BASE DEFENSE AT THE SPECIAL FORCES FORWARD OPERATIONAL BASE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

CURTIS W. HUBBARD, MAJ, USA
B.S., University of Miami, Miami, Florida, 1990

Fort Leavenworth, Kansas
2002

ABSTRACT

BASE DEFENSE AT THE SPECIAL FORCES FORWARD OPERATIONAL BASE by MAJ Curtis W. Hubbard, USA, 122 pages.

Special Forces forward operational bases (FOB) are essential for mission and contingency planning as well as for the preparation, infiltration and exfiltration of Operational Detachment Alphas (ODA). Therefore, the defense of this command and control headquarters is critical for preserving combat power and synchronizing military actions in a theater of operations. Because the enemy has the capability of projecting forces with the objective of disrupting US military operations, FOBs have become likely targets.

According to SF doctrine, FOBs should be located in secure areas with MP or host-nation personnel providing the bulk of the security force. Although this situation is preferable, it is by no means assured. FOBs should be able to provide their own security in the event other forces are not available or when rapid deployment restricts the flow of conventional forces into a theater of operations. After-action review results from the Joint Readiness Training Center demonstrate that many SF battalions are not prepared to execute base defense tasks without the assistance of other forces. Many SF commanders do not consider base defense a mission essential task and the result is a lack of training by many of their personnel.

This study analyzes joint and SF doctrine, observations from the field, and the effects of the contemporary operating environment to identify weaknesses in the readiness of SF battalions. This project attempts to answer three major questions that are the basis for the research. 1) With the emergence of an asymmetrical threat in the contemporary operating environment, does current doctrine adequately and realistically address base defense measures at the FOB? 2) Can SF commanders assume that attachments from other units will be available to defend FOBs? 3) Has the nature of the threat changed significantly enough to alter current thinking? This study leads to the conclusions that SF should make base defense a priority, modify its doctrine, implement new training strategies, and procure base defense equipment.

ACKNOWLEDGMENTS

First, I must thank my wife Michelle, my brother Glenn, and my mother Glenda for their love and support--you are the best. During every phase of my life I have been blessed with amazing friends, both in the US and abroad. There are too many to list here, but suffice to say that all of those from my hometown in Boone, NC, college in Miami, FL, and those I have met in the army and on visits overseas, have made life rewarding and worthwhile; for that I am eternally grateful. I would like to thank my committee, LTC (Ret) Occhiuzzo, LTC (Ret) Babb, and Dr. Willbanks (LTC, Ret) for their guidance and professionalism during the course of this project. Thanks also to Carolyn, Sylvia, Glenn, Glenda, Michelle, and Helen Davis for support and proofreading help while attempting to understand SF operations and our associated acronyms.

Thank you to my previous battalion commanders, LTC Zeigler and COL Ruggley, for providing guidance and support without micro management during my commands. To the men of 3rd Special Forces Group (Airborne)--you are the unsung heroes of SF.

And to my Dad who is my true North seeking arrow.

TABLE OF CONTENTS

LIST OF TABLE

Table Page

ACRONYMS

AAR	after-action review
AO	area of operations
AOB	advanced operational base
AOR	area of responsibility
ARSOF	Army Special Operations Forces
ARTEP	Army Training and Evaluation Program
BDOC	base defense operations center
BCOC	base cluster operations center
C2	command and control
CA	civil affairs
CHECO	Contemporary Historical Examination of Current Operations
CI	counterintelligence
CINC	commander in chief
COG	center of gravity
DOD	Department of Defense
FM	field manual
FOB	forward operational base
FSOP	field standing operating procedure
FTX	field training exercise
HHC	headquarters and headquarters company
HSC	headquarters and support company

ISOFAC	isolation facility
JFC	joint forces command
JRAC	joint rear area coordinator
JRTC	Joint Readiness Training Center
JSOA	joint Special Operations area
JSOTF	joint Special Operations task force
JTF	joint task force
QRF	quick reaction force
MASCAL	mass-casualty
MEDEVAC	medical evacuation
METL	mission-essential task list
MI	military intelligence
MID	military intelligence detachment
MOOTW	military operations other than war
MP	military police
MTOE	modified table of organization and equipment
MTW	major theater of war
NCO	noncommissioned officer
OC	observer-controller
ODA	operational detachment alpha
OPCEN	operations center
OPFOR	opposing forces
PME	peacetime military engagement

PZ	pick-up zone
RAOC	rear area operations center
ROE	rules of engagement
RTOC	rear tactical operations center
SF	Special Forces
SFG(A)	Special Forces group (airborne)
SFOB	Special Forces operational base
SIGCEN	signal center
SJA	staff judge advocate
SO	Special Operations
SOF	special operations forces
SOG	sergeant of the guard
SOP	standing operating procedure
SOSCOM	Special Operations Support Command
SPTCEN	support center
SSC	smaller-scale contingency
TAP	*The Army Plan*
TCF	tactical combat force
THP	take home packet
THREATCON	threat condition
TTP	tactics, techniques, and procedures

US	United States
UW	unconventional warfare
XO	executive officer

CHAPTER 1

INTRODUCTION

Special Forces Base Defense

Although the operating environment has changed since the fall of the Berlin Wall in 1989, US Army Special Forces (SF) doctrine associated with base defense at the forward operational base (FOB) has not adapted. SF doctrine is vague and does not provide guidance to deployed battalions that must be able to execute missions both independently or as part of a joint task force. It is vital that the force implements creative solutions to these doctrinal shortcomings in order to prevent future casualties at SF FOBs.

Field Manual (FM) 3-05.20, *Special Forces Operations*, states that, "Whenever possible, an MP [military police] or infantry security platoon element is requested and attached to an SFOB [Special Forces operational base] or FOB for personnel and physical security. . . . If the supporting US MP element cannot fully perform the base defense mission, the SF base commander may have to divert operational and support personnel to augment MP capabilities" (1999, 5-46, 5-73). In theory, these statements appear to make sense. Unfortunately, the interpretation by the SF community is that base defense training for FOB personnel is not necessary because MP, host-nation, or other security forces will be available to secure the operating base. This interpretation is based on an assumption stemming from early 1980s doctrine, when the Army was much larger. However, due to a reduction in the overall size of the force and the increase of contingency operations throughout the world, manpower may no longer be available to support this requirement on every deployment. Many SF units now use this assumption

as an excuse not to train on skills necessary for providing adequate base defense measures. Although the primary focus of a battalion is the Operational Detachment Alpha (ODA), base defense is an essential force and operational protection measure necessary for preserving the combat power of strategic-level assets.

Doctrine dating back to the Vietnam War suggested that SF battalions should be located in a safe area, out of harm's way. Usually, this meant locating the base in a friendly neighboring country near a supportable airfield. Although a noncontiguous battlefield of the future may be similar to the one in Vietnam, the task organization of an FOB is significantly different today than it was in the 1960s. For this reason, one cannot assume that by simply comparing organizational strength a substantial conclusion can be reached--context is critical. In addition, a company headquarters in Vietnam performed many tasks a battalion does today. For the purpose of this study, base defense at the FOB (SF battalion) is the focus. However, the same principles can and should be used at the company level when an advanced operational base (AOB) is the primary, forward-deployed, command and control (C2) headquarters.

Another element FOB personnel should consider when preparing for deployment is the nature of the threat. Although the US is likely to have conventional encounters in the future, FOBs are much more likely to become engaged by terrorist elements or insurgent forces now than they were in the past. Since the mid-1980s terrorist acts, including attacks on American soil, have become more frequent. Today's terrorists are better trained, equipped, organized, and more audacious than those in the past; they are experts in unconventional warfare and are willing to plan for several years, as in the case of the bombers in Tanzania, Kenya, and the US, to attack. Because of this threat, finding

a safe, friendly country from which to deploy forces is becoming a concept of the past. Where will the next attack occur? Although SF battalions should, by doctrine, be located away from conflict, in an area where it is safe to operate with minimal defensive measures, does a place like this exist? Currently, doctrine appears to be incomplete, causing a ripple effect within the force that has directly affected training and readiness. If MPs or other forces are not available, SF battalions must use their organic support personnel to secure compounds. Are these cooks, mechanics, riggers, and supply soldiers adequately trained to deter or defeat a terrorist attack by well-trained individuals who have conducted detailed planning and rehearsals? FOBs will be targeted in the future, and they must be prepared to deter or defeat any threat, anywhere in the world, at any time.

Although SF groups operate similarly, they are all responsible for executing unique missions in different regions of the world. Therefore, specific techniques, procedures, and experiences associated with these various regions are all different. Even within an SF group, each battalion uses a variety of deployment techniques specific to its own theater of operations. For this reason, very few SF officers have a broad experience base necessary to compare and contrast techniques across the entire force. For example, an officer in 1st Special Forces Group (Airborne) may routinely deploy to areas in Korea, where host-nation forces and US MPs secure SF facilities. If an officer starts his career at the detachment level as a captain, returns to command a company as a major, and eventually becomes a battalion commander in the same unit, he can safely assume that this procedure is the norm. However, another officer who starts his career in 3rd Special Forces Group (Airborne) and never has a single MP soldier available during multiple

deployments to Africa will most likely have contrasting beliefs. No one group perspective is representative of all. Although experiences may be different, FOB defense is applicable to every battalion, regardless of geographical location or mission peculiarities.

The Research Question

With the emergence of an asymmetrical threat in the contemporary operating environment, does current doctrine adequately and realistically address base defense measures at the SF forward operational base?

Secondary Questions

Can SF commanders assume that attachments from other units will be available to defend FOBs?

Has the nature of the threat changed significantly enough to alter current thinking?

Assumptions

Due to documented shortcomings demonstrated by SF units training at the Joint Readiness Training Center, Fort Polk, Louisiana, base defense has consistently been identified as a weakness by observers-controllers (OC). The assumption is that this weakness is a valued indicator of a negative trend in the SF community. Therefore, SF must institute changes to better prepare base defense forces at the FOB level. SF battalions will increasingly be deployed on contingency operations during peace, war, and operations other than war, and for this reason base defense is a mission essential task. Differences of opinion exist as to who should be responsible for providing the base

defense force, but few would disagree that the protection of US soldiers is critical for mission accomplishment on every deployment.

Definitions

Like many other professional organizations, the military has created a unique language that is often misunderstood by civilians, as well as military personnel. In addition, the Army, Air Force, Navy, and Marines use service-specific acronyms, words, and phrases that do not necessarily have the same meaning. For this reason, the following alphabetized list clarifies key terms and allows for easy reference while reading this study.

Advanced Operational Base (AOB). The AOB is an SF company inserted into an area of operations to provide further C2 and support of operational detachment alphas (ODAs). The AOB does not have organic assets to isolate ODAs, but usually is the last staging area where a detachment can conduct final inspections and rehearsals prior to insertion. Other AOB operations include "establishing a deployment and recovery site, a radio relay site, and a mission support base" (FM 3-05.20 1999, 4-5).

Center of Gravity (COG). "Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight . . . the hub of all power and movement, on which everything depends" (FM 101-5-1 1997, 1-24).

Force Protection. Force protection includes the measures friendly forces use to insure the safety of soldiers while deployed or during training. It implies a planning process that considers the enemy threat, as well as environmental factors. This planning

process insures compliance with appropriate safety measures to reduce the risk of death or injury of US soldiers.

Forward Operational Base (FOB). An FOB is a battalion-level C2 element for deployed SF units. This headquarters node isolates and deploys ODAs, and consists of the primary battalion staff with augmentation. Typically, the FOB has 150 to 250 personnel, including the attached security force and the four major centers: the signal center (SIGCEN), that is responsible for all communications to higher and lower echelons; the operations center (OPCEN), that conducts current and future planning; the support center (SPTCEN), that plans and executes all logistics; and the isolation facility (ISOFAC), that provides a secure area for those detachments preparing for future operations. Doctrinally, FOBs should be located "at secure and logistically sustainable locations outside the combat zone. The bases do not necessarily need to be in the AOR they support" (FM 3-05.20 1999, 5-1). Ideally, they should be in friendly neighboring countries that are close enough for rotary (helicopters) or fixed wing (airplanes) assets to insert ODAs into their areas of operation (AO).

Joint Readiness Training Center (JRTC). The JRTC, located at Fort Polk, Louisiana, is one of two major training centers in the US. The center is unique because of its replication of warfare that tests both the fighters and the supporters. The opposition force (OPFOR) is a well-trained, active duty, parachute infantry battalion. Also unique to this training experience is the presence of OCs, who provide continuous feedback to leaders at every level. Although nothing is completely representative of warfare itself, the JRTC replicates some of the complexities of modern war, such as civilians on the battlefield, local police officials, the media, and an enemy force that is well trained in

guerrilla and small unit tactics. An FOB typically deploys to Fort Polk (or a location of its choosing), isolates and deploys detachments to remote locations on and off post (out of Louisiana), and tracks mission progress of these detachments.

Joint Special Operations Task Force (JSOTF). "A JSOTF is established to plan, conduct, and support joint SO [Special Operations] in a specific theater of operations or to accomplish a specific joint SO mission. Establishment of a JSOTF is appropriate when SOF command and control requirements exceed the capabilities of the theater SOC staff" (FM 3-05.20 1999, 4-3). When SF is the predominant land component, the JSOTF can be formed around a group headquarters. In this capacity, the JSOTF is normally the C2 element directly above the FOB, as well as other SO assets.

Observer-controller (OC). OCs are full-time facilitators of training at Army training centers and are responsible for monitoring and controlling exercises. They provide feedback on all facets of the exercise through after-action reviews (AARs), both written and verbal. Because SF OCs observe battalions from all active and National Guard groups, they are able to identify positive and negative trends and to offer solutions to problems that are affecting the force as a whole. In addition to AARs, OCs produce an annual *JRTC Special Operations Training Bulletin* that addresses problem areas affecting the entire SF community.

Operational Detachment Alpha (ODA). ODAs are the common denominator for SF units. Often called "A" teams or detachments, these elements consist of twelve individuals who are specially trained in unconventional warfare. Each ODA has weapons, demolitions, medical, communications, and small-unit tactics experts. All detachment members are cross-trained and speak at least one foreign language.

Special Forces (SF). SF is an Army component of SO that has five active and two National Guard groups. They "plan and conduct Special Operations across the range of military operations. Their tactical actions often may have operational or strategic effects. . . . The unique SF skills consisting of language qualification, regional orientation, area studies, and interpersonal relations which are key to the success experienced by the SF units in the field" (FM 100-25 1999, 3-1). SF operations are mission specific, require specialized skills, and are often located in the enemy's rear area.

Special Operations (SO). "Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or informational objectives by unconventional military means in hostile, denied, or politically sensitive areas" (FM 3-05.20 1999, G-26).

Special Operations Forces (SOF). "Those activities and reserve component forces of the military services designated by the Secretary of Defense and specifically organized, trained, and equipped to conduct and support special operations" (FM 3-05.20 1999, G-27). SOF are not Army specific and include specially trained personnel from each service.

Tactics, Techniques, and Procedures (TTPs). TTPs involve the use of military art and science, as well as the specific methods necessary to win at war. TTPs are specific and describe the standards and the procedures necessary to accomplish a task (FM 101-5-1 1997, 1-151). It is something that works well for a specific unit or section and should be part of a unit's standard operating procedures (SOPs) to pass along from one chain of command to the next.

Terrorism. Terrorism "involves the use or threat of violence as a method or strategy to achieve certain goals, and that, as a major part of the coercive process, it seeks to induce fear in its victims" (Vetter 1991, 4). Terrorists are motivated by causes that can be religious, political, or personal in nature.

Unconventional Warfare (UW). "UW is a broad spectrum of military and paramilitary operations, predominantly conducted through, with, or by indigenous or surrogate forces organized, trained, equipped, supported, and directed in varying degrees by an external source. UW includes but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery" (FM 3-05.20 1999, 2-1).

Limitations

Several limitations are beyond the control of the researcher. First, most SF historical data focus on the actions of ODAs and not FOBs. Second, most SF manuals do not mention base defense. Finally, the classification of this study prevents detailed discussion of current operations, the locations of FOBs involved in the war on terrorism, and the base defense security posture of these FOBs.

Delimitations

Although SF does not have one manual available explaining base defense methods and procedures, the conventional force has many. For this reason, conventional methods of employing security forces in support of base operations constitute the backbone of the study. Additionally, joint doctrine and lessons learned from training exercises at the JRTC are the driving forces behind recommended changes to *Special Forces Operations* (FM 3-05.20). Included are interviews with Vietnam veterans and

soldiers in the force today, most of whom were commanders of headquarters and support companies (HSC) or involved with the defense of an FOB during exercises or real-world deployments.

Significance of the Study

This study explores an issue that receives very little attention from the SF community until a battalion prepares for a deployment. Many commanders consider base defense training to be unnecessary, since the priority of most battalions is the training of ODAs. Even after terrorist attacks in Kenya, Tanzania, Japan, England, Israel, Pakistan, Yemen, and most recently the United States, many commanders still do not place emphasis on self-defense measures necessary for preserving their combat power. SF personnel are critical theater assets that can be rendered useless by one catastrophic event, such as a bombing, ambush, or chemical attack. Soldiers trained to cook, repair engines, or pack parachutes will most likely be responsible for securing the FOB with or without the assistance of additional security forces.

This study is designed to show that SF base defense doctrine is incomplete and does not adequately address the current operating environment. Many SF leaders make two major assumptions fostered by the interpretation of this doctrine. First, MPs or other forces will be available for FOB security during all contingency operations. Second, the FOB will be located in a secure location, without a significant threat. This study will show that, although these options are possible and preferred, they are by no means assured. SF must institute solutions that outpace emergent threats that are growing in sophistication and are willing to strike US interests both at home and abroad. This study

is relevant and should assist in the development of base defense doctrine and training priorities for SF FOBs.

Organization and Methodology

This study consists of six chapters that identify shortfalls associated with SF base defense doctrine, the threat, assumptions that permeate the SF community, and recommendations to address the problems. The study focuses on three general areas: (1) joint and Army doctrine, (2) current readiness issues associated with nonspecific SF doctrine, and (3) the operating environment.

Chapter 1, "Introduction," exposes the fundamental problem that is the reason for the study. The chapter discusses the background, research questions, assumptions, definitions, limitations, delimitations, organization, methodology, and the significance of the project.

Chapter 2, "Literature Review," addresses key research sources and their significance. This chapter consists of a review of Army and joint manuals, books, AARs, interviews, and articles, as well as other Department of Defense documents that were significant to the study.

Chapter 3, "Doctrine," discusses base defense doctrine in joint and Army publications. Doctrine concerning rear area security is the factual cornerstone of the study, and its lack of specificity relating to SF base defense is critical for understanding readiness issues in the force today.

Chapter 4, "Observations from the Field," identifies how SF doctrine is affecting the training of FOBs by discussing negative trends exposed by the JRTC. The chapter discusses technology and equipment issues, as well as problems associated with

multinational operations. Additionally, AARs from Haiti and Somalia expose several base defense problems experienced by American forces during real-world contingency operations.

Chapter 5, "The Contemporary Operating Environment," addresses the nature of the threat, how it operates, and certain characteristics that make it more dangerous to FOBs than in the past.

Chapter 6, "Conclusions and Recommendations," addresses ways in which SF can improve base defense planning and execution in the future. Specific changes to doctrine, prioritization, training, and equipment are all critical to the overall improvement of SF base defense capabilities.

Included in the study is a TTP section, found in appendix A, that includes lessons learned from multiple JRTC rotations from 1999 to 2001. Although chapters 1 through 6 target senior leaders in SF, the TTP section focuses on HSC commanders and first sergeants preparing for deployment. These procedures, if executed properly, greatly enhance a unit's success not only at the training centers, but, more importantly, also during real-world deployments. Appendix B reviews critical base defense lessons learned from the Vietnam War that are still applicable today. Appendix C lists five techniques for C2, and appendix D provides an annotated base defense operation order (shell) from *Joint Tactics, Techniques, and Procedures for Base Defense* (JP 3-10.1) units should use when preparing for deployment.

CHAPTER 2

LITERATURE REVIEW

Introduction

The purpose of this chapter is to review the most critical sources that either directly or indirectly support the research questions in chapter 1. Because the understanding of doctrine is critical to this study, an entire chapter has been dedicated to its explanation (chapter 3). Unfortunately, SF do not have one manual pertaining to the subject of base defense. This fact is significant to understanding why commanders do not make its training a priority. Why dedicate training time and resources to an activity that is not perceived as a critical task? In the case of base defense at the FOB, the absence of any definable doctrine on the subject supports the overall recommendations in the final chapter. On the other hand, the description of the contemporary operating environment is an area that receives a great amount of attention from both US civilian and military leaders. The threat environment after the Cold War has become the subject of countless books, manuals, and articles, and this study focuses on several that are critical for the SF community.

This chapter reviews national security documents, joint and US Army manuals, AARs, historical studies, books, and interviews relating to base defense, SF operations, and the current operating environment. The Combined Arms Research Library at Fort Leavenworth, Kansas, and the Special Warfare Center Library at Fort Bragg, North Carolina, were the two primary research facilities used in this study. The chapter is

divided into four sections: (1) strategic level documents, (2) joint and US Army doctrine, (3) AARs, and (4) other sources.

Strategic Level Documents

A National Security Strategy for a Global Age. The document that addresses the operating environment at the national level is *A National Security Strategy for a Global Age,* endorsed by President Clinton in December 2000; the Bush administration has not produced another version. This document discusses national interests, American values, and the role the US will have in shaping the future. The strategy is based on worldwide engagement that supports security goals while promoting prosperity. While military power is one of the elements of national power that shapes the international environment, it must be used in conjunction with diplomatic, economic, and informational programs and policies. Through military engagement in times of peace, the US attempts to prevent war; world stability directly impacts the nation's ability to prosper. *A National Security Strategy for a Global Age* discusses smaller-scale contingencies (SSC) that are characterized as resource intensive, long duration, and challenging: "These challenging operations are likely to arise frequently and require significant commitments of human and fiscal resources over time. . . . Resolving SSCs gives us the chance to prevent greater and costlier conflicts that might well threaten US vital interests" (Clinton 2000, 27).

Quadrennial Defense Review. The US Department of Defense released *The Quadrennial Defense Review Report* on 30 September 2001, just two weeks after the terrorist attacks on the Pentagon and the World Trade Centers. In the preface to the report, Secretary of Defense Donald Rumsfeld states, "We can identify threats, but cannot know when or where America or its friends will be attacked. . . . A central

objective of the review was to shift the basis of defense planning from a 'threat based' model that has dominated thinking in the past to a 'capabilities based' model for the future" (2000, II-IV). This shift is the catalyst for change within the Department of Defense. The report identifies the difficulty of determining sources of conflict as one of the most-significant factors of the new operating environment. Because the US will not be able to prepare its military for conflict in a specific region or against a specific adversary, the military will be forced to intervene against an enemy that has a wide range of capabilities. In order to prepare for this eventuality, the US military must adapt (2000, 6).

The Army Plan. *The Army Plan (TAP)* is midterm planning and programming guidance, endorsed by the Secretary of the Army, that connects the strategic goals of the National Command Authorities with those who are responsible for mission execution within the Department of the Army. *The Army Plan* provides direction for the Army over a sixteen-year period, attempting to define future threats and friendly capabilities necessary for defeating them. The 1998 *TAP* discusses global trends and sources of conflict that may have implications for Army operations in the future. Weakening ex-states, ethnic divides, and religious extremism plague the operating environment, which could have a major effect on future military actions. Although regional powers remain a threat to US interests, transnational dangers present an even greater problem, since they can involve multiple countries without a common, distinctive objective. The *TAP* defines asymmetric threats as those that "counter US capabilities by unconventional or inexpensive approaches that circumvent our strengths, exploit our vulnerabilities, or confront us in ways we cannot match in kind or effectively counter" (1998, I-9). In

response to the many threat scenarios, the *TAP* states that the military must be prepared to deter aggression during peace, fight and win major theaters of war, fight multiple smaller-scale contingencies short of war simultaneously, and support humanitarian operations at home and abroad (1998, I-13). In short, the military must be prepared to operate in virtually every environment and overcome any challenge.

Joint and US Army Doctrine

Operations (FM 3-0). With a changing environment come new ways of achieving strategic objectives. Because of these changes, the face of the military is changing and leaders are attempting to provide a common vision that will guide training and force development programs for the next thirty years. The Army cornerstone manual is *Operations*, which replaced the older FM 100-5 series. This new version is extremely "joint oriented" by design and focuses on the transformation of the Army. Instead of a Soviet-based threat, the Army is now developing strategies based on an enemy that is not easily definable and does not operate in accordance with predictable doctrine. The idea of asymmetric warfare will become the norm for training, developing mission essential task lists (METLs), and adapting doctrine. In the past, Army leaders studied scenarios based on a conventional threat with a definable forward line of troops and known enemy capabilities. Now the battlefield transcends country borders and is more unconventional in nature. Military operations other than war (MOOTW) is accepted as the most likely environment for future military activities, and its effects will directly influence the positioning of FOBs, as well as the training of those soldiers tasked with security. This environment is more ambiguous and requires a greater understanding of the rules of engagement, psychological operations, and the operating environment. As the sole

superpower, the US needs an Army capable of defeating an enemy that avoids direct confrontation; he understands the US center of gravity, the nation's will, and will attempt to achieve victory through disinformation, subversion, and direct attacks on American interests at home and abroad.

Doctrine for Joint Special Operations. *Doctrine for Joint Special Operations* (JP 3-05) "provides basic concepts and principles to guide the Services and the combatant commands to prepare for and conduct special operations" (1998, I-1). It is the highest level manual for the employment of joint special operations forces that affects Navy, Air Force, and Army operations. This joint manual describes the strengths and weaknesses of SOF and establishes their principal missions: direct action, combating terrorism, foreign internal defense, unconventional warfare, special reconnaissance, psychological operations, civil affairs, information operations, and counterproliferation of weapons of mass destruction. JP 3-05 recognizes that SOF have adapted to the growing needs of the current operating environment by identifying collateral activities that must be executed using inherent capabilities present in their fundamental missions. These activities include coalition support, combat search and rescue, counterdrug activities, countermine activities, foreign humanitarian assistance, security assistance, and special activities. Although the manual focuses on C2 in the joint environment, there is no mention of base defense or security operations for SOF forces (1998, II-4, II-11).

Doctrine for Army Special Operations Forces. *Doctrine for Army Special Operations Forces* (FM 100-25), that will be renamed FM 3-05 under new doctrine restructuring, is the highest level document explaining the doctrine for Army Special Operations Forces (ARSOF), including SF, rangers, Army special operations aviation,

psychological operations, and civil affairs. "FM 100-25 describes the ARSOF strategic landscape; fundamentals; missions; capabilities; command and control; intelligence; command, control, communications, and computers (C4); and sustainment involved in the full range of military operations" (1999, iv). Significant is the description of the range of military operations--war, conflict, and peace--that are described in detail in chapter 5, "The Operating Environment," of this study. Although ARSOF functions and the framework for C2 in the joint environment are described, there is no mention of base defense requirements at forward deployed bases.

Special Forces Operations (FM 3-05.20). *Special Forces Operations* (FM 3-05.20) is an SF-specific manual guiding the conduct of all operations, training, and planning. It is a continuation of the doctrine found in *Doctrine for Joint Special Operations* (JP 3-05) and *Army Special Operations Forces* (FM 100-25). Although the manual focuses on the operational level of SF, it does discuss every command from the ODA to the United States Army Special Forces Command. FM 3-05.20 discusses the missions and employment options for SF while describing full-spectrum operations, relating tactical actions and activities to the operational environment. The manual is significant because it is the highest level SF document discussing base defense and security options at operational bases. Although FM 3-05.20 discusses aspects of security and lists three options for base defense, there is little detail. Employment considerations for MPs is not consistent with joint doctrine and threat levels are not addressed.

After-Action Reviews

The Joint Readiness Training Center (JRTC)

Because JRTC is the only US training location that routinely conducts base defense exercises, its lessons learned are essential for understanding the magnitude of the problem. OCs monitor every aspect of the exercise and conduct numerous AARs with the training unit. From these AARs OCs prepare a written report called a Take Home Packet (THP), which every battalion receives at the conclusion of the rotation. The purpose of the THP is to assist the unit in modifying SOPs and developing TTPs that could prove useful on future deployments. In addition to AARs and THPs, OCs produce the *JRTC Special Operations Training Bulletin* which combines major lessons learned from all rotations that year. After reviewing THPs from the past three years and bulletins dating back to 1993, OCs have consistently identified base defense as a problem.

Center for Army Lessons Learned (CALL)

The Center for Army Lessons Learned, an organization within the US Army Training and Doctrine Command, produces AARs for all major operations conducted by the Army. These AARs highlight aspects of military operations that were successful and those that were not. Because the overall objective of an AAR is to improve the force as a whole, their observations can result in changes to doctrine and unit training plans. For the purpose of this study, lessons learned from Operation Uphold Democracy in Haiti and Operation Restore Hope in Somalia were significant because of their explanations of base defense procedures in a MOOTW setting.

Contemporary Historical Examination of Current Operations

Contemporary Historical Examination of Current Operations (CHECO) was a means for Air Force units to pass lessons learned from one unit to the next during the Vietnam War. Because the nature of operations in Vietnam was extremely varied across the theater, the Air Force did not have established procedures for combating an unconventional threat. *CHECO* was a series of documents outlining effective TTPs of the enemy and the results of both positive and negative friendly counteractions. Most interesting to this study is the similarity between SF FOBs and Air Force bases supporting operations in Vietnam. Thailand had a lower threat level and was considered safer than Vietnam. Therefore, its operating environment was similar to the one recommended by SF doctrine for the positioning of FOBs. *CHECO Report 62* specifically recorded the events that took place on several bases in Thailand, hundreds of miles from the areas of operation they were supporting. The Air Force made assumptions at the time that correspond directly to those assumptions SF make today concerning base defense and force protection: (1) the enemy will not have a force projection ability capable of influencing US operations in "friendly" supporting countries; (2) during wartime, security forces will be made available to defend major C2 nodes; and (3) if a dedicated force is not available, one can be formed ad hoc from other occupational specialties (additional duty concept). In addition, the US did not initially have significant numbers of trained security forces and relied heavily on host-nation soldiers (Royal Thai Army) for support. This reliance on Royal Thai forces posed significant issues involving training, weapons, equipment, and communications. Without dedicated security forces, Air Force leaders were forced to use airmen that were not trained to execute base defense

tasks. This lack of training coupled with the limitations of host-nation support resulted in the deaths of Americans, as well as the disruption of offensive combat operations in Vietnam. *CHECO Report 62* is significant and shows how determined, unconventional forces in small elements can interdict major lines of communications and C2 nodes far from actual combat areas. Specific observations from this document are discussed in chapter 4, "Observations from the Field" (US Air Force 1973).

Other Sources

Books

Perspectives in Terrorism further defines the current operating environment and supports the conclusions that many US military and civilian leaders make concerning the nature of the threat. Because the future is unknown, many writers have begun to study the effects of the collapse of the Soviet Union, religious fanaticism, and terrorism. By studying the characteristics of the modern battlefield, the military has begun a transformation process to prepare US forces for an enemy that does not follow one common doctrine. Because most transnational actors do not have the ability to attack the US with conventional forces, potential enemies will resort to unconventional methods. Through the study of political and social factors that influence the interactions of all countries in the world, the US is able to prepare its forces for upcoming contingencies.

U.S. Army Special Forces, written by Colonel Francis J. Kelly, and other historical documents were especially useful for explaining how SF have developed during the past fifty years. Because many do not realize that the doctrinal method for employing SOF has changed, historical references are critical for understanding differences to force structure, C2, and mission parameters. The study of SF base defense

would be incomplete without a general understanding of forward-deployed bases in the past, and how they differ today.

Interviews

Although there are few references in this study to specific interviews with veterans and those in the force today, their impact is great. Without studying the nature of operations in Vietnam and base defense measures associated with remote base camps, it would be difficult to understand certain assumptions concerning security that many in the force believe today. Interviews with officers and NCOs from every SF group were essential for determining the differences in base defense procedures; no two battalions operate in the same area of the world using the exact same methods. For this reason, interviews added perspective to a subject that receives little attention in most AARs and SOPs.

Summary of Literature

Much of the literature reviewed in this chapter exposes weaknesses associated with SF base defense doctrine at the FOB level. Because this doctrine is incomplete, conventional methods of base defense will be discussed later in this study. The operating environment has changed since the collapse of the Soviet empire, and the military is just beginning to respond through changes in doctrine, force structure, training, intelligence, and TTPs. This chapter reviewed sources that are critical for understanding a problem that has great security implications if current procedures are not modified. SF cannot expect to be successful with their primary missions if appropriate security measures are not established immediately upon entry to a theater of operations and maintained throughout the deployment. The review of literature shows that although many believe

the contemporary operating environment to be extremely dangerous and unpredictable, there are few resources available for FOB commanders to reference concerning base defense techniques and methods.

CHAPTER 3

BASE DEFENSE DOCTRINE

Introduction

Army doctrine "provides a common language and a common understanding of how Army forces conduct operations. . . . where conflicts between Army and joint doctrine arise, joint doctrine takes precedence" (FM 3-0 2001, 1-14). Doctrine derives from the thought process that those that operate using a similar set of procedures will prevail during the confusion of war; it is the foundation for training plans, TTPs, and SOPs. Because war does not always allow time to orchestrate a decisive, well-coordinated plan at each subordinate level, leaders must have the ability and authority to act independently toward a common goal. Unfortunately, the lack of a true doctrinal approach for base defense has led to several misguided assumptions by SF leaders. Although doctrine recommends locating the FOB in a secure environment and employing MPs as the security force, these options are not assured. In order to understand the basis for many of these assumptions, it is necessary to consider the following six areas:

1. SF battalion organization
2. Organization of an FOB
3. SF doctrinal criteria for the location of the FOB
4. SF doctrinal security options for the FOB
5. MP doctrine and threat levels
6. Joint base defense doctrine

Because all of these areas contribute to the difficulties shared by those tasked to secure FOB compounds, their review is critical. The purpose of this chapter is to discuss doctrinal concepts for base defense and the location of the FOB. The conclusions and recommendations section found in chapter 6 is based on SF doctrine's applicability to current and future Army operations.

Organization of a Forward Operational Base

FOBs are critical C2 nodes within an area of operations (AO) that deploy and recover SF ODAs. The FOB is normally formed around an SF battalion headquarters and is the primary link between the detachments that are conducting operations within the Joint Special Operations Area (JSOA) and the higher headquarters, the Joint Special Operations Task Force (JSOTF), which is the controlling headquarters for all SO assets in theater. Mission requirements usually originate at the Joint Task Force (JTF), are analyzed and resourced at the JSOTF, and passed to the FOB which isolates and deploys the ODAs. Although the situation may differ from theater to theater, this is the preferred method for C2 within a joint operational area. The FOB could be as small as a staff section with several ODAs (fewer than 100 personnel total), or as large as 300-plus, with multiple company headquarters, ODAs, and support units. The supporting units could include MPs, engineers, medical personnel, civil affairs and psychological operations personnel, aviators, and sister service SO elements. The FOB has planners and intelligence experts who provide guidance to the detachments preparing for missions, as well as signal personnel who provide communications support. It also has soldiers who are responsible for maintenance, supply, religious, and administrative support.

SF battalions have three companies with six ODAs in each, and an HSC; every detachment consists of twelve personnel, with a captain as the commander. Under normal circumstances, because of personnel shortages, there are usually only eight or nine soldiers in each detachment, and now only five teams per company. Therefore, each company has approximately sixty to seventy personnel. The HSC, commanded by a captain, provides support to the entire battalion. This company includes the headquarters staff element, the signal detachment, and the service detachment, which has cooks, riggers, mechanics and other support personnel. The company consists of approximately 140 soldiers. In reality, the HSC commander has direct control over the signal and service detachments only. All subordinate staff NCOs and officers fall under the supervision of the primary staff officers. The cooks, riggers, and other support personnel are detached from the company and located at the SF group level (equivalent to a conventional brigade), where they perform their day-to-day staff duties in a consolidated work environment. Because these soldiers are detached from the HSC, they do not train with the unit or habitually deploy with their assigned battalions. Many may not know specific procedures, policies, or theater characteristics until deployed to the operational area. Therefore, leaders need time to bring their units together once deployed.

The commandant, who is usually the HSC commander and SPTCEN director, is tasked to plan, execute, and provide C2 of the security forces at an FOB. For the most part he employs riggers, cooks, radio operators, mechanics, and other soldiers to act as security and quick reaction forces (QRF) while they are off-duty from their regular day-to-day tasks. Doctrinally, uncommitted ODAs fall under his command for use as a base defense force, but most prefer having them train for upcoming missions. The base

defense operations center (BDOC) is the primary C2 headquarters for the defense of an FOB; it is the heart of a centralized system that connects the entire compound. All security personnel, ODAs conducting training, and the QRF, must coordinate with the BDOC before commencing operations. The BDOC sergeant of the guard (SOG) is the primary executor of the base defense plan. He inspects patrols, coordinates FOB security support, and is the focal point for all base defense activities. Most FOBs have separate day and night SOGs, and both work for the first sergeant and HSC commander. The commander, first sergeant, and the BDOC SOG prepare the defensive plan to deter "surface or air attack[s], including acts of sabotage and terrorism" (FM 3-05.20 1999, 5-16). If attachments are involved, such as MPs, engineers, or infantrymen, the senior attached individual could become the SOG. Beneath the SOG is the security force and QRF. The security force secures the compound, controls entry at the gate, and mans key positions. They can also control key access points within the compound, including the ISOFAC and OPCEN entry locations. The QRF is a ground element the SOG can deploy immediately in case of any attack or civilian disturbance. Because 100 percent alert of a compound takes several minutes, the QRF acts as a valuable economy of force element until the FOB can build sufficient combat power.

The most difficult aspect of the base defense plan is the synchronization of all FOB centers. The BDOC provides C2 and the majority of security forces, but the other centers are equally important in making the base defense successful. One key center that must be integrated immediately upon arrival to a theater of operations is the medical center. Because medical evacuations require security personnel for either pick-up zone (PZ) security or for accompanying a ground ambulance to the next higher treatment

center, neither center can successfully accomplish its mission without the other. Close coordination between these two centers is especially important during mass casualty (MASCAL) events when time is limited and lives are at risk.

Another critical center, the SIGCEN, is responsible for all communications with the next higher headquarters, as well as the supporting medical treatment facility. Although the BDOC may be able to coordinate directly with host-nation assets for medical and police support, the SIGCEN is the link to outside US or coalition resources and support; it must be integrated with the BDOC. As previously mentioned, direct communication with host-nation assets may be possible for the BDOC SOG, but it is more likely he will have to coordinate through the civil affairs (CA) officer or the CA military operations center located on or near the compound. In this case, the CA element must also be integrated into the base defense planning and execution process.

Although not typically associated with the BDOC, the staff judge advocate (lawyer) is essential for ensuring every soldier in the compound understands the rules of engagement (ROE). ROE have been an issue on real-world deployments, and JRTC exercises where most training units have at least one ROE-related incident; many have more. These incidents range from the shooting of unarmed civilians to the inability to return fire because of self-imposed or misunderstood ROE restrictions. For this reason, the lawyer is a critical link in the planning process and must be readily available to the BDOC to make "on the spot" decisions. Because the ISOFAC houses detachments prior to deployment, it is a pool of assets that may be used during an attack or incident. The ISOFAC has snipers, demolition experts, and most importantly, medical personnel, who are immediately available if coordination and rehearsals have been conducted. The

battalion commander, XO, and operations officer are all located in the OPCEN; it too is a primary link in the base defense process. The XO is responsible for the battalion time line and can assist the HSC commander by allotting time on the master schedule for full announced and unannounced rehearsals, both day and night. During an actual fight the battalion commander must be continuously updated on the current situation in order to reallocate assets as necessary. Because he has overall responsibility for the lives of the soldiers inside the compound, he must know when displacement or reallocation criteria have been met.

Special Forces Doctrinal Security Options for the Forward Operational Base

Special Forces Operations (FM 3-05.20) includes three options for base defense. The primary option is for an all-US force (not SF) to secure the compound and provide external patrols. Ideally, the FOB would be internal to a larger existing military facility, and MPs or infantry soldiers would comprise the force (1999, 5-71). The second option is for a combined MP or infantry force to augment host-nation personnel tasked with security. In this option, the compound could be part of a larger existing host-nation facility (1999, 5-72). Internal security remains the responsibility of US forces, but the external perimeter is secured by the host-nation. FM 3-05.20 mentions that if MPs are not available, the "SF base commander may have to divert operational and support personnel to augment MP capabilities. This option should serve as a last resort and be relied upon only when absolutely necessary." The third option is for the host-nation to provide forces for both internal and external security; contracted forces can also be used (1999, 5-74). FM 3-05.20 also mentions the use of a security platoon as a separate organization within the support center. A security platoon of MPs should be used

"whenever possible," but requires coordination "because of the lack of formal security augmentation agreements between the Special Forces Group (Airborne) and the ASCCs [Army Service Component Command]" (1999, 5-10).

Doctrinal Criteria for the Location of the Forward Operational Base

According to the 1999 publication of FM 3-05.20, the "group commander should locate the SFOB or FOBs at secure and logistically sustainable locations outside the combat zone. The bases do not necessarily need to be in the AOR they support" (5-1). Because FOBs are strategic C2 centers, they should be located in secure areas. The JSOAs should be within range of air, sea, or land transportation assets, but FOBs do not need to be forward to do this. As long as they can maintain C2, support the detachments logistically, and assist in their rescue if necessary, FOBs can be located several hundred miles away. In order to deploy and redeploy ODAs, FOBs should be close to airports, airstrips, sea ports or helicopter pickup zones. Often, host-nation or US military bases in friendly or coalition-supporting countries have the infrastructure necessary to support SF operations. Unfortunately, a larger US footprint could result in a greater chance of a direct terrorist attack (1999, 5-1). SF assets can be dispersed to reduce their ground signature, but this leads to C2 gaps and thins an already lean security force. With supporting Navy assets, operational bases can be afloat, reducing the support package and preventing the need for additional security assets.

Military Police and Threat Levels

Because SF doctrine recommends the use of MPs to protect forward-deployed bases, one would think that the MP corps would agree. However, their cornerstone manual, *Military Police Operations* (FM 3-19.1), contradicts SF doctrine by stating that

individual unit commanders are responsible for Level I threats. Joint Pub 3-10.1, *Joint Tactics, Techniques, and Procedures, for Base Defense*, reiterates that "most of the personnel for defense will be obtained from the units devoted to the accomplishment of the base's primary missions" (1996, IV-4). This means that the operational unit never loses responsibility for base defense, and its personnel will comprise the majority of the defense force. MPs can assist in the process, but their assets are too few to secure every operational base in the theater. If the geographical CINC attaches an MP unit to an SF battalion, their forces will most likely complement an already existing base defense capability.

The US Army uses predetermined criteria to evaluate a threat's ability to conduct offensive action. A Level I threat is the lowest of the three threat levels but is not necessarily considered "safe" because of the enemy's ability to operate clandestinely. It can be resource intensive due to the complexity of finding and defeating an enemy that presents few overt indicators. This level encompasses many enemy actions that could potentially disrupt an FOB including subversion, sabotage, kidnappings, sniper attacks, small-scale raids, and ambushes. Level I threats also include civil disturbances that could damage the morale and training of soldiers inside the compound and the indigenous civilians, as well as the American population (2001, 3-11, 3-12).

Level II threats include attacks from guerrilla, unconventional warfare, and small tactical unit forces. These forces can be irregular, indigenous, and trained by enemy advisors. The effects of these elements are especially dangerous because of their ability to move undetected throughout the AO without arousing suspicion; these forces can move freely, attack suddenly, and blend back into the local population. The differences

between Levels I and II are difficult to separate and not necessarily discernable on the ground. At both levels, enemy elements have the ability to conduct offensive combat operations and intelligence-gathering activities. The threat levels are based on the enemy's potential to conduct operations as interpreted by intelligence analysts. A Level II threat implies a larger, coordinated force that has hostile intentions, and is not necessarily just gathering intelligence. Although the distinction between threat Levels I and II can be blurred, each level does have a direct link to the force protection posture that is appropriate for an FOB conducting operations in theater (FM 3-19.1 2001, 3-11, 3-12).

Level III threats are conventional forces trained in combat operations that could significantly disrupt or destroy key American interests in a contingency theater. Because this is the highest threat level, these activities could have disastrous effects on the ability of US forces to successfully execute strategic operations. Unless an FOB is supplemented with substantial augmentation, deployment to an area with a known Level III threat is not recommended. FOBs could be established in a position where Level I and II threats are in the AO, but a Level III is beyond the normal scope of an SF battalion's defensive capability.

> Potential threat forces are capable of projecting combat power rapidly by land, air, or sea deep into the rear area. Specific examples [Level III] include airborne, heliborne, and amphibious operations; large, combined-arms, ground-forces operations; and bypassed units and infiltration operations involving large numbers of individuals or small groups infiltrated into the rear area, regrouped at predetermined times and locations, and committed against priority targets. (FM 3-19.1 2001, 3-11)

Table 1 simplifies the threat level status by showing examples of enemy activity and the appropriate response forces necessary to defeat them. In all cases for a Level I

threat, the base commander is responsible for his own defense. Only when a commander feels that the threat's capability is above his level of training or defensive posture will he receive MP support. *MP Operations* (FM 3-19.1) was written with conventional rear echelon forces in mind and did not mention SF specifically. However, this is the current doctrine for MP forces. Even when they are tasked to assist a base commander with his defense, MPs provide external security to complement an existing internal base defense network; MPs are rarely responsible for the defense of another unit's compound. Since some parallels exist between air bases and SF FOBs, MPs could be employed similarly. MPs "are responsible for the air base's external defense. Its internal defense is primarily the responsibility of the Air Force's security forces. The security force provides in-depth defense for weapons, weapons systems, command centers, personnel, and other priority resources established by the base commander. . . . The security force is trained and equipped to detect, delay, and deny Level I and II threats" (2001, 4-34).

Table 1. Threat Levels and Response Mechanisms

Threat Level	**Example**	**Response**
I	Agents, saboteurs, sympathizers, and terrorists	Unit, base, and base-cluster self-defense measures
II	Small tactical units, unconventional-warfare forces, guerrillas, and bypassed enemy forces	Self-defense measures and response forces with supporting fires
III	Large tactical-force operations (including airborne, heliborne, amphibious, infiltration, and bypassed enemy forces)	Timely commitment of a TCF (Tactical Combat Force)

Source: FM 3-19.1 2001, 3-12

The use of MPs to man gates and prevent access to key facilities within a compound is a waste of assets that could be used more effectively somewhere else. MPs should be used for external mounted and dismounted patrols, route security, individual personnel security, and for controlling technical assets designed to detect the enemy before getting to the internal defensive line.

> A base commander's defense plan is the cornerstone for protecting rear-area and sustainment operations. The base commander is responsible for defeating all Level I threats. When this threat exceeds his capabilities, he requests MP support. The MP located near bases or patrolling or conducting operations consolidate their forces, respond as quickly as possible, and conduct combat operations to destroy the enemy. (FM 3-19.1 2001, 4-35)

This is the doctrinal method to employ MP assets. However, many believe that when MPs are attached they will be tasked to secure points of entry, maintain access rosters, and man key fighting positions. The MP corps does not recommend this method of employment. Currently, MPs come to FOBs expecting to be used in accordance with their doctrine, while many SF leaders expect them to provide the bulk of the security force for both the internal and external perimeters.

Joint Base Defense Doctrine

Because most engagements will involve more than one service component, *Joint Tactics, Techniques, and Procedures for Base Defense* (JP 3-10.1) establishes defensive doctrine common to all. The guidance is authoritative, but can be adapted to particular situations when host-nation forces are involved or when other exceptional circumstances dictate otherwise (1996, i). For the most part, joint doctrine mirrors rear area Army doctrine, but in the case of SF, there is no other branch-specific document available that establishes distinctly different procedures. Although joint doctrine is designed for

conventional rear areas, the same principles can be applied to FOBs when deployed independently or with another JTF headquarters. Because FOBs are usually located near major logistics nodes and airfields, it is likely that one could be established in the joint rear area (JRA). Joint doctrine prescribes methods for effective C2, communications, logistics management, and integration with host-nation forces, as well as TTPs associated with the establishment and execution of a base defense plan. Critical to this study is the joint interpretation of C2, threat levels, terrorism, and the employment of security forces.

The CINC is ultimately responsible for all joint rear operations within his theater. He provides the guidance necessary to establish sufficient security measures for all units operating under his span of control. Through guidance, the CINC determines the classification of bases in his AOR by establishing single-service bases or a joint base that includes more than one service component. The joint force commander (JFC) is immediately subordinate to the CINC and is the commander of a combatant command, subordinate unified command, or JTF. The JFC organizes forces to best accomplish all assigned missions and insures a coordinated effort for logistics, intelligence, and operational support. Supporting combatant commanders provide support to the combatant commands and may either collocate or establish separate base clusters. In order to provide C2 for all units in the rear area, the JFC normally establishes a joint rear area coordinator (JRAC), who has the responsibility of coordinating the overall security for supporting and supported units operating in the area. When the threat level is high (Level III), the JFC may designate a subordinate commander the responsibility of countering the threat and restoring the JRA security. The JRAC coordinates with the combatant commanders exercising control over their individual areas of responsibility by

establishing a clear chain of command during the rear area fight (JP 3-10.1 1997, II-1, II-2).

Because the JRA is large and may include multiple units, separate services, airfields, ports, and other logistics facilities, it is divided into AOs that are the responsibility of subordinate commanders. These subordinate commanders "plan, coordinate, control, and execute rear security operations through rear area operations centers (RAOCs) or rear tactical operations centers (RTOCs)" (JP 3-10.1 1997, II-5). These areas are further divided into bases that are grouped into base clusters. Commanders are responsible for their individual bases while a base cluster operations center (BCOC) connects multiple bases, providing a centralized C2 headquarters within the cluster. Each base commander is responsible for establishing a BDOC, maintaining liaison with adjacent bases and the RAOC, and disseminating attack warnings. Individual units at each base must provide personnel to support the BDOC, conduct individual and collective training on defensive tasks, provide a communications link to the BDOC, and allocate soldiers for their own internal security. Base defense is a shared responsibility of all units on the base.

Although bases must be able to react appropriately to a Level I threat, they may not have sufficient combat power to defeat Level II and III threats. For this reason, the area commander may designate a response force commander with the task of supporting multiple bases within the AO. This force coordinates, rehearses, and supplements existing base defense forces to defeat Level II threats. For Level III threats, the JFC designates a tactical combat force (TCF) commander, who has sufficient combat power and flexibility to support several threatened bases or base clusters. Prior to hostilities the

TCF rehearses contingency plans with all bases or base clusters to insure the establishment of proper C2 procedures throughout the AO. Whether an FOB is located in the JRA or separately, base defense remains its responsibility. Joint doctrine mirrors that of MP doctrine and states that "day to day activities are conducted by the forces assigned to the base, usually as tasks in addition to their primary duties" (JP 3-10.1 1997, IV-6). Specifically, when there is a Level I threat, "available base assets should be able to detect and defeat enemy activities" (JP 3-10.1 1997, IV-6).

Joint Tactics, Techniques, and Procedures for Base Defense (JP 3-10.1) lists six terrorist threat factors for determining threat levels: existence, capability, intentions, history, targeting, and security environment. An analysis of these factors assists planners in the implementation of decisions, as well as training requirements, that ultimately prepare security forces for terrorist acts. By analyzing terrorist behaviors, their demonstrated ability for conducting operations, and the security environment, bases can prepare appropriate levels of defense. Warnings of terrorist activity come from US intelligence sources, foreign sources, the local population, security forces, or the terrorists themselves. Indicators of the threat's potential for combat operations are essential for determining the appropriate level of protection. Because security force capabilities are reduced when placed on "high alert" for long periods of time, the command must determine when to raise and lower the security posture. Once the base commander has considered these factors he can determine an appropriate threat condition (THREATCON) level (JP 3-10.1 1997, G-1, G-2).

The military uses the aforementioned factors to determine the severity of the terrorist threat. Through analysis, the unit commander establishes a THREATCON level

that corresponds directly to the threat's capability of conducting operations; each level has associated force protection actions. THREATCON Alpha (normal) is the lowest of threat levels and applies when terrorist activity is present but negligible (routine posture). THREATCON Bravo exits when there is terrorist activity, but the exact nature and extent are unpredictable. Under Bravo conditions the defense forces may have to implement higher measures of security, but specific enemy intentions are unknown. The defense force must be able to operate under these conditions indefinitely. THREATCON Charlie applies when there has been an incident or when intelligence predicts that an attack is imminent. Because THREATCON Charlie is resource intensive, the base may require augmentation for sustaining this level for long periods of time. THREATCON Delta is usually a localized warning and applies when there has been an attack in the immediate area or when one is expected. As in the case of THREATCON Charlie, THREATCON Delta requires augmentation for longer periods and should be reduced to a lower level as soon as possible (JP 3-10.1 1997, G-2, G-3).

Summary of Doctrine

The purpose of this chapter is to discuss key doctrinal concepts for base defense and the location of the FOB. A review of MP, joint, and SF base defense doctrine reveals several discrepancies. First, both joint and MP doctrines state that Level I threats are the responsibility of the individual unit and not that of attached security forces. Each unit must be able to operate in this environment indefinitely without outside assistance. SF doctrine does not currently recognize this concept and lists three options for base defense that are not based on threat levels, but instead on the assumption that attached security or host-nation forces will be available. Second, because the Army rarely conducts

operations unilaterally, it is very likely that FOBs will be located in the JRA where they will be responsible for supporting the overall theater base defense plan; SF doctrine does not address this possibility either. Although it is still preferable to locate the FOB in a friendly country without a high-threat level, commanders cannot safely assume this option will be the norm in the future. Whether in the JRA or another location altogether, base defense is and will continue to be the responsibility of the FOB commander. SF doctrine and its flaws are the focal point for developing corrective strategies addressed later in this study.

CHAPTER 4

OBSERVATIONS FROM THE FIELD

I don't give a damn about base defense (SF Battalion Commander, 2000).

Introduction

With the exuberance demonstrated by the above quotation from an actual SF battalion commander, units deploy to and execute training missions at the JRTC. Battalions attempt to accomplish base defense tasks often without mission essential equipment, adequate numbers of soldiers, and sufficient training time to prepare for the exercise. Because there is no "forcing function" by senior commanders, base defense is one area that is routinely neglected and often requires improvement at the conclusion of the exercise. This chapter shows how the inadequacy of current doctrine is reflected in training and real world operations; the consequences of TTPs and lessons learned not being incorporated into SOPs; and how flawed assumptions relating to the roles and missions of security forces further compound the problem. All of these factors combine to make FOB base defense a serious issue requiring changes at several levels of command.

Base Defense Experience

The idea, "train as you fight," is one that is significant to every leader in the military (FM 25-100 1988, 1-3). Realism is the key to maintaining an effective, proficient force. Also, because of significant cutbacks in manning, equipment, and resources, all leaders must make the best of what they have. At the same time, SF assumes that MPs or other attachments will secure forward-deployed bases. If "train as

you fight" is a correct maxim, then MP attachments should be part of every deployment to the JRTC. Is this happening? Out of the last eleven rotations to this training center, only two units had MP support (1999-2001). Of these, only one unit had a large enough MP contingent that no SF personnel were dedicated to the security force. It is disturbing that in two years of rotations, only one unit conducted operations using the preferred doctrinal method.

A key factor in the development of the doctrinal idea that SF do not need to provide their own security comes from the 1980s philosophy, when there was a bigger Army. Reductions in personnel at the Army level have had an impact on the MPs' ability to provide security forces for all deployed units. Although downsizing has affected the force, doctrine has not kept pace with these changes. SF doctrine pertaining to FOB security has remained unchanged since the early 1970s. Is it reasonable to believe that FOBs will always have security forces available? Although it is easier to assume these assets will be available than to train SF personnel, this is not a viable solution to the problem.

For those that have not been responsible for the base defense of a compound, the tasks involved appear fairly simple compared to those staff planners and deploying detachments execute. However, base defense is not limited to manning key points of entry or installing wire outside the compound. Instead, a base defense plan includes the synchronization of all other centers and the training of every soldier in the compound. It involves the use of technical and human resources to detect, contain, and destroy the enemy while preserving vital resources (US Air Force 1967, 57). The overall objective of a sound defense plan is to allow for uninterrupted operations of the FOB; the priority

of effort is the C2 of detachments that are deploying in support of operational and strategic objectives. Without an effective defense every disturbance, whether caused by the enemy or a rioting civilian population, may cause C2 interruptions. Therefore, the establishment of a base defense plan is the most critical first step for any operation.

One problem associated with this issue is a general lack of base defense knowledge by senior officers and NCOs. Most commanders, whether at company or battalion level, have not been on a deployment where there was a significant enemy threat. Because battalions go to JRTC only every eighteen months, and executive and operations officers change positions yearly, only one-half of the senior leaders have first-hand knowledge of base defense. Of the more than twenty captains in a battalion at any given time, only the HSC commander participates in exercises where base defense is his primary concern. Therefore, when captains become majors, most have very little base defense experience. JRTC is by no means the only place in the world where base defense is an issue. However, it is the only training environment where a trained OPFOR insurgent cell attempts to penetrate the compound. Many units, such as the 1st, 5th, and 10th Special Forces Groups, deploy routinely to areas of the world where they collocate with existing security forces. Even though base defense is a concern for these units, they do not validate their operating procedures and systems with an OPFOR cell (due to real-world issues). Other units participate in exercises where the host-nation or MPs secure the compound, but the likelihood of a trained insurgent OPFOR actively conducting offensive operations is low. Even in examples of MPs providing 100 percent security of a compound, few appreciate that the HSC commander and first sergeant are still heavily involved in the process by providing C2, as well as additional soldiers for security

purposes. In this case the MPs appear to be providing the entirety of the defense, but in reality are supplemented by other battalion assets. Commanders should understand the complexity of FOB defense and appreciate that all soldiers need to have at least a basic understanding of TTPs for the overall plan to be effective.

Observations from the JRTC

The lack of specificity in SF doctrine has resulted in training shortfalls by many SF battalions. This lack of training may be seen by observing the actions of soldiers tasked to execute security procedures. A review of observations from more than fifty JRTC exercises reveals two major categories of deficiencies: (1) synchronization and (2) individual and collective soldier training.

Synchronization

Synchronization is "the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time" (FM 101-5-1 1997, 1-149). A good base defense plan synchronizes operations through constant coordination with the ISOFAC, OPCEN, SPTCEN, as well as outside agencies, including nongovernmental organizations (NGO), host-nation forces, and the local government. A base defense plan is not limited to the BDOC and the security forces; everyone must be involved in order for it to be successful. For this reason, whether MPs are providing the majority of the security force or not, base defense is a collective task that must be planned in detail and rehearsed routinely. Many FOBs conduct rehearsals that involve the security force only and do not include soldiers from other centers. For many, base defense is a low priority until attacked by an OPFOR element or disrupted by

a civil disturbance. Only then do commanders appreciate the critical need for a trained security force.

The problem of synchronization begins when planners first receive word that an FOB deployment is imminent. Most of the battalion's resources are dedicated to the support of deploying detachments and support of the FOB as a whole. Although the battalion staff conducts mission planning, the HSC commander, first sergeant, and SOG often do not participate in the process. In addition, many units do not prepare a base defense annex to the battalion operation order (see appendix D). This lack of coordination from the initial stages of deployment was identified by OCs in the 1993 *JRTC Special Operations Training Bulleting 5*. They observed that "establishing and implementing an adequate plan for base defense remains a significant weakness. Many SPTCEN directors do not begin planning the base defense until after the FOB is established and the staff's attention is focused on tactical mission planning" (1993, 10). If the FOB waits to conduct planning until after they have arrived in theater, the overall defense will suffer.

Every soldier located at the FOB should have at least a general level of knowledge of the ROE, base defense operating systems, and the nature of the threat before arriving in a theater of operations. Because everyone will be involved in constructing wire obstacles, building bunkers and fighting positions to standard, rehearsing alert procedures, and supporting personnel accountability systems, training is critical. In addition, even the most routine of operations should be synchronized with the BDOC. For example, a detachment leaving the compound to conduct rehearsals prior to an infiltration must coordinate with the ISOFAC for vehicles, which requests them from

the SPTCEN. Forces will most likely be requested to travel with the detachment for convoy security and to secure the rehearsal site. The first sergeant, in conjunction with the BDOC SOG, reallocates security personnel to support this movement. If multiple detachments are training, even more security assets will be needed. Prior to anyone leaving the compound, the counterintelligence NCO from the OPCEN conducts security sweeps of the route and the training area. The SIGCEN deconflicts frequencies and monitors the radio net, since the rehearsal site will most likely be out of range of the hand-held radio used by the SOG. The battalion XO coordinates all of these activities, insuring that the master training schedule and time line support its execution. The SOG musters the security force, rehearses or discusses contingencies, conducts radio checks, and ensures that all soldiers manning gates and key positions are aware that elements will be moving outside the wire. Therefore, an event as simple as moving ten SF soldiers to a training site involves every center in the battalion. The BDOC becomes a key coordination link for the entire process. Battalions cannot expect an event as routine as the movement of a detachment to execute smoothly without extensive planning, wargaming, and rehearsals.

Realistic rehearsals are critical to the success of the overall base defense plan. Rehearsals should involve every center in the compound. Even if MPs are the primary security force, every center must also be involved. The 1997 *JRTC Special Operations Training Bulletin 10* identifies rehearsals as a primary failure of many SPTCENs.

> Rehearsals need to be conducted for all base defense operations, MEDEVAC [medical evacuation], MASCAL [mass casualty], and resupply operations. The basis of any good base defense is a good, well thought out plan. . . . Within the BDOC, the unit should rehearse all actions: guard force briefings, alert notifications, directing defensive operations from within the BDOC, using all of

> the communications systems that the BDOC has at its disposal, directing and conducting FOB displacement, destruction plans, etc. . . . Rehearse centers' internal notification procedures and accountability procedures during defensive actions, such as a sniper or civil disturbance. Also rehearse actions in which centers must man the wire on their portion of the defensive perimeter. (1997, 7)

Additionally, the 1999 *JRTC Special Operations Training Bulletin 11* observes that, "Only about half of rotational units plan and conduct base defense rehearsals" (1999, 6). Many SPTCENs provide exercise support during battalion-level training events at the home station and rarely get the opportunity to train on security tasks. Base defense procedures appear simple to many, but the synchronization of all battalion assets to support the overall plan is difficult. Because the FOB has multiple SF companies, detachments, and elements from other services, rehearsals are necessary to synchronize the overall effort. The first time an FOB rehearses these procedures should not be after the first contact with enemy forces.

Individual and Collective Soldier Training

Most evident to OCs at the JRTC is the lack of basic soldier skills by FOB security forces. Although most of the problems are associated with younger, less mature, support soldiers, they are not the only ones that experience difficulty during the exercise. SF soldiers tasked to supplement base defense forces discover that an uncertain environment (described in chapter 5) that has civilians, combatants, host-nation police, and military forces all intertwined can be extremely difficult. Additionally, the base defense force is usually comprised of soldiers from multiple organizations that do not have the same level of training. Because security forces must always be alert and expect the unexpected, it is difficult to balance adequate levels of force protection with combat fatigue. Most of the obvious training deficiencies occur several days into a rotation,

when soldiers are tired and the proximity of civilians brings combatants and noncombatants together. It is for this reason that training on basic soldier skills is a fundamental first step for overall mission accomplishment.

The most obvious example of inadequate training is an accidental discharge of a weapon. Over the course of the last three years, units average one of these per rotation; some have had as many as four. These incidents are caused not only by support soldiers but also by MPs and SF personnel. Although accidental discharges usually occur with a soldier's assigned weapon, such as an M4 carbine, there have been examples with crew-served weapons, such as the .50 caliber and M240 machine guns. Many discharges could have been prevented if leaders were constantly inspecting soldiers and conducting daily training. Units do not always establish SOPs determining when weapons should be loaded, when they should be locked and loaded, and when they should be carried with no magazine in at all. Although this is a basic task for soldiers, it is important to understand that other problems in more difficult situations result from a lack of these fundamental combat skills. It is not uncommon for an FOB to alert their compound of a sniper attack, man every position, and deploy the quick reaction force only to find that a soldier accidentally fired his weapon and was too embarrassed to admit it.

Fratricide is a problem OCs have identified as an issue that has individual and collective training implications. On average, every JRTC exercise has at least one fratricide and many near-fratricide incidents. Some of these incidents occur within the confines of the compound, while others are between guard towers and patrols, between two separate patrols, and between the host-nation police force and FOB soldiers. For the most part, C2 problems between the BDOC SOG and the patrol leaders are to blame.

However, the inexperience of the soldiers manning the gates and guard towers also contributes. The SOG often does not have sufficient experience controlling multiple units in close proximity. Many SOGs are support soldiers who perform their normal duties during the year and are tasked to run the BDOC once deployed. Usually, the first sergeant or HSC commander is also present in order to assist in the C2 of maneuver forces. Although the use of these key leaders is recommended, rehearsals are essential for maintaining control at all times. Control can pass quickly from a patrol leader who is involved in an engagement, to the SOG, and then to the first sergeant or HSC commander. In some cases the operations officer, ISOFAC commander, XO, or even the battalion commander becomes involved in the process. Control becomes an even greater issue when the compound is at THREATCON Delta and every fighting position is manned. Because FOBs typically do not have radios or field phones in every position, information dissemination also becomes a major issue. Training and rehearsals are critical for establishing effective SOPs and for increasing the confidence level of all soldiers in the compound.

Many believe that assigning MPs to secure FOBs solves the problem of base defense; however, synchronization and basic soldier skill issues will still be present without adequate training and rehearsals. According to MP and joint doctrine, MPs are best used for external patrols, convoy security, and quick reaction forces, while FOB soldiers execute the majority of base defense tasks (FM 3-19.1 2001, 4-34). The overall responsibility for the well being of all soldiers in the compound remains the FOB commander's; he cannot delegate the entire defense plan to an attached security force. The FOB will continue to have inherent responsibilities for C2, and for training soldiers

who will secure gates, conduct local patrols, and man fighting positions. (Appendix A contains a complete listing of base defense lessons learned and associated TTPs from JRTC.)

Base Defense Equipment and Technology

Although the training of soldiers is essential for the successful execution of a base defense plan, integrating technology is also important. Base defense equipment, such as cameras, sensors, motion detector lights, night vision goggles and scopes, and radios, are not available on SF battalion MTOEs (modified table of organization and equipment). Battalions have some hand-held communications equipment available, but those tasked with providing security are typically last on the priority list (well behind the detachments). Every member of the security force should have a radio, and each bunker or observation position should have a field phone. All centers should also be connected to the BDOC through a wire communications system. Vehicles leaving the compound should have a radio for internal convoy traffic, as well as for coordinating with the BDOC upon their return. Most battalions do not have enough radios to support all of these operations concurrently. Communications equipment is the single most important item for the security force; without it, C2 is virtually impossible. Some units have experimented with camera systems that were borrowed from other organizations for use during JRTC rotations. These cameras produce amazing results when incorporated with conventional defensive measures, but they are still not available to every FOB. Sensors, both acoustic and infrared, are all also essential for detecting the enemy early and for monitoring areas that are not observable. Again, most battalions do not have this equipment on their MTOE.

AARs from Operation Uphold Democracy in Haiti observed that combining technology with basic security procedures is of great benefit to those conducting operations in a MOOTW environment. The report stated, "Infantry units that are required to conduct security operations in a permissive environment may require additional equipment augmentation not normally found in the TO&E [table of organization and equipment]. . . . Units were required to conduct security operations more on the lines of military police operations" (CALL 1994, 131). Because internal base defense is doctrinally the responsibility of the unit, soldiers tasked with this duty should have the most appropriate equipment available. An example from this AAR describes a "field expedient" method of searching individuals for hidden weapons using a mine detector prior to their entering the compound. Eventually, the unit acquired metal detector wands from the airport to replace the mine detector (CALL 1994, 131). SF FOBs can expect to deploy to similar environments in the future. Items, such as metal detectors, are easy to obtain and relatively inexpensive. Other examples include mirrors for observing under vehicles, explosive material detection devices, digital cameras, bull horns, and hasty obstacles designed to puncture car tires. Training with law enforcement officials, independent security agencies, and MPs should be part of SF training plans to prepare soldiers for basic security operations. The lack of technological devices for base defense has been identified in the past and will continue to be a problem in the future if commanders do not make it a priority.

Even though technology is important, it is only as good as those that are trained to use it. Integrating technology is difficult if training is not conducted routinely prior to deployment. Many find that integrating cameras and sensors into the overall base

defense plan proves more tedious than any other training aspect. They also find that when technology becomes the main focus, soldiers become complacent and the enemy finds ways to counter the "high-tech" means of detection. Many battalions have difficulty integrating technology with human assets. For this reason, practice with technological tools, combined with base defense training, is essential for every effective defensive plan.

Host-Nation Security Forces

Special Forces Operations (FM 3-05.20) discusses three options for base defense: (1) MPs or infantry soldiers, (2) combined MP or infantry soldiers with host-nation personnel, and (3) host-nation or contracted forces (1999, 5-74). Although having MPs is definitely preferable, SF doctrine recommends the use of host-nation forces in two of its three courses of action for base defense. Host-nation security forces should be used whenever available, but the responsibility for the compound remains the FOB commander's. Having host-nation or foreign forces assigned as the security force is beneficial; however, training and coordination procedures are more difficult than when using an all-US force. In addition, host-nation forces may have individuals who are part of local insurgent organizations, making a counterintelligence plan critical. Virgil Carter, an SF officer in Vietnam states, "Every camp I knew of assumed that as a minimum ten to fifteen percent of the CIDG [Civilian Irregular Defense Groups] were VC-NVA [Viet Cong-North Vietnamese Army] supporters or actives. All of us went to sleep every night, in the camp and on operations, not really expecting to wake in the morning" (Carter 2001). The use of host-nation or coalition security forces is a viable course of action for FOB security; however, certain negative aspects should be considered.

CHECO Report #62 provides valuable insight into the difficulties involved with host-nation forces. Because the US bases were located in Thailand, they were thought to be in secure areas. Thailand had good relations with the US, and there was no reason to believe that their forces would not provide adequate security. In addition, the bases were collocated with Royal Thai Air Force units that already had security measures in place. However, lower levels of training, poor quality of integrated rehearsals, and lack of equipment contributed to their inability to properly secure US compounds.

> Despite the apparent willingness of RTAF [Royal Thai Air Force] forces to assist in internal security of vital resources, USAF [United States Air Force] security personnel chose not to utilize the available infantry force in any direct defense role. The reason for this was the inadequate RTAF training and their lack of familiarity with the USAF tactics and positions. . . . In January 1972, the RTA (Royal Thai Army) failed to provide external defense despite the fact that intelligence estimates indicated a strong possibility of enemy action. The only reason ever offered for this lack of cooperation by local RTG (Royal Thai Government) authorities was that they needed POL [petroleum, oils, and lubricants] support for their transportation. Thirteenth Air Force promptly authorized this support, but there was no increased cooperation. When Ubon was attacked on 4 June, Udorn RTAFB entered a Red Alert Security Condition and urgently requested RTA support under the May, 1972 joint-defense plan. None was forthcoming, and this prompted USA advisors to comment: "Advisors here feel that the quick reaction capacity committed to the RTAF base defense in the plan existed only on paper and did not, in effect, exist. . . . The external defense provided by the RTG and Provincial Police forces is adequate; however, their true capability and effectiveness is seriously limited. The Thai units. . . . are highly motivated, adequately trained and willing to help. . . . however, their combat capability is limited by adverse manning, outdated weapons, lack of communications equipment, limited vehicle fleet, and inadequate fuel allocation for their vehicles. (US Air Force 1967, 51, 54)

Although the Thai soldiers were motivated, they were not well trained and did not have the equipment necessary to provide an effective base defense force.

Other recent examples demonstrate similar difficulties in conducting combined operations with host-nation and coalition forces. During Operation Restore Hope in

Somalia, many US units used multinational forces to secure compounds and provide security during movements. AARs identify that the ROE were interpreted differently by many of these coalition forces. Most significant to the interpretation of the ROE was the use of graduated force. Each country used different levels of force in response to hostile situations (CALL 1993, XIV-4). Another AAR from the same operation states, "Base cluster defense in a joint and combined operation poses unique challenges which require close coordination between all nations, services, and other organizations" (CALL 1994, III-12-2). Challenges discussed include language barriers, levels of training, discipline problems, and a general lack of aggressiveness.

> External security was assigned to the United Arab Emirates (UAE). . . . Responsibility for internal security was assigned to Pakistan and to the Somali police. Neither allocated adequate resources to perform in a satisfactory manner, so the US requested augmentation from Nigeria, which provided a platoon of infantry to assist with internal security. (CALL 1994, III-12-2, III-12-3)

Even with this sizeable coalition force the defense was still not adequate. Eventually, an entire US infantry company was required to assist the multinational force with security (CALL 1994, III-12-3).

Although every situation is different, SF cannot assume that host-nation forces will be trained or equipped to US standards. There are many places in the world where host-nation forces perform just as well as US forces. However, knowledge of their weaknesses and strengths will most likely be incomplete until deployment to a contingency theater. Because the commander is responsible for the security of the FOB, it is his responsibility to insure that all participating host-nation and coalition forces are prepared. The American populace will not accept an excuse that host-nation security

forces were responsible for the death of an American soldier; security is ultimately a US responsibility.

SF cannot expect that every nation will be trained and have the equipment necessary to act in a base defense role. Many smaller nations deploy forces to contingency theaters expecting the US or the United Nations to provide logistical, administrative, and operational support. These soldiers often arrive without mission essential equipment. Therefore, there is an implied responsibility for SF base defense personnel to train, assist, and provide equipment for those forces that are tasked to secure the FOB. The BDOC has an even greater role when operating with these forces; C2 is much more difficult due to language and cultural barriers. In many cases, the command relationship with host-nation forces is not well defined and political factors are often more important than operational considerations. Synchronization and fratricide prevention are both extremely difficult, and the assumption that all host-nation forces support US goals and policies cannot be made in every situation. Because of these difficulties, all SF personnel must deploy with a high level of base defense expertise in order to train those foreign forces that do not.

Summary

The base defense plan involves everyone, and is not just the responsibility of the first sergeant or HSC commander. It is difficult to plan, even more difficult to execute, and must be rehearsed fully before implementation. Synchronization is critical for proper execution to prevent unnecessary delays in response to attacks and civilian disturbances. Training at the individual level is the key building block most often left out of training events. Although leaders are the primary planners and eventual managers of the

program, they are not usually the executors. The soldiers that see suspicious activity first will most likely be the lowest ranking; usually they have less experience and only a vague understanding of the overall situation (especially if this is not their primary duty). Therefore, support soldiers in this capacity require more supervision and constant training on basic combat skills and the ROE. Soldiers must be equipped and trained to use the best, most appropriate, security equipment available. Whether through normal Army supply channels or from civilian security agencies, SF needs the capability of supplementing human security procedures with technological devices. Because SF cannot assume coalition and host-nation forces will arrive with sufficient skills and equipment to support the base defense plan, the FOB must conduct exercises once deployed. Whether independently, with MP or host-nation support, or through a combination of all available assets, the FOB must be prepared to conduct base defense operations.

CHAPTER 5

THE CONTEMPORARY OPERATING ENVIRONMENT

Introduction

After reviewing doctrine and observations from the JRTC, the current situation is further complicated by the effects of the operating environment. The US now faces an unconventional threat that has the ability of projecting combat forces throughout the world. With this capability in mind, the US military has begun to take significant measures to transform its force for the post-cold war era; the future Army will be a more-responsive, less logistically heavy force. Unlike Desert Storm where the US had six months to establish combat power and form a coalition, future contingencies may not allow a long build-up period. This chapter analyzes characteristics of the contemporary operating environment, terrorism, and the effects of this new environment on the location and security posture of FOBs.

Background

Terrorists, saboteurs, and insurgents fight unconventionally in an asymmetric manner. This fact is nothing new, but the US Army consistently attempts to defeat this type of threat with a conventional mind-set. The security force responsible for the defense of an FOB compound probably will not be conducting counterinsurgency operations, but it will be part of the force that is; its location could be a target for enemy forces operating in the area. For this reason every soldier must understand the operating environment, as well as the capabilities of the enemy. Since World War II, the majority of warfare has been of an unconventional nature. Yet, the military is still more

comfortable in a conventional fight, such as Desert Storm. The British have lost soldiers every year since World War II, and except for three years in the Korean War, ten days during the Suez Canal crisis, twenty-five days during the Falkland Islands War, and 100 hours in Desert Storm, all were killed in low intensity conflicts. In 1983, 569 different terrorist groups were operating throughout the world. Eighteen years later, this number has nearly doubled. In addition to more groups, their capabilities have also increased, as most recently demonstrated in the destruction of the World Trade Center towers in New York City. "The continuing proliferation of insurgent organizations since World War II suggest that insurgency and terrorism are still widely perceived as an effective means of either achieving power and influence or bringing national or international attention to a cause" (Beckett 2001, 59).

Although insurgents have improved methods, weapons, and capabilities, not much has changed for US forces; the majority of training time still goes toward defeating conventional threats. This should come as no surprise, and history supports the idea that the Army has always considered unconventional warfare as "pretend" war. In 1763, William Smith predicted the type of warfare that he expected to see during the Pontiac Rebellion. He stated, "The war will be a tedious one. . . . Instead of decisive battles, woodland skirmishes--instead of Colours and Cannons, our trophies will be stinking scalps. Heaven preserve you. . . . from a war conducted by a spirit of murder rather than of brave and generous offence" (Beckett 2001, 62). Two hundred years later, a prominent US general officer in Vietnam remarked, "I'll be damned if I permit the United States Army, its institutions, its doctrine, and its traditions, to be destroyed just to win this lousy war" (Beckett 2001, 59). This is the danger of fighting a creative, hidden

enemy: he will attack when and where he desires and is not bound to ROE historically thought to be acceptable during war.

The Operating Environment as Defined by the US

Since the fall of the Berlin Wall, military leaders and US government officials have attempted to define the operating environment. Without a clear vision, the military cannot be proactive and runs the risk of becoming antiquated. Should the US military maintain the capability of fighting two major theaters of war or just one? Will the threat be unconventional or conventional in nature? Does the military currently have the ability to rapidly deploy forces across the world prior to a conflict, preventing a war altogether? Even prior to the most recent terrorist attacks on US soil, clearly demonstrating the resolve of the nation's enemies, government leaders began defining an operating environment unlike the Cold War era. The military, traditionally funded, resourced, and trained to defeat a conventional threat, is now beginning a transformation process designed to defeat an enemy that is not necessarily state sponsored or motivated by purely military objectives. Therefore, the future operating environment requires greater flexibility and creativity by lower-ranking soldiers on the ground, includes unconventional warfare, and mandates precision engagement preventing the accidental killing of noncombatants that could negatively sway world opinion.

Because the post-Cold War environment is less certain, many smaller nations are now facing uncertain futures. These smaller nation-states could potentially become the battlefields of tomorrow without proper intervention and support. Although SSCs may not directly involve key national security interests, "resolving SSCs gives us the chance to prevent greater and costlier conflicts that might well threaten US vital interests"

(Clinton 2000, 27). The military has successfully been used and will continue to be used for preventive purposes; thus, more-frequent deployments to crisis areas are likely in the future. Instead of using a conventional model that is predictable, the military is preparing forces to defeat an enemy that has capabilities, but no one single standardized doctrine. This is the rationale for a flexible force that can rapidly deploy to a contingency theater without a prerequisite buildup period. The geopolitical setting following the cold war is unpredictable and constantly changing. This environment has already demanded the involvement of US military intervention on every continent. The military cannot train to defeat one threat, but instead must be able to respond quickly and lethally with a flexible force that is capable of adapting to any opponent's tactics (US DOD 2000, 3, 6).

The Army Plan addresses transformation within the force with the objective to "achieve and maintain a capabilities-based, threats-adaptive Total Army that is postured to support the nation's military strategy through the near-, mid-, and far-term futures" (US Army 1998, I-1). Although there are currently 170 to180 nation-states, those numbers could increase well beyond the 250 mark, the result of religious and ethnic division. The disintegration of these nation-states brings instability to the majority of regions in the world and is a reason to transform the military into a more mobile, flexible force. Because these smaller countries are not necessarily developed, there is a greater divide between those who are "haves" and those who are "have nots." The world's demographic situation fosters instability, increasing the likelihood of SSCs. "The net result of this social and political flux will be more world players, more variables, and more volatility in geopolitical interactions" (US Army 1998, I-5). Because of the splintering of larger nation-states into less supportable, smaller states, many of the

world's weapons of mass destruction have become items for sale. It is now possible for regional powers with access to wealth, information, and technology, to use nuclear, biological, and chemical weapons. Using preexisting telecommunications systems, future enemies have the ability to synchronize several military actions to produce massive political and military effects on US interests. Because the distinction among criminals, terrorists, and insurgents in failed nation-states is now blurred, the operating environment is complex and extremely dangerous for friendly forces.

Operations (FM 3-0) describes the spectrum of conflict by establishing the parameters between which the military executes operations. These parameters are war and MOOTW. Within these parameters, the military is able to execute a range of operations, including offense, defense, stability, and support. Offensive and defensive operations are usually associated with the "war" side of the spectrum while stability and support operations are mostly executed in MOOTW. Although this is the norm, there are always exceptions, such as humanitarian operations within the context of a major theater of war. This example shows that MOOTW characteristics are frequently apparent during war. Similarly, aspects of the offense and defense are found in the MOOTW framework. Within the context of war and MOOTW, *Operations* further divides the spectrum into three areas: major theater war (MTW), SSC, and peacetime military engagement (PME). PME falls on one side with MTW on the other. Most significant to this study are SSCs, which transcend both. Because contingencies have aspects of both peacetime engagement and war, it can be the most difficult environment to conduct military operations (FM 3-0 2001, 1-15).

Special Forces Operations (FM 3-05.20) places war and MOOTW on opposite sides of the operational spectrum but further defines the relationship by adding environmental conditions for each: permissive, hostile, and uncertain. A permissive environment is associated with peacetime military engagement focused on "prevent[ing] conflict through early intervention" (1999, 1-11). SF soldiers are key to each geographic CINC's peacetime engagement strategy by overtly demonstrating US resolve and interest throughout his AOR. Because these missions fall under the context of peace, there is little to no enemy threat, making the environment permissive. Advisors have freedom of movement, most likely do not carry weapons, and can conduct training or operations without a high probability of enemy offensive action. In contrast, a hostile environment is associated with war and includes different mission parameters than that of peace. Some of the missions in a hostile environment include special reconnaissance, direct action, and unconventional warfare. For the most part, SF soldiers will execute these missions forward of friendly lines, well beyond the operational reach of most friendly conventional forces. Once on the ground, they will not be able to move freely or operate in an overt manner; security is paramount for these operations. The enemy in a hostile environment is directly engaged with US forces and will attempt to destroy any forces conducting operations in the rear area.

Between environments labeled permissive and hostile are those identified as uncertain. While the hostile environment relates to war and the permissive environment relates to peace, the uncertain environment has aspects of both, and is associated with SSCs. In this environment the involvement of US conventional forces may be politically or militarily inappropriate. Therefore, commitment of these forces could cause

escalation, making matters worse in the long term. In this case, SF could be used to positively affect the overall outcome without great visibility from other nations, the media, or potential enemies in the AOR. As an example, SF advisors could train host-nation personnel in counterinsurgency operations without raising the suspicions of enemy unconventional warfare assets operating in the area. In this situation the threat is operating in the area, but is not necessarily targeting US personnel. This environment can move quickly to war or move back into the realm of peace, depending on the actions of the supported government and US forces. Because this environment is uncertain and unpredictable, it is difficult to prepare force protection plans that are appropriate for the situation without being too restrictive or excessively lenient. It is within this context that insurgents are expected to conduct intelligence gathering activities in preparation for small-scale, hit-and-run attacks on US compounds and activities. Because overt indicators of their presence are not always visible, an uncertain environment can be extremely resource intensive and often lacks a clearly definable end state.

Because the FOB must be located in a position where it has the ability to deploy, C2, and recover ODAs, it will most likely be in an area not considered hostile. However, the enemy may be operating in the area and there may be direct action against US personnel or bases, making the environment uncertain. In most cases the FOB deploys to support operations in peace and MOOTW, where these conditions are the norm. The FOB could only operate in a hostile environment with significant augmentation. The preponderance of operations for SF battalions occurs during MOOTW or peace. Therefore, this study focuses on the abilities, techniques, and procedures of terrorists and insurgents operating in these environments (FM 3-05.20 1999, 1-11).

The Most Likely FOB Operating Environment

SF units conduct combat operations in every operating environment, whether permissive, uncertain, or hostile. However, leaders must determine the most likely threat scenario to focus training plans and leader development programs. After considering joint and Army doctrine it is clear that the most likely environment for FOBs falls under the category of MOOTW. This environment is uncertain by nature and prevalent during SSCs. Although detachments may deploy into an environment that is hostile under the context of war, the FOB will most likely operate either in the JRA or independently with or without MP or host-nation support. The greatest threat to an FOB in this situation is an insurgent or terrorist group operating unconventionally in team-sized elements (four to ten personnel). Most likely enemy offensive operations consist of ambushes, sniper attacks, bomb attacks, and other actions designed to erode US will and disrupt the FOB's ability to conduct combat operations. If FOBs can detect and destroy enemy elements in MOOTW, they can also successfully operate in a permissive environment, where threat levels are usually much lower. If an FOB is ever required to operate in a hostile environment for any amount of time, it must receive additional forces or collocate with a unit capable of defeating Level II and III threats. Because today's battlefield is not limited to the AO where the predominance of US forces are conducting operations, the FOB must be able to deter enemy aggression wherever it is located. Joint doctrine stipulates that Level I threats are the responsibility of the unit; therefore, FOBs must be able to operate under these conditions indefinitely with or without additional forces.

Asymmetrical Threats

The idea of asymmetry is as old as warfare itself, and it explains the leverage smaller disadvantaged militaries use to fight those with greater military advantages. Asymmetry refers to a means of accomplishing objectives without a direct confrontation. "Engagements are symmetric if forces, technologies, and weapons are similar; they are asymmetric if forces, technologies, and weapons are different, or if a resort to terrorism and rejection of more conventional rules of engagement are the norm" (FM 3-0 2001, 4-30). Differences between the capabilities of two militaries can be considered asymmetric in nature when each is trying to exploit the other's weaknesses. For the purpose of this study, the idea of asymmetry means more than just exploiting a weakness. Because the US does not have a peer competitor with the ability to sustain a conventional, head-to-head fight, future threats will attempt to erode the US center of gravity through other means. Direct combat is not a preferable option for a lesser country or insurgent organization. Examples of asymmetric fights are the bombings of the African embassies, the Khobar towers in Saudi Arabia, and the Marines in Lebanon. The most difficult task for the military is to prevent the terrorist from setting the conditions necessary to strike; identifying key enemy payoff targets and preventing their destruction is paramount. Because the threat does not have the same power projection capabilities as the US, it will attempt to conduct limited attacks domestically and on forward-operating locations throughout the world. This is an assumption that is currently driving strategic planning and is setting the stage for more asymmetrical thinking in the future (NDU QDR Working Group 2001, 28, 57).

The Nature of Terrorism

Terrorism is the means for a physically and financially inferior aggressor to inflict devastating losses on a superior force. The killing of friendly forces by terrorists leads to dwindling public support, crippling a center of gravity that is critical to the morale and spirit of the US. This form of warfare is inexpensive for a terrorist, extremely unpredictable, and difficult to fight. Because a terrorist can pick the time and place for an event, defenders run the risk of maintaining extremely high force protection measures for long periods of time. Not only does this cause fatigue and cloud judgment, but it lowers the morale of friendly forces. Unfortunately, fatigue ultimately increases the likelihood of ROE transgressions and makes it easier for an incident to occur. Terrorism itself can be defined as "the use or threat of violence as a method or strategy to achieve certain goals, and that, as a major part of this coercive process, it seeks to induce fear in its victims" (Vetter 1991, 4). Within the broad category of terrorists are three subcategories of "crusaders, criminals, and crazies" (Vetter 1991, 5). "Criminals" may execute acts that look like those of a terrorist, but are actually a means to their immediate purpose of robbery. "Crazies" might believe they are working for a higher cause, but actually have a mental disorder that is the root of their hostility. For the purpose of this study, a terrorist is one who is a "crusader"--he works for a higher cause that cannot be achieved without terror and intimidation. More often than not the goals are political in nature. For this reason, battlefields are everywhere, and they must be fought abroad and domestically simultaneously. Is there such a thing as a friendly or safe country?

Why has terrorism replaced conventional armed conflicts? If a terrorist had the ability to effect immediate, unfaltering change through a direct, conventional conflict, he

probably would. The lack of a middle class in respect to military power has created the need for another process, one that levels the playing field. The price of conventional war is high, and its destructive nature leaves economically undeveloped countries in ruins. Because terrorist acts are smaller by nature, they are less likely to draw countries into open warfare, while still influencing public and world opinion. Terrorism is cost effective and makes better use of valuable resources, training, and time. Instead of training a large, combined arms team to defeat an enemy force, squad-sized units can kill more, with less loss, on higher-value targets. The anonymous nature of terrorism enables smaller countries or groups to conduct long contracted wars without the other side risking international outrage for retaliation (Vetter 1991, 19, 20).

Many believe terrorists to be amateur, uneducated criminals that have only self-taught skills in bomb-making and basic rifle marksmanship. Although some fit this description, a growing trend throughout the world has been a shift to state-sponsored terrorism. The terrorists who were responsible for some of the more recent events were well trained, organized, and mission focussed. They prepared for the task with extensive rehearsals and detailed intelligence planning. The bombings of two US embassies in Africa--Nairobi, Kenya and Dar Es Salaam, Tanzania--were not the work of amateurs. During recent court proceedings, many alarming facts surfaced concerning the nature of terrorist organizations, and specifically those that were trained by Usama bin Laden.

According to a recent article prepared by the Department of Energy titled "USA v. Usama bin Laden: Technical and Tactical Insights from the Trial," the terrorists responsible for the bombings were well financed and prepared. The terrorist cells that bombed the embassies displayed classic unconventional warfare techniques. The cells

were compartmentalized and the members did not know their superiors. Those in the logistical net did not know the bomb's target, but were responsible for other facets of the operation. Cellular organizations of this nature did not appear overnight and required tremendous amounts of clandestine training to prevent security breaches or compromise. Although the bombers on trial described their organizations slightly differently, several similarities are worth noting. First, multiple cells were used to carry out the bombings. One cell conducted logistical estimates and planning while still others were part of a reconnaissance cell (intelligence). The surveillance of the embassies included taking pictures and actually going into embassy compounds to refine sketches and confirm the feasibility of certain targets. Others were responsible for building and transporting the bombs, while other cells were responsible for the actual execution of the missions. Altogether, these efforts produced a coordinated, well-executed attack on politically sensitive targets. One of the most alarming facts was that the actual surveillance took place nearly four years prior to the attacks. Patience was critical for the successful execution of these missions, and this quality demonstrated that these terrorists were not amateurs (Leader 2001, 3, 4).

Understanding terrorist target selection is critical to understanding how they operate and how the US should best prepare. In the case of Nairobi, one terrorist told the court the embassy was selected because "1) it was occupied by many Americans, including press and military attaches and intelligence officers; 2) it was easy to hit; and 3) it had a female Ambassador whose death would result in more publicity" (Leader 2001, 4). In addition, he stated that during his training in Afghanistan he learned target priorities were: "1) US military bases, 2) US diplomatic missions and posts, and 3)

kidnapping Ambassadors" (Leader 2001, 4). Supposedly, these attacks in Africa were intended to "pave the way" for attacks on American soil. In addition, "it is interesting to note that despite some security around the US Embassies (guards, walls, gates and access controls), the facilities apparently were considered easy targets, perhaps due to the lack of stand-off distance and the fact that host-nation guards were unarmed" (Leader 2001, 5).

To further disprove the theory that terrorists are not well trained, the trial of those associated with the bombings elevated chilling facts concerning their level of preparedness. These terrorists were able to cross multiple country borders using false names in order to conduct training and operations. Specifically, some trained in Afghanistan, Sudan, and Lebanon "using explosives to destroy large buildings." Witnesses testified to receiving training in seven specific areas: "1) Islamic law and jihad; 2) explosives and advanced explosives training; 3) small arms training; 4) assassination training (some involving the use of chemicals, poisons, and toxins); 5) hand-to-hand combat training: 6) physical fitness training; and 7) training in operational principles, including collecting target intelligence and communications" (Leader 2001, 5, 6). These terrorists were not just maniacs with bombs but had spent years preparing for an event that would last seconds. They had manuals, advanced demolition training, higher-level operational planning courses, and supervision that coordinated two separate attacks to occur near-simultaneously.

The nature of terrorism has changed significantly over the course of the past ten years. Terrorists are now experts in unconventional warfare operations and receive extensive training prior to carrying out attacks. Because their organizations are cellular in nature, operational planning is compartmentalized, preventing compromise of the

entire organization if one or more individuals are captured. They are also able to operate under cover, cross country borders unrestricted, and synchronize multiple operations simultaneously. Terrorists, such as Usama Bin Laden, are patient, committed, industrious, and most likely to attack soft targets having political, military, or psychological value. FOBs could be considered one of these targets.

Effects of the Threat and the Operating Environment on the FOB

Because FOBs typically remain stationary for long periods of time in order to C2 deployed ODAs, they are logical soft targets. FOBs have high volumes of traffic by both ground and air assets and have a distinctive signature due to the amount of radio antennas, personnel, and equipment in the compound. A trained insurgent can easily recognize that the American forces operating in an FOB are significantly different from those of general purpose, conventional forces. For this reason the assumption can be made that FOBs will be part of a terrorist's high-payoff target list. After recent activities in Afghanistan, most countries in the world now understand the significance of SF and the impact they have on the modern battlefield. Terrorists know that the US Air Force and Army aviation are most effective when soldiers on the ground can direct fire and identify targets. Most terrorist organizations do not have the ability to prevent US air assets from flying, but they can reduce overall effectiveness by preventing ground forces from entering the fight and by disrupting their operations once they are inserted. Using asymmetric techniques, a terrorist can focus attacks on supporting bases throughout the theater of operations. By constantly disrupting SF operations at the FOB, training, communications, and C2 will all be negatively affected.

Although it is preferable to deploy FOBs to friendly countries outside the theater or AOR they are supporting, this has not necessarily been the case in the last ten years. FOBs have been located forward during military actions in the Gulf, Haiti, Somalia, Bosnia, Kosovo, and Afghanistan. Because every deployment is different, each SF group has a different AOR, and no two contingencies have the same enemy threat, there is no specific force protection model that every battalion follows. Understanding the environment and the threat's potential are critical for the execution of proper force protection measures, including base defense.

A permissive environment is the most preferable environment for an FOB since enemy offensive action is not likely. Typical missions in a permissive environment include peacekeeping, humanitarian, and disaster relief operations, and counterdrug or demining activities. In this situation an FOB could be positioned forward to facilitate the C2 of ODAs operating in the immediate area. While the FOB remains stationary near a key logistical or communications capable area, the ODAs move to their designated JSOAs and begin executing missions. In this scenario base defense measures could be as passive as increasing counterintelligence sweeps of the area, coordinating with the regional security officer in the embassy, or erecting a chain link fence around key facilities. An FOB could be called upon, without extensive external support, to coordinate relief efforts, assist nongovernmental organizations, and provide advisors for local host-nation military and police units.

An uncertain environment does not necessarily display distinctive characteristics making it permissive or hostile. A perceived threat is known, but its intentions may not be. Several ethnic divisions could be present in the AOR, making the outcome even less

predictable. An FOB could be directed to coordinate the efforts of several ODAs in this environment, mandating its forward presence (as opposed to being positioned in a secure location). This situation has become the norm for the majority of contingency operations in the last ten years. From Desert Storm until the present, FOBs have been situated in uncertain environments that required some type of base defense. An uncertain environment may appear calm, but tensions can build quickly and unpredictably, making it dangerous for military operations. Both permissive and hostile environments have indicators that make the situation somewhat predictable. An uncertain environment has aspects of both and can move from one to the other without warning. Base defense at this level is more overt and active, requiring training in soldier skills as well as the rules of engagement.

Hostile environments are the most resource intensive, risky, and constrained of the three, but they are also the most predictable. Under these circumstances enemy intentions and capabilities are known, and friendly elements make necessary adjustments. This environment most resembles the situation of "A" Camps in Vietnam. Soldiers knew the situation was hazardous and created base camps designed to defeat the threat. This situation is the least preferable for an FOB and is not recommended. Any element moving into a hostile environment, whether an ODA or FOB, requires great assistance in implementing a defense that is capable of sustaining combat operations with a minimum of disturbance. A hostile environment at the FOB level mandates support from infantry or MP units. It also implies at least a Level II threat that could peak to Level III. FOBs are not capable of sustaining ODAs in the field while simultaneously engaging

determined enemy elements; a hostile environment is the least preferable and requires augmentation by conventional forces.

Summary

Although SF doctrine implies FOBs should always be positioned in a safe area without a significant threat, the current operating environment described by US civilian and military leaders does not account for this possibility. Whether in Miami or Afghanistan, FOBs can be targeted anywhere; they must have the ability to implement sufficient security measures capable of defeating terrorist actions. Terrorist forces are well trained, motivated, and have the ability to blend in with the local population. They are patient and willing to wait for the right opportunity to use unconventional or asymmetric techniques against US forces. Because SF must have the ability to move rapidly into any contingency theater in support of national objectives, FOBs should have a firm understanding of base defense principles necessary to prevent the disruption or destruction of this critical C2 headquarters.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

> Fences only keep honest people and cattle out; they don't stop determined sapper squads.
>
> (US Air Force 1973, 58)

Purpose

The purpose of this chapter is to provide answers to the research questions, discuss major conclusions of the study, and recommend solutions to the overall issue of base defense at the SF FOB. A review of current doctrine, observations from the field, and the effects of the contemporary operating environment, leads to the conclusion that base defense is a problem requiring solutions at several levels of command. The "recommendations" section provides a systematic approach designed to increase the base defense capability and overall readiness posture of FOBs. This chapter is divided into three sections: 1) a restatement of research questions, 2) conclusions, and 3) recommendations.

Research Questions

Primary Research Question

With the emergence of an asymmetrical threat in the contemporary operating environment, does current doctrine adequately and realistically address base defense measures at the FOB? SF base defense doctrine is vague and is not consistent with *Joint Tactics, Techniques, and Procedures for Base Defense* (JP 3-10.1) and *Joint Doctrine for Rear Area Operations* (JP 3-10). Although it is still preferable to have MPs or other forces available to provide security, it is not always possible. Base defense is the

responsibility of the FOB rather than attached security forces, and the commander maintains responsibility for training and force protection. Because a lack of available conventional forces is a reality in forward areas, FOBs must be able to secure their compounds independently. Effects of the current operating environment further complicate the issue due to increased capabilities of unconventional threats; they are becoming more aggressive and are likely to use asymmetric techniques. SF doctrine does not address current threat capabilities and their potential negative impact on FOB operations. Because SF will most likely be targeted in the future, doctrine and TTPs must change to outpace the growing capabilities of those organizations determined to undermine the national security strategy of the US.

Secondary Research Questions

Can SF commanders assume that attachments from other units will be available to defend FOBs? It is obviously beneficial for FOBs to have additional security on extended deployments to areas that have a legitimate threat; however, a Level I threat is the responsibility of the FOB. During a major crisis, such as Operation Enduring Freedom, the joint force commander may not have forces available to supplement those FOBs deploying to permissive or unknown environments (where the threat level is perceived to be lower). In addition, SF may deploy to contingency theaters before suitable force protection packages are organized and ready for movement. Under both circumstances, FOBs must secure their compounds independently. Recent activities in Afghanistan demonstrate that this scenario is highly probable and will continue to be an issue in the future. Several FOBs involved in the war on terrorism have been deployed to areas with Level I threats without additional security forces.

Has the nature of the threat changed significantly enough to alter current thinking? Although it is still preferable to locate FOBs in permissive environments where the threat level is lower, it cannot be assumed that these areas are out of harm's way. Since terrorist organizations are not bound by restrictive ROE or influenced by negative political reactions by governments, they have the ability to attack at the time and place of their choosing (often without impunity). These characteristics make him dangerous, unpredictable, and capable of sustaining prolonged unconventional warfare campaigns. For these reasons, base defense is a critical force and operational protection measure necessary for preserving the combat power of SF.

Conclusions

Doctrine

SF FOB base defense doctrine is inadequate, dated, and does not address changes to the current operating environment. Modern battlespace cannot be defined in terms of forward and rear areas with implied threat levels for each; FOBs can be targeted anywhere in the world, even outside the theater of operations they are supporting.

FOB commanders do not abdicate the responsibility for base defense when additional security forces are attached; the safety of all assigned and attached personnel remains the responsibility of the FOB commander. Due to the operational limitations involved in projecting sizeable conventional force packages into theaters of operation rapidly, FOBs should have the ability to defend against Level I threats indefinitely with organic forces. The employment of additional security forces is preferred, but cannot be assumed to be available for every FOB deployment. When MPs, host-nation, or

multinational forces are attached or assigned to the FOB, they should be tasked to secure the outer perimeter while FOB soldiers secure the inner perimeter.

FOBs should be prepared to operate in the JRA and assist the RTOC, RAOC, and BCOC in the synchronization and implementation of a theater-wide base defense plan. The Army rarely conducts operations unilaterally as a service. Therefore, an understanding of the joint environment is essential for synchronizing efforts in a theater of operations. FOBs will be collocated with other service components in the future, and they should develop SOPs based on joint TTPs for base defense to prepare for this eventuality.

Observations from the Field

Many commanders, believing that base defense is not a mission essential task, do not include defensive tasks on their battalion METLs. Training deficiencies at the JRTC demonstrate that many battalions do not currently have the capability of defeating or deterring Level I threats without additional security forces. Even when MP or host-nation forces are available, they are often tasked to secure both the inner and outer perimeters of the FOB. This technique is possible when larger force packages are available in theater, but should not be considered the only doctrinal method of employment. In the future FOBs may be deployed to areas where no additional security forces are available; in these cases FOBs must operate independently. The lack of base defense equipment on battalion MTOEs further complicates this problem. Although some battalions have been able to procure security equipment prior to exercises and deployments, they rarely have time to incorporate these assets into the base defense plan.

Incorporating technology is difficult and requires training time to establish effective methods of employment.

Host-nation and multinational forces have and will be tasked to provide security for FOBs; many of these soldiers are not trained or equipped to US standards. Because security is the responsibility of the FOB, SF must be prepared to train, advise, and assist these forces. Whenever possible, FOBs should conduct assessments prior to deployment to determine additional needs for training and equipment. Once deployed, US personnel must provide C2, as well as combined training exercises, to insure that appropriate levels of security are maintained.

The Contemporary Operating Environment

Emergent threats are growing in sophistication and will attempt to strike US interests throughout the world. They are becoming more aggressive with time, using asymmetric techniques which are not limited to a particular theater of operations. These factors combine to make the current operating environment extremely complex and dangerous. Even forces operating in environments assumed to be permissive could be targeted by terrorists or insurgent groups sympathetic to anti-US policies and ideals. Following the success of Operation Enduring Freedom in Afghanistan, foreign militaries and insurgent groups have observed the employment of SOF, and understand that precision weapons are most effective when directed by forces on the ground. Additionally, they observed SF advisors training, assisting, and equipping indigenous forces in support of the overall campaign plan. Because foreign militaries and insurgent groups have difficulty affecting US forces once they are inserted into a theater of operations, they will attempt to degrade friendly operations asymmetrically by disrupting

C2 nodes. The FOB is a critical headquarters for SOF, and if disrupted could have a strategic-level impact on the overall theater engagement plan. Therefore, FOBs should be considered likely threat targets and defended appropriately.

Recommendations

The following recommendations should not be interpreted as an "all or nothing" approach for improving the base defense capability of SF FOBs. There are no simple solutions; however, implementation of some or all of these recommendations is a positive first step. This section is subdivided into four areas: doctrine, prioritization, training, and resources.

Doctrine

Special Forces Operations (FM 3-05.20) should include a detailed section on base defense responsibilities of FOBs and address the following changes: 1) FOBs may be deployed without additional security forces, even when Level I threats are known to be present; 2) FOBs may be located in the JRA (implied base defense responsibilities); 3) FOBs may be deployed to areas that are not considered secure (contrary to previous doctrine); and 4) an external security force should normally be employed to secure the outer perimeter, while FOB personnel maintain responsibility for securing the inner perimeter. The assumption that an external security force will always be available is no longer valid.

The Special Warfare Center and School, Department of Training and Doctrine (DOTD) should publish an SF-specific base defense manual. This manual should incorporate TTPs from real-world deployments and training exercises that explain how to plan, rehearse, and execute base defense operations. Additionally, it should address the

following: 1) methods for synchronizing base defense operations with the FOB; 2) effective communications systems; 3) C2 procedures; 4) base defense at the ODA, AOB, FOB, and SFOB levels; 5) techniques for conducting operations with MPs (their strengths, weaknesses, and recommended methods of employment); 6) operating with multinational forces and effective techniques for their training, advising, and equipping; and 7) an explanation of the JRA based on *Joint Tactics, Techniques, and Procedures for Base Defense* (JP 3-10.1). Although there is currently a "base camp" manual being developed by DOTD, it focuses on bare-base construction (engineer-related activities) and not base defense; these two topics are completely different and require two separate manuals.

Prioritization

Commanders must emphasize the importance of base defense at the FOB level. Training plans and METLs should prepare battalions for deployment without additional security forces. Because many SF battalions do not currently have a robust base defense capability, the United States Army Special Forces Command (USASFC) should make this training a priority. Although every battalion will have AOR-specific training plans, each must have the ability to defeat Level I threats immediately upon arrival to a theater of operations. Because time is limited and rarely will an entire battalion be able to train together, creativity is an essential ingredient to the overall solution of improving the defensive capability of FOBs. Base defense is a mission essential task, and making it a priority is a critical first step.

Training

Battalion exercises and weekly training plans should include base defense operations. Although the SPTCEN normally supports exercises logistically, it must also have an opportunity to train on basic defensive tasks. If time is limited, establishing the BDOC for a two or three-day period during a weeklong exercise is preferable to no training at all. Whenever the battalion trains, an aggressor force of two to six personnel should be used to represent a Level I threat. Even if this force does not attack the FOB, it can provide valuable feedback by conducting target analysis of the compound. Target analysis is an effective tool for confirming or denying the effectiveness of FOB defensive procedures by identifying weak spots, dead space, possible targets, key leaders, and vulnerabilities. Without this verification, battalions have no way of knowing whether their procedures are effective.

SOGs should be identified and trained throughout the year--not just prior to deployment; they need to be security experts. SOGs must have a solid tactical background combined with technical security training. Each battalion should train a minimum of two (day and night) and allocate funds for them to attend civilian security schools. These soldiers should become the primary trainers of all base defense personnel.

Resources

Commanders should allocate time for base defense training. HSC commanders and first sergeants need time to train their soldiers on basic defensive skills prior to deployment and after entry to a theater of operations. Additionally, every SF battalion should have base defense equipment on its MTOE. This equipment includes cameras, sensors, lights, and radios at a minimum. Stocks of barrier material, old parachutes, and

wire should also be made available to any deploying battalion. An alternative to equipping every battalion is to consolidate all base defense equipment at the group service company and sub-hand receipt needed items to deploying FOBs.

Closing

In order to improve the base defense capability of SF battalions, changes are necessary at several levels of command. Doctrine must change to reflect the effects of the current operating environment on the location of FOBs, stating clearly that base defense is the responsibility of the SF battalion commander. Attached or assigned forces may eventually comprise the bulk of the security force, but the FOB commander never abdicates the responsibility for security. Commanders should make base defense training a priority; it is a mission essential task and should be treated as such. In order to increase the level of training of SF support soldiers, METLs and training schedules should change allowing HSC commanders more flexibility. In addition, the HSC commander needs time and dedicated equipment to prepare his soldiers for deployment. SF will continue to be deployed with little warning, and they must establish appropriate levels of security the first day in a theater of operations.

Areas for Future Study

This study could not cover every subject related to FOB base defense and the following areas are identified for future study.

1. Creation of an organization at Special Operations Support Command that is capable of acting as an interim security force for deployed operational bases until conventional units can be moved into theater
2. Future roles of SF operational bases in the joint environment.

3. Integration between SF operational bases and the IBCT

4. Base defense equipment requirements for SF battalion MTOEs

5. Emerging security technology and its applicability to SF operational bases

6. Revisions to the *Mission Training Plan for the Special Forces Group and Battalion* (ARTEP 31-805-MTP)

7. The applicability of civilian security schools for SF security force personnel

8. Duties, roles, locations, and C2 architecture for SF FOBs since Desert Storm

9. TTPs for base defense at the ODA, ODB, FOB, and SFOB levels

10. Threat assessment analysis for potential SF operational base locations

APPENDIX A

BASE DEFENSE TACTICS, TECHNIQUES, AND PROCEDURES

Although joint and MP doctrines address base defense, there are no SF specific defense manuals available. All battalions have FSOPs, but their base defense annexes are not usually detailed and do not discuss TTPs, synchronization, rehearsals, or training plans. The base defense plan involves everyone and it is essential to conduct realistic training exercises at home station that involve as many battalion personnel as possible. Because the focus of most exercises is on the training of detachments and the staff, many SPTCENs do not have an opportunity to experiment with base defense techniques and procedures; most provide backside support only. Due to the rapid turnover of staff officers, commanders, and senior NCOs, those battalions that do not deploy regularly lose valuable lessons learned. Even experienced battalions often deploy to areas that are permissive, where base defense is not a priority. All of these factors contribute to a lack of base defense experience throughout SF. This appendix is designed to give new SPTCEN and battalion leadership specific TTPs that can be used on real-world deployments and exercises (JRTC and home station), and to add detail to FSOPs. (*SFC Edward Leblanc and I authored this document while assigned to Special Operations Training Detachment at JRTC as the SPTCEN observers-controllers.)*

1. Base Defense Predeployment Planning

a. Collocate the BDOC with the SPTCEN (S-1, S-4, legal, movement control/dispatch and HSC commander/first sergeant). Centralization is essential for C2 reasons and expedites the process for those leaving the compound (one-stop shopping).

b. Centrally locate the SPTCEN/BDOC in the compound. It is often located where it is not naturally in a position to act as a C2 headquarters, causing confusion during events. *(While observing one battalion the JRTC OC team noticed that the HSC commander was fighting one fight, the OPCEN was fighting another, and the BDOC controlled nothing. No one had the whole picture and C2 was nonexistent. A centrally located BDOC that had the authority to "fight the fight" would have fixed this problem.)*

c. Involve the counterintelligence (CI) representative. The CI NCO should be part of the PDSS/ADVON and prepare the force protection annex. He should incorporate his findings into the base defense plan, advise the BDOC SOG of new threat indicators, and recommend improvements to the plan throughout the deployment.

2. Administrative

a. Coordinate early and continuously with the ISOFAC. Decide who is responsible for building targets, organizing convoys, and providing security for detachments conducting rehearsals and moving to the departure airfield. The ISOFAC normally has only enough personnel to push out one team at a time; the SPTCEN should be prepared to support the rest. Clearly establish "left and right limits" for each center early.

b. ODA movements. Each movement of an ODA is a mission in itself and requires detailed planning. The centers should have a meeting, chaired by the ISOFAC commander (or representative) or battalion XO, to de-conflict resources and to insure a complete and workable plan (at least eighteen hours prior to every detachment infiltration). Although the S-4, service detachment commander, and HSC commander, are responsible for the majority of logistical actions, they cannot do it all themselves. At the meeting they should discuss (at a minimum) final supply issues (ammo/battery draw), critical times, communications procedures, security forces, load plans, HAZMAT certification, deception plans, CI sweeps, routes, contingency plans, bump plans, push packages, ADVON parties at the departure AF, and recovery vehicles. Identify action officers for each. *(One ISOFAC moved a team by ground, several hours away, to the closest departure airfield. When they arrived they found that no one was HAZMAT qualified, load plans were incorrect, and no subject matter experts were available. This caused a four-hour INFIL delay and almost cost the mission altogether. A coordination meeting between the centers would have identified these issues, preventing the mishap altogether.)*

c. Rules of Engagement. Many SOF soldiers are killed or wounded at JRTC due to ROE related issues. Although most units pass out ROE cards to all soldiers once in country, the cards themselves do not always clarify the "can do's" and "can't do's." Soldiers need to know exactly what the ROE means; not in lawyer terms, but in "Joe" terms. They need the details the most (even more than ODA members). For this reason many battalions have the lawyer in the SPTCEN where he is always available to answer specific questions quickly (this is not a rule but a technique since most would rather be in the OPCEN). The HSC commander and first sergeant should ask and receive answers to many important questions. "Can we lock and load while on guard or patrol? Can we search and detain unarmed civilians? Can we shoot someone who has a weapon and is running away? Can we detain vehicles using lethal force? Can we bring injured civilians into the compound? Can we buy goods from civilians? What do I do if an unarmed civilian jumps the gate and starts running through the compound? Can we lock and load within the compound?" These are all questions that require specific answers to prevent a scared, tired soldier at the gate from making a bad decision under stressful conditions. The gray area can be reduced significantly with daily communication to the JSOTF/JTF and through careful analysis at the battalion level. Even if he is not physically located within the SPTCEN, the lawyer is an integral part of the base defense plan. Record the specific "can do's" and "can't do's" and post them with the gate guards.

A good technique is for the lawyer and/or his NCO to walk through the compound talking to the soldiers in the bunkers and manning the gates. Through discussions they can present different scenarios to reinforce the most recent ROE while also validating the information dissemination process. *(During one rotation an SF battalion interpreted the ROE to mean that soldiers could not lock and load their weapons when leaving the compound. However, they planned on stopping and searching suspicious vehicles. After observing a vehicle circling their compound, the BDOC dispatched two HMMWVs with .50 cal machine guns to stop and question those in the vehicle. The vehicle stopped and the two HMMWVs parked in front of and behind to prevent its escape. The two HMMWVs were engaged by small arms fire in a close ambush, and within twenty seconds, five of the six security force members were killed--only one was able to return fire [less than five rounds]. The OPFOR placed demolition charges in both HMMWVs destroying the guns, radios, and night vision gear [the entire attack lasted less than two*

minutes]. During the AAR the security force NCOIC said that he did not think he was allowed to lock and load [explaining why there was little returned fire]. This unit did not understand the ROE, did not properly wargame contingencies, and did not train their soldiers for mounted operations [most of the soldiers in the HMMWVs had their weapons stored behind their seats].)

d. Shift Change. Include an intelligence update. The CI representative should be part of the BDOC, not the OPCEN. Get as many soldiers to the shift change as possible to help with the information dissemination flow. Changeovers do no good if the information stays at the upper NCO/officer level.

e. Information Dissemination. This is the single hardest task for the HSC commander/first sergeant. Radios, field phones, and rehearsals are a critical first step. Have a means to communicate to all bunkers and maneuver elements, and rehearse the information flow between centers. Practice ACE reports and insure that off-duty soldiers are included (someone could be shot through a building and might be dead by the next morning unless checked on). Insure that detachments going out to train are connected by the same radio link (if possible) to the BDOC. The alternate to this is going through the SIGCEN (less C2). Post critical information for all FOB personnel in common areas, such as the billets or mess hall, to re-emphasize key points. Leaders need to question the soldiers on the gates to insure that information is being passed to the lowest levels.

f. Do not use the HSC commander or first sergeant in mission planning cells; they are responsible for the defense and sustainment of the entire compound, and this is a full-time job. The overall readiness of the FOB suffers when they are asked to perform tasks in other areas.

g. Force Protection. Force protection measures should become more restrictive once there is evidence of increased enemy activity. Although eating off the local economy is important for the rapport building process, it should be carefully balanced with force protection. Once the enemy engages friendly soldiers at one of these locations, it is likely that he will do so again. If the command determines that it is important for morale to eat or shop off the economy and there is a threat in the area, the routes and establishments must be secured. Although obvious to most, there have been examples at JRTC where ASTs and isolated detachment members have been involved in OPFOR events at local establishments. Personnel that could compromise strategic level assets should not be the ones allowed off the compound (depending on the threat level). Again, METT-T and the threat's capability dictate, but force protection should be the overriding factor before personal comfort. Although many battalions have the AST accompany the teams during infiltration and push resupply bundles, this is not the

preferred technique. ASTs have operational knowledge of their detachment's mission as well as the missions of other detachments. If captured, they could compromise several theater-level assets.

h. Movement Control. Movement control is one of the most critical elements for maintaining accountability of all soldiers. Develop a system that is manageable and unavoidable. A good technique is to have the movement control section physically located in the SPTCEN next to the S-1, S-4, and movement control NCO. When a soldier draws a vehicle he must sign out with the S-1, receive a dispatch log, and check out with the movement control section. If these sections are collocated the process is quick and easy. In addition, vehicle keys should be attached to cards that have a signature line of the approving authority (S-1 or movement control NCO). Because the gate guard can check the signature card prior to the vehicle departing, he can confirm that the individual has authorization (final check) to leave. Many battalions prefer that the isolation facility sign for vehicles at the beginning of the exercise and control their own movements. This has proven to be an ineffective technique since they can bypass the movement control section altogether. It is best to consolidate all the vehicles, have the ISOFAC request the number of vehicles they need, and have them sign out at the SPTCEN. Positive control is key! The HSC commander and first sergeant must maintain accountability of everyone in the compound--it is <u>their</u> responsibility.

3. Base Defense Tactics, Techniques and Procedures

a. WARGAME! WARGAME! WARGAME! The HSC commander, first sergeant, and SOGs should prepare detailed courses of action for all potential threat scenarios. The wargame should determine responses, resources, and the actions necessary to prevent the disruption or destruction of the FOB. Post the results of these wargames in the BDOC and validate their effectiveness during rehearsals. Because the defense of the compound involves everyone, it is preferable to conduct a mass briefing with all soldiers in the compound once the procedures are established and approved by the FOB commander. Wargaming should begin with a one-dimensional problem such as a sniper attack, sapper attack, media visit, riot, car bomb, ruck-bomb, or an ambush. Once the wargame is complete for each of these, develop courses of action for two or three-dimensional problems by combining two or more of these events.

b. Economy of Force. Identify personnel requirements based on the threat vulnerability assessment. Do <u>not</u> design the base defense plan around the number of soldiers available. Determine what is needed first and then decide who is available to support the plan. One of the biggest problems is getting the command to support the emptying of key centers to support the defense. By determining actual numbers needed, minimum and maximum, the HSC commander will be able to explain the rationale for the security plan. A Level I threat does not necessarily mandate the manning of all fighting positions. One soldier in a good observation point, with a clear field of view, might be able to observe an entire side of the compound. This soldier acts as an economy of force measure that allows the reallocation of forces in places that are not observable;

concentrate patrols and sensors in these areas. Bunkers are not usually the best observation points. Don't confuse a good defensive position with a good observation point. Consider using second floor windows, towers, and other elevated areas for observation. Have the QRF ready to move once the enemy is identified.

c. Signals. Establish signals to identify the active gate to prevent vehicles from going to the wrong one (a VS-17 panel works well). This technique is effective during attacks or civilian disturbances at a gate when returning soldiers may not know what to do. If the assets are available, give a radio to each vehicle leaving the compound. Have them call forward when they are about to re-enter the compound alerting the gate guard. This technique facilitates movement through a known choke point that is vulnerable to enemy attack. In addition, establish a system for alerting the entire compound of an attack or civilian disturbance. (*One effective technique for alerting the compound is the use of car horns wired in a series throughout the compound, linked to a battery with the toggle switch in the BDOC. PSYOPS equipment, air horns, and PA equipment are other examples. The FOB must understand the proper actions to take once alerted [rehearse].)*

d. Quick Reaction Force (QRF). Although the QRF is a doctrinally sound concept, most do not have the assets available to support one. The QRF should be a dedicated force without any other mission. They should rehearse contingencies, conduct mounted and dismounted patrols both in and outside the wire, and respond immediately to the SOG in a crisis. For most, however, the QRF is more of a "minute-man" concept using on-duty soldiers from the centers. In this example the soldiers work in their respective centers and respond to a crisis once alerted by the BDOC. The soldiers must report to the SOG prior to each shift to insure that the force has been identified and is prepared to conduct combat operations. The "minute man" concept requires greater C2 from the BDOC and more frequent rehearsals to be successful. This is not the preferred option. (See appendix C for C2 options with dedicated, "minute-man," and MP QRFs.)

e. Active Base Defense. The base defense plan should be offensive by nature. A complacent, reactive plan has a negative effect on morale and does not effectively deter enemy aggression. Prevent the enemy from taking action instead of reacting to it. An offensive spirit begins with a pro-active base defense plan designed to detect the enemy early. Supplement static defenses with LP/OPs and external patrols; do not be afraid to leave the wire!

(1) Give patrols a task and purpose (basic patrol order) as well as NAIs and specific reporting requirements. Establish and rehearse contingency plans, medical evacuation procedures, vehicular convoys, and be sure not to set patterns. Use sand tables or maps to brief/debrief patrols. Because support personnel usually execute most of these operations (unless MPs or uncommitted ODAs are available), they require more control. Do not send out soldiers with the task of "looking around for the enemy." With this guidance they will literally "look around" for an hour and return. Be specific and take the time to establish contingency plans and SOPs. The SOG should inspect and back brief each patrol before they leave the compound.

(2) Coordinate with the ISOFAC for a counter-sniper team. This team should prepare sniper positions both in and outside the compound that provide the best observation and fields of fire (tops of buildings or windows as examples). Insure they have communications with the SOG to de-conflict fires (preventing fratricide).

(3) "Adopt a private program." If the FOB has personnel shortages, the HSC commander and first sergeant must establish an availability system that manages everyone in the compound. Soldiers cannot be expected to perform MOS-specific tasks during the day and execute security operations at night. Although this technique works for short-duration exercises, it is not sustainable. A rotating schedule must include a rest plan to insure that soldiers are not being over worked. In order to do this the first sergeant and HSC commander must make a list of every available soldier in the FOB. The list must be updated daily as requirements change. Riggers may have parachutes to pack and bundles to rig prior to detachment infiltrations, but will have less to do at other times. The dining facility head count may change as personnel leave the compound allowing cooks to participate in the defense of the base (one cook for every fifty soldiers is a normal planning factor). Once teams deploy, the OPCEN, SIGCEN and ISOFAC may have personnel that can be used elsewhere. Monitor the soldier workload daily and consider all available assets.

One course of action for training younger, less experienced soldiers is to combine senior NCOs with them on patrol. Use combat arms volunteers to act as patrol leaders with support personnel as patrol members. As the less experienced soldiers are trained, use them as patrol leaders.

(4) When an event occurs at the gate (media, riots, etc) deploy counter-sniper teams and/or patrols outside the wire for security. Remember to watch the "back door!" Don't focus all assets at the point of attack or where the event is occurring (there may be a diversion). However, there are times when it is best to be "buttoned up" within the compound. During deliberate attacks it might be too late to get a patrol out. For this reason it is best to conduct predictive analysis to determine times when the enemy is most likely to be active. Prior to any known event, such as a media or mayor's (VIP) visit, it is best to put out a patrol or counter-sniper team. These known events can give the FOB an upper hand if wargamed properly.

(5) Rehearse motorized/mounted operations. Most SPTCEN personnel do not have training using HMMWVs while on patrol. Mounted operations require more control from senior leaders than dismounted (due to increased mobility). Soldiers must know how to employ their weapons while mounted, stop vehicles, and avoid getting trapped in ambushes. Mounted patrols should consist of two mutually supporting HMMWVs at a minimum.

(6) With proper coordination, detachments conducting training outside the wire can be used as maneuver elements for the BDOC. On the way to and from their training locations, the SOG can task ODAs to observe NAIs that could have enemy

activity. The security force must know where the detachments are at all times. Helicopters can also sweep the area prior to and after taking off for a mission. Early coordination, synchronization with other centers, and the creative use of all assets available are critical for a proactive plan.

f. BDOC C2. The BDOC is the single C2 headquarters for all defensive actions at the FOB. The SOG must establish fire control measures to deconflict fires both in and outside the compound. Security personnel need to know the exact location of friendly patrols at all times. If multiple patrols are out, they must have specific guidance of where and when to shoot in order to prevent fratricide. One technique is to use road and natural terrain features to deconflict fires. If a squad knows that their limit of advance is a road, and they are not allowed to engage the enemy on the other side, the squad should be able to move freely without the fear of friendly fire. If a squad sees movement out of their boundary, they must send a SITREP immediately to the SOG. The SOG can give permission to coordinate directly with other patrols, enabling them to engage. Fratricide has been an issue in the past, especially between gate guards and mounted/dismounted patrols. The SOG must know where all maneuver elements are all the time and maintain an open line of communications. During an event, the SOG's first step (can be a subordinate) is to inform all centers of the current situation. In the case of a successful breach of the FOB compound this is even more important. *(The best approach following a penetration is to keep as many personnel as possible within locked buildings and allow the security force and QRF to react. This technique reduces confusion and the possibility of fratricide within the confines of the compound. Following an attack of this nature, take the time to secure the entire inner perimeter once hostilities have ceased.)*

g. Sergeant of the Guard (SOG). Insure the SOG wargames contingencies, records the results, and posts them for easy access within the BDOC. This technique cuts down on confusion when he is fatigued or stressed. The day and night SOGs should prepare SOPs together insuring standardization between the shifts. *(The SOG should be identified prior to deployment and allocated time for training during exercises. He should understand small unit tactics, technological security measures, and how to integrate the two.)*

h. Integration of Technology

(1) Floodlights and motion detector lights prevent the enemy from observing night operations inside the compound. They also serve as a passive defense measure that may prevent an attack altogether. Motion detector lights are extremely effective, inexpensive, and can be bought off the local economy at most department stores.

(2) Issue digital cameras to the gate guards. Because gate guards are often the ones that detect suspicious enemy activity around the compound first, they can assist the CI NCO in refining the daily threat assessment. Photographs are important for confirming or denying the presence of enemy agents.

(3) Integrate technology whenever possible (IREMBASS, cameras, etc). Because nothing replaces the eyes of a soldier on the ground, insure that the cameras are complementary and not the main effort. The soldiers tasked with observing camera monitors should change out every two hours at the most. Eye fatigue can be the greatest enemy when using many of these technological devices.

(4) Although it is not considered "high tech," old parachutes or camouflage nets hung between buildings (as close to the outside as possible) can prevent the enemy from seeing into the compound. They are inexpensive and easy to install.

i. Patterns. Do not establish regular patterns for active gates, patrols, rehearsals, PT, or re-supply operations.

j. Base destruction and evacuation plan. Base evacuation is extremely difficult to plan and must be coordinated with every FOB center. Have a means to get all FOB personnel to a new location quickly. Establish SOPs based on the best and worst case scenarios. The best-case scenario is knowing beforehand of a proposed, massed enemy attack (Level II threat or higher). This allows the FOB time to request additional security forces, reallocate internal assets, or move to a new location. The worst-case scenario is a surprise attack with no intelligence indicators. Because FOBs do not typically have enough vehicles to move the entire battalion at one time, prepare dismounted and mounted plans. Be sure that the ISOFAC has a means of getting out of its own internal wire if it has to displace.

k. Rehearsals. Conduct rehearsals continuously throughout all exercises and deployments. The first two or more 100% full alert rehearsals (THREATCON Delta) for the entire compound should be announced. Once SOPs are solidified, conduct unannounced rehearsals, both day and night. Front-load as many rehearsals as possible prior to the commencement of hostilities. Incorporate medical exercises (assess casualties) into each and pre-position medical supplies and litters in key areas for easy accessibility. Coordinate with the battalion XO for rehearsal times and conduct AARs as soon as possible after each event.

Continue rehearsals once deployed to a contingency theater. Because FOB personnel will have live ammunition, maintain even more control over those inside and outside the wire. Insure that everyone understands the purpose of the planned rehearsal and that external security patrols have a clear signals plan (fratricide prevention). If using friendly patrols to identify "dead spots" between sensors, cameras, and observers, insure key leaders are with each moving element (connected by radio).

l. Deception. Deception techniques are critical for preventing the enemy from obtaining a clear understanding of friendly operations. Consider using deception convoys prior to detachment infiltrations, "dummies" in unmanned fighting positions, and fake bunkers that will not necessarily be used. Load infiltrating detachments in trucks behind buildings or other concealed areas to prevent the enemy from determining friendly

strengths, capabilities, and intentions. Mission essential equipment such as boats, SCUBA gear, Guilly suits, and sniper weapons should remain out of view. If painting weapons, do so in areas that are unobservable. Be aware that the enemy can predict future activities, the nature of upcoming operations, and numbers of ODA members by seeing uniforms drying outside, equipment being modified for a certain AO, and other exposed gear. *(Load the detachment's equipment on trucks several hours prior to the actual load time. If using floodlights, consider turning them off in certain areas of the compound periodically to confuse the enemy. This is also a good technique because it allows the security force on the inside to maximize their optical advantage through the use of night vision goggles. Since there are only a few gates available at a compound, deploying patrols is difficult. By turning off lights, the patrols can get out quickly, find suitable cover and concealment, and continue on their mission. Once they are out, the lights can be turned back on. The same system works well when returning. The patrol calls ahead and alerts the gate guards that they are ready to re-enter. The guards open the gate at the same time the patrol is arriving, preventing a bottleneck at a known choke point. In addition, prevent setting patterns by occasionally turning off lights when patrols are not departing. Many units have been successful by leaving one side of the compound "dark" to draw the OPFOR in on the FOB's stronger, but less lit side. To the OPFOR the compound appears weak where it is dark, but through the use of cameras, sensors, and night vision, it is actually the stronger side.)*

4. Issues from the Joint Readiness Training Center. At JRTC, the observer-controllers provide a list of sustains and improves to the training unit at the completion of each rotation. These results are compiled in an overall AAR called a take home packet (THP) that describes aspects of the exercise that went well, and those that did not. The following are combined results from SPTCEN THPs over the past three years (base defense specific).

a. Sustain
    1) Medical expertise and procedures
    2) Movement control and personnel tracking
    3) Daily supply operations (sustainment operations)
    4) Shift change briefings
    5) MOS specific skills

b. Improve
    1) ISOFAC and SPTCEN integration
    2) CI not incorporated into the base defense plan
    3) Base defense C2 (who is fighting the fight?)
    4) Base defense integration of technology
    5) Misunderstanding of the ROE
    6) Integration of medical rehearsals
    7) Not continuously improving the FOB's defensive posture
    8) Accuracy of the situation map in the BDOC
    9) 100% involvement of all centers during base defense rehearsals

10) Dissemination of information
11) MP integration into the base defense plan (can't let them do it all)
12) Basic soldier skills
13) Physical placement of centers (BDOC not centrally located)
14) Lack of detail in FSOP (should be a "how to" manual)

5. Conclusion. Special Forces SPTCENs are capable of sustaining FOBs anywhere in the world. However, base defense is not generally a strength of most battalions. In addition, FSOPs are not focused on warfighting skills and procedures. Commanders should allow SPTCENs to operate during exercises as they would in war. The HSC commander and first sergeant need time and resources to train their personnel on basic soldier skills and base defense procedures. Aggressors should be used during exercises to validate base defense procedures, synchronization, and the level of individual training of FOB personnel. Base defense at the FOB is a critical task, and the SPTCEN cannot be expected to perform well without regular and realistic training.

APPENDIX B

VIETNAM BASE DEFENSE LESSONS LEARNED

The operational similarities between base defense at FOBs and detachment-level "A" Camps in Vietnam are few; however, many specific TTPs apply to both. Although the threat level for "A" Camps was a II or III, most FOBs should never be in an area higher than a Level I (peaking to a II at times). Because of their remoteness and high threat level, "A" Camp defensive measures were more extensive than those most FOBs implement today. Even though there are differences, techniques that were critical to the success of "A" Camps forty years ago are still applicable.

(This appendix is a compilation of TTPs from multiple Vietnam War era sources to include On Camps, the "Alpha Detachment Handbook" from 5th SF Group (ABN), Counterinsurgency Lessons Learned no. 62 from US MACV, and interviews with veterans.)

1. Establishing an initial “A” Camp

a. Conduct an extensive site survey prior to setting up camp. The success or failure of the camp is based on quality planning during the preparation phase (intelligence preparation of the battlefield). This includes an area assessment that provides detailed knowledge of the area and its people.

b. Priorities of work

(1) Establish security using either host-nation or friendly forces (this includes reconnaissance patrols).

(2) Position weapons in accordance with the construction plan. Dig hasty fighting positions for protection (these can be modified as camp construction progresses).

(3) Establish clear fields of fire to improve observation and deny concealment to enemy forces. Vegetation is a continuous problem; once fixed defensive positions are in place, use fire or defoliants to maintain good observation from the bunkers.

(4) Establish a communications and observation system immediately. Augment radios with field phones (wire). Begin establishment of lookout towers and OPs as soon as possible.

(5) Employ Claymore mines, barriers, and obstacles. Ensure that obstacles are covered by direct fire at a minimum, and indirect fire whenever possible. Protective wire should hold attackers hand grenade distance away from the fighting positions. Because Concertina Wire is easy to employ it should be part of the initial barrier plan.

(6) Improve weapons emplacement and fighting positions. All fighting positions must have overhead cover, drainage systems, and ammunition storage.

(7) Prepare and improve the resupply facility which is usually a DZ/LZ. Secure the immediate area and route to camp, and begin clearing an airstrip. The ability to airland supplies is much preferred to only having a DZ/LZ.

(8) Ensure there is a water supply and a water storage area (this is important during a continued attack). A well is of great value to the camp’s sustainability.

(9) Maintain alternate fighting positions for at least half of the indirect fire weapons. Always change the location of direct and indirect fire weapon systems after dark when enemy observation is the worst. “Weapons which will return fire initially when the camp is probed, should not remain in the primary defensive bunker.

The purpose of a probe will very likely be to determine the position and number of crew served weapons" (US Army 1967b, 44).

2. Camp improvement and construction

a. Once the camp is deemed defendable, begin construction of its defenses. Replace hasty positions with reinforced bunkers.

b. The camp's defenses are based on METT-T but will include the following:

(1) a C2 bunker with an observation tower in the middle of camp.

(2) compartmentalization within the camp in case of a penetration.

(3) a communications trench (zig-zag) behind each wall that connects all fighting positions.

(4) alternate fighting positions for crew served weapons.

(5) overhead cover for automatic weapons and grenade sumps for all positions. Use mesh wire over entrances of bunkers to protect against grenades.

(6) a secondary defense inside the perimeter (inner perimeter).

(7) prepositioned ammunition so that it is readily available at the primary, alternate, and supplemental positions.

(8) a lighting system to cover the outside perimeter.

(9) hardened sleeping quarters with overhead mortar protection at a minimum.

(10) "Machine guns may be mounted permanently to prevent them from being turned on the camp (this prevents displacement of the gun and prevents defenders from using the gun if the camp is penetrated)" (US Army 1967b, 50). The gun can also be chained to its mount (or a field expedient mount formed by cutting off the mount legs, and spot welding it into a pipe that is set in concrete) to prevent its movement.

c. Place mesh wire (chicken wire) two feet above and several feet in front of all bunkers to detonate RPGs and mortar rounds prematurely.

3. Defensive Planning

a. Include at a minimum:

(1) Fire plan.

(2) Final protective fires.

(3) Sectors of fire for machine guns.

(4) Principle direction of fire for automatic weapons.

(5) Preplanned indirect fires (pre-register if possible).

(6) Coordinated and rehearsed air fire support.

(7) Prepared range cards.

(8) Control measures preventing enemy probes from discovering crew served weapons positions (use mortars and individual weapons to engage enemy elements that do not severely threaten positions).

(9) Sector of fire stakes.

(10) Bunkers. Because bunkers are permanent in nature, they are also the most vulnerable. They should be located fifty meters behind the inner wire (out of hand grenade range), have overhead cover that can withstand a mortar blast, and be camouflaged and mutually supporting.

b. Task organization

(1) Establish a reaction force to support patrols outside the wire in case they are engaged by a superior force or take casualties.

(2) Establish a reserve force inside the wire that can reinforce any point or deploy outside the camp to attempt a spoiling attack (offensive maneuver while in the defense).

(3) Establish a clear chain of command to prevent confusion when key personnel become casualties (unity of command).

c. Barrier Plan

(1) Barriers must provide sufficient depth to prevent the enemy from advancing within grenade throwing range.

(2) Although the barriers themselves will not prevent a determined attack from penetrating, they are designed to canalize and slow down the enemy. Insure there is an alert plan in place so defenders can get in position before the barriers are compromised.

(3) The Claymore Mine is extremely effective when used appropriately. Do not use only one row but place them in depth. Use mines to cover dead space or likely avenues of approach. "Alert training should include proper timing for firing the Claymore. Premature use of these weapons can leave an inviting gap in the defense. In the excitement of a firefight, it is possible that the mines will be fired at a less than lucrative target. They should not be fired at a target that can be destroyed by some other means. It is an ace in the hole which must be fired at the proper time when the target is at the proper distance" (US Army 1967b, 54). Check mines and their wires daily to make sure they are operating properly. One technique to prevent Claymores from falling over is to permanently set them in concrete, buried so that they cannot be moved without great effort. Because they are electrically detonated, consider using a redundant ignition system such as a blasting machine or another expedient method. Fire a mine periodically to insure that the system works. To prevent accidental ignition, Claymores can be fixed to the inside of a lid on an ammunition box that is buried in the ground. When there is great traffic in front of the mines or when friendly forces are nearby, the mine can be rotated over so that it is below the surface of the ground. Once the traffic has passed, the mine can be lifted back into position by rope or wire.

d. Counterintelligence

(1) Forbid everyone that does not have business in the camp to come in. Civilians that require medical attention should be treated outside the camp.

(2) Use host-nation personnel with unquestioned loyalty to act as an interior intelligence net (when operating with host-nation or multi-national forces).

(3) Do not hire anyone that has not been thoroughly security checked.

(4) Employ guards in pairs of two to lesson the chance of enemy saboteurs compromising the position.

(5) Conduct frequent checks of host-nation positions both day and night.

(6) Vary camp routines (prevent setting patterns).

(7) Turn off lights at night to prevent the enemy from using them as control measures or target reference points. This also maximizes the use of night vision devices.

(8) Inform troops as late as possible of future operations to prevent host-nation personnel from informing fellow saboteurs.

(9) Monitor the actions of local civilians to determine if they are changing their routines (an attack is imminent).

(10) "Search civilian workers on their departure from the installation to prevent removal of arms, ammunition, or other property" (US MACV 1967, 14). Sweep all areas where the civilians worked to insure they did not leave markers identifying key areas within the compound.

2. Proactive Base Defense Measures. "The offense is and always has been the best defense. If the "A" detachment fails to press an active offensive, then it is subjecting the camp to attack and destruction. The value of the offensive has been profoundly emphasized in recent operations by CIDG and Free World Forces which foiled VC and NVA plans for a successful monsoon offensive. A completely defensive camp will not accomplish its mission, and will be a burden on essential resources and forces" (US Army 1967b, 61).

a. Establish aggressive combat patrolling beyond the range of enemy weapons to prevent a surprise attack.

b. Disperse personnel and vulnerable equipment.

c. Build revetments around vulnerable or exposed equipment.

d. Maintain a reserve force near the command post to use during a penetration or to deploy outside the wire.

e. "Forces outside the camp should be prepared to consolidate and if nothing more, bring fire on the attacking force or destroy supporting weapons. This force may consist of an operation which is out and can be called back, or it can be the small night ambushes which are deployed for local security" (US Army 1967b, 62).

f. Place light sets forward of positions to blind the enemy but situated so friendly forces can still see out.

g. Use guard dogs whenever possible. "Guard duty hours for sentry dogs should be about four hours long, covering a post approximately 200 yards in length. Rotation between guard posts should be on a regular basis to prevent the dogs from becoming overconfident and less alert in familiar surroundings" (US MACV 1967, 15).

h. Use interior lines to your advantage. Maintain the ability to mass fires anywhere on the perimeter and fire in concentrations whenever possible.

i. Limit movement inside the compound at night. If the enemy is suspected to have penetrated the wire everyone must freeze in a firing position. "Anyone running around should be considered enemy" (US MACV 1967, 13). Use signals to identify friendly forces and be sure to include the reserve. Clear the entire compound after the firing ceases.

j. Establish a redundant means of communication to bunkers and outposts (radio and wire).

k. Disperse key personnel, equipment, and weapons to avoid excessive loss.

l. Rehearse medical evacuation as well as the tasks necessary to restore communications if they are lost.

m. "Increase security forces on nights of extremely limited visibility (no moon) and during periods of heavy rain. The enemy often attacks at these times" (US MACV 1967, 15).

n. Rehearse defense plans and SOPs.

3. Patrols (when operating from remote "A" Camps)

a. Each operation should last a minimum of two days, and longer when possible.

b. One third of the camp should conduct continuous operations at least 2000 meters from the camp. One operation per week should extend past 10 kilometers.

c. Use small patrols whenever possible to maximize broad coverage. More frequent smaller patrols are preferable to a few larger ones.

d. Employ more than one at a time.

e. Conduct briefings prior to each (operation order with sand table).

f. Conduct rehearsals and inspections prior to launching (based on actions at the objective).

g. Conduct AARs.

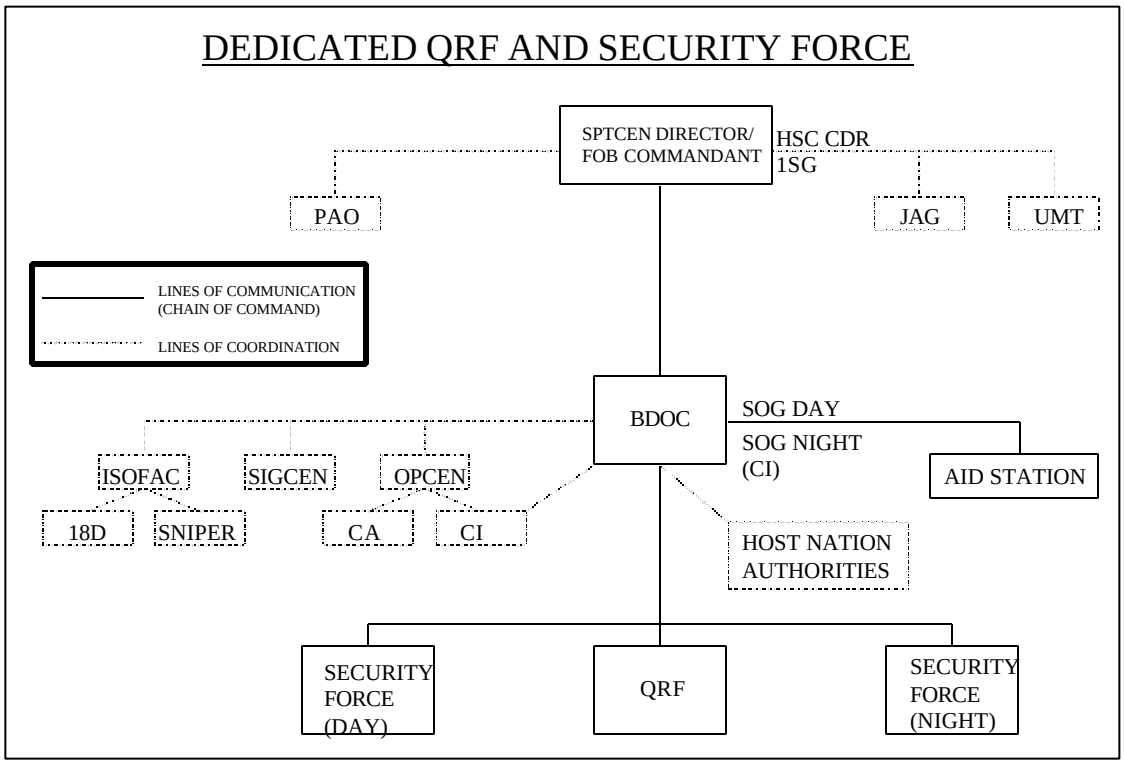
h. "Imaginative, unpredictable, and aggressive tactics will be used to keep the enemy off balance and force him on the defensive" (US Army 1967b, 64).

i. Use local patrols around the camp but avoid setting patterns. Maintain communications with these elements at all times. Ensure that patrols are going to their assigned locations and are not avoiding the bad terrain where the enemy often hides.

APPENDIX C

BASE DEFENSE COMMAND AND CONTROL OPTIONS

The purpose of this appendix is to provide multiple C2 options when preparing a base defense plan. The first four options are recommended when an FOB deploys without additional security forces. When MPs or host-nation personnel are not available, the first option using a dedicated QRF and security force is the most preferable. When the number of FOB soldiers is limited, the next three options are recommended with the "Ad Hoc Security and QRF" being the least preferable. The fifth option, the use of MPs, is most preferred and only employs FOB personnel in the BDOC and for internal security. For the most part, MPs should secure the outer perimeter while FOB personnel secure the inner. Although each of these options can be modified, depending on the situation, it is important to establish the command structure and lines of coordination during planning in order to implement effective procedures immediately upon entry to a theater of operations.



NOTES:

1. Use the same QRF for both day and night (standing by, conducting rehearsals and patrols).

2. The counterintelligence NCO is most effective when dedicated to the BDOC.

3. The SOG should have an assistant to monitor the battle, coordinate with the centers, call local authorities, and deconflict fires in and outside the compound (allowing the SOG to move freely to the point of contact).

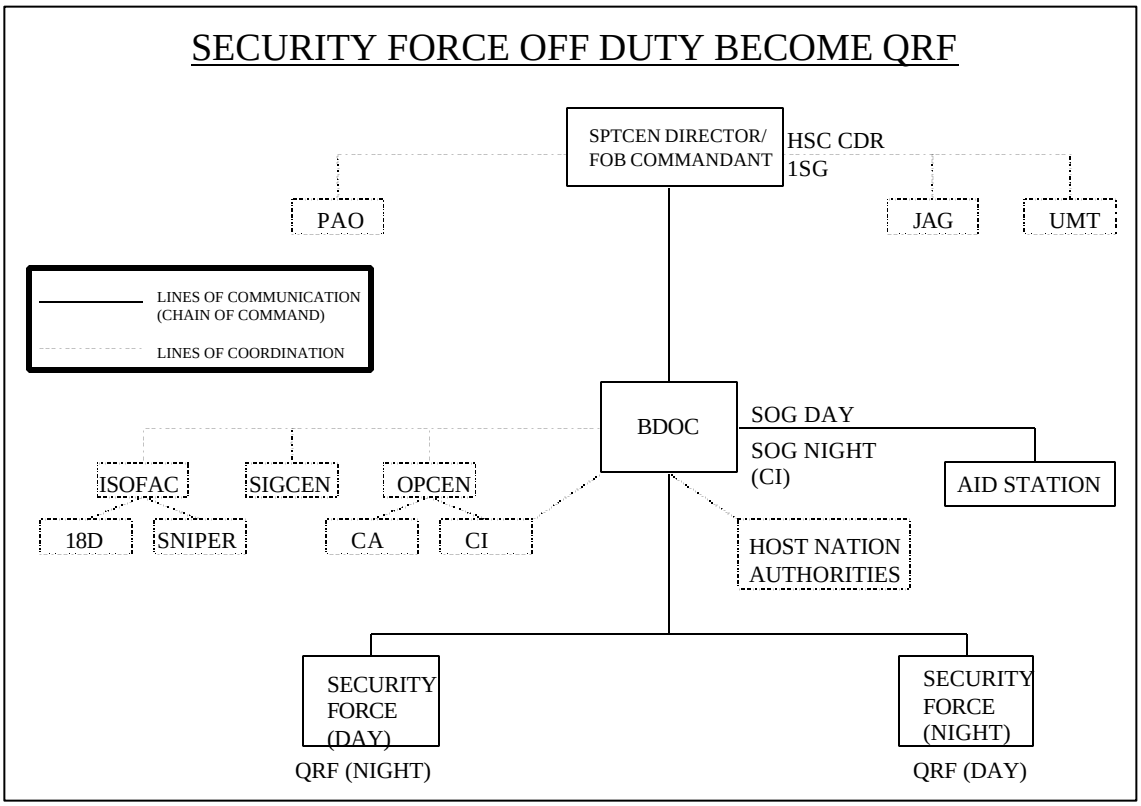
4. The HSC commander and first sergeant monitor the net and "float" within the compound.

5. The BDOC has direct communications to all centers, bunkers, and maneuver elements. The SIGCEN is the primary communications link for MEDEVAC.

6. The on-call sniper comes from the ISOFAC, has predetermined firing points, carries a radio, and receives clearance to fire from the SOG.

7. Be prepared to use the PAO, lawyer, CI NCO, CA officer/NCO, and chaplain during events that involve civilians (often they do better than the security force).

8. Rehearse procedures for receiving 18D support from the ISOFAC for MASCALs.



NOTES:

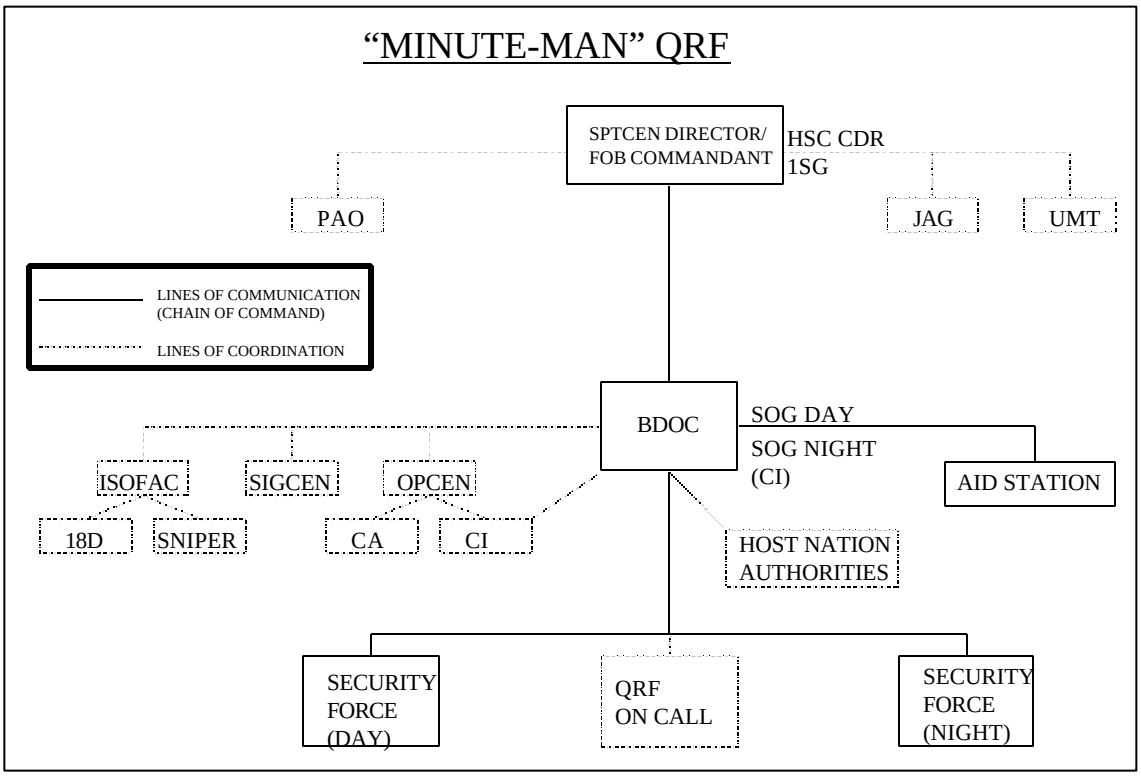
1. Soldiers that come off shift become the standing QRF.

2. The security force is dedicated.

3. Billet all security force personnel together in a "ready room" (prepared to move at a moment's notice).

4. The QRF assembles at the BDOC before moving to the point of contact (mass force before departure).

5. This option is good for establishing continuity and SOPs but is difficult to maintain for extended periods (battle fatigue).



NOTES:

1. The security force is dedicated but the QRF is on-call from the centers.

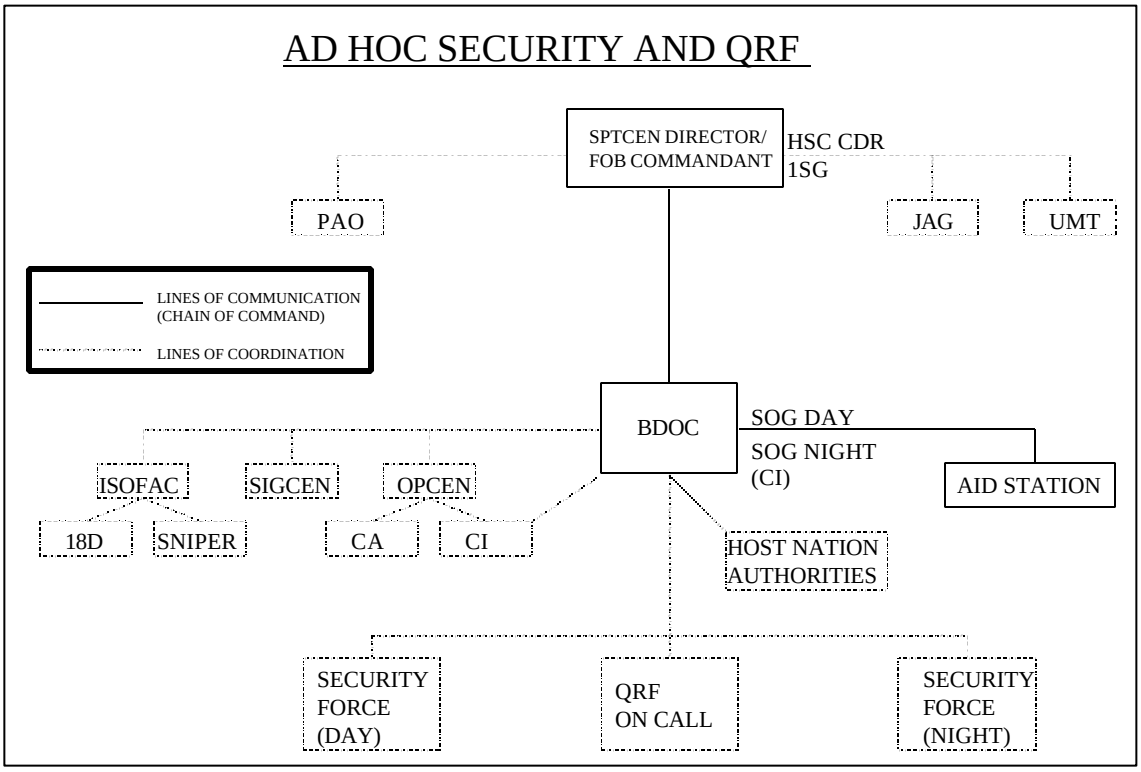
2. Rehearse the QRF moving from their centers to the BDOC, and then to the point of contact.

3. All QRF personnel report to the BDOC at the start of each shift to receive an intelligence update and review/rehearse contingency plans (before reporting to their respective centers).

4. All individual equipment must be on-hand to facilitate immediate movement from the centers once alerted.

5. All QRF personnel report to the BDOC SOG immediately upon notification (before moving to point of attack); the SOG must mass the force.

6. With this option, maintaining SOPs and information disseminating is difficult.



NOTES:

1. Use personnel from the centers as ad hoc security and QRF forces (not dedicated).

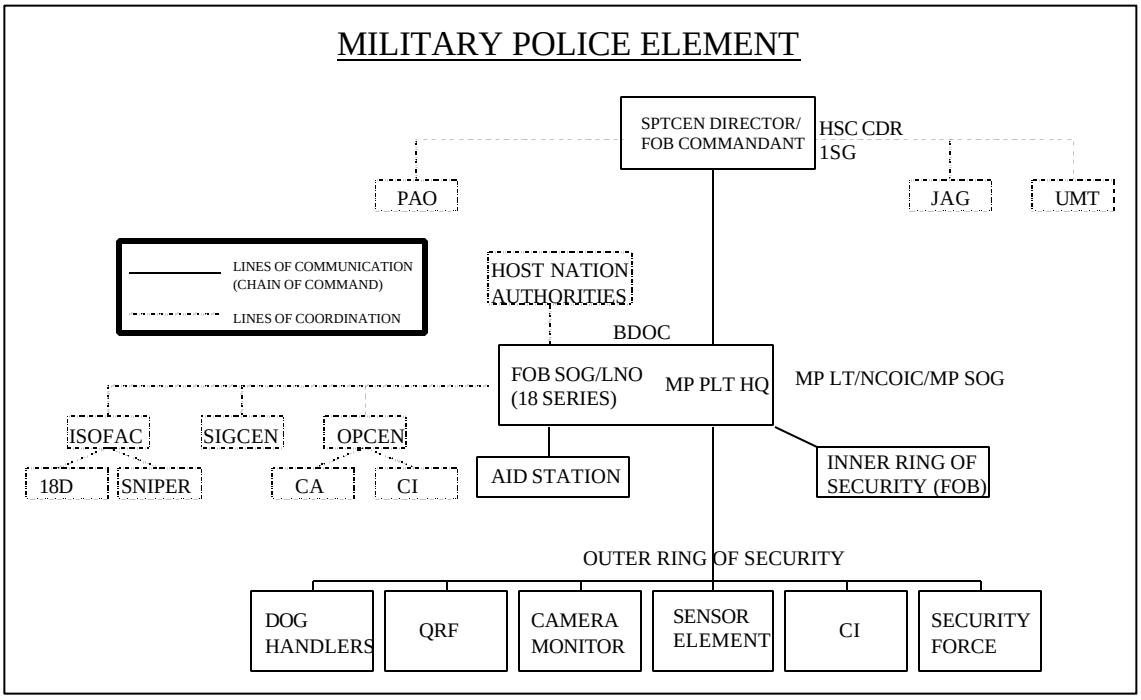
2. This option is the least preferable; it is difficult to establish, train, and maintain SOPs.

3. Only use this option when manpower is severely limited.

4. If possible, dedicate as many of the security force as possible and use other personnel from the centers as needed (maintain as much consistency as possible).

5. Employ at least one combat arms soldier per guard shift.

6. This option requires great C2 to prevent ROE and fratricide issues, and frequent rehearsals to maintain consistency.



NOTES:

1. This option is the most preferable.

2. Conduct rehearsals to incorporate MPs into FOB functions (reporting).

3. The security force must be able to talk on the same radio net (the MPs cannot be on their own internal net).

4. Provide NCOs to act as LNOs, connecting the MPs with the FOB.

5. The MPs “fight the fight” while the LNO coordinates with the centers, local authorities, and the aid station.

6. Supplement MPs with FOB personnel and rehearse SOPs.

7. Establish a clear chain of command.

8. The HSC commander and first sergeant must be involved in the defense of the compound (their responsibility).

9. MPs secure the outer perimeter while FOB personnel secure the inner.

APPENDIX D

JOINT BASE DEFENSE OPERATION ORDER FORMAT

Many FOBs currently do not prepare base defense annexes prior to deployment. In order to synchronize operations, the battalion operation order (OPORD), normally written by the S-3 and his staff, must include input from the HSC commander, first sergeant, and counterintelligence NCO. The threat vulnerability assessment, force protection annex, and base defense OPORD should all be included in the battalion OPORD. This appendix is an example of a base defense OPORD found in *Joint Tactics, Techniques, and Procedures for Base Defense* (JP 3-10.1, Annex E, 1-7). Although not SF specific, the OPORD should be used to prepare FOBs for deployment, and continuously updated to reflect procedural changes once in theater.

(In Joint Operation Order [OPORD] 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 operation order, 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 or Air Force SP response forces, fire support, naval coastal warfare forces, special operations forces, engineers, NBC decontamination or smoke units, EOD, HN military or police organizations, and public and private civilian organizations of both the United States and HN.)

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Authority. (Give authority for access.)

2. Criteria. (Give access criteria for unit contractor personnel and local police and armed forces.)

3. Identification and Control

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

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

(b) Materiel Control Procedures

1. Incoming

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

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

2. Outgoing

a. (List required documentation.)

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

c. (List classified shipments.)

(c) Vehicle Control

1. (State policy on registration of vehicles.)

2. (State policy on search of vehicles.)

3. (State policy on parking.)

4. (State policy on abandoned vehicles.)

5. (List controls for entering restricted areas.)

(d) Train Control

1. (State policy on search of railcars.)

2. (State policy on securing railcars.)

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

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

(a) Protective Barriers

1. Definition.

2. Clear zones.

a. Criteria.

b. Maintenance.

3. Signs.

a. Types.

b. Posting.

4. Gates.

a. Hours of operation.

b. Security requirements.

c. Lock security.

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

(b) Intrusion Detection System

1. Types and locations.

2. Security classifications.

3. Maintenance.

4. Operation.

5. Probability of Detection.

a. Limitations.

b. Compensating measures.

c. Redundant capabilities.

(c) Communications

1. Types.

a. Primary

b. Alternate

2. Operation.

3. Maintenance.

4. Authentication.

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

(a) Composition and organization. (NOTE: In military operations other than war environment, the interior guard may be a contracted civilian security force.)

(b) Tour of duty.

(c) Essential posts and routes.

(d) Weapons and equipment.

(e) Training.

(f) Military working dogs.

(g) Method of challenge.

(h) Alert force.

1. Composition.

2. Mission.

3. Weapons and equipment.

4. Location.

5. Deployment concept.

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

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

(a) Individual actions.

(b) Alert force 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 Forces.

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

4. Administration and Logistics. (This paragraph sets forth the manner of logistic support for base defense. State the administrative and logistic arrangements applicable to the operation. If the arrangements are lengthy, include them in an annex or a separate Administrative and Logistics Order. Include enough information in the body of the order to describe the support concept.)

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

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

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

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

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

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

5. Command and Signal.

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

b. Command.

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

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

6. Acknowledgment Instructions
Annexes:
A. Task Organization
B. Intelligence
C. Operations
D. Logistics
E. Personnel
F. Public Affairs
G. Civil Affairs
H. Engineer Support
J. Command Relationships
K. Command, Control, and Communications
L. Force Protection

M. Host-Nation Support
N. NBC Defense
Distribution:
Authentication:

REFERENCE LIST

Beckett, Ian. 2001. Forward to the past. *Harvard International Review* 23, no. 2 (summer): 59-64.

Bunker, Rober J. 1997. The terrorist: Soldier of the future? *Special Warfare Magazine* 10, no. 1 (winter): 7-11.

Burton, Paul S. 1998. *Urban operations, untrained on terrain*. Thesis, US Army Command and General Staff College, Fort Leavenworth, Kansas.

Carsner, Chris. 2002. Interview by author 7 February, Fort Leavenworth, Kansas.

Carter, Virgil. 2001. Electronic mail interview by author 2 September, Fort Leavenworth, Kansas.

Center for Army Lessons Learned (CALL). SEE US Army, Center for Army Lessons Learned.

Clinton, William. 2000. *A national security strategy for a global age*. Washington, DC: Government Printing Office.

Costa, Christopher P. 1992. Changing gears: Special Operations intelligence support to Operation Provide Comfort. *Military Intelligence Professional Bulletin* 18, no. 4 (October-December): 24-28.

Dummar, Fred. 2002. Interview by author 20 March, Fort Leavenworth, Kansas.

Echevarria II, Antulio. 1997. Optimizing chaos: Nonlinear battlefield. *Military Review* 77, no. 5 (September-October): 26-31.

Field Manuals (FMs). See US Army.

Hoffman, Bruce. 1993. Future trends in terrorist targeting and tactics. *Special Warfare Magazine* 6, no. 3: 30-35.

Huntington, Samuel P. 1996. *The clash of civilizations and the remaking of world order.* New York: Simon and Schuster.

Joint Publication (JP). See US Department of Defense, Chairman, Joints Chief of Staff.

Joint Readiness Training Center (JRTC). 1992a. Special Operations training bulletin 1. Joint Readiness Training Center Publication, Fort Polk, Louisiana, February.

_____. 1992b. Special Operations training bulletin 2. Joint Readiness Training Center Publication, Fort Polk, Louisiana, July.

_____. 1992c. Special Operations training bulletin 3. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 1993a. Special Operations training bulletin 4. Joint Readiness Training Center Publication, Fort Polk, Louisiana, July.

_____. 1993b. Special Operations training bulletin 5. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 1994a. Special Operations training bulletin 6. Joint Readiness Training Center Publication, Fort Polk, Louisiana, July.

_____. 1994b. Special Operations training bulletin 7. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 1995. Special Operations training bulletin 8. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 1996. Special Operations training bulletin 9. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 1997. Special Operations training bulletin 10. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 1999. Special Operations training bulletin 11. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

_____. 2000. Special Operations training bulletin 12. Joint Readiness Training Center Publication, Fort Polk, Louisiana.

Jones, Pappy. 1990. *On camps.* Base camp construction lessons learned from Vietnam. Special Forces local distribution, Fort Bragg, North Carolina.

Kelly, Francis J. 1973. *U.S. Army Special Forces, 1961-1971*. Washington, DC: Government Printing Office.

Leader, Stefan. 2001. USA v. Usama bin Laden: Technical and tactical insights from the trial. U.S. Department of Energy and Nuclear Regulatory Commission, Eagle Research Group, Washington, DC, April.

Leonard, Kevin. 2002. Interview by author 19 March, Fort Leavenworth, Kansas.

Markowski, Dave. 2002. Interview by author 12 March, Fort Leavenworth, Kansas.

NDU QDR 2001 Working Group. 2001. *Strategy-driven choices for America's security.* Washington: National Defense University Press.

Orman, Doug. 2002. Interview by author 4 January, Fort Leavenworth, Kansas.

Ruggley, Larry D. 1998. *Forward operating base field standard operating procedures.* 3rd Battalion, 3rd Special Forces Group (Airborne), Fort Bragg, North Carolina.

SF Battalion Commander. 2000. SF commander's remarks to his battalion. JRTC, Fort Polk, Louisiana.

Shaw, Robert C. 1982. *Special Operations forces doctrine in Haiti.* Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.

Turabian, Kate L. 1996. *A manual for writers.* 6th ed. Chicago, IL: Chicago University Press.

US Air Force. 1973. Contemporary historical examination of current operations no. 62 (CHECO). Southeast Asia report, base defense in Thailand. Headquarters, Pacific Air Force Publication.

US Army. Center for Army Lessons Learned (CALL). 1993. Operation Restore Hope lessons learned report (operations other than war). Fort Leavenworth: US Army Combined Arms Command.

_____. 1994a. (Haiti) Operation Uphold Democracy initial impressions. Fort Leavenworth: US Army Combined Arms Command, December.

_____. 1994b. US Army operations in support of UNOSOM II (operations other than war). Fort Leavenworth: US Army Combined Arms Command, April.

_____. 1997. Bulletin Number 95-16, *Urban combat operations*. Fort Leavenworth: US Army Combined Arms Command.

US Army. 1951a. Field Manual (FM) 31-20, *Operations against guerrilla forces*. Washington, DC: Government Printing Office.

_____. 1951b. Field Manual (FM) 31-21, *Organization and conduct of guerrilla warfare*. Washington, DC: Government Printing Office.

_____. 1951c. Field Manual (FM) 31-21A, *Guerrilla warfare and Special Forces operations*. Washington, DC: Government Printing Office.

_____. 1961a. Field Manual (FM) 31-15, *Operations against irregular forces*. Washington, DC: Government Printing Office.

_____. 1961b. Field Manual (FM) 31-21A, *Special Forces operations.* Washington, DC: Government Printing Office.

_____. 1963. Field Manual (FM) 31-16, *Counterguerrilla operations*. Washington, DC: Government Printing Office.

_____. 1965a. Field Manual (FM) 31-21, *Special Forces operations*. Washington, DC: Government Printing Office.

_____. 1965b. Field Manual (FM) 31-20, *Special Forces operational techniques.* Washington, DC: Government Printing Office.

_____. 1967a. Field Manual (FM) 31-16, *Counterguerrilla operations*. Washington, DC: Government Printing Office.

_____. 1967b. Alpha Detachment Handbook, 5th Special Forces Group, 1st Special Forces. Fort Bragg, North Carolina, Headquarters, Department of the Army.

_____. 1969. Field Manual (FM) 31-21, *Special Forces operations*. Washington, DC: Government Printing Office.

_____. 1970. Field Manual (FM) 31-21 (Change 1), *Special Forces operations.* Washington, DC: Government Printing Office.

_____. 1988. Field Manual (FM) 25-100, *Training the force*. Washington, DC: Government Printing Office.

_____. 1990. Field Manual (FM) 100-20, *Military operations in low intensity conflict*. Washington, DC: Government Printing Office.

_____. 1993. Field Manual (FM) 90-10-1, *An infantryman's guide to combat in built-up areas*. Washington, DC: Government Printing Office.

_____. 1995a. Field Manual (FM) 100-16, *Army operational support*. Washington, DC: Government Printing Office.

_____. 1995b. Army Training and Evaluation Program (ARTEP) 31-805-MTP, *Mission training plan for the Special Forces group and battalion*. Washington, DC: Government Printing Office.

_____. 1997. Field Manual (FM) 101-5-1, *Operational terms and graphics*. Washington, DC: Government Printing Office.

_____. 1998a. The Army plan (TAP). Washington, DC: Secretary of the Army, Headquarters, Department of the Army, Washington, DC: Government Printing Office.

_____. 1998b. Army Training and Evaluation Program (ARTEP) 31-807-MTP, *Mission training plan for the Special Forces Operational Detachment Bravo (SFODB).* Washington, DC: Government Printing Office.

_____. 1999a. Field Manual (FM) 3-05.20, *Special Forces operations*. Washington, DC: Government Printing Office.

_____. 1999b. Field Manual (FM) 100-25, *Doctrine for Army Special Operations Forces.* Washington, DC: Government Printing Office.

_____. 2001a. Field Manual (FM) 3-19.1, *Military police operations.* Washington, DC: Government Printing Office.

_____. 2001b. Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office.

US Department of Defense (DOD). 2001. *Quadrennial defense review report*. Washington, DC: Government Printing Office.

US Department of Defense Chairman, Joints Chief of Staff. 1996a. Joint Publication (JP) 3-10, *Joint doctrine for rear area operations.* Washington, DC: Government Printing Office.

_____. 1996b. Joint Publication (JP) 3-10.1, *Joint tactics, techniques, and procedures for base defense*. Washington, DC: Government Printing Office.

_____. 1998. Joint Publication (JP) 3-05, *Doctrine for Joint Special Operations*. Washington, DC: Government Printing Office.

US Military Assistance Command, Vietnam (US MACV). 1967. Salient lessons learned. *Counterinsurgency lessons learned no. 62*, Headquarters, United States Military Assistance Command, Vietnam.

_____. 1968. Viet Cong base camps and supply caches. *Counterinsurgency lessons learned no. 68.* Headquarters, United States Military Assistance Command, Vietnam.

_____. 1971. The Vietnamese village handbook for advisors. Translations and Publications Branch, Management Support Directorate. Headquarters, United States Military Assistance Command, Vietnam.

Vetter, Harold J., and Gary R. Perlstein. 1991. *Perspectives on terrorism*. California: Brooks and Cole Publishing.

Young, Frank J. 1997. Clausewitz and counterterrorism: The relevance of his theory to policy options and force doctrine in dealing with terrorist acts. Core Course 5602 Essay, National Defense University, Washington, DC, National War College.

Wyman, Irwin W. 1975. *A Special Force: Origin and development of the Jedburgh Project in support of Operation Overlord.* Thesis, US Army Command and General Staff College, Fort Leavenworth, Kansas.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   U.S. Army Command and General Staff College
   250 Gibbon Ave.
   Fort Leavenworth, KS 66027-2314

2. Defense Technical Information Center/OCA
   8725 John J. Kingman Rd., Suite 944
   Fort Belvoir, VA 22060-6218

3. LTC (Ret) Joseph Occhiuzzo
   CAS3, Room 295
   1 Reynolds Ave
   Fort Leavenworth, KS 66027-1352

4. LTC (Ret) Geoff Babb
   DJMO
   USACGSC
   1 Reynold's Ave.
   Fort Leavenworth, KS 66027-1352

5. Dr. James H. Willbanks
   CSI
   USACGSC
   1 Reynold's Ave.
   Fort Leavenworth, KS 66027-1352

6. Commander
   1st Special Forces Group (Airborne)
   Fort Lewis, Washington 98433

7. Commander
   3rd Special Forces Group (Airborne)
   Fort Bragg, North Carolina 28307

8. Commander
   5th Special Forces Group (Airborne)
   Fort Campbell, Kentucky 42223

9. Commander
   7th Special Forces Group (Airborne)
   Fort Bragg, North Carolina 28307

10. Commander
    10th Special Forces Group (Airborne)
    Fort Carson, Colorado 80913

11. Commander
    19th Special Forces Group (Airborne)
    P.O. Box 1776
    Draper, Utah 84020

12. Commander
    20th Special Forces Group (Airborne)
    Alabama National Guard
    5601 Oporto-Madrid Boulevard
    Birmingham, Alabama 35210

13. Commander
    U.S. Army Special Forces Command
    Fort Bragg, North Carolina 28307

14. Commander
    U.S. Army Special Operations Command
    Fort Bragg, North Carolina 28307

15. Dr. John Partin
    U.S. Special Operations Command
    Attention: Historian SOHO
    Macdill Air Force Base, Florida 33608-5000

16. Commander
    U.S. Army John F. Kennedy Special Warfare Center and School
    Fort Bragg, North Carolina 28307

17. Commander
    Special Operations Training Detachment
    Joint Readiness Training Center Operations Group
    Fort Polk, Louisiana 71459-5000

18. Director
    Department of Training and Doctrine
    John F. Kennedy Special Warfare Center and School
    Fort Bragg, North Carolina 28307

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 31 May 2002

2. Thesis Author: MAJ Curtis W. Hubbard

3. Thesis Title: Base Defense at the Special Forces Forward Operational Base

4. Thesis Committee Members _____

   Signatures: _____

   _____

   _____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).