Is U.S. Army Rear Area and Base Security Doctrine Sound for Sustaining Operations on the Noncontiguous Nonlinear Battlefield?

A Monograph
by
Major Anthony M. Coston
U.S. Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
AY 02-03

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
22-05-2003	monograph	18-06-2002 to 22-05-2003

4. TITLE AND SUBTITLE
Is U.S. Army Rear Area and Base Security Doctrine Sound for Sustaining Operations on the Noncontiguous Nonlinear Battlefield?
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Coston, Anthony M. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
US Army School of Advanced Military Studies
Eisenhower Hall
250 Gibbon Ave
Fort Leavenworth, KS66027

8. PERFORMING ORGANIZATION REPORT NUMBER
ATZL-SWV

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Army FM 3-0, Operations replaced the term rear operations with sustaining operations, introduced fundamental changes to the operational framework, and suggested leaders use adaptive combinations of contiguous and noncontiguous areas of operations with linear and nonlinear operations in the execution of full spectrum operations. This conceptual shift of sustaining operations on a noncontiguous nonlinear battlefield requires fundamental changes in rear area and base security doctrine.This monograph reviews Joint and Army doctrine; assesses the threats to sustainment operations base on the COE and Army transformation; and explores historical case studies of Russian operations in Afghanistan. The monograph analyzes these findings against the TRADOC Doctrinal Literature Programs? characteristics of sound doctrine to determine if U.S. Army rear area and base security doctrine is sound for sustaining operations on the noncontiguous nonlinear battlefield.The analysis concludes that components of Army doctrine do not meet the TRADOC criteria for sound doctrine. Doctrinal definitions for the threat levels are reactive, use of the term rear area is inconsistent; and command relationships are not comprehensible. Additionally, the doctrinal concepts for rear area security are not enduring and the lack of a preemptive concept is inconsistent with the NSS, JV 2020, and the Objective Force. Finally, force design capabilities are not acceptable or well researched based on recent Russian operations, or flexible based on the unique requirements of the noncontiguous nonlinear battlefield.The monograph recommends several changes to doctrine definitions, concepts, and capabilities. Recommendations include improving threat level and rear area definitions, introducing preemption and operational level force protection concepts, and enabling support organizations with organic, flexible force protection and preemptive capabilities.

15. SUBJECT TERMS
United States; Army; Sustaining operations; Rear operations; Rear area; Base security; doctrine; Noncontiguous nonlinear battlefield; Joint operations; Current operating environment (COE); Transformation; Russia; Afghanistan; TRADOC; Force design; Preemption; Force protection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
			Same as Report (SAR)	58	Buker, Kathy kathy.buker@us.army.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 913758-3138 DSN 585-3138

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Anthony M. Coston

Title of Monograph: Is U.S. Army Rear Area and Base Security Doctrine Sound for Sustaining Operations on the Noncontiguous Nonlinear Battlefield?

Approved by:

_____	Monograph Director
COL Brian F. Waters, MMAS	
_____	Professor and Director Academic Affairs, School of Advanced Military Studies
Robert H. Berlin, Ph.D.	
_____	Director, Graduate Degree Program
Philip J. Brookes, Ph.D.	

Abstract

Is U.S. Army Rear Area and Base Security Doctrine Sound for Sustaining Operations on the Noncontiguous Nonlinear Battlefield?

by MAJ Anthony M. Coston, U.S. Army, 55 pages.

The recent publication of Army Field Manual (FM) 3-0, *Operations* replaced the term rear operations with sustaining operations, introduced fundamental changes to the operational framework, and suggested leaders use adaptive combinations of contiguous and noncontiguous areas of operations with linear and nonlinear operations in the execution of full spectrum operations. This conceptual shift of sustaining operations on a noncontiguous nonlinear battlefield requires fundamental changes in rear area and base security doctrine.

This monograph reviews existing and emergent Joint and Army doctrine; assesses the current and emergent threats to sustainment operations based on the Contemporary Operating Environment (COE) and transformation to the Interim and Objective Force; and explores historical case studies of Russian nonlinear and noncontiguous operations in Afghanistan and Chechnya. The monograph analyzes these findings against the Training and Doctrine Command (TRADOC) Doctrinal Literature Programs' characteristics of sound doctrine - effective, acceptable, well researched, enduring, flexible, comprehensible, consistent, and concise – to determine if U.S. Army rear area and base security doctrine is sound for sustaining operations on the noncontiguous nonlinear battlefield.

The analysis concludes that there are components of Army rear area and base security doctrine that do not meet the TRADOC criteria for sound doctrine. Doctrinal definitions for the threat levels are reactive, incomplete, and ineffective; use of the term rear area is inconsistent throughout doctrine; and command relationships and required coordination with response forces are not comprehensible. Additionally, the doctrinal concepts for rear area security are not enduring for Army transformation, and the lack of a preemptive concept in doctrine is inconsistent with the National Security Strategy, Joint Vision 2020, and the Objective Force. Finally, force design capabilities are not acceptable between joint and army doctrine, well researched based on recent Russian operations in Afghanistan, or flexible based on the unique requirements of the noncontiguous nonlinear battlefield.

The monograph recommends several changes to doctrine definitions, concepts, and capabilities. First, it recommends changing the doctrine definitions for threat levels and rear area concepts. These proposed definitions are based on the area utility, hazard severity, and threat probability and assist commanders in prioritizing and allocating resources. Second, it recommends improvements to doctrine concepts including preemption and an operational level force protection doctrine to counter asymmetric threats. Finally, it recommends enabling support organizations with an organic, flexible force protection and preemptive capability.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Chapter 1: Introduction

Vignette

On 24-25 December 1979, Soviet forces invaded Afghanistan. Airborne troops conducted a surprise air insertion into Kabul International Airport and the military base at Bagram while a simultaneous conventional ground column of three to four motorized rifle divisions began securing the ground lines of communications from the Soviet frontier. Over the following decade, Soviet forces conducted major combined arms army-level operations employing up to two motor-rifle divisions and maintained a force presence of roughly 110,000 Soviet soldiers stationed in Afghanistan at any time.[1] In spite of this, the strength and resilience of the Mujahideen irregular forces prevailed as they employed tactics and strategy of unconventional war. By 1988 the Soviet Union, lacking public support for the war and feeling its economic strain, began the withdrawal of forces from Afghanistan.

While the lack of political will was the primary factor for the Soviet withdrawal, Dr. Robert Baumann, in *Compound War Case Study: The Soviets in Afghanistan*, cites another factor. He states:

> Yet another practical constraint was the undeveloped character of the Afghan theater. Afghanistan's minimal road network could scarcely accommodate the traffic necessary to sustain the 110,000-man force sent there in the first place. Furthermore, according to 40th Army commander Lieutenant General Boris Gromov, from 30 to 35 percent of that force was tied down defending those same lines of communications, guarding convoys, and carrying out other security missions. Even the relatively close proximity of Soviet air bases in Central Asia, which facilitated airlift, could not fundamentally alter the logistical equation. So dependent were the Soviets on the few available routes that the Mujahideen were afforded spectacular opportunities to ambush Soviet columns and keep the invaders off balance.[2]

---

[1] Robert F Baumann, *Compound War Case Study: The Soviets in Afghanistan*, accessed 25 February 2002 available from http://www.cgsc.army.mil/csi/research/comwarbaumann.htm; Internet. 6.
[2] Ibid., 10.

Over their decade in Afghanistan, the Soviet Army learned many lessons. They slowly instituted changes to doctrine, organization, and tactics to protect rear area operations on their noncontiguous nonlinear battlefield. Despite these efforts, they failed.

Doctrine Evolution and Research Question

The 1982 edition of Field Manual (FM) 100-5, *Operations* introduced the concept of "rear battle" which was refined with the 1985 version of FM 90-14, *Rear Battle*. By 1986, however, FM 100-5, *Operations* replaced "rear battle" with "rear operations." Integrating rear operations into FM 100-15, *Corps Operations*, and FM 71-100, *Division Operations* made a separate FM 90-14, *Rear Battle* obsolete.[3] Most recently, the 2001 edition of FM 3-0, *Operations* replaced the term "rear operations" with "sustaining operations", introduced fundamental changes to the operational framework, and suggested leaders use adaptive combinations of contiguous and noncontiguous areas of operations with linear and nonlinear operations in the execution of full spectrum operations. Is this new concept of "sustaining operations" merely a change in semantics or are there fundamental changes required in the continuing evolution in rear area and base security doctrine? Does the U.S. Army need to adapt and improve elements of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF), as the Soviet Army did in Afghanistan, to succeed on the future battlefield? This monograph will determine if current U.S. Army rear area and base security doctrine is sound for sustaining operations on the noncontiguous nonlinear battlefield.

[3] Summary available from Combined Arms Doctrine Development (CADD) paper "Evolution in Rear Operations", Draft (unpublished), dated 18 April 2001. Additional review of 1982 and 1986 obsolete versions of FM 100-5, *Operations* and the 1985 obsolete version of FM 90-14, *Rear Battle.*

Literature Review

There are two prominent works that recently addressed rear area and base security doctrine. The Association of the United States Army Institute of Land Warfare published the first, *Threat to the Rear: Real or Myth,* in 1989. The author, General Glenn K. Otis, USA (Ret.) served as the commanding general of both United States Army Europe (USAREUR) and Training and Doctrine Command (TRADOC) during the 1980's. His thesis was that the U.S. Army war-fighting doctrine of his generation - AirLand Battle - focused on the deep and close fight and potentially overlooked the battle in the rear area.[4]

Otis presented Operation BARBAROSA – the German invasion of Russia in June 1941 – as a historical case study to evaluate doctrine against threat. He researched the partisan, regular, and irregular threats the German Army faced. He recorded partisan tactics ranging from all out conventional attacks to small raids and ambushes on supply routes and captured the cumulative effect of these tactics in draining manpower and resources from the German Army and its efforts to maintain the lines of communication. Additionally, Otis presented Soviet conventional forces including bypassed units, infiltrated ground troops, and an airborne division capable of disrupting enemy rear area activities, destroying stocks of ammunition and fuel, and seizing airfields, bridges, and other tactical objectives. Finally, Otis outlined irregular Soviet Special Forces (SPETSNAZ) operations in the German rear.[5]

After presenting these historical threats to the German Army, Otis answered the "so what?" of his thesis in relation to the U.S. Army doctrine of the 1990's. He challenged that the required U.S. response for the rear area fight must include a well-organized intelligence network, specially trained forces, and unity of command. He believed intelligence must be human source intelligence (HUMINT) based with the goal "to prevent a rear area threat from occurring rather

[4] Glenn K. Otis, "Threat to the Rear: Real or Myth?," *Land Warfare Paper*, no. 2 (November 1989): 2.
[5] Ibid., 20-27.

than fighting one after it matures," and he called for counter guerrilla training and equipment under a unified command. Overall, he faulted a U.S. rear area protection doctrine that depended on a reactive, ad hoc response force designed to counter a sporadic overt threat.[6]

MAJ Ernest A. Szabo wrote the second key work, "Does the Army have an Effective Doctrine for the Conduct of Rear Area Security and the Protection of Support Troops?" for his SAMS monograph in 1996. Szabo's primary recommendations were tactical in nature and addressed the training, organization, and arming of support troops in the rear to increase their ability to protect themselves from Level I threats. For Level II and III threats, he proposed creating an organic corps area security force based on a Light Armored Cavalry Regiment (ACR) organization.[7] Many of Szabo's recommendations are still relevant today; however, his monograph is dated and does not address emergent threats; future organizations of the Interim Brigade Combat Team (IBCT) or Objective Force; or, most importantly, fundamental changes to rear area and base security doctrine based on the new operational framework in FM 3-0, *Operations*.

Both of these works are based on a common framework: they portray operations on a linear and contiguous battlefield – the deep, close, rear, battlefield of AirLand Battle – and present a recognizable enemy to the front and friendly forces on the flank and rear. The conceptual framework for rear area and base security doctrine is still evolving. In the Institute of Land Warfare paper *Conceptual Foundations of a Transformed U.S. Army*, Huba Wass de Czege and Richard Hart Sinnreich stated we are handicapped "by an Army organizational design optimized for set-piece battles with clearly defined and contiguous deep, close and rear battle areas, and far less well suited to operations in highly fluid conditions in which the operational focus changes rapidly, and in which a secure rear area cannot be guaranteed without retarding operational

[6] Ibid., 28-32.

tempo."[8] This monograph will continue where the works by Otis and Szabo left off and determine if current U.S. Army rear area and base security doctrine is sound for sustaining operations on the noncontiguous nonlinear battlefield.

Research Topic Criteria

To answer this research question, this monograph will assess the threat to sustainment operations, review existing and emergent Joint and Army doctrine, and analyze these findings against the characteristic of sound doctrine. These characteristics - effective, acceptable, well researched, enduring, flexible, comprehensible, consistent, and concise - are found in TRADOC Regulation 25-36, *The TRADOC Doctrinal Literature Program*.[9] After analysis, this monograph will suggest possible changes for improvement.

---

[7] Ernest A. Szabo, "Does the Army have an Effective Doctrine for the Conduct of Rear Area Security and the Protection of Support Troops?" (Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 20 December 1996), 36-45.
[8] Huba Wass de Czege and Richard Hart Sinnreich, "Conceptual Foundations of a Transformed U.S. Army," *Land Warfare Paper*, no. 40 (March 2002): 10.
[9] Department of the Army, *The TRADOC Doctrinal Literature Program (DLP)*, TRADOC Regulation 25-36, (Fort Monroe, Virginia: U.S. Army Training and Doctrine Command, 5 April 2000, accessed 25 January 2003); available from http://www.tradoc.army.mil/tpubs/regs/r25-36fram.htm; Internet. 7-8.

Chapter 2: Doctrine

Joint Doctrine

JP 3-10, *Joint Doctrine for Rear Area Operations.*

Joint Publication 3-10, *Joint Doctrine for Rear Area Operations* serves as the capstone rear area operations doctrine for the military. It describes the concept of the joint rear area (JRA); discusses the command, control, communications, computers, and intelligence (C4I) requirements; provides guidance on security considerations; and covers combat operations in the JRA. As authoritative doctrine, JP 3-10 governs operations to achieve overall security of the JRA through reliable C4I, command relationships, and assignment of responsibilities.

The concept for the joint rear area includes definitions, operations within, and threats to the JRA. JP 3-10 defines the JRA as a specific land area within a joint force commander's (JFC) operational area designated to facilitate protection and operation of installations and forces supporting the joint force. While the size may vary, the JRA is normally to the rear of the combat zone and may be co-located with the communications zone. The geographic combatant commander appoints a joint rear area coordinator (JRAC) who is responsible for the overall security including the coordination of all intelligence, counterintelligence, and communications in the JRA.[10]

The operations within the JRA either protect the JRA or support the joint force operating there and include the following eight functions: security, communications, intelligence, sustainment, area management, movements, infrastructure development, and host-nation support. Security operations protect against hostile threats to ensure sustainment mission capability and require effective communications and intelligence support utilizing joint and interagency assets. The primary mission of forces in the JRA is executing sustainment operations. To succeed, area

commanders must manage the positioning of subordinate units and movement control operations to maximize distribution. Finally adequate infrastructure development and host-nation support ease the burden on the JRAC and maximize the efforts of the JRA.[11] Of these eight functions, security operations - developed further in JP 3-10.1,*Joint Tactics, Techniques, and Procedures for Base Defense* - primarily guide the formation of Army rear area and base security doctrine.

The detailed threats to the JRA are theater-dependent; however, the broad categories are divided into three threat levels – Level I, Level II, and Level III - and cover a wide range of enemy capabilities, identify the required response to counter them, and provide a common reference for planning guidelines. Joint doctrine does not clearly define these threat levels; instead, it provides the typical threats associated with each level and the likely appropriate response to counter it. The JRA threat levels, examples, and required response are shown in Figure 1.[12]

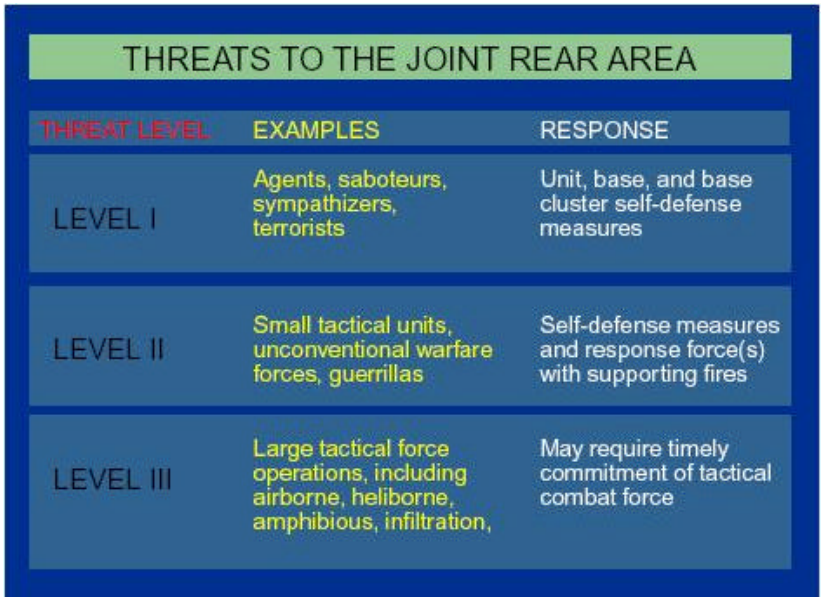

Figure 1. Threats to the Joint Rear Area (from JP 3-10 page I-7)

---

[10] Department of Defense, *Joint Doctrine for Rear Area Operations,* Joint Pub 3-10, (Washington, D.C.: U.S. Department of Defense, 28 May 1996), I-1 to I-2.
[11] Ibid., I-3 to I-4.
[12] Ibid., I-5 to I-7.

JP3-10 predicts an enemy employing air, ground, space, surface, and subsurface operations to detect friendly targets, destroy capabilities, delay or disrupt movement and supply, weaken C2, prepare the battlefield for future operations, and create panic and confusion throughout the JRA. Typical enemy priority targets may include: airfields and air bases; port facilities; main supply routes and chokepoints; key LOCs; and critical logistic facilities.[13] It is the responsibility of the JFC, the JRAC, and service component commanders to protect these targets and U.S. forces operating in the JRA.

After describing the concept of the JRA with definitions, operations within, and threats to the JRA, JP 3-10 lays out the command, control, communications, computers, and intelligence (C4I) requirements. Doctrine states JRA operations are an economy of force mission. The joint force commander is responsible for all JRA operations including force protection and base defense measures. The JFC dedicates necessary assets to conserve resources and prevent degradation of support and appoints a joint rear area coordinator (JRAC) to manage the overall security of the JRA through a joint rear tactical operations center (JRTOC). The JRAC has a wide range of responsibilities including the coordination of: security posture and defense plans; response and tactical combat forces; threat and vulnerability assessments; LOC, infrastructure, movements and sustainment operations protection; subordinate unit and facilities positioning; and liaison with multinational and host nation commands. To accomplish these tasks, the JFC may segment the JRA along component commands enabling each service to achieve unity of command and unity of effort for their area of responsibility. These component commanders will organize bases into base clusters and appoint base and base cluster commanders (see Figure 2).[14]

[13] Ibid.
[14] Ibid., II-1 to II-9.

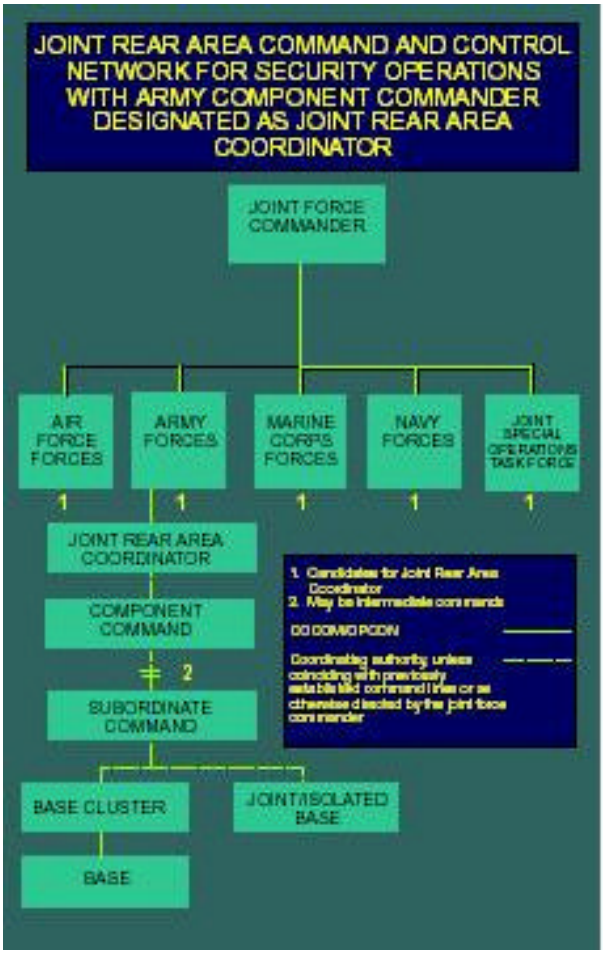

Figure 2. Joint Rear Area Command and Control Network for Security Operations (from JP 3-10 page II-5)

The base and base cluster are the fundamental building blocks of base defense operations. A base cluster – defined as a collection of bases, geographically grouped for mutual protection and ease of command and control - integrates a number of bases to improve overall support and security and deconflict subordinate defense plans. A base cluster commander coordinates the defense of the bases within the base cluster and establishes a base cluster operations center (BCOC) to facilitate the tactical command, control, and communications with higher commands. Likewise, the base commander coordinates the defense of the base – defined as a locality from which operations are projected or supported - and establishes a base defense operations center

(BDOC) for tactical command and control. The base commander employs transient forces into the base defense plan and serves as the area commander when emergencies arise in the base defense area.[15]

All forces in the JRA strive to accomplish the seven joint objectives of security operations in the JRA. The seventh objective – assess and prioritize bases – requires commanders to assess the threat and prioritize assets for protection and damage repair. These seven objectives are summarized in Figure 3.[16]

Figure 3. Objectives of Security Operations in the Joint Rear Area (from JP 3-10 page III-1)

In response to the threats to the JRA and in order to accomplish the objectives of security operations, the JFC determines the need for a tactical combat force (TCF) and its command and control relationship, employment conditions, and rules of engagement (ROE). The JRAC advises the JFC, recommends forces, coordinates required effects, and establishes communications with the TCF. Doctrine suggests eight options for a TCF including: tactical units passing through the JRA, units assigned security missions or undergoing reconstitution in the JRA, or a task organized force from assets disembarking in the theater. In appointing a TCF, commanders must

[15] Ibid., II-10 to II-12.

consider four tenets for successful combat operations by the TCF: knowledge of the enemy; unity of command through the JFC, JRAC, component, base cluster, and base commanders; economy of force; and responsiveness through immediate reaction, rapid deployment, timely intelligence, and reliable communications.[17]

In summary, JP 3-10 outlines generic concepts, definitions, and threat levels of the JRA. The flexible command and control elements are an economy of force mission and must accomplish seven key objectives to maintain security in the JRA. To accomplish this feat, a TCF serves as a responsive reaction force for the JFC.

JP 3-10.1, Joint Tactics, Techniques, and Procedures for Base Defense.

Joint Publication 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense* mirrors the doctrine of its parent manual, JP 3-10, in outlining the JRA concepts in chapter I. It further develops responsibilities for command, control, and communications in chapters II and III, and it expands upon base defense operations doctrine in chapter IV by providing detailed tactics, techniques, and procedures in order to accomplish security operations in the JRA. The base defense operations doctrine in chapter IV requires an understanding of the fundamentals of base defense, defensive factors, intelligence responsibilities, and planning.

Before reviewing the base defense operations, it is important to outline the command responsibilities from the JFC, JRAC, component, base cluster, and base commanders established in JP 3-10 and their expanded relationship to the response and tactical combat force (TCF) commanders in JP 3-10.1. A response force is a mobile force with appropriate fire support, usually designated by the area commander to deal with Level II threats in the rear area. A response force may be TACON to base commanders or assigned its own AO. A TCF is a combat unit, with its own organic combat support and combat service support assets designated by the

---

[16] Ibid., III-1 to III-3.
[17] Ibid., IV-1 to IV-6.

JFC to respond to Level III threats in the JRA. When committed, the TCF is assigned its own AO requiring close coordination with component, area, base cluster, and base commanders.[18] These commanders must collectively plan and execute base defense operations.

There are eight fundamentals of base defense summarized in Figure 4.[19]

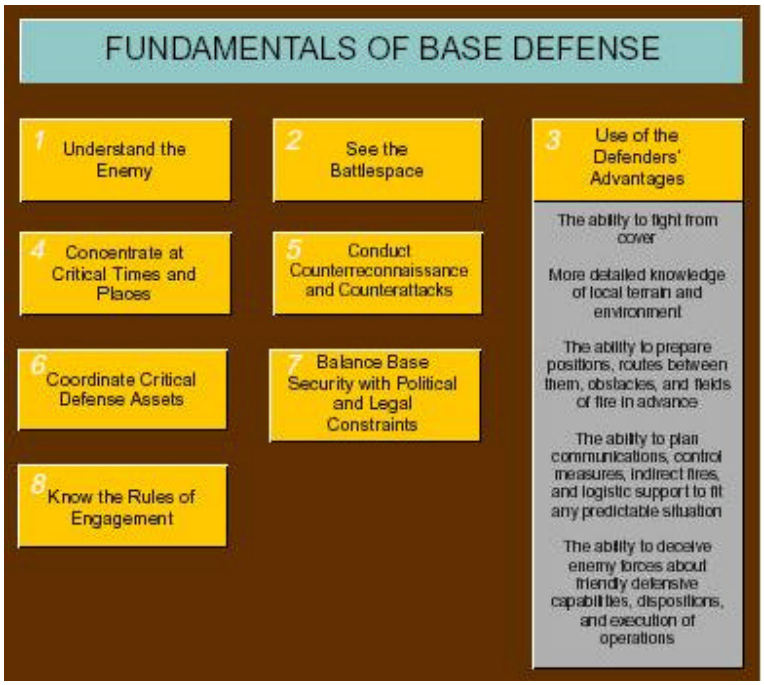

Figure 4. Fundamentals of Base Defense (from JP 3-10.1 page IV-1)

Commanders must consider these fundamentals of base defense in conjunction with the defensive factors of mission, enemy, terrain and weather, troops, and time available (METT-T). To accomplish the mission of supporting the joint force, each base must be able to defend itself. This requires the ability to detect the enemy, warn friendly forces, deny enemy access, and destroy the enemy when possible or delay the enemy until destroyed by the proper response force. Base defense operations must determine enemy capabilities and intentions through the use of priority intelligence requirements and information requirements. Because doctrine requires

[18] Department of Defense, *Joint Tactics, Techniques, and Procedures for Base Defense*, Joint Pub 3-10.1, (Washington, D.C.: U.S. Department of Defense, 23 July 1996), II-7 to II-8.

organic base assets to detect and defeat Level I threats and delay or disrupt Level II and III threats, commanders must consider the troops available to execute these missions, their capabilities and training level, and the time available to conduct base defense training while balancing mission support. These tasks, often performed by non-combat arms personnel, include: controlling direct and indirect fires; patrolling and surveillance; conducting mobility, countermobility, and survivability tasks; operating in an NBC environment; employing OPSEC; and conducting deception operations.[20]

Successful planning for base defense operations is an integrated, aggressive, and in-depth process. Base commanders are responsible for their area of operation and doctrine requires a clearly defined boundary between sectors assigned to subordinate units. They must employ observation posts, listening posts, and patrols throughout the depth of the AO and link these assets with sensors and communications to provide a common operating picture for the necessary command and control of forces. Doctrine suggests a mobile, armor, vehicle mounted reserve with an antiarmor capability linked to indirect fire assets through the fire support element (FSE) or fire support coordination cell (FSCC) of the BDOC. For a large JRA, commanders may require aviation support for an airmobile response force, TCF, and aviation fire support. When faced with a Level II or Level III threat, the area commander commits a response force or requests the commitment of the TCF. The tactical situation determines the C2 relationship (TACON or OPCON) between the base commander, base defense force, response force, and the TCF. (See Figures 5, 6, and 7)[21]

---

[19] Ibid., IV-1 to IV-3.
[20] Ibid., IV-3 to IV-6.
[21] Ibid., IV-7 to IV-12.

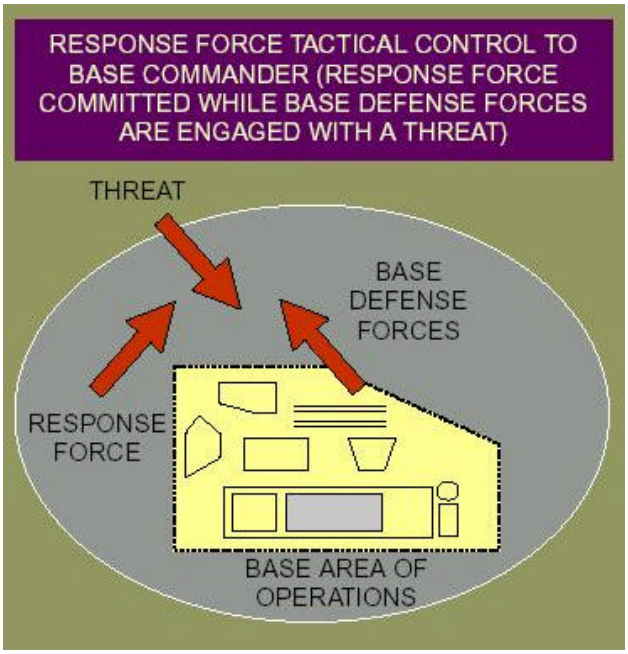

Figure 5. Sample Base Defense Force and Response Force Operations and Command Relationships (from JP 3-10.1 page IV-9)

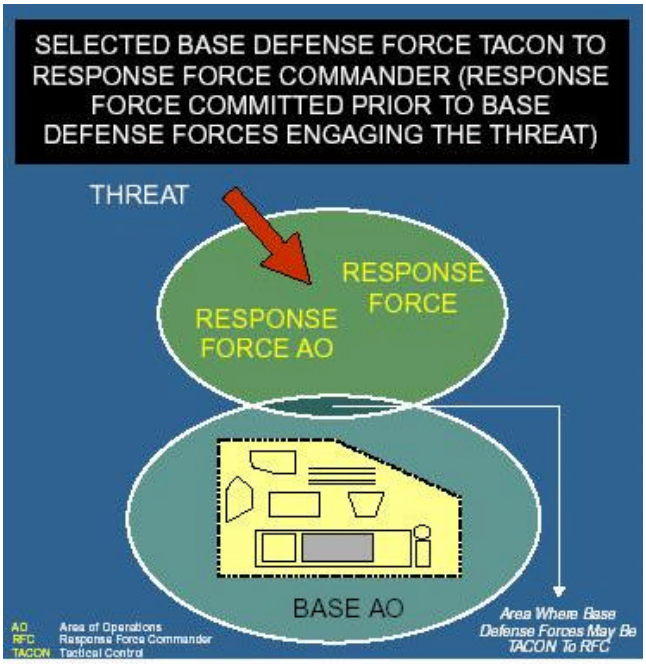

Figure 6. Sample Base Defense Force and Response Force Operations and Command Relationships (from JP 3-10.1 page IV-10)

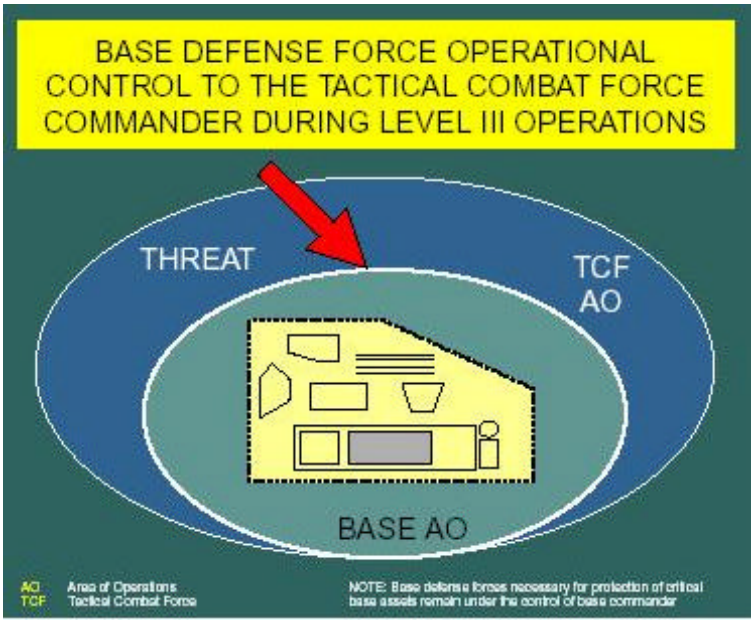

Figure 7. Sample Base Defense Force and Tactical Combat Force Operations and Command Relationships (from JP 3-10.1 page IV-11)

In addition to base defense operations TTPs, the appendixes in JP 3-10.1 also provide a broad overview of specific operational force protection topics including: nuclear, biological, and chemical defense (NBC); air and missile defense; security; and terrorism operations. While JP 3-10.1 provides detailed, almost tactical guidance for base defense operations, it elevates the force protection requirements to operate in an NBC, air or missile threat, or terrorism environment to the operational level. Instead of including these environments as part of the holistic base defense doctrine, it treats them as an anomaly, relegates them to an appendix, and refers the reader to additional doctrine.

Army Doctrine

FM 3-0, *Operations*

The Army published FM 3-0, *Operations* on 14 June 2001 while celebrating its 226th birthday. This edition attempts to expand the 1993 version of FM 100-5 and guide the post-Cold

War Army into the early 21st century. Part one lays the foundation of the Army and the role of land power and introduces the elements of combat power and the concept of full spectrum operations – offensive, defensive, stability, and support operations – into army doctrine.

Combat power includes maneuver, firepower, leadership, protection, and information. Protection includes air, space, and missile defense; nuclear, biological, and chemical defense; antiterrorism; defensive information operations; and security to operational forces and means. At the operational level, rear area and base security contributes to force protection.[22]

Chapter four builds on the full spectrum foundation and introduces the operational framework. This framework enables the arrangement of friendly forces and resources in time, space, and purpose with respect to each other and the enemy situation. The operational framework consists of the area of operations, battlespace, and the battlefield organization.[23] These doctrinal changes in the area of operations and battlefield organization serve as two of the primers for this monograph.

As a component of the operational framework, the area of operations (AO) allows the commander to employ organic, assigned, and supporting systems within their capabilities and boundaries. Subordinate unit areas of operations may be contiguous with a common boundary separating them or noncontiguous without a shared boundary. When operating in a noncontiguous area of operations, the higher headquarters is responsible for the unassigned area between subordinates.[24] Figure 8 presents a sample of contiguous and noncontiguous areas of operations.

[22] Department of the Army, *Operations*, FM 3-0, (Washington, D.C.: Headquarters, Department of the Army, 14 June 2001), 4-8 to 4-9.
[23] Ibid., 4-18.
[24] Ibid., 4-19.

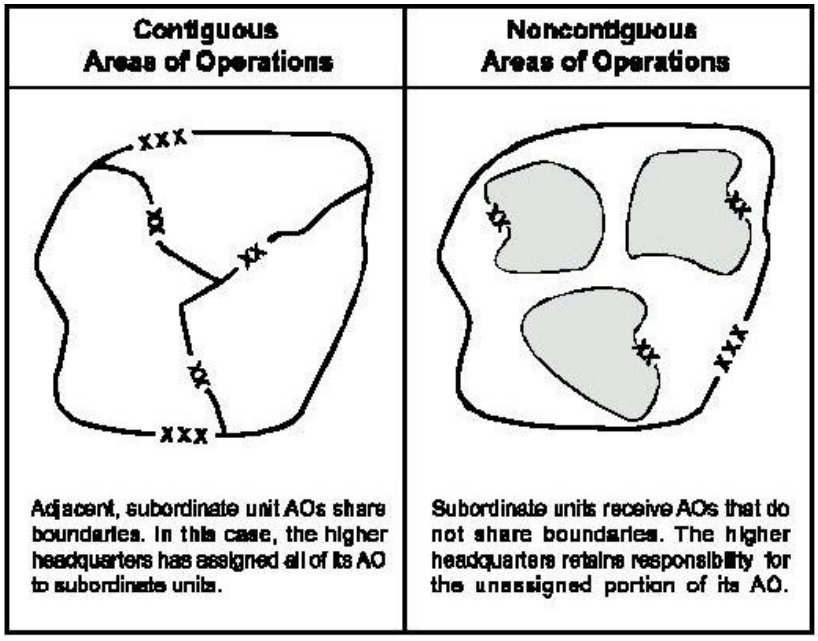

Figure 8. Contiguous and Noncontiguous Areas of Operations (from FM 3-0 page 4-20)

Battlefield organization is an additional component of the operational framework. It is a product of the commander visualizing the battlespace and provides a concept to arrange forces. FM 3-0 defines the battlefield organization as "the allocation of forces in the AO by purpose. It consists of three all-encompassing categories of operations: decisive, shaping, and sustaining."[25] The change to FM 3-0 requiring the allocation of forces in the battlefield organization by purpose, not location, is a significant change; a traditional "rear area" comprised of logistic units may now be the "decisive operation" – especially in full spectrum support operations.

In the battlefield organization, sustaining operations are defined as "operations at any echelon that enable shaping and decisive operations by providing combat service support, rear area and base security, movement control, terrain management, and infrastructure development."[26] Rear area and base security functions include measures taken by units to protect themselves from acts

[25] Ibid., 4-22.
[26] Ibid., 4-24.

designed to impair operations and effectiveness. There are four components: intelligence, base and base cluster self-defense, response force operations, and combined arms tactical combat force (TCF) operations.[27] Army sustaining operations are similar to the Joint rear area operations, and Army rear area and base security functions are similar to the Joint base defense operations.

While introducing the battlefield organization by purpose (decisive, shaping, and sustaining operations), FM 3-0 continues the spatial reference of deep, close, and rear areas and may inadvertently confuse readers to associate the deep area with shaping operations, close area with decisive operations, and rear area with sustaining operations. FM 3-0 acknowledges, "These spatial categories (deep, close, and rear) are especially useful in operations that are generally contiguous and linear and feature a clearly defined enemy force."[28]

After introducing the new operational framework, chapter five discusses battle command and the aspects of leadership - visualize, describe, and direct – inherent therein. The elements of operational design, which conceptually link ends, ways, and means, are one of the tools available to the commander to help visualize the battlefield. Linear and nonlinear operations are one of the nine elements of operational design.

Linear operations usually involve forces operating in a contiguous AO with combined arms directed towards a common enemy. The array of forces emphasizes geographic position creating a continuous forward line of own troops (FLOT). This FLOT protects rear area lines of communication and enables freedom of action over extended periods of time. Linear operations are still appropriate against an echeloned enemy force, when severely outnumbered, when LOCs are threatened, or when lacking the required information dominance to conduct nonlinear operations.[29] However, as presented in the following chapter, the future threat may drive an increase in nonlinear operations.

---

[27] Ibid.
[28] Ibid., 4-22.
[29] Ibid., 5-12.

Nonlinear operations are becoming more prevalent and involve maneuver forces orienting on objectives without geographic reference to adjacent units. These operations involve multiple lines of operation and decisive points and employ simultaneous effects to overwhelm the enemy. Doctrine states LOCs will diverge and may require CSS units to move with maneuver units or resupply by air in order to provide distribution-based logistics.[30]

Finally, chapter six presents tools to plan, prepare, execute, and assess the conduct of full spectrum operations. This chapter recommends the use of adaptive combinations of battlefield framework and operational design by incorporating contiguous and noncontiguous AOs with linear and nonlinear operations. These four combinations are depicted in Figure 9.[31]

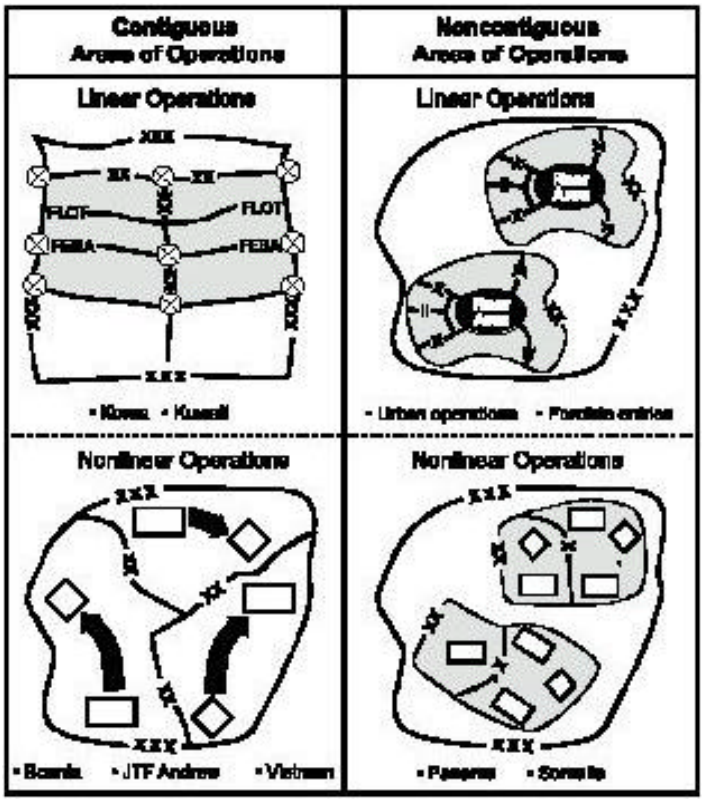

Figure 9. Combinations of Contiguous and Noncontiguous Areas of Operations with Linear and Nonlinear Operations (from FM 3-0 page 6-16)

[30] Ibid., 5-11.
[31] Ibid., 6-15.

While the Army has conducted operations in each of these four combinations, subordinate doctrine - including rear area and base security doctrine - may not be sound for each combination.

FM 3-90, *Tactics*

FM 3-90, *Tactics*, expands on the conceptual foundation laid in FM 3-0, *Operations* and provides the tactical "nuts and bolts" of how the U.S. Army fights. It is organized into four parts. Part one presents the tactical fundamentals including the art of tactics, common tactical concepts, and graphic control measures. Parts two and three discuss offensive and defensive operations respectively. Part four presents the tactical enabling operations and the appendices, including the Rear Area and Base Security Appendix, which outline additional operations.

Chapter two reviews the operational framework presented in FM 3-0 and examines the contiguous and noncontiguous AO in further detail. Army commanders employ a contiguous AO – defined as all of the subordinate forces' AOs sharing one or more common boundary – based on analysis of METT-TC. Contiguous AOs are normally within supporting distance and range of one another, and they reduce the risk of being defeated due to an incomplete operational picture or when significantly outnumbered by providing a greater concentration of combat power in the contiguous AO. Commanders employ a noncontiguous AO – defined as one or more of the subordinate forces' AOs not sharing a common boundary – also based on the METT-TC analysis. Because subordinate units are normally out of supporting range from each other in a noncontiguous AO, units are more vulnerable, and commanders require greater situational understanding and tactical mobility to mitigate this increased risk. While noncontiguous AOs do not have distinctive forward, rear, and lateral boundaries, commanders who establish them for subordinates still designate an echelon rear area (see Figure 10).[32]

[32] Ibid., 2-15 to 2-17.

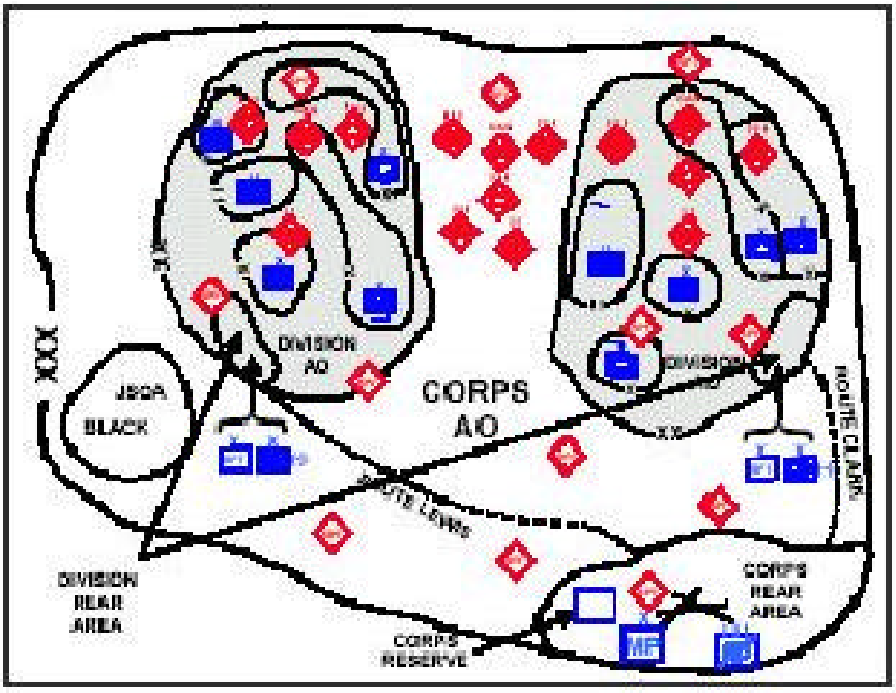

Figure 10. Corps with Noncontiguous Areas of Operations (from FM 3-90 page 2-17)

Doctrine acknowledges that commanders operating in noncontiguous AOs must employ innovative measures to conduct sustaining operations. In the corps noncontiguous AO shown in Figure 10 above, the corps retains responsibility for the AO (including ROUTE LEWIS and ROUTE CLARK) not assigned to the subordinate divisions or the corps rear area. FM 3-90 proposes three possible solutions for establishing the intermittent ground lines of communications (LOCs) from the corps rear area to the subordinate divisions. In the first option, the corps could assign a subordinate (e.g. the corps military police brigade) the mission to provide convoy security for each convoy. In the second option, the corps could assign a subordinate (e.g. the corps armored cavalry regiment) an AO including each route with the mission to provide route security for each route. In the third option, the corps could assume risk and have the corps

support command (COSCOM) provide their own organic self-defense for their convoys with an additional corps unit capable of responding to threats beyond the COSCOM convoy capability.[33]

FM 3-90 amplifies the battlefield organization and spatial references to the deep, close, and rear area, and *requires* the designation of the rear area, in both the contiguous and noncontiguous AO, for the performance of support and sustainment functions including: CSS, rear area and base security, movement control, terrain management, and infrastructure development. Doctrine acknowledges that the rear area focus on predominately non-combat operations renders it vulnerable to enemy threats. In a noncontiguous AO, the physical separation from combat units further magnifies this vulnerability.[34]

While chapter two of FM 3-90 reviewed and expanded on the fundamentals of the operational framework (including contiguous and noncontiguous areas of operation) and rear area functions, Appendix E, *Rear Area and Base Security* provides the basic guidance for commanders in organizing forces, employing control measures, and planning, preparing, and executing rear area and base security operations across full spectrum operations to achieve the purpose of preventing interruption of current and future operations. Army rear area and base security doctrine includes: command responsibilities, control exercised by area commanders, base and base cluster defense operations, route security, and convoy security operations.

Rear area commanders are responsible for their echelon's sustaining operations. The deputy corps commander normally serves as the corps rear area commander, the assistant division commander (support) as the division rear area commander, and the forward support battalion commander as the brigade rear area commander. In order to deconflict the command authority for units operating in these echelon rear areas, the echelon rear area commander assigns every unit to a base or base cluster, and these units are TACON to that base or base cluster commander during implementation of rear area and base security operations. Doctrine allows each echelon

[33] Ibid., 2-18.

rear area commander to further divide their rear area into subordinate AOs, base clusters, and bases.[35]

The echelon rear area commander has a staff to serve as the nucleus of an operations cell. In the corps rear area, the rear operations center (ROC) is an austere reserve component organization that dissolves into the corps rear command post and serves as the G2 and G3 for the deputy corps commander. The rear area operations center (RAOC) is also an austere reserve component organization, but unlike the ROC, it retains its own separate unit identity and supports the corps support group commanders with rear area and base security planning and operations.[36]

The base and base cluster, as in the joint doctrine, are the building blocks for the rear area. Army doctrine further defines the base as having a defined perimeter with established access controls. The base commander is the senior Army commander (usually a battalion commander) charged with defending the base, and his battalion staff serves as the base defense operations center (BDOC) responsible for base security and defense. The base commander must integrate into the area security operations of the BCOC, RAOC, or RTOC. The BDOC maintains the current situation; plans and executes active and passive defense; reduces conflicts; collects, processes, and disseminates information and intelligence; and provides command and control.[37]

Army doctrine states a base cluster normally doesn't have a defined perimeter or controlled access. It serves as the higher headquarters for bases and contains from two to seven bases. A CS or CSS brigade or group commander is the base cluster commander and his staff serves as the base cluster operations center (BCOC). The BCOC performs many of the same BDOC functions and is additionally responsible for providing functional elements operating in the rear area with specific information on: LOC status, area communications, the common operational picture,

---

[34] Ibid., 2-25 to 2-26.
[35] Ibid., E-3.
[36] Ibid., E-4.
[37] Ibid., E-4 to E-6.

enemy weapons of mass destruction location or use, and battlefield hazard tracking with explosive ordnance disposal (EOD) support.[38]

Army doctrine clearly defines threat levels in doctrine. A Level I threat is a small enemy force that can be defeated by CS and CSS units operating in the rear area or by the perimeter defenses established by friendly bases and base clusters. A Level II threat is enemy activities that can be defeated by a base or base cluster augmented by a response force. A Level III threat is beyond the defensive capability of both the base and base cluster and any local reserve or response force. The friendly response to a Level III threat is a TCF.[39] The threat levels, in both joint and army doctrine, are not defined by the type or size of enemy threat or the impact on friendly operations. The threat levels are defined by the required friendly response to counter them.

FM 3-90 also introduces a category of utility – critical, priority, general control, and no importance - for different locations. Critical areas are essential to accomplishing sustaining operations (e.g. an APOD). Priority areas if disrupted, can be transferred to an alternate location within an acceptable amount of time (e.g. a bridge over a major waterway). Areas under general control permit sustaining operations to move to other locations without major problems (e.g. MSRs where parallel ASRs exist). The utility of different locations is not a component of the threat levels.

FM 3-90 outlines the organization of forces in executing base and base cluster defense. These forces include Army initiated base and base cluster defense forces in addition to the rear area security forces (response forces and TCF) outlined in joint doctrine. The base commander establishes a base defense force (BDF) defined as a security element established to provide local security to a base. The BDF is composed of soldiers assigned from organic or subordinate units assigned to the base, and it assists in defeating Level I threats, patrolling outside the base

[38] Ibid., E-6 to E-7.

perimeter, and providing interior guards to the BDOC. Doctrine acknowledges that providing this force "out of hide" has two undesirable effects. First, it reduces the operational effectiveness of the units providing the BDF assets, and secondly, it tasks soldiers with duties outside their specific MOS. Doctrine also recommends that soldiers assigned to the BDF remain in their positions in order to facilitate training, provide continuity, and ensure efficiency. The base cluster defense force is merely a collection of the BDFs within the base.[40]

Army doctrine expands on the joint TCF guidance and states the TCF should be a dedicated force to ensure it is available when needed. While METT-TC determines the requirements for a TCF, doctrine suggests at least on battalion task force for a corps and a reinforced company team for a division. The TCF should be ground and air mobile due to limited reaction time and extended distances in the rear area.[41]

FM 3-90 lists the same eight fundamentals of base defense as JP 3-10.1 and adds one – responsiveness. Base and base cluster commanders achieve responsiveness through clearly established authority, wide-area information systems providing flexible warning, robust communications systems, and capable response forces with a mixture of firepower, protection, and mobility.[42]

FM 3-90 also introduces route and convoy security operations as separate components of rear area and base security. Route security operations are defined as a specialized kind of area security operation conducted to protect lines of communication and friendly forces moving along them. Route security operations are defensive in nature and terrain oriented. They include passive security, route reconnaissance, cordon security, and combat security techniques. Cordon security is defined as the security provided between two combat outposts positioned to provide mutual support. While cordon security physically protects covered portions of a route, it is a

[39] Ibid., E-7 to E-8.
[40] Ibid., E-10 to E-13.
[41] Ibid., E-14 to E-15.

resource heavy operation and does little to eliminate the overall rear area threat. Combat security is a technique where combat units provide route security by seizing and securing terrain along the flanks of a route. It is the most costly technique for route security and usually requires a battalion-sized force to secure routes in a division-sized AO. Convoy security operations are defined as specialized area security operations conducted to protect convoys. These operations are also resource intensive and require a maneuver or MP company to protect an average-size convoy of 50 vehicles by providing the advance guard, security, escort, and rear guard elements to ensure front, flank, and rear security for the convoy.[43]

There are consistent threads through joint and army doctrine. Units in the rear area organize in often ad hoc bases and base clusters and depend on unity of command, timely intelligence, and mutual support for their security. They require responsive and often proactive combat forces of increasing capability to counter a myriad of enemy threats that are defined by the required friendly response. While this "circle the wagons" mentality has worked in the past, is it still appropriate based on the future threat in an evolving operational framework?

[42] Ibid., E-18.
[43] Ibid., E-31- E-40.

Chapter 3: Threat

Legacy Force Threat

The evolution of threats facing sustainment operations can be deduced from a sample of the development of corps, forward, main, and base support battalion mission training plans (MTP) which guide the training of support units in rear area and base security operations.

In the late 1980's, MTPs for the corps, forward, and main support battalions supporting heavy and motorized divisions focused unit training by providing a threat annex. These threat annexes support AirLand Battle doctrine and portray an echeloned armor heavy force that would smash through enemy defenses in an effort to strike the operational rear quickly to disrupt the rear area command and control, communications, supply facilities, and airfields. These attacks came from aviation, fires, maneuver, electronic combat, and NBC warfare. Aviation threats included reconnaissance and surveillance, tactical air attack, and helicopter gunships with rocket, missile, and machine gun fires. Fires threats included artillery, rocket, and missile attacks and would cause about 50% of the total casualties and range up to 40 kilometers from the forward line of troops (FLOT). Maneuver threats ranged from Level I to Level III threats. Level I threats included unconventional warfare, special purpose (SPETSNAZ) forces, agents, and insurgents. Level II threats consisted of company sized units conducting raids, ambushes, reconnaissance, and heliborne assaults in the rear. Level III threats included the operational maneuver group or battalion (OMG/OMB). Our doctrine today continues to be defined by the friendly response to this Soviet style maneuver threat (Level II requires base and base defense forces, Level II requires a response force, and Level III requires a TCF). Electronic threats included direction finding, jamming, and deception operations to disrupt our command, control, and communications. Finally, NBC threats would deny our use of vital supplies and facilities.[44] These threats, based on

[44] Department of the Army, *Mission Training Plan for Battalion Headquarters, Forward Support Battalion, Heavy and Motorized Divisions*, ARTEP 63-005-MTP, (Washington, D.C.: Headquarters, Department of

a predictable, echeloned enemy served as the model for our doctrine and training for several decades. Ironically, the current editions of the MTPs for the FSB and MSB, published in October 2001, omit the threat annex entirely as if the Army is unsure of the current threat.

The Contemporary Operating Environment (COE) and Guerrilla Warfare

The end of the Cold War, marked by the fall of the Berlin Wall in 1989 and subsequent collapse of the Soviet Union, found America in a state of uncertainty. U.S. Army doctrine evolved to counter the Soviet threat of a massive, mechanized, and predictable army echeloned on a linear battlefield and introduced AirLand Battle doctrine; maneuver weapon systems including the Abrams tank, the Bradley fighting vehicle, and the AH-64 Apache helicopter; and the combat training centers. The Threat Support Directorate at Fort Leavenworth, Kansas began the search for a replacement to the Soviet threat. They created the Contemporary Operating Environment (COE).

An operational environment (OE) is defined as a composite of the conditions, circumstances, and influences that affect the employment of military forces and bear on the decision of the unit commander. The contemporary operational environment (COE) is the operational environment that exists in the world today and is expected to exist until a peer competitor arises. The goal of the COE implementation is to produce an objective force of leaders, soldiers, and units capable of rapidly adapting and optimizing capabilities to achieve mission objectives – to fight and win – in a complex and evolving environment across the spectrum of conflict.[45] COE is about changing our Cold War mindset and seeing warfare through a different lens.

---

the Army, 03 October 1988) pages Threat 1-6 and *Mission Training Plan for Battalion Headquarters, Main Support Battalion, Heavy and Motorized Divisions*, ARTEP 63-125-MTP, (Washington, D.C.: Headquarters, Department of the Army, 30 March 1989), Threat 1-6. Both MTP Threat annexes are identical.

[45] Buck Shaw, *The Contemporary Operating Environment (COE)*, accessed 18 January 2003 available from http://www.cascom.army.mil/multi/training/CSS_Training_Support_Packages/COE/COE%20Fact%20Sheet.doc; Internet, 1-2.

There are twelve key variables that serve collectively as the foundation for understanding the COE and provide a framework to analyze potential adversaries. The first four variables are: the physical environment including terrain and weather; the nature and stability of the state and its leadership; the sociological demographics of the people; and the regional and global relationships, alliances, and coalitions. The next four variables are: conventional and unconventional military capabilities; asymmetric warfare to avoid U.S. strengths and target perceived weaknesses; technology exploitation; and information operations including computer network attacks and psychological warfare. The final four variables are: external organizations including non-government organizations (NGOs); the national will of both the U.S. and the enemy; time and tempo; and economics.[46] While these variables may be "contemporary", they are not all new.

During World War I, T.E. Lawrence, a British intelligence officer, worked with insurgents in the Arabian Peninsula fighting alongside the Arab Bedouin tribes against the Ottoman Turks. Lawrence observed and later recorded his theories on guerrilla warfare, and he distilled his experience into a theoretical framework of "six pillars of guerrilla warfare." Lawrence wrote that to achieve success the guerrilla movement must: operate from an unassailable base; confront a technologically sophisticated enemy whose reliance on communications and logistics are a vulnerability; fight a numerically weak enemy unable to occupy the disputed territory in depth; have the passive support of the populace; possess the speed, endurance, and logistical freedom of movement; and possess advanced weapons to strike at the enemy logistics and signal vulnerabilities.[47] Countering these pillars and the contemporary operating environment is a challenging task to rear area and base security sustaining operations and should guide U.S. Army transformation and doctrine development.

[46] Ibid., 3-6.
[47] James J. Schneider, "T.E. Lawrence," *Strategy and Tactics*, June 1992, 16-19.

Transformation

As the Army began the conceptual debate for transformation and the development of the COE, Huba Wass de Czege wrote, "Throughout most of the Cold War, the major threat confronting the Army was that posed by the Soviet Union and by other nations that, with regional variations, patterned their military forces after those of the Soviets. The very consistency of that pattern simplified the design of the Army's doctrine, organization, equipment, and training. When the threat diverged from threat pattern, however, as it did in Vietnam, the Army had to improvise."[48] The U.S. Army has begun this improvisation and is embracing the changing threat through the interim and objective force.

Interim Force Threat

The manuals ARTEP 63-106-MTP, *Mission Training Plan for Headquarters, Brigade Support Battalion (BSB), Interim Brigade Combat Team (IBCT)* and ARTEP 63-390F-30-MTP, *Mission Training Plan for the Combat Service Support Company (CSSC), Interim Brigade Combat Team (IBCT)* reinstate the use of the threat analysis annex deleted in current legacy force support battalion MTPs. These new annexes are vastly different than the Soviet based predecessor of only a decade ago, and they begin to focus on the threats outlined in the COE.

The IBCT is designed for primary employment in Small Scale Contingencies (SSCs) in complex and urban terrain. The IBCT effectiveness depends on the integration of operational and logistical planning through advances in CSS command and control, situational understanding, and information fusion. In supporting the IBCT, the BSB and CSSC threat annexes portray an enemy that is asymmetric, urban based, and offers no safe rear area. They further predict that U.S. lines of communication will be unsecured, the enemy will target our CSS assets, and CSS units will have to rely on self-protection because military police or a TCF reaction will be limited or non-existent. Convoy operations will be more difficult in urban terrain and vehicles will require

appropriate force protection. In addition to the urban threat, the MTPs call for increased capabilities against medical threats including directed energy; blast effect; flame and incendiary; and nuclear, biological, and chemical weapons.[49]

Objective Force Threat

Building on the Interim Force, *The United States Army Objective Force Operational and Organizational (O&O) Plan for Unit of Action* (Change 1 to TRADOC Pamphlet 525-3-90/O&O) describes a future operational environment of difficult terrain, adverse weather, and adaptive enemies, along with a social, physical and economic context of failed states, fractured societies, rampant crime with international linkages, and religious and ethnic tension.[50]

The Objective Force enemy will be an adaptive learning opponent and target the U.S. military capability across the levels of war. At the strategic level, the enemy will attack U.S. national will across the elements of power – diplomatic, informational, military, and economic – to preclude our regional engagement. Operationally, the enemy will engage in access denial to target strategic lift and deny ports of debarkation through employment of Special Purpose Forces (SPF) and long-range fires including cruise missiles and improved tactical ballistic missiles. Tactically, the enemy will conduct operations to achieve operational or strategic effects including the targeting of C4ISR; information operations including computer network attack, defense, and electronic warfare; and psychological and deception operations. Through the element of surprise, the enemy will employ strike techniques in a non-linear fashion and rapidly close and mass effects to destroy the opponent and then disperse. Across all levels, the enemy will seek niche

---

[48] de Czege and Sinnreich, "Conceptual Foundations," 2.
[49] Department of the Army, *Mission Training Plan Combat Service Support Company, Interim Brigade Combat Team*, ARTEP 63-390F-30-MTP, (Fort Lee, Virginia: U.S. Army Combined Arms Support Command, September 2002), F1 to F-7 and *Mission Training Plan Headquarters, Brigade Support Battalion, Interim Brigade Combat Team*, ARTEP 63-106-MTP, (Fort Lee, Virginia: U.S. Army Combined Arms Support Command, August 2002), F-1 to F-5.
[50] Department of the Army, *The United States Army Objective Force Operational and Organizational Plan for Unit of Action*, Change 1 to TRADOC Pamphlet 525-3-90/O&O, (Fort Monroe, Virginia: U.S. Army Training and Doctrine Command, 25 November 2002), 2-2.

technologies to achieve parity and selected overmatch. These efforts will attempt to deny situational understanding to US forces.[51]

Case Study: Russian Armed Forces in Afghanistan

Russia's war in Afghanistan from 1979-1990 provides a recent example of operations on a noncontiguous nonlinear battlefield. Julian Thompson summarized the Soviet war in Afghanistan best when he stated, "The battle in Afghanistan was, and is, for control of the lines of communication."[52] Afghanistan was an austere environment lacking infrastructure and railroads; therefore all movement went by air or ground over a treacherous road system. Soviet convoys were extremely vulnerable to ambush and required heavy augmentation of combat troops for protection. Likewise, the proliferation of surface to air missiles among the Mujahideen endangered the air resupply and required additional Soviet forces to defend airbases. By the wars' end, only one third of Soviet forces were actively engaged in combat operations – the remaining two thirds performed defensive escort duties, manned fortifications, conducted engineering support, or conducted static patrolling around key installations.[53]

Soviet lessons learned during their "highway war" – dorozhnaia voina – had a major impact on the logistic and movement support concepts for the Soviet military. Lester Grau stated, "Afghanistan is not Europe, yet the Soviet Army that occupied Afghanistan in late December 1979 was trained to fight NATO on the northern European plain. Consequently, the Soviet Army had to reequip, reform and retrain on-site to fight the insurgent Mujahideen (holy warrior) guerrillas. The Soviets were forced to revise their tactics and tactical methodologies in order to

[51] Ibid., 2-5 to 2-7.
[52] Julian Thompson, *The Lifeblood of War: Logistics in Armed Conflict* (Oxford: Brassey's, 1991), 308.
[53] Graham H Turbiville, "Ambush! The Road War in Afghanistan," *Army*, January 1988, 32-35.

meet the demands of this very different war."[54] These modified tactics included both defensive and offensive measures to protect the Soviet LOCs.

Mujahideen tactics against the Soviets included ambushing the lead and trail vehicle in a convoy then destroying the convoy in segments. To counter this, the Soviet Army created a special movement-security detachment called OODs (otriad obespecheniia dvizheniia). These detachments were flexible in size and tailorable in composition. Sub unit modules included reconnaissance, mine/barricade removal, and road/bridge repair with capabilities of electronic mine detection, roller equipped tanks, and trained dogs.[55] These OODs provided some protection to Soviet convoys.

The Mujahideen guerillas destroyed over 11,000 Soviet trucks, 1,300 armored personnel carriers, 140 tanks, and 400 artillery pieces in almost a decade.[56] The Soviets learned from these losses, changed their force structure, and began proactive ambush operations on the Mujahideen. They created the bronegruppa (armored group) of 4-8 tanks, BMPs or BTRs with organic *dismounted* infantry and fires as an offensive threat. In the article *High-desert Ambush: Hard Lessons Learned the Hard Way*, Lester Grau cites eleven vignettes as recounted by Soviet officers who conducted successful ambush operations on the Mujahideen. Grau summarizes these Soviet lessons learned. First, the ambush force must be highly mobile and integrate organic direct and indirect fires. Additionally, the force must have modular components including C2, diversion, combat, and snatch capabilities. Finally, the force must integrate new technology including infrared sights, robotics, and remote-controlled weapons and sensors.[57]

---

[54] Lester W. Grau, *High-desert Ambush: Hard Lessons Learned the Hard Way*, Accessed 18 February 2003, Available from http://fmso.leavenworth.army.mil/fmsopubs/issues/ambush/ambush.htm; Internet. 1.
[55] Robert F. Baumann, *Russian-Soviet Unconventional Wars in the Caucasus, Central Asia, and Afghanistan*, (Fort Leavenworth, KS: Combat Studies Institute, U.S. Army Command and General Staff College, 1993), 164-165.
[56] Lester W. Grau, *Road Warriors of the Hindu Kush: The Battle for the Lines of Communication in the Soviet-Afghan War*. Accessed 18 February 2003. Available from http://fmso.leavenworth.army.mil/fmsopubs/issues/roadwar/roadwar.htm; Internet. 12.
[57] Grau, *High-desert Ambush*, 29-31.

After Afghanistan, the Soviet army studied the United States Army experience in Vietnam, incorporated their own lessons learned from Afghanistan, and created the combat strike group (udarno-boevaya gruppa-UBG). These are three to four man teams organized in a battalion-sized unit. Each team is equipped with small arms, silencers, grenade launchers, mines, and radios. These teams will operate at night, establish ambush sites to deny the enemy use of LOCs, and simultaneously secure LOCs for friendly use.[58]

The Soviet innovations in rear service support began with a conceptual shift to an active or proactive defense coupled with a modular force structure combining troop missions, logistical support, and combat capability into a single unit or sub-unit. Initial efforts were to minimize the dependence on ground LOCs. Pipeline troops, for example, were created to construct fuel pipelines from the USSR to Afghanistan reducing the dependence on ground convoys. However, ground lines of communication remained vital, and Soviet commanders constructed fixed fortified security garrisons along these LOCs to protect key bridges and facilities. During the convoys, support troops were integrated into the combat formations augmented with engineer capability for mine clearing and road construction. These capabilities enabled them to defend themselves against attack without relying on a response force.[59] While these efforts did not eliminate the threat, they portray the adaptability of the Soviet military to combat the threat to their LOCs and support forces.

Case Study: Russian Armed Forces in Chechnya

In Chechnya, Russia faced a flexible Chechen force structure with a myriad of capabilities. Chechen volunteers joined Mujahideen guerrillas in forming their own independent battalions responsible to Allah and not a centralized government. Chechens formed suicide regiments – including women – to protect their leadership. Chechen formations dressed in Russian uniforms

[58] Ibid.,30.

(violating the Laws of War) and committed hostile acts against their own people as part of their information operation campaign. For example, some formations, dressed as Russian soldiers, mined the oil wells and created a "second Kuwait" to influence public opinion. Special purpose units were created from municipal police, National Guard, self-defense forces, and mercenaries; these units also lacked uniforms or an identifiable chain of command.[60]

These flexible force structures and their unique capabilities enabled the Chechens to implement a strategy of concentric rings to defend Grozny. The first outermost ring of civilians and Chechen fighters harassed the Russian advance with sniping and skirmishing while the second ring – approximately 20 to 30 kilometers outside of Grozny – employed conventional resistance including MLRS rocket attacks and offensive counterattacks. The third ring was the core of Grozny defined by intense house-to-house urban warfare. In executing this concentric rings urban strategy, Chechen rebels employed various tactics including mines, human roadblocks and shields, snipers, sabotage, and psychological and disinformation operations to target Soviet morale and influence public opinion.[61]

---

[59] Stephen J. Blank, *Operational and Strategic Lessons of the War in Afghanistan, 1979-1990* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1991), 49-51.
[60] Timothy L Thomas, *The Caucasus Conflict and Russian Security: The Russian Armed Forces Confront Chechnya* (Fort Leavenworth, KS: Foreign Military Studies Office, 1995), 28-48.
[61] Ibid., 28-48.

Chapter 4: Analysis and Conclusion

After presenting the rear area and base security doctrine in chapter two and the current and emerging threats in chapter three, this chapter will determine if this doctrine is sound on the noncontiguous nonlinear battlefield. Before this analysis can occur, this chapter will define doctrine and the characteristics that make it sound.

Joint Doctrine is defined as, "Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application."[62] FM 3-0, *Operations* adds that, "Army doctrine provides a common language and a common understanding of how Army forces conduct operations. It is rooted in time-tested principles but is forward-looking and adaptable to changing technologies, threats, and missions."[63] The U.S. Army Training and Doctrine Command (TRADOC) is responsible for Army doctrine and published TRADOC Regulation 25-36, *The TRADOC Doctrinal Literature Program* to guide its development.

In addition to outlining the procedures for developing doctrine, TRADOC Regulation 25-36, *The TRADOC Doctrinal Literature Program,* also provides the characteristics of sound doctrine. It states, "How the Army intends to conduct operations in the future and the capabilities required to execute those operations set the azimuth for doctrine development. The developer's objective is to produce sound doctrine that will enhance the Army's ability to accomplish missions across the range of military operations. It must be effective, acceptable, well researched, enduring, flexible, comprehensible, consistent, and concise."[64] These eight characteristics of sound doctrine serve as the evaluation criteria for this chapter.

---

[62] Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02, (Washington, D.C.: Department of Defense, 10 June 1998), 142.
[63] FM 3-0, 1-14.
[64] TRADOC Regulation 25-36, 7-8.

Characteristics of Sound Doctrine

Effective doctrine describes how we organize, train, fight, and support soldiers, thereby contributing directly to the successful execution of operations.[65] Effective doctrine for rear area and base security should clearly outline the organization and training of forces and soldiers to accomplish the mission.

Acceptable doctrine will be believed and practiced, thus supporting a unity of effort. Acceptability results from consensus building. Aligning doctrine with applicable DA/TRADOC policy aids in achieving consensus.[66] Doctrine is accepted when Army commanders and soldiers "practice what we preach."

Well-researched doctrine incorporates lessons learned from relevant history, exercises, and recent operations, reflecting a solid understanding of the art and science of military operations.[67] Well-researched doctrine includes reviewing full spectrum operations on every type of battlefield by any nation not just when the U.S. military is directly involved. In the past, the U.S. Army has re-written doctrine based on sound research. General William DePuy, the first commander of TRADOC, rewrote FM 100-5, *Operations* in 1976 based on the United States' indirect involvement in and subsequent study of the 1973 Arab-Israeli war.[68]

Enduring doctrine accounts for current and near-term anticipated realities and for force modernization and organizational evolution.[69] The Department of the Army Mission Training Plans and the TRADOC Operational and Organizational (O&O) concepts for the Interim and Objective Force anticipate a future threat and the organizations required to fight it. Enduring rear area and base security doctrine should enable rather than hinder this evolution.

---

[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Paul H. Herbert, *Deciding What Has to Be Done: General William E. DePuy and the 1976 Edition of FM 100-5, Operations* (Fort Leavenworth, KS: Combat Studies Institute, 1988), 25-36, 68-72.
[69] TRADOC Regulation 25-36, 7-8.

Flexible doctrine gives soldiers, leaders, and organizations the leeway to adapt to many different, or changing, circumstances.[70] Flexible rear area and base security doctrine will enable full spectrum operations across the operational framework.

Comprehensible doctrine conveys a common understanding of how to think about conducting operations and provides a common language for discussion. It uses clear, well-defined terms and concepts and is written at the level of the target audience.[71]

Consistent doctrine does not conflict with other Army doctrine, joint doctrine, or multinational agreements.[72] Consistent rear area and base security doctrine should maintain a common thread from JP 3-10, *Joint Doctrine for Rear Area Operations* and JP 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense,* to FM 3-0, *Operations* and FM 3-90, *Tactics*.

Concise doctrine provides a comprehensive body of thought while minimizing repetition from other doctrinal and administrative publications/documents.[73]

This monograph set out to determine if current U.S. Army rear area and base security doctrine is sound for sustaining operations on the noncontiguous nonlinear battlefield. This analysis will compare three themes of rear area and base security doctrine – definitions, concepts, and capabilities - against TRADOC's eight characteristics of sound doctrine to answer the research question. The table below graphically depicts the analysis of characteristics compared to rear area and base security doctrine. The narrative following the matrix will explain this analysis in detail.

[70] Ibid.
[71] .Ibid.
[72] Ibid.
[73] Ibid.

TRADOC 25-36 Characteristics of Sound Doctrine	Three Components of Army Rear Area and Base Security Doctrine		
	Definitions	Concepts	Capabilities
Effective?	**No**	Yes	Yes
Acceptable?	Yes	Yes	**No**
Well-researched?	Yes	Yes	**No**
Enduring?	Yes	**No**	Yes
Flexible?	Yes	Yes	**No**
Comprehensible?	**No**	Yes	Yes
Consistent?	**No**	**No**	Yes
Concise?	Yes	Yes	Yes

Figure 11. Comparison of Army Rear Area and Base Security Doctrine definitions, concepts, and capabilities with the TRADOC characteristics of sound doctrine

Effective:

The Joint and Army doctrine threat definitions for Level I, Level II, and Level III threats are not effective. These definitions are based on the required friendly response to counter the threat. This may have been adequate against a Cold War linear and echeloned maneuver threat (in fact the support battalion MTPs defined the *maneuver* threat with these exact same threat level definitions). Rear area commanders operating in a contiguous and linear rear area may still have the time and space to maneuver response or TCF forces to counter a conventional enemy penetration. But defining the threat level by these responses may not be effective against an enemy employing asymmetric and unconventional threats on a noncontiguous nonlinear battlefield. For example, a TCF response to a Level III threat of WMD employment or a computer network attack against the logistic information systems is ineffective (how does a TCF counter an unseen computer network attack?) These definitions lack flexibility across the growing depth and breadth of the "rear area" and are not entirely effective.

Acceptable:

The force design capabilities for Army commanders attempting to command and control rear area and base security operations in the joint rear area are not acceptable. JP 3-10 states the JFC

may designate a subordinate commander or a member of the JFC staff as the JRAC.[74] This designation may be an Army commander. Yet the Army rear area and base security doctrine in FM 3-90, *Tactics* is at the tactical level and does not address theater or operational level force protection. The Army requires an operational level rear area operations capability and doctrine in order to serve as the JRAC.

Well-researched:

The capabilities for rear area and base security doctrine are not well researched. As shown in the case study, Soviet operations on a noncontiguous and nonlinear battlefield in Afghanistan required changes to the Soviet Army's force design for convoy security. Additional research into historical case studies should guide sound doctrine to ensure the flexible capability to operate in complex combinations of the operational framework.

Enduring:

Rear area and base security doctrinal concepts are not enduring in supporting Army transformation. The Objective Force O & O introduces the concepts of pulsed sustainment and battlefield distribution. Conceptually, these ideas enable the intermittent multi-modal flow of goods and services and eliminate the requirement to maintain a secure LOC at all times. Instead, the maneuver commander secures the LOCs for a specific time in accordance with his operational and sustainment plan.[75] The Objective Force O & O envisions sustainment operations "comfortable" operating in an often-unsecured rear area. Conceptually, rear area and base security operations on the noncontiguous nonlinear battlefield must enable the pulsing intermittent supply for transformation.

[74] Joint Pub 3-10, II-3.
[75] Change 1 to TRADOC Pamphlet 525-3-90/O&O, 4-81 and 4-83.

Flexible:

The capabilities of response forces in Army rear area and base security doctrine are not flexible enough on the noncontiguous nonlinear battlefield. Doctrine relies on ad hoc perimeter and base defense forces, response forces, and TCF forces often performing an on order mission. While adequate on the linear and contiguous battlefield in a generally "safe" rear area, the noncontiguous nonlinear battlefield lacks this safety and presents a challenge to force design capabilities. Huba Wass de Czege wrote, "The shift from a readily definable military threat based on widely common capabilities and a relatively consistent pattern of operations to a growing range of threats reflecting varying objectives, capabilities and methods presents a force design dilemma all its own."[76] He went on to state, "Given its discontinuous character, future operational maneuver will require the deliberate protection of combat support and sustainment organizations that traditionally have relied for security on rearward positioning, collocation with combat units, or both….rearward positioning would offer no guarantee of safety, while the routine collocation of combat and support units, especially in the early days of a campaign, would unacceptably drain offensive momentum."[77] Instead, rear area and base security doctrine requires changes to the force structure to increase the capability of organic forces and enable flexible and effective responses at each level of command.

Comprehensible:

The doctrine outlining the command relationships, commander responsibilities, coordinating staff (JRAC, RTOC, BCOC, BDOC), and the required response force is confusing. The Joint doctrine is too broad covering from the JFC to the individual base. The Army doctrine is too tactical covering predominately base and base cluster operations. The delegated responsibilities

[76] de Czege and Sinnreich, "Conceptual Foundations," 3.
[77] Ibid., 27.

are not comprehensible when distributed between commanders or coordinators at the joint, service, subordinate unit, or area level.

Consistent:

Rear area definitions are not consistent. Huba Wass de Czege stated, "For all practical purposes, there no longer will be any distinction between communications and combat zones."[78] FM 3-0 makes great strides in removing this distinction by introducing the battlefield organization, not by location on the battlefield, but by purpose (decisive, shaping, and sustaining operations). It further defines the sustaining functions – CSS, rear area and base security, movements control, terrain management, and infrastructure development – by their purpose. Yet doctrine undermines this effort by retaining the spatial use of deep, close, and rear areas (perhaps for joint and coalition understanding). FM 3-90 compounds this inconsistency and requires commanders to designate a rear area for both contiguous and noncontiguous operations.

Additionally, rear area and base security concepts are inconsistent. In the September 2002 National Security Strategy (NSS), the President of the United States addressed preemptive actions to counter a sufficient threat to national security. The NSS stated, "the greater the threat, the greater is the risk of inaction – and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack."[79] Full dimensional protection, one of the operational concepts of Joint Vision 2020, is the ability of the joint force to protect its personnel and other assets required to decisively execute assigned tasks. It includes active and passive defensive measures, offensive countermeasures, security procedures, antiterrorism measures, enhanced intelligence collection and assessments, and

[78] Ibid., 29.
[79] The White House, *The National Security Strategy of the United States of America*, accessed 18 January 2003, available from http://www.whitehouse.gov/nsc/nss.html; Internet, 15.

proactive engagement strategies.[80] Likewise, the Army's concept for the Objective Force requires units to see first, understand first, act first, and finish decisively.[81] Perhaps rear area and base security concepts – to be consistent with strategic guidance, joint vision, and Army transformation - should become more preemptive rather than reactive in nature. The dependence on response forces or a TCF, by their nature, is a reactive response. A move to preemptive capabilities requires a change in doctrinal concepts and force design capabilities.

Concise:

Rear area and base security doctrine is relatively concise. Integrating this doctrine in an appendix of FM 3-90, *Tactics* instead of its own separate manual ensures that it is concise.

Conclusion:

There are components of Army rear area and base security doctrine that do not meet TRADOC's criteria for sound doctrine on the noncontiguous nonlinear battlefield. The doctrinal definitions for the threat levels are not entirely effective, the use of the term rear area is not consistent among doctrine, and the command relationship and required coordination with response forces are not very comprehensible. Additionally, the doctrinal concepts for maintaining rear area security are not enduring for Army transformation, and the lack of a preemptive concept in doctrine is inconsistent with the NSS, JV 2020, and the Objective Force. Finally, force design capabilities are not acceptable between joint and army doctrine, well researched based on recent Russian operations in Afghanistan, or flexible based on the unique requirements of the noncontiguous nonlinear battlefield. Minor changes will have a holistic effect on rear area and base security doctrine.

---

[80] Department of Defense, *Joint Vision 2020*, (Washington D.C.: US Government Printing Office, June 2000) 26.

[81] Department of the Army, *United States Army White Paper – Concepts for the Objective Force*, accessed 18 January 2003, available from http://www.objectiveforce.army.mil/pages/ObjectiveForceWhitePaper.pdf; Internet, iv.

Chapter 5: Recommendations

"Rear protection may very well be an emerging Achilles' heel for future U.S. military forces."[82]

The conclusions of the analysis drive recommended changes in three areas – doctrine definitions, concepts, and force design capabilities – to make Army rear area and base security doctrine more sound on the noncontiguous nonlinear battlefield. Each of these categories is discussed below.

Doctrine Definitions:

To set the stage for holistic improvements, Joint and Army doctrine should begin by redefining the Threat Levels to compare the combined area utility of the base, unit, or activity (critical, priority, general control, and no importance from FM 3-90) and the hazard severity of its loss with the probability of the threat occurring. These new definitions would use the Army Risk Assessment Matrix from FM 100-14, *Risk Management* as a model. The table below shows this matrix and the following paragraphs define the table's entries.

Threat Level Table:		Threat Probability (from FM 100-14)				
Area Utility (from FM 3-90)	Hazard Severity (from FM 100-14)	Frequent	Likely	Occasional	Seldom	Unlikely
Critical area	Catastrophic	IV	IV	IV	IV	III
Priority area	Critical	IV	IV	III	III	II
General area	Marginal	III	III	II	II	I
Negligible area	Negligible	II	II	I	I	I

Figure 12. Suggested Threat Level Table

[82] Huba Wass de Czege and Jacob D. Biever, "Force Protection: From Fort to Foxhole," *Army*, June 2001, 19.

The suggested new Threat Levels would increase from three levels to four levels and would be defined as the following.

- Level I Threats pose up to occasional threats to negligible areas and unlikely threats to general areas.
- Level II Threats pose up to frequent threats to negligible areas, occasional threats to general areas, and unlikely threats to priority areas.
- Level III Threats pose up to frequent threats to general areas, occasional threats to priority areas, and unlikely threats to critical areas.
- Level IV Threats pose at least a likely threat to priority areas and a seldom threat to critical areas.

The Hazard Severities from FM 100-14, Risk Management are defined as the following.[83]

- Catastrophic: The loss of ability to accomplish the mission or mission failure
- Critical: Significantly (severely) degraded mission capability or unit readiness
- Marginal: Degraded mission capability or unit readiness
- Negligible: Little or no adverse impact on mission capability

The Threat Probabilities are adapted from FM 100-14, Risk management and are defined as the following.[84]

- Frequent: Occurs very often, continuously experienced
- Likely: Occurs several times
- Occasional: Occurs sporadically
- Seldom: Remotely possible; could occur at some time
- Unlikely: Can assume will not occur, but not impossible

[83] Department of the Army, *Risk Management*, FM 100-14, (Washington, D.C.: Headquarters, Department of the Army, 23 April 1998), 2-10.
[84] Ibid.,2-8 to 2-9.

Redefining the Threat Level in this suggested manner is more effective. These definitions will enable commanders to prioritize the allocation of finite assets including modular, functional response teams based on the utility, hazard, and threat probability. This capability is also consistent with joint doctrine and accomplishes the joint security operations objective - assess and prioritize bases – from JP 3-10, *Joint Doctrine for Rear Area Operations*.

In addition to redefining the Threat Levels, Army doctrine should strike the use of "rear area" from the doctrine and replace it with "sustainment area" or "sustainment operations". Replacing rear area is more than semantics. Using sustainment area or operations in FM 3-90, *Tactics* will ensure the consistency that FM 3-0, *Operations* initiated by introducing the battlefield organization by purpose (decisive, shaping, and sustaining) instead of location. Likewise, FM 3-90 should lift the requirement for commanders to designate a rear area for both contiguous and noncontiguous operations.

These changes to doctrine definitions enable a more effective, consistent, and comprehensible doctrine. They also pave the way for changes in concepts and improvements to force design capability.

Doctrine Concepts:

Rear area and base security doctrine concepts are not enduring in view of the emerging asymmetric threat and Army transformation and are not consistent with the preemptive concepts in the NSS or JV 2020.

To meet the enduring criteria, doctrine must account for current and near-term anticipated realities for force modernization and organizational evolution. While current doctrine states the higher headquarters is responsible for the unassigned areas on the noncontiguous nonlinear battlefield, Army force structure does not provide the means to accomplish this without draining combat forces. Huba Wass de Czege recommends an "area security command for infrastructure protection, which may be (and in large-scale contingencies typically will be) augmented with

dedicated combined-arms formations."[85] In his monograph, Szabo recommended a similar capability called the Corps Security Force (CSF) centered on a light armored cavalry regiment with augmentation by Corps engineer, aviation, and military police.[86] While continuing the force design debate is useful (but most applicable to a contiguous and linear battlefield), perhaps Army doctrine should become conceptually comfortable with the increasingly unsecured rear and forgo attempts to create a large conventional force to protect this area. Instead, doctrine should empower units performing sustainment operations with the organic capability to protect themselves during the intermittent pulsed sustainment operations envisioned in transformation. Rather than a large conventional forces serving as a "super TCF" at the operational level, debate and research should continue to search out concepts to counter the asymmetric threats of computer network attack, air and missile defense, antiterrorism, or weapons of mass destruction.

Additionally, rear area and base security doctrine should be consistent with concepts in the NSS, JV 2020, and the Objective Force vision. These three documents all call for preemption. Changing the definitions of the threat level as mentioned above begins the transition from a reactive response. By defining the threat based on utility, severity, and probability, the rear area commander can prioritize assets to protect these bases and attempt to preempt their attack. Pre-emption of asymmetric threats requires operational and strategic intelligence. Capabilities to preempt these threats would also primarily occur at the strategic and operational level, but the Army lacks an operational level force protection manual.

Douglas Darling, a DA civilian in the Combined Arms Doctrine Development (CADD), wrote a strategic research project *Force Protection in Large Unit Operations* while attending the Army War College in 2002. He proposed creating an operational force protection manual along the structure of the FM 3-0 *Operations* force protection tasks - air, space, and missile defense;

[85] de Czege and Sinnreich, "Conceptual Foundations," 35.
[86] Szabo, "Does the Army have an Effective Doctrine for the Conduct of Rear Area Security and the Protection of Support Troops?" 42-44.

nuclear, biological, and chemical defense; antiterrorism; defensive information operations; and security to operational forces and means. In addition to the operational force protection doctrine, he recommends joint doctrine assign the ARFOR Commander with the responsibility for the JRA & the JRAC.[87] Adopting Mr. Darling's proposal provides a fixed staff with appropriate doctrine capable of preempting asymmetric threats in the sustainment area.

Doctrine Capabilities:

Current rear area and base security doctrine force design capabilities require an echeloned level of conventional response including base defense forces, response forces (usually MPs), or a Tactical Combat Force (TCF) for the base and base cluster level. Chapter four presented that these capabilities were not acceptable, flexible, or well researched for the noncontiguous nonlinear battlefield.

The organization of forces into bases and base clusters remains sound for mutual protection; however, as the battlefield continues its noncontiguous nonlinear expansion, reliance on these "ad hoc" conventional response forces is not acceptable or flexible. Instead, doctrine should allocate a more robust base and base cluster, route, and convoy security capability to each support battalion headquarters.

The draft Unit of Action (UA) organization charts for the FSB addresses this requirement. This draft doctrine provides an organic FSB security section of 16 military police with organic mobility and fires integration augmented with four armed robotic vehicles (ARV) for reconnaissance and intelligence fusion (see Figure 11).[88]

---

[87] Douglas A. Darling, "Force Protection in Large Unit Operations" (USAWC Strategy Research Project, U.S. Army War College, Carlisle Barracks, Pennsylvania, 13 March 2002), 52-53.
[88] Draft slides from the Future Combat System Unit of Action brief on 17 September 2002 by LTC Brian T. Boyle, Director, Concepts, Organization, Doctrine and Training Directorate, UAMBL.

Figure 13. Draft Objective Force FSB Security Section (from the Navigator Development Group briefing to SAMS on 17 September 2002 on the Future Combat System Unit of Action)

This security section is a good beginning for increasing CSS unit organic mobility and responsiveness in the future objective force. This organic capability would enable a command and control structure for route, convoy, and base security operations. Doctrine should allocate this structure to every support battalion – forward, main, corps and base support battalion – to enable each base commander the minimal shell for an organic response force at the tactical base level. This basic building block would provide a flexible, minimally acceptable level of organic capability.

Additionally, adopting a force design capability similar to this security force would support well-researched doctrine. As illustrated in the case study on the Russian armed forces in Afghanistan, the Soviet army faced many of these same challenges on their noncontiguous nonlinear battlefield. They evolved and developed the OOD, bronegruppa, and UBG to counter these threats. These concepts enabled the Soviets with a more self-sufficient force protection and an added preemptive capability. Well-researched doctrine for the U.S. Army should learn from the Soviets' experience in Afghanistan.

Conclusion

The battlefield and threat continue to change. While FM 3-0 ushers in new concepts for full spectrum operation and the operational framework, the U.S. Army should encourage professional

dialogue and conceptual debate to ensure the rear area and base security doctrine continues its evolution. These recommended changes to doctrine definitions, concepts, and force structure capability will ensure rear area and base security doctrine is sound for the noncontiguous nonlinear battlefield.

BIBLIOGRAPHY

de Czege, Huba Wass and Jacob D. Biever. "Force Protection: From Fort to Foxhole." *Army*, June 2001, 17-19.

de Czege, Huba Wass and Richard Hart Sinnreich. "Conceptual Foundations of a Transformed U.S. Army." *Land Warfare Paper*, no. 40. (March 2002).

Baumann, Robert F. *Compound War Case Study: The Soviets in Afghanistan*. Accessed 25 February 2002. Available from http://www.cgsc.army.mil/csi/research/comwarbaumann.htm; Internet.

_____. *Russian-Soviet Unconventional Wars in the Caucasus, Central Asia, and Afghanistan*. Fort Leavenworth, KS: Combat Studies Institute, U.S. Army Command and General Staff College, 1993.

Blank, Stephen J. and Earl H. Tilford, Jr. *Russia's Invasions of Chechnya: a Preliminary Assessment*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1995.

Blank, Stephen J. *Afghanistan and Beyond: Reflections on the Future of Warfare*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1993.

_____. *Operational and Strategic Lessons of the War in Afghanistan, 1979-1990*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 1991.

Bogart, Adrian T., III. "Weapons of Mass Destruction and the Joint Rear Area." *Army Logistician*, March-April 2002, 21-24.

Darling, Douglas A. "Force Protection in Large Unit Operations" USAWC Strategy Research Project, U.S. Army War College, Carlisle Barracks, Pennsylvania, 13 March 2002.

Davis, Rodney G. "Weapons of Mass Destruction Civil Support Teams." *Army Logistician*, July-August 2001, 2-4.

Grau, Lester W. *High-desert Ambush: Hard Lessons Learned the Hard Way*. Accessed 18 February 2003. Available from http://fmso.leavenworth.army.mil/fmsopubs/issues/ambush/ambush.htm; Internet.

_____. *Road Warriors of the Hindu Kush: The Battle for the Lines of Communication in the Soviet-Afghan War*. Accessed 18 February 2003. Available from http://fmso.leavenworth.army.mil/fmsopubs/issues/roadwar/roadwar.htm; Internet.

Grau, Lester W. and Mohammad Yahya Nawroz. "The Soviet Experience in Afghanistan." *Military Review* LXXV, no. 5 (September-October 1995): 17-27.

Grau, Lester W. and Timothy Smith. "A 'Crushing' Victory: Fuel-Air Explosives and Grozny 2000." *Marine Corps Gazette*, August 2000, 30-33.

Grau, Lester W. and Timothy L. Thomas. "Soft Log and Concrete Canyons: Russian Urban Combat Logistics in Grozny." *Marine Corps Gazette*, October 1999, 67-75.

Herbert, Paul H. *Deciding What Has to Be Done: General William E. DePuy and the 1976 Edition of FM 100-5, Operations.* Fort Leavenworth, KS: Combat Studies Institute, 1988.

Huston, James A. *The Sinews of War: Army Logistics 1775-1953*. Washington, D.C.: Office of the Chief of Military History, United States Army, 1966.

Lawrence, T. E. "The Evolution of a Revolt". Fort Leavenworth, KS: Combat Studies Institute, 1989. available at http://www.cgsc.army.mil/carl/resources/csi/Lawrence/lawrence.asp

Nikolaev, Yu. V., ed. *The Chechen Tragedy: Who is to Blame. Commack*, NY: Nova Science, 1996.

Norton, Timothy. "Force Protection in the Future." *Army Logistician*, July-August 2002, 12-14.

Otis, Glenn K. "Threat to the Rear: Real or Myth?" *Land Warfare Paper*, no. 2 (November 1989).

Schneider, James J. "T.E. Lawrence." *Strategy and Tactics*, June 1992: 16-19.

Shaw, Buck. *The Contemporary Operating Environment (COE*). Accessed 18 January 2003. Available from http://www.cascom.army.mil/multi/training/CSS_Training_Support_Packages/COE/COE%20Fact%20Sheet.doc; Internet.

Shrader, Charles R., ed. *United States Army Logistics, 1775-1992: an Anthology (volume 3).* Washington D.C.: Center of Military History United States Army, 1997.

Szabo, Ernest A. "Does the Army have an Effective Doctrine for the Conduct of Rear Area Security and the Protection of Support Troops?" Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 20 December 1996.

The White House. *The National Security Strategy of the United States of America.* Accessed 18 January 2003. Available from http://www.whitehouse.gov/nsc/nss.html; Internet.

Thomas, Timothy L. *The Caucasus Conflict and Russian Security: The Russian Armed Forces Confront Chechnya*. Fort Leavenworth, KS: Foreign Military Studies Office, 1995.

Thompson, Julian. *The Lifeblood of War: Logistics in Armed Conflict*. Oxford: Brassey's, 1991.

Turbiville, Graham H. "Ambush! The Road War in Afghanistan." *Army*, January 1988, 32-35.

U.S. Department of the Army. *Mission Training Plan Combat Service Support Company, Interim Brigade Combat Team.* ARTEP 63-390F-30-MTP. Fort Lee, Virginia: U.S. Army Combined Arms Support Command, September 2002.

_____. *Mission Training Plan Headquarters, Brigade Support Battalion, Interim Brigade Combat Team.* ARTEP 63-106-MTP. Fort Lee, Virginia: U.S. Army Combined Arms Support Command, August 2002.

_____. *Mission Training Plan for Battalion Headquarters, Forward Support Battalion, Heavy and Motorized Divisions.* ARTEP 63-005-MTP. Washington, D.C.: Headquarters, Department of the Army, 03 October 1988.

_____. *Mission Training Plan for Battalion Headquarters, Main Support Battalion, Heavy and Motorized Divisions.* ARTEP 63-125-MTP. Washington, D.C.: Headquarters, Department of the Army, 30 March 1989.

_____. *Operations.* FM 3-0. Washington, D.C.: Headquarters, Department of the Army, 14 June 2001.

_____. *Risk Management.* FM 100-14. Washington, D.C.: Headquarters, Department of the Army, 23 April 1998.

_____. *Tactics.* FM 3-90. Washington, D.C.: Headquarters, Department of the Army, 4 July 2001.

_____. *The TRADOC Doctrinal Literature Program (DLP).* TRADOC Regulation 25-36. Fort Monroe, Virginia: U.S. Army Training and Doctrine Command, 5 April 2000. Accessed 25 January 2003. Available from http://www.tradoc.army.mil/tpubs/regs/r25-36fram.htm; Internet.

_____. *The United States Army Objective Force Operational and Organizational Plan for Unit of Action.* Change 1to TRADOC Pamphlet 525-3-90/O&O. Fort Monroe, Virginia: U.S. Army Training and Doctrine Command, 22 July 2002.

_____. *United States Army White Paper – Concepts for the Objective Force.* Accessed 18 January 2003. Available from http://www.objectiveforce.army.mil/pages/ObjectiveForceWhitePaper.pdf; Internet.

U.S. Department of Defense. *Department of Defense Dictionary of Military and Associated Terms.* Joint Pub 1-02. Washington, D.C.: U.S. Department of Defense, 10 June 1998.

_____. *Joint Doctrine for Rear Area Operations.* Joint Pub 3-10. Washington, D.C.: U.S. Department of Defense, 29 May 1996.

_____. *Joint Tactics, Techniques, and Procedures for Base Defense.* Joint Pub 3-10-1. Washington, D.C.: U.S. Department of Defense, 23 July 1996.

_____. *Joint Vision 2020.* Washington D.C.: U.S. Government Printing Office, June 2000.

Van Creveld, Martin L. *Supplying War: Logistics from Wallenstein to Patton.* New York, NY: Cambridge University Press, 1997.

Wright, Burton, III. "Deep Attack – and I do Mean Deep." *Army Logistician*, July-August 2001, 25-26.