marine Corps Operations*.
- b. Marine Corps Doctrine Publication 4, *Logistics*.
- c. MCRP 3-41.1A, *MAGTF Rear Area Security*.
- d. MCRP 5-12D, *Organization of Marine Corps Forces*.
- e. MCWP 3-11.3, *Scouting and Patrolling*.
- f. MCWP 3-16.6, *Supporting Arms Observer, Spotting, and Controller*.
- g. MCWP 3-33.5, *Counterinsurgency Operations*.
- h. MCWP 3-21.1, *Aviation Ground Support*.
- i. MCWP 3-41.1, *Rear Area Operations*.

8. Navy Publications

- a. NTTP 3-10.1, *Naval Coastal Warfare Operations*.
- b. NTTP 3-11.23, *Multi-Service Tactics, Techniques, and Procedures for Installation CBRN Defense*.
- c. Navy Warfare Publication 3-01.01, *Fleet Air Defense*.

9. Other Sources

Weapons Technical Intelligence Handbook.

APPENDIX E ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent for this publication is the US Army. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Supersession

This publication supersedes JP 3-10, *Joint Security Operations in Theater*, 03 February 2010.

4. Change Recommendations

- a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J7-JED//

- b. Routine changes should be submitted electronically to the Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697, and info the lead agent and the Director for Joint Force Development, J-7/JED.

- c. When a Joint Staff directorate submits a proposal to the CJCS 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. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification*, and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information*.

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at <https://jdeis.js.mil/jdeis/index.jsp> (NIPRNET) and <http://jdeis.js.smil.mil/jdeis/index.jsp> (SIPRNET), and on the JEL at <http://www.dtic.mil/doctrine> (NIPRNET).

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified JP to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA, Defense Foreign Liaison/PO-FL, Room 1E811, 7400 Pentagon, Washington, DC 20301-7400.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

| | |
|-------|--|
| AADC | area air defense commander |
| ADC | area damage control |
| ADRP | Army doctrine reference publication |
| AFH | Air Force handbook |
| AFTTP | Air Force tactics, techniques, and procedures |
| AO | area of operations |
| AOR | area of responsibility |
| APOD | aerial port of debarkation |
| AT | antiterrorism |
| ATP | Army technical publication |
| ATTP | Army tactics, techniques, and procedures |
| | |
| BCOC | base cluster operations center |
| BDOC | base defense operations center |
| | |
| C2 | command and control |
| CA | civil affairs |
| CAAF | contractors authorized to accompany the force |
| CAS | close air support |
| CBRN | chemical, biological, radiological, and nuclear |
| CCICA | command counterintelligence coordinating authority |
| CCIR | commander's critical information requirement |
| CI | counterintelligence |
| CJCSI | Chairman of the Joint Chiefs of Staff instruction |
| CJCSM | Chairman of the Joint Chiefs of Staff manual |
| CMO | civil-military operations |
| COM | chief of mission |
| CRF | coastal riverine force |
| CRS | coastal riverine squadron |
| | |
| DATT | defense attaché |
| DOD | Department of Defense |
| DODD | Department of Defense directive |
| DODI | Department of Defense instruction |
| DODM | Department of Defense manual |
| | |
| EOD | explosive ordnance disposal |
| | |
| FCC | functional combatant commander |
| FM | field manual (Army) |
| FOB | forward operating base |
| FP | force protection |
| FPD | force protection detachment |

| | |
|---------|---|
| FPWG | force protection working group |
| FSCC | fire support coordination center (USMC) |
| FSCM | fire support coordination measure |
| | |
| GCC | geographic combatant commander |
| | |
| HDC | harbor defense commander |
| HN | host nation |
| HNS | host-nation support |
| HUMINT | human intelligence |
| | |
| I2 | identity intelligence |
| IADS | integrated air defense system |
| IAW | in accordance with |
| ICW | in coordination with |
| IED | improvised explosive device |
| IGO | intergovernmental organization |
| | |
| J-2 | intelligence directorate of a joint staff |
| J-3 | operations directorate of a joint staff |
| JDDOC | joint deployment and distribution operations center |
| JFACC | joint force air component commander |
| JFC | joint force commander |
| JFLCC | joint force land component commander |
| JFMCC | joint force maritime component commander |
| JIOC | joint intelligence operations center |
| JIPOE | joint intelligence preparation of the operational environment |
| JISE | joint intelligence support element |
| JLSB | joint line of communications security board |
| JMC | joint movement center |
| JOA | joint operations area |
| JP | joint publication |
| JSA | joint security area |
| JSC | joint security coordinator |
| JSCC | joint security coordination center |
| JSO | joint security operations |
| | |
| LOC | line of communications |
| | |
| MAGTF | Marine air-ground task force |
| MANPADS | man-portable air defense system |
| MCM | mine countermeasures |
| MCRP | Marine Corps reference publication |
| MCWP | Marine Corps warfighting publication |
| MDSU | mobile diving and salvage unit |

| | |
|------------|---|
| MEB | maneuver enhancement brigade |
| MILDEC | military deception |
| MNF | multinational force |
| MOA | memorandum of agreement |
| MP | military police (Army and Marine) |
| MSF | mobile security force |
| | |
| NCO | noncommissioned officer |
| NGO | nongovernmental organization |
| NTTP | Navy tactics, techniques, and procedures |
| | |
| OA | operational area |
| OCS | operational contract support |
| OP | observation post |
| OPORD | operation order |
| OPSEC | operations security |
| | |
| PIR | priority intelligence requirement |
| PR | personnel recovery |
| PSC | private security contractor |
| PSU | port security unit |
| | |
| ROE | rules of engagement |
| RSO | regional security officer |
| | |
| SAM | surface-to-air missile |
| SDO | senior defense official |
| SecDef | Secretary of Defense |
| SITREP | situation report |
| SJA | staff judge advocate |
| SOFA | status-of-forces agreement |
| SPOD | seaport of debarkation |
| | |
| TACON | tactical control |
| TCF | tactical combat force |
| TCN | third country national |
| TIM | toxic industrial material |
| | |
| UAS | unmanned aircraft system |
| UFC | Unified Facilities Criteria |
| USCG | United States Coast Guard |
| USG | United States Government |
| USTRANSCOM | United States Transportation Command |
| | |
| VAAP | vulnerability assessment and assistance program |

PART II—TERMS AND DEFINITIONS

alert force. None. (Approved for removal from JP 1-02.)

area command. A command that is composed of elements of one or more of the Services, organized and placed under a single commander and designated to operate in a specific geographical area. (Approved for incorporation into JP 1-02.)

area damage control. Measures taken before, during, or after hostile action or natural or manmade disasters, to reduce the probability of damage and minimize its effects. Also called **ADC**. (JP 1-02. SOURCE: JP 3-10)

base boundary. A line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas. (JP 1-02. SOURCE: 3-10)

base cluster. In base defense operations, a collection of bases, geographically grouped for mutual protection and ease of command and control. (JP 1-02. SOURCE: JP 3-10)

base cluster commander. In base defense operations, a senior base commander designated by the joint force commander responsible for coordinating the defense of bases within the base cluster and for integrating defense plans of bases into a base cluster defense plan. (JP 1-02. SOURCE: JP 3-10)

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. Also called **BCOC**. (JP 1-02. SOURCE: JP 3-10)

base commander. None. (Approved for removal from JP 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 United States forces. (Approved for incorporation into JP 1-02.)

base defense forces. None. (Approved for removal from JP 1-02.)

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. Also called **BDOC**. (Approved for incorporation into JP 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. (JP 1-02. SOURCE: JP 3-10)

combat service support elements. None. (Approved for removal from JP 1-02.)

force protection working group. Cross-functional working group whose purpose is to conduct risk assessment and risk management and to recommend mitigating measures to the commander. Also called **FPWG**. (JP 1-02. SOURCE: JP 3-10)

joint base. In base defense operations, a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located. (Approved for incorporation into JP 1-02.)

joint security area. A specific surface area, designated by the joint force commander to facilitate protection of joint bases and their connecting lines of communications that support joint operations. Also called **JSA**. (JP 1-02. SOURCE: JP 3-10)

joint security coordination center. A joint operations center tailored to assist the joint security coordinator in meeting the security requirements in the joint operational area. Also called **JSCC**. (JP 1-02. SOURCE: JP 3-10)

joint security coordinator. The officer with responsibility for coordinating the overall security of the operational area in accordance with joint force commander directives and priorities. Also called **JSC**. (JP 1-02. SOURCE: JP 3-10)

mobile security force. A highly mobile and dedicated security force with the capability to defeat Level I and II threats in a joint security area. Also called **MSF**. (Approved for incorporation into JP 1-02.)

port security. The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accidents; thefts; or other causes of similar nature. (JP 1-02. SOURCE: JP 3-10)

rear area operations center/rear tactical operations center. None. (Approved for removal from JP 1-02.)

regional security officer. A security officer responsible to the chief of mission (ambassador), for security functions of all United States embassies and consulates in a given country or group of adjacent countries. Also called **RSO**. (Approved for incorporation into JP 1-02.)

response force. None. (Approved for removal from JP 1-02.)

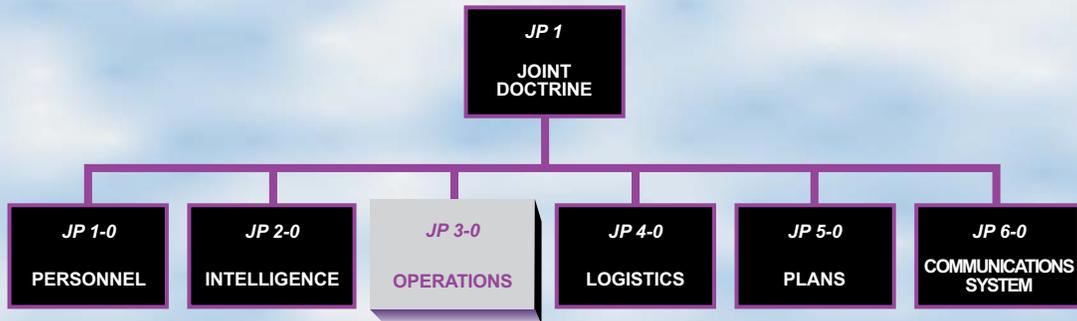
security. 1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. With respect to classified matter, the condition that prevents unauthorized persons from

having access to official information that is safeguarded in the interests of national security. (JP 1-02. SOURCE: JP 2-0)

tactical combat force. A rapidly deployable, air-ground mobile combat unit, with appropriate combat support and combat service support assets assigned to and capable of defeating Level III threats including combined arms. Also called **TCF**. (Approved for incorporation into JP 1-02.)

vehicle-borne improvised explosive device. A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Also called **VBIED**. (Approved for incorporation into JP 1-02.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-10** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

