NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AIR BASE DEFENSE: DIFFERENT TIMES CALL FOR DIFFERENT METHODS

by

Jeffery T. Ditlevson

December 2006

Thesis Advisor: Maria Rasmussen
Second Reader: Michael Freeman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of the Naval Postgraduate School. They do not reflect the official position of the U.S. Government, Department of Defense, the United States Air Force or the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Air Base Defense: Different Times Call for Different Methods	5. FUNDING NUMBERS
6. AUTHOR(S) Jeffery T. Ditlevson	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

As the United States Air Force air base defense doctrine evolved over the years, implementation and execution errors were occasionally exploited by insurgent forces operating in the areas adjacent to U.S. occupied air bases. Executing unconventional attack methodologies, primarily via stand-off weapons, these insurgents were able to wreak havoc on U.S. and allied air bases, causing massive destruction and the loss of American lives.

An examination of the literature from air base (ground) attacks in Korea, Vietnam and at Khobar Towers indicated several problematic areas resonating in all three cases. These common areas include: inadequate intelligence (both organic and external), lack of proper focus on critical infrastructure and insufficient or absent force protection technologies.

Many of today's security experts are predicting future attacks on military infrastructure to include stateside and forward-deployed air bases. Today's slightly diverse, yet consistent insurgent enemy, with attack methodologies mirroring those of Korea, Vietnam and Khobar Towers, remains a constant and formidable threat.

As the Air Force moves forward with its newly implemented *Integrated Base Defense* doctrine, specific attention must be paid to improving upon the problem areas from the past. This thesis focuses on the specific problematic areas, and provides policy recommendations for force protection planners.

14. SUBJECT TERMS Air Base Defense (ABD), Integrated Base Defense (IBD), Critical Infrastructure Protection (CIP), Intelligence, Technology, Korea, Vietnam, Khobar Towers, Air Police, Security Police, Security Forces, Antiterrorism/Force Protection	15. NUMBER OF PAGES 131
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AIR BASE DEFENSE: DIFFERENT TIMES CALL FOR DIFFERENT METHODS

Jeffery T. Ditlevson
Major, United States Air Force
B.S., Minnesota State University, 1988

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2006**

Author: Jeffery T. Ditlevson

Approved by: Professor Maria Rasmussen
Thesis Advisor

Professor Michael Freeman
Second Reader

Professor Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the United States Air Force air base defense doctrine evolved over the years, implementation and execution errors were occasionally exploited by insurgent forces operating in the areas adjacent to U.S. occupied air bases. Executing unconventional attack methodologies, primarily via stand-off weapons, these insurgents were able to wreak havoc on U.S. and allied air bases, causing massive destruction and the loss of American lives.

An examination of the literature from air base (ground) attacks in Korea, Vietnam and at Khobar Towers indicated several problematic areas resonating in all three cases. These common areas include: inadequate intelligence (both organic and external), lack of proper focus on critical infrastructure and insufficient or absent force protection technologies.

Many of today's security experts are predicting future attacks on military infrastructure to include stateside and forward-deployed air bases. Today's slightly diverse, yet consistent insurgent enemy, with attack methodologies mirroring those of Korea, Vietnam and Khobar Towers, remains a constant and formidable threat.

As the Air Force moves forward with its newly implemented *Integrated Base Defense* doctrine, specific attention must be paid to improving upon the problem areas from the past. This thesis focuses on the specific problematic areas, and provides policy recommendations for force protection planners.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

ABD	Air Base Defense
AF CAMS	Air Force's Critical Assets Management System
AF CIP	Air Force Critical Infrastructure Program
AFOSI	Air Force Office of Special Investigations
AFR	Air Force Regulation
AP	Air Police
ARVN	Army of the Republic of Vietnam
AT/FP	Antiterrorism Force Protection
BDOC	Base Defense Operations Center
BOLO	Be on the Lookout
CAP	Civil Action Program
CCD	Command and Control Display
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIP	Critical Infrastructure Program
COCOM	Combatant Command
CONOPS	Concept of Operations
CONUS	Continental United States
CSP	Combat Security Police
CTC	Counterterrorist Center
DARPA	Defense Advanced Research Project Agency
DCA	Defense Critical Assets
DCIP	Defense Critical Infrastructure Program
DOD	Department of Defense
DIA	Defense Intelligence Agency
HD/LD	High-demand, low-density
HLD	Homeland Defense
HLS	Homeland Security
HMMWV	Highly Mobile Multi-Wheeled Vehicle
HSPD	Homeland Security Presidential Directive

IBDSS	Integrated Base Defense Security System
ICE	Immigration and Customs Enforcement
IO	Intelligence Oversight
FEMA	Federal Emergency Management Agency
FPASS	Force Protection Airborne Surveillance System
JCS	Joint Chiefs of Staff
JIACG	Joint Interagency Coordination Groups
JITF-CT	Joint Intelligence Task Force–Combating Terrorism
JPEN	Joint Protection Enterprise Network
JTTF	Joint Terrorism Task Forces
IBD	Integrated Base Defense
MAAG	United States Military Assistance Advisory Group
MAJCOM	Major Command
MARE	Major Accident Response Exercise
MET	Mission Essential Task
MSV	Mobile Search Vehicle
NCTC	National Counterterrorism Center
NIPRNET	Non-Secure Internet Protocol Router Network
NORTHCOM	Northern Command
NSC	National Security Council
NVA	North Vietnamese Army
OCSW	Objective Crew Served Weapon
OICW	Objective Individual Combat Weapon
OPM-SANG	Office of Program Manager, Saudi Arabian National Guard
OSI	See AFOSI
PACAF	Pacific Air Force
PDD	Presidential Decision Directive
PDSS	Perimeter Detection and Surveillance Subsystem
SADS	Surveillance and Detection System
SAR	Suspicious Activity Report
SF	Security Forces
SFCC	Security Forces Control Center

SICA	Supporting Infrastructure Critical Assets
SIPRNET	Secure Internet Protocol Router Network
SP	Security Police
TALON	Threat and Local Observation Notice
TASS	Tactical Automated Security System
TCA	Task Critical Assets
TIA	Total Information Awareness
TSC	Terrorist Screening Center
TSWG	Technical Support Working Group
TWG	Threat Working Group
UAV	Unmanned Aerial Vehicle
UN	United Nations
USAAC	United States Army Air Corps
USAAF	United States Army Air Force
USAAS	United States Army Air Service
USAF	United States Air Force
USMACV	United States Military Assistance Command,Vietnam
VAMP	Vulnerability Assessment Management Program
VBIED	Vehicle Borne Improvised Explosive Device
VC	Viet Cong
VNAF	Vietnamese Air Force
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to both Professor Maria Rasmussen and Professor Michael Freeman for their unending support and superlative guidance in helping me complete this thesis. Without their help, I certainly could not have finalized my work.

I would also like to thank the U.S. Air Force for allowing me time away from my primary duties to fulfill the requirements for a Master's Degree in Homeland Security and Defense. I can only hope to repay this generous reward through my future contributions to the Force Protection and HLS/HLD missions. Yet, my being away from the operational Air Force for 15 months only meant someone else had to pick up the slack, and, therefore, I am grateful to those troopers who helped carry the SF load during my stay here.

Without the genius of Lt Col (retired) Roger Fox, completion of this thesis would have been nearly impossible. His meticulous and thought-provoking work in *Air Base Defense* enabled me to develop the foundation for both my proposed hypothesis and cultivated work.

Finally, and most importantly, I would like to thank my wife, Tiffanie, and daughter, Micayla, for their understanding and support throughout my 15-month program here. Living on opposite coasts for the duration of my studies has truly been difficult—emotionally, physically and mentally. They continued their "normal" existence there, so I could accomplish what I had to do here. My wife filled the roles of Mom and Dad, homeowner, taxi service for my daughter's activities and dog care provider, all while working full-time. I often wonder how she held it all together…she truly is my hero. Thank you for supporting me…I'm coming home.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM

During the Korean and Vietnam conflicts, U.S. Air Force (USAF) security forces were woefully unprepared for the guerrilla-style attacks upon their air bases.[1] Insurgent forces successfully deployed stand-off weapons (mortars and shoulder-fired rockets) and small explosives in an attempt to drive U.S. forces from their territories. Many of these attacks were successful, resulting in the loss of human lives and military war fighting assets. The Cold War changed the face of our enemy, and Air Force security members stood post on air bases around the world waiting for saboteurs, infiltrators and small, tactical units to penetrate their defenses in an effort to destroy and/or obtain our nuclear weapons. Since the fall of the Berlin Wall, we have witnessed fewer state-sponsored acts of aggression and sabotage and more transnational, insurgent types of attacks. With the future threat of attacks on air bases once again resembling more of an asymmetric form, the Air Force is attempting to counter this reemerging threat by adopting a variation on an old theme; morphing its air base ground defense into an Integrated Base Defense doctrine.[2]

This study will examine the development and implementation of earlier air base defense doctrine during the Korean and Vietnam conflicts as well as the more recent attack on Khobar Towers. This study will focus on insurgent/guerrilla attacks upon air bases in these specific areas and defended primarily by Air Force security personnel. It will also examine how and why these insurgent and unconventional attacks were successful against air bases/Air Force assets during these periods and whether air base

[1] For the purpose of this study, 'Security Forces' referred to in this document, describe U.S. Air Force security personnel only. In 1947, upon becoming a separate branch of the armed forces, the Air Force maintained the name *Military Police* (carried over from the Army Air Corps.) A year later, in an effort to establish individual identity, the name was changed to *Air Police*. In 1966, the name was changed yet again to *Security Police*. Finally, in 1997, in an effort to represent all aspects of the inherent mission parameters, the name was changed to *Security Forces* (defenders of the force.) All terms are chronologically applied throughout this work.

[2] Air Force Instruction 31-101, *Air Base Defense* (15 May 2002), focused primarily on compliance-based defense standards for Level I (agents, saboteurs) and Level II (small tactical units, guerrillas); while Air Force Tactics, Techniques and Procedures 3-10.1, *Integrated Base Defense* (20 August 2004), calls for capabilities and effects-based defense against primarily Level I and II threats.

defense doctrine has developed in an effort to match current enemy methodologies.[3] The threats facing USAF bases in future contingencies will more than likely resemble those encountered in Korea and Vietnam.[4] By examining earlier instances of often ineffective air base defense doctrine against the asymmetric insurgent threat, this researcher hopes to develop recommendations to prevent similar implementation errors against comparable enemies and threats faced both today and in the future.

Because implementation and understanding of this new Integrated Base Defense doctrine (adopted in 2005) is essential, this research will also examine other newly implemented and parallel force protection programs that impact Security Forces such as critical infrastructure protection and information/intelligence sharing. Incorporation of the Integrated Base Defense doctrine also often calls for enhanced physical security technologies to facilitate reduced manning in some critical areas. Therefore, this research will also explore several recent technology-driven force protection programs and other advances in technology in relation to air base defense.

B. SIGNIFICANCE OF RESEARCH

With the continuous and unpredictable terrorist and insurgent threat to military installations worldwide, coupled with an increased proliferation of high-tech weapons and WMD, it is imperative that the tactics, techniques and procedures employed by Air Force Security Forces members be maximized to meet this postulated threat.[5] Additionally, with highly unpredictable opponents threatening U.S. aerospace resources and assets, force protection programs today require an integrated and cross-functional effort on the part of all uniformed members. Finally, highly-effective understanding and implementation of several such newly adopted force protection programs must be achieved to prevent a repeat of mistakes made in the past.

---

[3] Empirical data will focus on attacks on air bases in Korea, Vietnam and Khobar Towers as there have been no attacks on CONUS/OCONUS air bases since the implementation of Integrated Base Defense doctrine. Empirical data, in relation to base attacks will relate only to those bases utilizing air base defense doctrine.

[4] Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases* (Santa Monica, CA: RAND, 1995), 110.

[5] Threats utilizing stand-off weapons and small bombing attacks stand to be increasingly more successful based on enhanced technologies and weaponry.

C. LITERATURE REVIEW

When the U.S. Air Force became a separate branch of the Armed Services in 1947, it was quickly thrust into a combat environment. Being called upon to defend its own installations and assets during the Korean conflict, with little or no air base ground defense capabilities, former Air Force leader Wayne Purser claims they were woefully unprepared to execute the air base defense mission.[6] Policy makers quickly developed ground base defense policy, but fell far short in the creation of Air Force Regulation 355-4, which stated: "Active local ground defense of Air Force installations by Air Force personnel…is an emergency function, normally short in duration, and the capability which the Air Force must achieve is an emergency capability."[7] Roger Fox highlighted the weak Air Force ground defense by stating: "effective security against sabotage and a workable ground defense system was {sic} never fully developed on most Air Force installations in Korea" because plans "were not correlated with the threat…or were beyond the units' capability to execute effectively." He goes on to say, "the Air Force security mission was to protect resources from theft and pilferage, not to defend bases from ground attack."[8] Benjamin Hettinga points out that despite the potential for damaging attacks against U.S. airfields, North Korean guerrillas, operating clandestinely in the area, almost completely ignored these lucrative and often unprepared targets.[9] However, when North Korean guerrillas finally tested coalition air base defense measures and clandestine attacks did occur, Air Police units were focused on defending the wrong infrastructure and preoccupied with interior security duties. Hettinga further states that after the war, intelligence failures (consistent and numerous inconsistencies between the perceived and actual threats), eroded the credibility of air base defense, resulting in

---

[6] LTC Wayne Purser, "Air Base Ground Defense: A Historic Perspective and Vision for the 1990's" (Research Report, Maxwell Air Force Base, AL: Air War College, 1989), 10-11.

[7] United States Air Force, *Air Force Regulation 355-4, Defense—Local Ground Defense of Air Force Installations* (Washington, D.C.: HQ AF, 3 March 1953), 1. The first official Air Force document on base defense.

[8] Roger Fox, *Air Base Defense in the Republic of Vietnam: 1961-1973* (Washington, D.C.: Office of USAF History, 1979), 16.

[9] Benjamin E. Hettinga, "The Defense of Tan Son Nhut Air Base, 31 January 1968: A Study in the Nature of Air base Security" (Masters Thesis, Ohio State University, 2001), 12. Guerrillas attacked airfields on two occasions, once at Pohang Airfield, which was successfully evacuated, and at an airstrip near Kunsan where guerrilla harassment prevented the opening of a USAF airstrip. Guerrillas also fired small arms at aircraft during take-offs and landings, but no aircraft were damaged or lost. Hettinga states approximately 30,000-35,000 North Korean guerrillas were operating in the UN territory.

drastic manning reductions and a continued lack of focus on the implementation and execution of air base defense doctrine.[10] Overall, the air base defense policy during the Korean conflict lacked requisite training and initiative, focused point defenses on the wrong infrastructure/portions of the air base and lacked adequate functional intelligence about the strength of the enemy.

Operating in an "industrial security model," defending fixed positions primarily within the interior portions of the air bases, USAF Air Police in Vietnam found themselves unprepared yet again for what would eventually become an onslaught of enemy guerrilla attacks. Vick's empirical data (from a RAND study) on air base attacks revealed 493 enemy attacks on air bases in Vietnam.[11] Fox's analysis of these attacks indicates air base defense policy and doctrine during the Vietnam campaign was inadequately developed, training was insufficient, parochialism existed amongst the services, host nation forces were unreliable and U.S. forces lacked quality intelligence and underestimated the capabilities of the enemy.[12] Fox further points out that using host-nation Vietnamese forces to protect air bases during the first few years of the war led to an "unplanned, uncoordinated and uncontrolled" security relationship between host nation and USAF security personnel.[13]

U.S. Army and Marine forces, more familiar with infantry tactics and base ground defense, were eventually sent to Vietnam to provide additional security near the inner perimeter of the air bases. General William Westmoreland, adamant about using his ground forces for offensive maneuvers only, immediately shifted many of these Army and Marine forces to the front lines. Once again, this left USAF personnel (and their yet unproven air base defense doctrine) responsible for defending air bases in their entirety. David Shlapak points out that while USAF security personnel focused on the interior portions of the base, small groups of Viet Cong and North Vietnamese Army (VC/NVA) guerrillas successfully conducted 96% of their mortar and sapper attacks from just

---

[10] Hettinga, 13.

[11] Vick, 127-153. 75% of these attacks were from stand-off weapons with 60% of the attacks seeking to knock out U.S. aircraft.

[12] Fox, 16-17, 27-28.

[13] Ibid., 12.

outside the perimeter fence.[14] Michael Bean's analysis of air base defense doctrine in Vietnam is similar to those of Fox and Vick in that ineffectual policy implementation resulted in exterior portions of the air base and other forward areas remaining completely unfamiliar to security personnel and ultimately undefended.[15] The Air/Security Police's inability to adapt to the enemy's guerrilla tactics led to frequent and successful enemy attacks resulting in the damage and/or destruction of nearly 900 aircraft in Vietnam alone.[16]

During the latter part of the Cold War, there were fewer failed states and terrorist and/or guerrilla attacks on air bases seemed to diminish.[17] The most recent attack against Air Force assets and personnel where Air Force Security Police provided primary base defense took place in 1996 at Khobar Towers, near Dhahran, Saudi Arabia when a septic tanker truck laden with explosives detonated near a military barracks killing 19 Air Force servicemen and women. This asymmetric attack created a shift in the mindset of military planners on not only how to protect deployed forces abroad, but also a change in force protection philosophy. Yet, lessons from Korea and Vietnam regarding stand-off attacks or even those coming from just outside the exterior of the perimeter seemed to have been forgotten as security assets and force protection recommendations at Khobar concentrated heavily on a penetration type of attack.[18] Several after-action reports indicate that General Schwalier, the Khobar wing commander, was passed over for promotion based on his "incomplete preparation to defend against a perimeter attack."[19] Additional findings from the Record Report and Downing Assessment Task Force highlighted

---

[14] David Shlapak and Alan Vick, *Check Six Begins on the Ground, Responding to the Evolving Ground Threat to U.S. Air Force Bases* (Santa Monica, CA: RAND, 1995), 34.

[15] Michael Bean, "United States Air Force Security Forces in an Era of Terrorist Threats" (Masters Thesis, School of Airpower Studies, Maxwell AFB, AL, 1999), 30.

[16] Vick, *Snakes in the Eagle's Nest*, 94.

[17] Fox, 154-157. According to Fox, there were only 19 attacks on air bases located around the world from 1979 to 1992.

[18] Penetration attacks are typically conducted at base entry points via explosive-laden vehicles or personnel. They also include small numbers of personnel breaching the base perimeter defenses (fences, barriers) in an attempt to gain access to the inner portions of the base where war-fighting assets are typically located.

[19] William S. Cohen, "Personal Accountability for Force Protection at Khobar Towers" (Letter presented to the President of the United States, Washington D.C., 31 July 1997), 9. Available at: http://www.au.af.mil/au/awc/awcgate/khobar/cohen.htm, (accessed 12 September, 2006).

physical security deficiencies, manning and training shortfalls, a lack of organic intelligence assets (despite numerous signs of an impending attack), problems with host-nation forces executing security measures outside the fence line, and improper execution of critical infrastructure protection.[20]

Nearly 10 years post-Khobar, and on the heels of the 9/11 tragedy, the Air Force has moved to a new air base defense doctrine, Integrated Base Defense or IBD. Earlier air base defense doctrine called for compliance-based standards designed to prevent single saboteurs or small groups of infiltrators from reaching fixed positions on the interior portions of the air base. With today's wide threat spectrum, including irregular and disruptive sources such as terrorism and insurgency, new base doctrine must be capabilities and effects based.[21] This calls for IBD forces to "see first, understand first, and act first."[22] With the proven successes of guerrilla/insurgent attacks from stand off locations just outside the air base (Korea and Vietnam) or directly adjacent to the base perimeter (Khobar), this new doctrine calls for defending air bases well past their physical perimeter, extending as far out as humanly or technologically possible. Current Air Force Chief of Staff, General Michael Moseley recently challenged Security Forces leadership to "go outside the wire, get their arms around threats to our airfields and facilities, and come up with a way ahead."[23] USAF air base defense doctrine was nonexistent just several years prior to the Korean Conflict. It remained relatively unchanged and mostly deficient during Vietnam and was again found wanting at Khobar. Therefore, it is imperative this new doctrine be implemented properly and executed efficiently.

Ironically, as the Air Force once again works through the growing pains of a new base defense doctrine, many terrorism experts and researchers claim terrorists will again

---

[20] Findings from General Wayne A. Downing, *Force Protection Assessment of USCENTCOM AOR and Khobar Towers, Report of the Downing Assessment Task Force* (Washington, D.C.: Department of Defense, 30 August 1996) and Lt Gen James F. Record, October, 31, 1996. "Independent Review of the Khobar Towers Bombing, Part A and B" (Maxwell Air Force Base, AL, Air University website. http://www.au.af.mil/au/awc/awcgate/khobar/recordf.htm (accessed on 10 May 2006).

[21] Headquarters, Air Mobility Command. *Integrated Base Defense Concept of Operations* (Scott AFB, IL: HQ AMC, 17 February, 2006), 2.

[22] Headquarters, United States Air Force, *Air Force Tactics, Techniques and Procedures 3-10.1, Integrated Base Defense* (Washington, D.C.: HQ Air Force, 20 August 2004), 10.

[23] *Security Forces Transformation Newsletter*, SF Pentagon Edition, 1:1, 21 March 06, 2.

seek out and target military installations in the future. Additionally, they feel that the composition of these terrorist groups will mirror those of the insurgent-style enemies faced in Korea, Vietnam and at Khobar. With terrorists unlikely to attempt conventional engagements against our superior military forces, Vick stipulates the threat facing USAF air bases in the future will most likely resemble those carried out by the VC/NVA in Vietnam, and that advances in weapons technology will make defending against stand off weapons even more challenging.[24] Clifton Dickey, in making comparisons to the guerrilla attacks during the Tet Offensive, makes the same argument, arguing future adversaries of the U.S. will likely employ some type of asymmetric strategy to diminish the effectiveness of our military superiority.[25] Shlapak agrees with this concept and adds that USAF counters for the standoff threat are somewhat limited, and without a serious effort to detect standoff attacks, high-value aircraft and other base operations could be jeopardized. Shlapak adds that he does not foresee a large armored (conventional) offensive overrunning an air base as the primary future threat. Rather, he foresees small units of well-equipped, well-trained forces attempting to disrupt USAF operations and destroy assets.[26] Several recent RAND studies predict Al Qaeda will retain a strong interest in striking 'hard' (or well protected) targets such as embassies and military installations. They also predict terrorists may strike at military installations and other critical infrastructure in rural areas due to their high target value.[27] As the war rages on in Iraq, Matthew Levitt argues that the U.S. cannot afford to be distracted by the situation there, as terrorists may seize that opportunity to strike at hardened stateside military installations which could have a devastating effect on the Iraq reconstruction effort.[28]

---

[24] Vick, *Snakes in the Eagle's Nest*, 110.

[25] Major Clifton Dickey, "Base Defense for the Air Expeditionary Force: More than Defending the Redline" (Masters Thesis, School of Advanced Airpower Studies, Maxwell Air Force Base, AL, 1998), 1.

[26] Shlapak and Vick, *Check Six Begins on the Ground*, xvi, 15.

[27] Bruce Hoffman, et al, *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act* (Santa Monica, CA: RAND: 2005), 16. Lois Davis et al, *When Terrorism Hits Home* (Santa Monica, CA: RAND, November 17, 2004), 108.

[28] Bruce Hoffman, Matthew Levitt and Daniel Benjamin, "The War on Terror in the Shadow of the Iraq Crisis", *PolicyWatch* 690 (December 12, 2002), 2. Also available online at www.iraqwatch.org/perspectives/winep-pw690-121202.htm (accessed on 24 April 2006).

D. METHODOLOGY

By incorporating a historical interpretation of air base defense doctrine over the years, observations can be made regarding comparisons of earlier methodologies to those being used today or being considered for the future. Despite the evolution and creation of new air base defense doctrine, empirical data from earlier attacks, compared against USAF security measures, policy and doctrine in effect at the time, may help determine why these attacks were successful and assist decision makers in formulating recommendations to prevent them in the future.

Indoctrinating the new air base defense policy must prove to be more effective and less problematic than its predecessor. Detailed analysis of air base defense doctrine during the Korea, Vietnam and Khobar attacks indicates repeated failures resonating in several critical areas:

1.) The failure of adequate **information/intelligence sharing** programs and initiatives (both internally and externally.)

2.) Insufficient security resources allocated to defending **critical infrastructure** (as well as improper placement/siting of said resources.)

3.) A lack of **technological capabilities** aimed at detecting and defeating enemy threats away from the air base.

Therefore, subsequent thesis chapters will examine specific and independent, parallel force protection programs pertaining to these core areas, such as the Joint Protection Enterprise Network, Critical Infrastructure Program, and various technology upgrades to determine their potential impact on the Integrated Base Defense program, as well as recommendations for Security Forces' participation in these programs. With similar mistakes made repeatedly against the 'old' insurgent threat, it is absolutely critical we avoid making those same mistakes against the 'new' threat. After all, "those who cannot learn from history are doomed to repeat it."[29]

[29] George Santayana. Wisdomquotes website. http://www.wisdomquotes.com/002322.html (accessed on 24 April 2006).

E. OUTLINE

1. Chapter II – Air Base Defense—The Early Years

Chapter II examines the genesis of air base defense doctrine and how it slowly evolved after the United States Air Force became an independent service and was quickly thrust into the Korean conflict. Air base defense implementation and execution errors highlighted in Korea lingered into the Vietnam era, and once again Air Force security personnel entered an intense conflict on foreign soil with an inadequate and poorly developed doctrine. The attack on Khobar Towers finally gave policy makers and military planners the feeling that their air base defense doctrine was lacking fundamental aspects of force protection, ultimately leading to the development of Integrated Base Defense (IBD).

2. Chapter III – Where are We Going?

Chapter III explores some of the differences and similarities between the new IBD doctrine and its predecessor, Air Base Defense (ABD). This chapter also examines potential and anticipated enemy attacks/methodologies on air bases and military infrastructure and how they compare/contrast to those of earlier air base attacks.

Chapters IV, V and VI provide accounts of various tactical, procedural and doctrinal errors made in the areas of intelligence sharing, critical infrastructure protection and technology implementation during the time periods studied. These chapters also introduce several emerging new force protection programs and concepts recently developed at the Department of Defense (DOD) and Air Force levels this author feels are essential in executing a highly effective IBD doctrine, particularly as they relate to each core problem area. Finally, each program/concept is discussed in detail in relation to its potential importance in the IBD integration and overall success of the program.

3. Chapter IV – Information and Intelligence Sharing

Chapter IV examines earlier doctrinal and procedural errors made in relation to intelligence gathering and analysis while performing the air base defense mission in Korea, Vietnam and at Khobar. This chapter also focuses on several key sources of military intelligence used by Security Forces in base defense planning and how this information moves from producer to consumer. Chapter IV also describes the

importance of the Joint Protection Enterprise Network (JPEN) and Security Forces' role in utilizing not only this database-style system, but other information sharing programs as well.

4. Chapter V – Critical Infrastructure Protection Programs (CIP)

Chapter V describes numerous tactical and procedural errors involving the protection of critical infrastructure located on air bases in Korea and Vietnam as well as several examples from Khobar Towers. This chapter also briefly describes the Department of Defense and Air Force Critical Infrastructure Programs (CIP) and Security Forces' role in executing this important mission.

5. Chapter VI – Technology: A Security Enhancer?

Chapter VI describes how various technologies were found lacking in Vietnam and at Khobar Towers. It also describes various current and future technologies and tactics that may potentially be used by Security Forces in defending air bases, however, may also be used by the enemy to attack them. Finally, this chapter discusses several planned and current Air Force programs designed to enhance force protection at its airbases, and the Security Forces role in this mission.

6. Chapter VII – Conclusion

The concluding chapter briefly describes the ongoing Security Forces transformation as it relates to the Integrated Base Defense mission.

As the Integrated Base Defense doctrine continues to emerge and develop, the roles and functions of the Security Forces members called upon to perform it will also undoubtedly change. They are now being asked to perform missions and tasks once thought to be strictly reserved for Army and Marine infantry units. The days of securing and patrolling only the rear area and/or interior portions of the air base are now long gone. Replacing it are the technologies and tactics employed by Security Forces members reaching out beyond the air base perimeter in hopes of detecting adversaries much, much earlier. In order to better understand where it is this new doctrine is ultimately heading, one must first understand where it came from.

II. AIR BASE DEFENSE: THE EARLY YEARS

Even in friendly territory, a fortified camp should be set up, a general should never have to say; 'I did not expect it'

The Emperor Maurice **30**

A. INTRODUCTION

Most terrorist groups/insurgents conduct extensive information collection activity in order to identify U.S. military weaknesses and vulnerabilities. Part of this collection activity includes surveillance, such as monitoring/videotaping military installations, associated critical infrastructure and locations frequented by members of the armed services. There are always two places terrorists are guaranteed to find you; at home and at work. Unfortunately, when we talk about events such as the Beirut bombings of the Marine barracks in 1983, Air Force installation bombings in Germany in 1981 and 1985, and the Khobar Towers incident in 1996, all of them targeted areas where U.S. servicemen and women both lived and worked. Terrorists normally represent an asymmetric-style vulnerability to U.S. armed forces. That is, they present a threat outside the range of what is commonly known as conventional warfare, and as a result are difficult to prepare for and counter. They typically have no regular army, economy, territory or population to protect. This presents a unique challenge to installation/air base commanders and those charged with security planning in the armed forces.

RAND research indicates few, if any; opponents can challenge the Air Force's airpower superiority.[31] If their study on asymmetric warfare is correct, RAND speculates future adversaries may look to alternative methods of demonstrating their hostile intent or countering our airpower supremacy.[32] As history dictates, attacks on Air Force installations and air bases could be one such alternative. By taking advantage of

30 Website for Technical Surveillance Countermeasures (TSCM), 1. http://www.tscm.com (accessed on 20 March 2006).

31 Project AIR FORCE, a division of the RAND Corporation, is the USAF federally funded research and development center for studies and analysis, providing the USAF with analysis of policy alternatives affecting development, employment, combat readiness and support of current and future aerospace forces.

32 Vick, xiii.

readily available forces and/or existing technologies, they may strive to reduce the effectiveness of U.S. air operations, temporarily or otherwise, by destroying high-value assets and/or critical infrastructure.

Aware of the importance of air forces not only in the air but on the ground, Giulio Douhet suggested that the best defense against enemy airpower was through indirect attacks on the enemy's airfields. Douhet claimed, "It is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air."*33*

Douhet's focus on air power dominance no doubt referred to air attacks of enemy airfields; however, studies have shown ground attacks are an equally effective alternative; the consequences of which have been, at times, devastating. According to a RAND study, air base ground attacks occurred at least 645 times in 10 separate conflicts, destroying or damaging over 2,000 aircraft in worldwide locations between 1940 and 1992.[34] It should be noted that RAND's numbers do not account for the numerous attacks Afghan rebels conducted on Soviet base camps or the more recent Iraqi and Afghan rebel attacks on American forces and bases in that region. Regardless of the precise numbers, one can conclude that attacks on air bases have been and continue to be successful in the eyes of the attacking force.

As the first Gulf War demonstrated, air power can have a devastating impact on the will and gumption of a smaller, weaker enemy. At times, enemy forces are placed in a position of disadvantage through the use of successive bombing raids or overwhelming ground forces. Often, these adversaries, understanding their limitations and unlikely victory, employ an asymmetric style of fighting mentioned previously. This often includes, but is not limited to, distracting ground defense forces through the use of ballistic missiles or mortar attacks. Alternatively, they may also attempt to interrupt base operations through the use of small insurgent teams of ground forces.[35] While numerous armies and governments have studied enemy ground attacks throughout the years and

---

[33] Giulio Douhet, *The Command of the Air* (Washington, D.C.: U.S. Air Force Office of History, 1983), 53-54.

[34] Shlapak and Vick, 21

[35] Ibid., 12

examined methods for countering the threats posed by them, the attacks continue and remain a constant danger to the efficacy of battle planning and/or conflict resolution. Throughout modern history and the development of what is now known as the United States Air Force, Security Forces remain the primary executor of Air Force base defense policy. This chapter will examine a historical perspective of air base defense from World War I through the attack on Khobar Towers, as USAF ground forces transformed from an air base ground defense construct during the ground wars of the 20th century to what would eventually become the Integrated Base Defense concept developed specifically for the "Global War on Terror."

B. WORLD WARS I AND II

During World War I, both allied and enemy air units operated from air bases ensconced behind massive trenches protecting them from both conventional and unconventional (guerilla-type) attacks. Because of the absence of probing-style enemy attacks, allied forces continued to harness all of their base defense energies towards the interior portions of their bases and defending aircraft on the ground was typically not a concern. While the intrinsic value of aircraft in combat was realized during this war, the nearly non-existent external enemy threat led U.S. Army Air Service (USAAS) leaders into a sense of complacency regarding the overall importance of air base security. This improper realization culminated in ownership of a poorly trained and unprepared ground force heading into World War II.

World War II witnessed the introduction of technologically advanced and more lethal aircraft. It was apparent to military strategists that air power would be a vital cog in deciding the outcome of the war. Nazi Germany realized this potential as well, and introduced their infamous blitzkrieg or "lightning war" style of mobile warfare designed to smash their European enemies. Allied forces in forward areas often succumbed to German bombers which skillfully avoided anti-aircraft weaponry allowing them to repeatedly dive-bomb sheltered base defenders. Meanwhile, German paratroopers dropping onto Allied air bases from above placed unsuspecting Allied troops at a surprising disadvantage. Since typical air bases in those days consisted of little more than a small patch of grass, they were often difficult to defend, leading to Germany

capturing a number of Allied air bases.[36] Control of the air became critical, yet defending the tools of this trade, aircraft, was not progressing at a satisfactory pace. In 1941, the Germans attacked and captured a British airfield in Maleme and subsequently took possession of an airfield in Crete. During the Crete invasion, a large and untrained British force was overrun by a much smaller German force.[37] These events culminated in the United States and Great Britain giving serious thought to the importance of air base defense and trained specially-dedicated airfield guardians. Prime Minister Winston Churchill reviewed British air base defense policy and found it wanting. He declared all Royal Air Force members were to be armed and trained…"ready to fight and die in defense of their airfields;…every airfield should be a stronghold of fighting air-ground men, and not the abode of uniformed civilians in the prime of life protected by detachments of soldiers."*38*

The United States recognized the need for a similar defense posture for their airfields. In June 1942, the United States Army Air Corps (USAAC) Chief of Staff formed the first air base defense battalions, created primarily to defend against enemy ground attacks.[39] Realizing the importance of outfitting these troops properly, the Army trained them in small unit tactics and issued the battalions M-2 half-tracks, heavy machine guns, 60mm mortars, tank platoons M1 rocket launchers and self-propelled 75mm guns.[40] The development of these battalions signaled a paradigm shift in the area of base defense. Their primary function was to secure the air base, including tanks, tank farms, bomb dumps and radar stations.[41] Capable of providing both fixed and mobile defense forces, they were given instructions to "hunt down the enemy immediately upon receiving information on him" and to "flank him or attack him in the rear as he engages fixed defenses."[42] As was often the case with newly-created organizations within the

---

[36] Fox, 2-3

[37] Ibid., 3.

[38] Ibid., 3

[39] Ibid., 3

[40] A.C. Carlson, "Air Base Defense" (Masters Thesis, Maxwell Air Force Base, AL,: Air Force, 1952), 5-6.

[41] Ibid., 6

[42] Fox, 7

military at that time, these groups were underutilized and misappropriated. Instead of protecting against parachute, glider and ground attacks, base defense personnel performed non-glamorous duties such as "guarding the gasoline, ammunition and ration dumps, entrances to the Officers clubs and hotels, vacant warehouses and dry cleaning establishments."[43]

By 1943, Allied dominance spread throughout Europe and the threats of enemy ground attack seemed to dwindle. Along with it diminished the importance of dedicated air base security. The United States Navy had exercised its own dominance in the Pacific theater during the Battle of Midway and destroyed Japan's military infrastructure to a point where they no longer posed a serious threat. The United States Army Air Force (USAAF) recognized this trend and began to deactivate the (still relatively new) air base security battalions until they were completely disbanded in 1945 after the Japanese surrender to the Allied powers.[44] The war had in fact ended, yet a standing air base defense policy remained ever-elusive.

Shortly after the end of World War II, the National Security Act of 1947 formed the United States Air Force as a separate branch of the armed services under the control of the Department of Defense. Debate over roles and missions ensued with ground defense responsibilities being a key issue. In 1947, under a joint service agreement between the Army and Air Force, each service acknowledged their responsibility for defending their own installations. In 1948, the Key West Agreement attempted to identify various base security roles and missions, more specifically for the Army, Navy and Marines[45]. However, it did not specify an Air Force ground combat mission, or specifically determine how the Air Force would defend its air bases. Hence, as the United States prepared to enter the war in Korea, the Unites States Air Force brought with it only a vague understanding of its air base defense doctrine and responsibilities.

C. AIR BASE ATTACKS DURING THE KOREAN CONFLICT

Upon entering the war in Korea, once dubbed by General Omar Bradley as "the wrong war, at the wrong place, at the wrong time, and with the wrong enemy," the United

[43] Fox, 7

[44] Ibid., 4

[45] Ibid., 4.

States Air Force, faced with a potential communist enemy of indeterminate strength, soon realized it lacked the requisite number of ground defense troops.[46] It began to build up its air base ground defense forces, expanding from 10,000 Air Police (AP) personnel in July 1950 to over 39,000 in December 1951.[47] These newly amassed forces entered the battle with infantry-type training, armored vehicles and associated weaponry. Additional personnel and new weapons could not hide the fact the Air Force still lacked an adequate base defense doctrine. Prior to entering the fray, the typical Air Police mission consisted of preventing thievery, pilferage and trespassing on and around the air bases. Many Air Force leaders felt since installations were typically located in the Army's defended rear area that defending these adjoined areas fell on the responsibility of the Army. Clearly, sufficient guidance was seriously lacking. On 3 March, 1953, the Air Force published Air Force Regulation (AFR) 355-4, *Defense – Local Ground Defense of Air Force Installations.*[48] This new regulation prescribed specific actions for installation commanders such that they may properly secure their installations from local attack. The new regulation provided specific details on denying hostile forces access to key areas of this base in addition to handling attacks such as:

- Infiltration
- Guerrilla warfare
- Civil Disturbances
- Local airborne, seaborne or ground attacks[49]

Responsibility for executing this particular mission rested on the shoulders of base defense task forces; typically augmented enlisted men from non-operational specialties and trained by Air Policemen. In addition to training this augmented force, AP's also provided listening/observation posts outside the base perimeter, conducted guerrilla detection patrols, and formed a mobile ground fighting unit.

---

[46] Taken from General Bradley's speech on May 14, 1951 to the Senate Committee on Armed Forces and Foreign Relations, The Military Situation in the Far East, Senate Hearings, http://education.yahoo.com/reference/quotations/quote/18185;_ylt=AvVKPJJVA6QiiLvS74Ou_2pcCc0F, (accessed on 28 July 2006).

[47] Fox, 5

[48] Ibid., 5

[49] Air Force Regulation 355-4, 1.

Additional guidance prevailed, determining that the Army, with its doctrine best suited as an offensive force, would remain in specific areas, while the Air Force would focus on point, or ground defense of its air bases.[50] Still, the Air Force perceived this ground defense role as an emergency function only, and typically short in duration. This belief carried over into the mindset that they were incapable of providing sustained air base defense operations.

Despite the potential for damaging attacks upon allied airfields, North Korean guerrillas operating in United Nations territory, surprisingly ignored attacking these unprepared and policy-confused targets. A Far East Air Forces Report found that, "effective security against sabotage and a workable ground defense system…never fully developed on most Air Force installations in Korea." They based their findings on the fact that drafted plans did not match the threat or were "beyond the unit's capability to execute effectively."[51]

Due to the lack of enemy activity, Air Police units in Korea found themselves preoccupied with interior guard duty and other inconsequential duties unrelated to defending the base. While AFR 355-4 was progressive and contained strategic vision, there existed a growing disparity between what it was designed to produce and what actually happened. The Air Force was slowly trying to develop functional air base defense doctrine, coupled with the required manpower, equipment and training. With what can only be attributed as good fortune, Air Force bases avoided serious threats or attacks during the Korean War. This lack of enemy activity, combined with amended intelligence estimates, a new national strategy focusing on 'containment', and a postwar budget reduction, led to Air Police manning requirements drawing significant congressional attention. Senior Air Force leaders, unfamiliar with the construct and vision of its air base defense strategy, could not properly handle congressional inquests regarding the need for continued and relatively high manning levels. Once again, the Air Force reduced not only its manpower, but its capability to properly defend its air bases.

[50] Fox, 6

[51] Ibid., 6

D. COLD WAR STRATEGY

With the dawn of the nuclear age, there was suddenly a major shift in national defense policy focused on "massive retaliation" to protect its vital interests. This shift in policy brought about significant changes to air base defense doctrine. The threats of air assaults upon air bases or infantries overtly advancing upon the flanks of air bases seemed highly unlikely. Replacing the threats and enemies the Air Force had trained and developed doctrine for were the threat of total nuclear war and clandestine attacks by teams of highly-trained Soviet agents attempting to disable our nuclear response capabilities. Accordingly, a 1957 Air Staff study concluded the practices currently employed under AFR 355-4 were "impractical, unmanageable and incapable of yielding defense-in-being consistent with up-to-date estimates and war planning concepts."[52] A shift in focus to protecting critical weapons systems, equipment, material and associated facilities led to the development of the Internal Installation Security Program, established by AFR 205-5 (ultimately replacing AFR 355-4). This program shifted the previous focus from local ground defense and placed a new emphasis on internal reinforced security, with an expanded interior guard system to counter covert threats considered 'inside the wire'. Unyielding AP policy enforcement of these critical areas became possible through the use of strict personnel access control. Additionally, small and mobile sabotage alert teams (similar to today's random antiterrorism measure and other mobile response teams) provided initial response. Off-duty Air Policemen and other trained base personnel provided a reserve force if required. This change in policy also had other immediate impacts in the AP arena. The Air Force cut it's AP overall end strength by 20% and closed the Air Base Defense School replacing it with an inadequate 40-hour preparation course; the only existing source of air base defense instruction for any/all base defenders.[53]

Difficult to fathom is the fact that despite the ever-changing shifts in air base defense policy coupled with the pendulous national defense policies throughout World War I, World War II and the Korean War, Air Force installations came out relatively

---

[52] Fox, 8

[53] Karl Hoover, "Air Base Ground Defense, the Training Controversy" (Research Report, Randolph Air Force Base, TX: History and Research Office, Air Training Command, 1991), 5.

unscathed. However, the Eisenhower administration's desire for an expanded interior guard concept of air base defense would not bode well with a change in administration and yet another shift in national policy, leaving the Air Force unprepared to embrace its air base defense mission in Southeast Asia once again.

E. AIR BASE ATTACKS DURING THE VIETNAM CONFLICT

As the Kennedy administration announced it would "support any friend, oppose any foe" in the assurance and survival of liberty, it brought about another shift in national defense policy, with an emphasis on flexible response.[54] The President, recognizing Communist issues developing in Southeast Asia, placed an emphasis on counterinsurgency warfare as he authorized the buildup of the U.S. Military Assistance Advisory Group (MAAG) in the Republic of Vietnam.[55]

From 1961 to 1964, the U.S. military, primarily in an advisory role, emphasized offensive operations, with the Army and Air Force focusing on separate playing fields. The Army developed search and destroy tactics, focusing on eliminating insurgent forces, while the Air Force leaned on offensive air operations. The Air Force, still focusing on internal security measures for countering Soviet sabotage-type threats, developed no local defense capability for themselves or their South Vietnamese counterparts.[56] In this loosely developed coalition, the Army of the Republic of Vietnam (ARVN) provided external and perimeter base defense, while the Vietnamese Air Force (VNAF) provided internal base security.[57] For reasons, mostly political, base security assignments for advisory units in country rested in the hands of these (often unreliable) augmented forces. The ARVN and VNAF not only burdened Air Police personnel with their untrained services, but also conflicting personal loyalties and rivalries. Continuous infighting persisted within the upper echelons of these services. In September 1964, the ARVN led

---

[54] Fox, 8.

[55] Ibid., 9

[56] General Curtis E. Lemay, Air Force Chief of Staff "approved a plan accenting counterinsurgency. The Air Staff took steps to devise special equipment, tactics and skills; to orient and train personnel; and to improve operational intelligence collection. This program did not actively consider the impact of insurgency warfare on air base defense. It overlooked the need to prepare indigenous forces to defend their own air bases, and to develop an organic USAF counterinsurgency ground defense capability. Insofar as air base security was concerned, the Air Staff remained preoccupied with the cold war threat", (*Air Base Defense*, Carlson, pp. 11-12).

[57] Vick, 76

efforts towards an attempted coup against the Saigon government. After the VNAF threatened to bomb them, relations between the two services remained diaphanous throughout the Vietnam conflict.[58] Fortunately for the Air Police and other air base personnel, the North Vietnamese and Viet Cong Armies (NVA/VC) practically ignored U.S and allied air bases throughout this timeframe, resulting in untested capabilities and a continued lack of attention on the importance of air base defense.

In 1962, the MAAG was reallocated as the U.S. Military Assistance Command, Vietnam (USMACV) and immediately Pacific Air Forces Command (PACAF) directed its Air Police to strictly enforce all internal security measures within the confines of Southeast Asia's operating bases.[59] The Air Force, recognizing their paltry presence (approx 280 men)[60] in Vietnam, requested a Numbered Air Force staff assistance visit to establish a more secure policy directive. The report suggested that "Air Police rely on standard Air Force procedures to detect and neutralize sabotage. It discouraged the use of ground force defense methods that entailed unfamiliar weapons and created support problems. While conceding that a large-scale enemy assault might require active USAF defense measures, the report warned that stocking more than a single basic load of small-arms ammunition might invite a VC/NVA attack."*[61]*

U.S. military personnel on the ground became wary of the often-tenuous USAF/VNAF security coalition. VNAF forces prevented Air Police from guarding their own aircraft, leaving them to secure only non-critical cantonment and supply areas. For the first time, the USAF Cold War viewpoint for base defense received serious scrutiny. Air Police commanders asserted this concept must be revised and more flexible rules and standards devised for the protection of USAF personnel and equipment in limited war areas. Based on field commander's recommendations, the Thirteenth Air Force launched reform proposals, subsequently ignored by both USMACV and PACAF.[62] With tensions escalating in the region after a Vietnamese attack on a U.S. Navy ship in the Gulf of

---

[58] Hettinga, 15-16

[59] Fox, 13.

[60] Ibid., 14.

[61] Ibid., 13

[62] Ibid., 14

Tonkin, the U.S. launched their first air attacks on North Korea in the fall of 1964. With the influx of aircraft into the region, military leaders took another hard look at their air base defense doctrine and begrudgingly sent several U.S Army officers forward to assist with the training aspects of the Air Police and ARVN coalition.[63] Subsequently, a month after the Tonkin assault, the Joint Chiefs of Staff (JCS) conducted a review of air base defense procedures in the region and declared them sound (based on the recommendations of several top military leaders).[64]

Exactly 60 days after the JCS labeled air bases secure in the region, Viet Cong guerilla troops launched a ferocious mortar attack on Bien Hoa Air Base. The base, severely unprepared due to RVNAF failures in sounding the alarm coupled with their delayed security response, resulted in the deaths of four U.S. personnel with thirty others wounded, the destruction of five B-57 aircraft and fifteen others damaged.[65] This marked the first ground attack on an air base in Air Force history. Unfortunately, many others were to follow.

The glaring security deficiencies on Vietnam air bases resulted in General Harris, Commander in Chief, Pacific Air Forces, to plead to the JCS for the deployment of Army and Marine Security Forces to secure these bases.[66] General Westmoreland, Commander, U.S. Military Assistance Command, Vietnam, was adamantly opposed to this idea. Westmoreland felt placing these infantry troops into defensive roles would ultimately cripple offensive operations. He ordered all installation commanders to initiate (self) defensive efforts and directed that all specialties of all services would organize, train and exercise to perform air base security functions at their installations. The Air Force interpreted this to mean their security personnel would continue to apply their air base defense energy on the internal portions of installations.

With the persistent focus on defending forward deployed air bases, coupled with repeated successful enemy attacks, the Air Force Chief of Staff, realizing Security Police

---

63 Fox, 14-16.

64 Ibid., 15

65 Hettinga, 16

66 William Delaney, "USAF Force Protection, Do We Really Care?" (Research Report, Maxwell Air Force Base, AL: Air Force, 1998), 19.

manpower numbers were drastically low in Vietnam, directed the organization of ten Security Police squadrons with an associated Security Police training school, stressing marksmanship and ground base defense skills. By March, 1968, the 821st Security Police Squadron was the first such unit to form, train, equip and travel to Vietnam.[67]

While Air Force security personnel performed adequately in regards to defending the internal portions of the base, 96% of the 475 air base attacks in Vietnam were the result of standoff weapons with no penetration of internal security.[68] With a Cold War precept in place, Air Force security personnel focused their energies on the inner and cantonment portions of base, and did not adapt to the guerrilla style warfare being used by the Viet Cong and North Vietnamese whose motives simply were to destroy U.S. and allied aircraft and kill or harass American military personnel. Insurgent forces operating in the area relied upon low-level intelligence gathering and reconnaissance. The Air Force base defense doctrine, calling for a static defense posture, simply was not effective against the enemy's *modus operandi*, and was often quickly compromised.

Korea and Vietnam taught us that defending air bases calls for an expanded ability to detect, deter and defend outside the base perimeter away from critical resources and personnel. With the dawn of asymmetric threats, the continued use of standoff weapons, the introduction of suicide bombers and other unconventional methods, the scope of defending air bases demanded new and improved doctrine.

F. A CHANGE IN MINDSET? OPERATION SAFESIDE

It is clear that the involvement of Air Force security personnel units during the Vietnam insurgency consisted primarily of internal security on remote and often-vulnerable air bases. It is also clear they focused primarily on protection against the covert threat of sabotage and/or penetration-style attacks on cantonment or inner portions of the air base. The bulk of security personnel in theater had received air base defense training focused towards the more conventional Soviet threat; however, the continued and often well-planned stand-off (mortar and small arms) attacks by organized NVA/VC battalion-sized guerrilla groups on coalition air bases eventually forced a change in

[67] Fox, 110

[68] Vick, 68. Vick reports an additional 18 attacks were later identified during the course of his research, bringing to total to 493.

mindset. The Air Force decided to shift its attention from a completely static or internally-focused doctrine to one providing well-trained, well-armed and highly motivated combat Security Police units capable of repelling enemy raids outside the perimeter of the air base and away from critical assets and operations.

In February of 1968, the Seventh Air Force Commander initiated a request for what would officially become the first in a line of highly-trained Combat Security Police (CSP) units focused on a new base security concept, one known as "active defense."[69] The formation of CSP units required a strict selection process as Security Police officers and non-commissioned officers were thoroughly screened for selection into what would become a fast-paced and physically rigorous training regimen specializing in hand-to-hand combat, special weapons training and other tasks commonly performed by Army Rangers. The project officer for OPERATION SAFESIDE, Colonel William Wise, was quoted as saying, "Local base Security Forces are responsible for the internal protection of air bases…and have been very effective against attempted penetrations by saboteurs. But when hostile groups overtly attack our base perimeters in large numbers, it is too late."[70] CSP units were thought to be the stopgap in preventing the enemy from getting close enough to the air base to attack it, even from a stand off distance, which had proven to be the Achilles Heel of air base defense up to that point.

Once operational, CSP units patrolled large areas of jungle and rice paddies, formerly the sole responsibility of the oft-inadequate host nation forces, with active defense tactics developed during their intense training. These tactics included daylight recon patrols, forward observation and listening posts, operation of tactical motor patrols with gun jeeps, sweep and clear operations, relocation of areas of population, as well as their primary active defense tactic: the ambush patrol, considered essential in an insurgent environment.[71] Air Force and Security Forces planners felt through the correct placement of combat essential resources adjacent to and outside the base perimeter, the

[69] Fox, 110. A six month test phase utilizing CSP was conducted earlier in January of 1967, yet funding and manpower allocations would not permit permanent assignment of these teams in Security Police squadrons, and they were returned home.

[70] S.J. Christaldi, Operation Safe Side, http://www.vspa.com/phan-rang-christaldi-safeside-1967.htm, (accessed on 24 June 2006), 2-3.

[71] SAFESIDE Association. 2005. OPERATION SAFESIDE: History of the Combat Security Police. http://safesideassociation.org (accessed on 26 June 2006), 1-2.

off base mortar attacks could be minimized. VC/NVA units lacked sophisticated intelligence aids and equipment and relied on low-level intelligence gathering, usually through reconnaissance methods. The existing, or static, air base defense posture was quickly compromised by that type of enemy activity.

CSP units deployed to Vietnam made a significant contribution to the overall base defense mission through their tactical maneuvers and weapon proficiency and often formed and responded to situations in less than an hour after being notified. Yet, despite the contributions of the CSP units to the overall air base defense mission, numerous implementation and integration problems are worth mentioning here in hopes to prevent similar errors in future programs. First, the initial placement of the SAFESIDE Headquarters at Schofield Barracks in Hawaii made it extremely difficult to communicate with the CONUS-located higher headquarters, causing potential oversight and logistical challenges.[72] Secondly, due to a shortage of available manpower, members of the SAFESIDE test unit were called upon to serve as instructors for future CSP units. These men, who had received only Army Ranger training, were neither formal instructors nor trained in small unit tactics associated with air base defense. CSP units who were rushed through this training learned land navigation, long-range ambush and recon patrols, stream crossing, rappelling and other Ranger-related activities, but air base defense operations typical of those experienced in Vietnam was often totally neglected.[73] The hurried training resulted in CSP units arriving in Vietnam with a distorted picture of the mission they were to perform. Many of the arriving CSP units believed since they were given Ranger and specialized training, they were in fact superior to existing/conventional Security Police units already in country. This sparked a fair amount of friction early on, which ultimately resolved itself. Finally, in addition to numerous technology shortfalls discussed later in Chapter VI, there were several distinct command and integration problems involved with the CSP units. CSP units arriving in country were never properly integrated, with some members called upon to perform normal air base security duties or pull shifts inside the Base Defense Operations Center (BDOC) due to manning shortfalls.

[72] CONUS is Continental United States

[73] Fox, 112.

There were also scattered reports that some CSP units were more preoccupied with killing Viet Cong guerrillas than providing an active air base defense posture.[74]

After a hastened upstart to the program, the rotation of CSP units ceased in August of 1969 due to both a lack of funding and the increasing withdrawal of U.S. troops from the region. In December, 1969, the SAFESIDE Program was discontinued and stateside training ceased.

All things considered, CSP units performed at a level commensurate to the limited substantive guidance and rushed training they received prior to arriving in Vietnam. As Air Force security personnel continue to exist as a HD/LD (high demand/low density) asset, and world events continue to push the operations tempo to heightened levels, military planners must consider the potential impacts of limited and/or 'just in time' type training. Air base defense in austere and hostile parts of the world today call for a properly trained force executing well planned and thoroughly developed air base defense doctrine.

G. THE ATTACK ON KHOBAR TOWERS

The United States has maintained at least a meager military presence in Saudi Arabia since the early 1950's, typically in a training capacity to help the Saudi's modernize their military infrastructure. Iraq's invasion of Kuwait in 1990 changed all that as the U.S. deployed over 500,000 military troops to the region to defend Saudi Arabia and liberate Kuwait from the Iraqi stronghold.[75] King Fahd, the Saudi ruler at the time, reluctantly agreed to absorb the masses of U.S. military on the promise they would all leave when the conflict ended. However, those days never came. Saddam's persistence to avoid cease fire and WMD resolutions led to the seemingly never-ending Operation Southern Watch and the housing of a military coalition at the Khobar Towers facility near Dhahran.

History has shown us American military presence in another country comes neither cheap nor without hardships. In November, 1995, terrorists detonated a car bomb containing an estimated 200-250 pounds of explosives near the Office of Program

[74] Fox, 112-113.

[75] William J. Perry, *Report to the President on the Protection of U.S. Forces Deployed Abroad*, September 15, 1996, www.fas.org/irp/threat/downing/report_f.html, 1-2, (accessed on 12 June 2006).

Manager, Saudi Arabian National Guard (OPM-SANG), killing five Americans.[76] Up until this event, security risks in the area were seen as manageable; troops maintained a low profile and followed standard security and force protection practices. Following the OPM-SANG bombing, that concept was reevaluated. The threat level in the region was elevated to "high" and extensive improvements were made in all Arabian Gulf region facilities. Intelligence reports indicated new attacks planned against American forces were possible, with Khobar Towers listed as a potential target. After action reports indicate security officials at Khobar enacted over 130 separate force protection enhancements/security measures to defend against this potential threat. Physical barriers were emplaced, perimeter fencing moved further out from living quarters, entrances restricted and hardened and guard forces increased. The approach was merely one of enhancing security of existing facilities despite their overall limitations, and this proved insufficient to protect U.S. forces. Seven months later, a truck bomb exploded near the Khobar Towers compound. The Defense Special Weapons Agency classified the explosion equivalent to more than 20,000 pounds of TNT.[77] Lieutenant General James Record, later called upon to conduct a separate inquiry into the Khobar bombing, stated, "This nation must never forget that the bombing of Khobar Towers was not an accident—it was a cold blooded terrorist act of murder."[78]

Following the Khobar bombing, former Secretary of Defense William Perry directed retired General Wayne Downing to conduct an investigation into the circumstances and facts surrounding the attacks at OPM-SANG and Khobar, as well as an assessment of the overall security of U.S forces in the region. The Downing Assessment Task Force identified 26 major findings and formulated another 79 recommendations in their report to improve DOD efforts to combat terrorism.[79] During the Downing investigation, it was learned Security Forces personnel were not briefed on the potential threat, no terrorist response exercises were conducted and no weapons

[76] Record, 1.

[77] Perry, 3.

[78] Record, 43.

[79] Wayne A. Downing, General (retired), *Force Protection Assessment of USCENTCOM AOR and Khobar Towers, Report of the Downing Assessment Task Force*, Washington, D.C.: US Air Force, 30 August 1996, available online at http://www.fas.org/irp/threat/downing/unclf913.html (accessed on 12 April 2006), 1.

training was conducted in country to practice in the environment they were expected to defend. The Task Force ultimately recommended a more comprehensive approach to force protection. While the Task Force recognized an environment free from all attacks was not possible, they determined commanders must create a force protection system combining training and awareness, advanced technology, increased intelligence, enhanced physical security and location-specific protection measures to assure an acceptable level of protection for U.S. forces stationed abroad.

After both the Korean and Vietnam Wars, military planners seemed to forget the specific challenges in dealing with an insurgent or guerrilla-style enemy. They seemed to forget the high rate of success their enemies achieved conducting stand-off attacks from outside their perimeter. At the termination of both conflicts, the security posture at air bases, both home and abroad, returned to defending against a Soviet-type saboteur threat, neglecting the hard lessons learned previously. After the horrific bombing at Khobar Towers, Pentagon officials adopted a radically different mindset on force protection and improved intelligence. Specifically, the Air Force, identifying needs in training, intelligence and overall structure, reorganized their forces, changing their name from Security Police to Security Forces. Additionally, they created not only a specialized tactical unit (the 820th Security Forces Group), but also the Force Protection Battlelab for the creation and testing of new force protection technology.[80]

However, the horrific attacks on 9/11 identified, among other things, lingering deficiencies in intelligence and advanced technology. The Air Force came to realize the days of traditional air base ground defense doctrine and defending against known enemies using conventional methods are now behind them. Future adversaries, unwilling to challenge us conventionally, will resort to what has worked for them in the past; unconventional, small-unit attacks upon our military installations and air bases. Korea, Vietnam and Khobar Towers indicate numerous examples of where air base defense doctrine has been found wanting in the past. Therefore, as we look ahead to the future security environment and its associated challenges, new force protection strategies and procedures are certainly in order.

[80] Robert Creamer Jr, and James C. Seat, "Khobar Towers: The Aftermath and Implications for Commanders" (Research Report, Maxwell Air Force Base, AL: Air War College, April 1998), 24.

THIS PAGE INTENTIONALLY LEFT BLANK

III. AIR BASE DEFENSE: TODAY AND TOMORROW

A. A NEED FOR A CHANGE

The history of air base defense is filled with seemingly erratic and episodic increases and decreases in security-associated manpower. Additionally, well-organized air base defense doctrine either did not exist or never fully developed during the campaigns discussed previously. Air base defense doctrine, training and manning all increased during Korea, only to dissipate soon after the war ended. Base defense planners in Vietnam were faced with a new type of warfare and an enemy persistent in executing it. Viet Cong and North Vietnamese Army guerrilla units continuously, and most often successfully, shelled Air Force bases with mortars, artillery and small arms fire. Despite gradual advances made in defending against this type of enemy/attack, the conventional way of thinking led military planners to believe Vietnam was an isolated occurrence and Army or host nation forces would supply external security in future wars.

The unconventional attack on Khobar Towers summarily led military planners to recognize that host nation security forces were certainly not sufficient to counter potential enemy threats to air bases and deployed military personnel. Unpredictable, asymmetric attacks by guerrilla or insurgent-type forces usually occur with little to no advance notice, often leaving host nation and/or U.S. military forces unprepared. Host nation and other external security forces, often faced with the task of deterring enemy forces before they approach U.S. air bases, seemed incapable of stopping these attacks, and enemy forces were able to destroy war fighting assets and kill U.S. military members from outside the perimeter fence line, away from the focus of Air Force security personnel monitoring the interior portions of the base.

The air base attacks in Korea, Vietnam and at Khobar Towers clearly indicate a need for properly integrated and effectively executed air base defense on Air Force bases at home and abroad. In these earlier examples, Air Force air base defense doctrine consistently did not maintain the organic capability and meet specific requirements necessary to defend its critical assets and infrastructure from asymmetric ground attacks. Shortly after the Khobar incident, General Ronald Fogleman, former Air Force Chief of

Staff, was quoted as saying, "Security no longer ends at the base perimeter. We must assume responsibility for a much larger tactical perimeter that will keep the threat away from our people and our equipment."[81] Therefore, it is obvious that the focus of Security Forces can no longer be limited to the interior portions of the air base to successfully defeat terrorist and insurgent attacks. Guerrillas and other small tactical units will attempt to attack air bases and military infrastructure. Air base defense doctrine must include the capability to view, assess and potentially respond to areas outside the base perimeter and as far away from critical resources and personnel as possible.

B. INTEGRATED BASE DEFENSE (IBD)

In 2005, the Air Force, recognizing compliance-based security methods designed to counter conventional threats were no longer sufficient, adopted the Integrated Base Defense (IBD) program as their installation security doctrine. Functional security demands a more adaptive construct to defeat elements of today's terrorism: irregular, catastrophic, asymmetric and disruptive. With today's enemies including guerrillas and insurgents capable of using weapons of mass destruction and other leveraged technology against our forces, compliance-based standards simply cannot match this threat. New approaches towards capabilities and effects-based standards using various risk and vulnerability assessments as a foundation to identify critical resources will ultimately determine effective countermeasures and tactics to defeat the threat.[82] The guiding principles of this new defense doctrine include the ability to: detect (to see first), assess (to understand first) and respond (to act first), each with the overall objective of keeping the initiative away from the enemy.[83]

While the elements of "see first," "understand first" and "act first" are directly connected to each other, each element possesses independent conditions designed for success.

---

[81] Headquarters, United States Air Force, *Air Force Doctrine Document 2-4.1: Force Protection* (Washington, D.C.: HQ/Air Force, 1999), 33.

[82] Headquarters, Air Mobility Command (HQ AMC), *Integrated Base Defense Concept of Operation*, 2.

[83] Headquarters, United States Air Force, *Air Force Tactics, Techniques and Procedures 3-10.1, Integrated Base Defense Tactical Doctrine*, 31.

- See first (to ensure the enemy sees last)
  - Relentless intelligence and information capture
  - Detect and identify threats
  - Predict threat courses of action (COA)
- Understand first (to ensure the enemy understands last)
  - Identify vulnerabilities
  - Tailor base defense plans
  - Know and manage risks
- Act first (to force the enemy to act last or incorrectly)
  - Determine options
  - Decide first
  - Act to remove threat[84]

Since this chapter/thesis is not intended to be a user's manual for IBD, some of the specific functions, capabilities and required tasks are purposely omitted. However, examination of official 'user's manuals' such as Air Force IBD publications and CONOPS, uncover several common themes from within the elements listed above.[85] Improved/actionable intelligence sharing (both internally and externally), the identification of and directed security for critical assets/infrastructure and an increase in assessment/surveillance technology remain essential components of IBD doctrine. It is important to remember these three elements, as they were the same three primary areas where this research determined base defense policy failed in the earlier examples, and therefore will be examined in great detail in subsequent chapters.

On the heels of an increased operations tempo and ever-increasing numbers of deployed personnel, the Air Force has shifted to a more expeditionary and war-ready force. General Jumper, former Air Force Chief of Staff, said, "Making the Air Force truly an expeditionary force will require more than just a light and lethal doctrine, it will mean breeding a new generation of air and space warriors." He went on to say, "In this culture, you have to get back to some basic institutional values; every airman a warrior,

84 United States Air Force, *Air Force Tactics, Techniques and Procedures 3-10.1*, 11-12.

85 Includes: *Integrated Base Defense Concept of Operation (CONOPS)* and *Air Force Tactics, Techniques and Procedures 3-10.1, Integrated Base Defense (IBD) Tactical Doctrine.*

every airman a sensor."[86] A reduction in available (non-deployed) security manpower places an increased emphasis on risk and vulnerability assessments as well as an amplified role in commander's risk management decisions. Fewer personnel equates to fewer security posts filled, with the exception of several mandated positions, Security Forces commanders will need to become actively involved in the placement of their remaining sentries.

With more and more Security Forces' and other Air Force members deployed in support of Operations *Iraqi Freedom* and others, one of the critical requirements of the new IBD doctrine is that every service member, support staff and civilian agency support and contribute to IBD while simultaneously fulfilling their primary obligations.[87] This will not require all installation personnel to draw a weapon and stand watch on an installation gate or security post, it simply implies all personnel will maintain a heightened sense of awareness of their surroundings and report anything deemed suspicious throughout their work day or wherever their duties take them (often defined as owner-user participation). This is akin to the time when General Westmoreland recalled all Army and Marine infantry units from U.S. air bases in Vietnam and left U.S. Air Force personnel to fend for themselves. Air Force commanders called for augmentation forces, and everyone who was capable provided some level of security on the air base. Prior to the IBD concept, Security Forces patrols performing base defense duties were relatively small in number and their efforts focused on areas close to critical AF assets. With IBD, all airmen (not just security personnel) contribute to the IBD concept, acting as a larger 'security force', enabling a larger concentration of force on a much wider battlespace.

The lessons of Korea, Vietnam and Khobar have taught us many valuable tactics regarding air base defense. Particularly in Vietnam, we noticed Security Forces waiting for emergency situations before responding, and their responses were often quite predictable, focusing on defense of the interior portions of the air base. As Figure 1 indicates, security responses under the IBD construct will no longer be reactive in nature,

86 John A. Tirpak, To Provide for a Powerful Force, Air Force Magazine Online, June 1988, vol. 81, no. 6, http://www.afa.org/magazine/june1998/0698force.asp (accessed on 16 August 2006).

87 Department of the Air Force, 3-10.1, 1.

but in an effort to preempt the threat, will take a more proactive approach, similar to what Operation SAFESIDE tried to accomplish in Vietnam.

Figure 1. Air Base Defense, Then and Now

Prior to IBD	**With IBD**
- Reactive in nature	- Proactive in nature
- Compliance-based defense plan	- Defense plan tailored to situation
- Static	- Flexible/maneuverable
- Security-functional responsibility	- CC and all airmen responsible
- Wait for the threat	- Preempts the threat
- Little reliance on intelligence	- Intelligence is a key element
- Predictable	- Unpredictable
- Little room for initiative	- Promotes initiative
- Personal experience/intuition	- Supported by technology
- Risks unknown/unmeasured	- Knows/accepts chosen risks

Security personnel in Vietnam and at Khobar also lacked efficient and timely intelligence, either externally or internally generated. IBD doctrine calls for and expects intelligence to be a key factor in executing security operations to achieve local and area dominance. Security personnel in Korea and Vietnam often relied upon gut instincts or what limited 'just in time' training they received prior to arriving in theater. IBD will augment improved air base defense training with technologically advanced detection and assessment equipment. IBD doctrine calls for a move from more traditional, static posts to more mobile and agile response forces able to cover a larger area more rapidly.

Removal of dedicated sentry positions in certain areas requires the implementation of technological security enhancements to support the response forces. While IBD is designed to provide a heightened security presence in both peacetime and contingency operations, technology enhancements are vital when/wherever appropriate to fill possible gaps left by ground forces. Commanders, requiring increased situational

awareness, will rely on technology to combine all sensor inputs, along with ground force assessments, to make quick and accurate decisions.[88]

The bottom line is this: to preserve Air Force war fighting assets on the ground, IBD capabilities must include anticipating and detecting the enemy as early as possible, denying or delaying him through whatever means necessary, and ultimately neutralizing and mitigating enemy forces/threats through rapid and strategic deployment of Security Forces.

C. FUTURE ADVERSARIES AND METHODS

Our adversaries know they cannot compete with AF assets while in the air, so the only logical countermeasure for them is to attempt to destroy them on the ground at air bases. The demonstrated capabilities of U.S. airpower, such as those displayed in Kosovo and Operations *Desert Storm* and *Iraqi Freedom*, may make Air Force bases a high-priority target for future enemies. Meanwhile, the military fights today with fewer overall resources, yet these same resources have higher individual strategic value. Losing one system or critical asset could severely impact overall operational capability and mission effectiveness.

It is clear that air and space operations and their associated assets will continue to face a transnational or insurgent type of threat employing unconventional and/or asymmetrical methodologies. Terrorism experts argue that future attacks on military installations and/or military infrastructure are extremely likely to occur. Falling in line with bin Laden's 1996 fatwa calling for light, mobile forces using guerrilla tactics to attack U.S. targets and personnel, Bruce Hoffman feels al Qaeda will maintain an active interest in attacking 'hard', or well protected targets, such as embassies and military installations. Hoffman feels the destruction of these targets, often difficult to penetrate, may improve bin Laden's credentials as a meaningful adversary, potentially building upon a support base for additional terrorist recruits.[89] Shlapak states that in lieu of large, armored conventional forces attacking air bases, we can expect smaller units, well armed and equipped and trained in small unit tactics. He further argues these opponents will seek to (1) destroy high-value, critical assets and infrastructure vital to war fighting

[88] Department of the Air Force, 3-10.1, 31.

[89] Hoffman, et al, *Trends in Terrorism*, 16.

operations, (2) attempt to disrupt sortie generation or mission flow, and/or (3) create a high-profile event with the goal of affecting public opinion and overall public support for ongoing military operations in other parts of the world.[90] Dennis Drew claims insurgencies appear to be the most likely, and perhaps the most threatening, kind of conflict the U.S. will face in the future. He further states these insurgent opponents are often more unpredictable, leaving U.S. aerospace and war fighting assets at in increased risk to enemy attack.[91] As of August, 2003, Iraqi insurgents, using mortars and shoulder-fired (stand-off) weapons, have fired upon 21 U.S. aircraft at Baghdad International Airport; another 9 U.S. helicopters were shot down using the same techniques.[92] In regards to anticipating enemy action, Paul Wilkinson argues that predicting a likely target of future terrorist attacks is not necessarily difficult. He anticipates over one half of all terrorist attacks will involve business or industrial facilities, while at least 5% will include government facilities and military air bases. He further argues that while military targets are often hardened, military personnel are roughly equal in vulnerability to being a terrorist target.[93]

When it comes to terrorist groups seeking to change public opinion or distract military interests, Matthew Levitt feels terrorist groups in Iraq and Afghanistan may attack hardened military installations both home and abroad, with the ultimate goal of disrupting U.S. military operations. Hoffman and Levitt both suggest U.S. military personnel (and infrastructure) would be an irresistible target for al-Qaeda and other terrorist groups.[94] Claiming the political fate of most modern societies is highly determined by what happens in its cities, Ian Lesser feels terrorists seeking to influence political conditions will target symbolic targets located in urban settings.[95] Wilkinson agrees insurgents/guerrillas possess the ability to change public opinion, perhaps to

---

[90] Shlapak, 15.

[91] Dennis Drew, "Airpower in the New World Order" (Research Report, Carlisle Barracks, PA: US Army War College, 1993), 3.

[92] H. John Poole, *Tactics of the Crescent Moon: Militant Muslim Combat Methods* (North Carolina: Posterity Press, 2004), 153-154.

[93] Paul Wilkinson, *Terrorism versus Democracy: The Liberal State Response* (Portland, OR: Frank Cass Publishing, 2000), 208.

[94] Bruce Hoffman, Matthew Levitt and Daniel Benjamin, p. 2-3.

[95] Ian Lesser et al., *Countering the New Terrorism* (Santa Monica, CA: RAND, 1999), 143.

achieve short or long-term political goals. He argues guerrilla/insurgent leaders firmly believe their style of warfare itself is usually not sufficient enough to achieve victory against a militarily superior opponent. Rather, it is when the 'anti-guerrilla' side underestimates the guerrilla or insurgent threat or simply fails to commit sufficient resources to defeating it that this method actually has a chance of success—often having an effect on domestic or international opinion.[96]

Two fairly recent examples of thwarted terrorist attacks provide evidence our adversaries are seeking to attack military targets and installations. In September 2002, German authorities arrested a pair of terrorists, with links to al Qaeda, possessing 287 pounds of chemicals and 5 pipe bombs in their apartment in Waldorf, Germany. The two were suspected of plotting bomb attacks against nearby U.S. military installations on the anniversary of September 11th.[97] In August, 2005, Los Angeles law enforcement units traced the origins of a newly formed Islamic extremist group operating in Southern California. The group, comprised of two former inmates from a Sacramento prison, also included a Pakistani immigrant and a Muslim convert. Through gas station robberies and other illicit activities, the group raised cash to purchase large caches of weapons and ammunition. Prior to their arrest, the group was actively recruiting additional Muslim members and conducting surveillance of military air bases in Southern California. This researcher has worked in air base security for nearly 13 years and has witnessed and heard of many indicators of terrorist surveillance, probes and/or plots involving military air bases. One can safely assume that for every plot that is uncovered or disrupted, there are undoubtedly many that go undetected.

Hence, it is clear through an examination of the existing literature that military installations and air bases remain viable targets to small groups of terrorists or insurgents employing asymmetric or unconventional methods to attack them. As Vick points out in his research, large enemy forces are not required to conduct attacks upon U.S. air bases. Smaller units using unconventional methods of attack have proven to be quite effective.[98]

---

96 Wilkinson, 10-11.

97 Jim Lehrer. 2002. Germany arrests two suspected of planning Sept 11-related attack: Online NewsHour-Combating Terrorism. http://www.pbs.org/newshour/terrorism/combating/index.html (accessed on 14 April 2006).

98 Vick, 107.

He also claims preparing defenses against large-unit attacks should not be completely discounted, but expects future adversaries to conduct operations in smaller units or networks. However, what is more interesting, and perhaps even more alarming, is that many researchers claim that not only do we face the probability of attacks on air bases from similar groups and methods, but that these attacks will also closely resemble those seen in Korea, Vietnam and Khobar Towers. Considering the preponderance of successful attacks on air bases in Vietnam were accomplished via standoff weapons, Shlapak is concerned that U.S. Air Force capabilities to meet this threat in the future may be extremely limited. VC/NVA mortar attacks were able to easily penetrate and defeat perimeter defenses like machine guns and observation posts. He feels with the expectation of our adversaries to utilize this same method of attack, the Air Force is likely to lose critical war fighting assets and/or experience major disruptions in military operations.[99] He further states that with future adversaries resembling those seen in Vietnam, air base defenders unable to reconnaissance or maintain visibility on the exterior portions of the air base will undoubtedly meet a similar fate.[100] Vick agrees with this theory, stating the most likely threat facing U.S. Air Force air bases in the future will resemble those seen exhibited by the Viet Cong/North Vietnamese Army in Vietnam. He feels standoff threats and the use of mortars, self-propelled rockets and other external attacks will continue to challenge air base defenders. Vick also stipulates that advances in technology, allowing for the use of precision-guided mortars and other more accurate munitions, will only make the threat more serious and more difficult to defend.[101] Air bases typically employ infrared and thermal imagers, security sentries, canine patrols and motion-tracking cameras along their perimeter fence lines. Unconventional adversaries will typically not wish to encounter these active layers of defense face-to-face, but rather employ tactics that can disrupt military operations from a distance. Claiming the effectiveness of unconventional, standoff attacks similar to that used by the VC/NVA during the Tet Offensive, Dickey claims our future adversaries will likely employ some form of asymmetric strategy to defeat or diminish the overall effectiveness of the U.S.

99 Shlapak, xvi.

100 Ibid., 37.

101 Vick, 110.

military might.[102] As a result, standoff attacks undoubtedly represent one of the largest asymmetric threats to air bases in the future.

Previous attacks on air bases have also involved small units of attackers penetrating the base perimeter and utilizing explosive charges to destroy infrastructure, aircraft, or kill U.S. military personnel. While guerrilla insurgents operating in Korea and Vietnam had limited technologies, they often did not detonate ordnance remotely. They typically used claymores, trip wires and pressure devices and preferred close-in combat. Recently, we have seen the rapid escalation of explosives used not only in vehicle-borne improvised explosive devices (VBIED), but also in suicide bombings, with an apparent preference towards close combat attacks. The Marine barracks in Beirut, Oklahoma City and Khobar Towers are prime examples of VBIEDs and their potential destructive capability. The notable concern over VBIEDs is their overall effects in both penetration-style attacks (Beirut) as well as standoff-style attacks (Oklahoma and Khobar Towers). Similarly, we have seen the advent of both suicide and roadside bombs in Iraq, and most recently in Afghanistan, produce devastating effects and high numbers of casualties on U.S military personnel in those regions. Al Qaeda and other Iraqi insurgents have become quite adept at hiding roadside bombs in burlap bags, food containers, vending carts and animal carcasses located along the road.[103] An examination of Al Qaeda tactics demonstrates their preference for hit-and-run type tactics, with strengths existing in both ambushes and road-side bombs. H. John Poole's research indicates their frequent use of explosives, rocket attacks and indirect fire (similar to Korea/Vietnam.)[104] Shlapak believes we will continue to see both standoff and explosive attacks used in the future with an increase in their lethality based on exponential technology gains, often keeping pace with U.S. countermeasures.[105]

In addition to the terrorism and security experts, Air Force publications also predict potential attacks from unconventional adversaries in the future. Air Force Instruction (AFI) 31-301, *Air Base Defense*, states, "Asymmetric threats will increasingly

---

[102] Dickey, 1-2.

[103] Poole, *Tactics of the Crescent Moon*, 148-149.

[104] Ibid., 192-193.

[105] Shlapak, 35.

challenge base defense forces. Historically, elements such as special forces, light infantry, airborne, airmobile, terrorist, guerrilla and irregular units have successfully employed unconventional warfare tactics to harass personnel and destroy vital resources."[106] Poole states Al Qaeda has developed a state-of-the-art urban assault and street fighting strategy that would undoubtedly impact Security Forces members defending air bases in urban areas. These attacks are typically initiated by rocket propelled grenades taking out guard shacks and installation entry controllers. After the initial shock, walls and perimeter fences are breached by hand-placed explosives in multiple locations. Shoulder-fired weapons and command-detonated explosives are then typically used to attack key infrastructures and strategic assets.[107] While the Viet Cong would typically rehearse an attack for weeks or perhaps a month, Muslim insurgents have been known to prepare for these types of assaults for years at a time. They may not be as tactically proficient as the Viet Cong, but their perseverance and dedication to the overall mission should be a concern to air base security personnel.

Considering the obvious misapplication of air base defense doctrine and procedures during Korea, Vietnam and Khobar Towers, combined with the likelihood we may be facing similar enemies using similar attack methods, it is imperative Security Forces personnel and base defense planners understand what they are up against and what to expect. Air base ground defense remains a vital mission for the Air Force if it expects to maintain its air superiority. As the nature of ground threats to air bases will undoubtedly continue to evolve, it may be difficult to predict which threats pose the greatest risk to air bases and their infrastructure. As our past experiences in Korea, Vietnam and Khobar Towers have demonstrated, air base defense forces simply cannot wait until the base and its infrastructure are under attack before they take action. The Air Force must find methods of securing their air bases beyond the maximum effective range of the security patrols (and their weapons) operating inside the base perimeter.

In examining the existing literature on air base attacks during Korea, Vietnam and Khobar Towers, this researcher identified several common and distinct areas that were shown to be problematic for security personnel in all cases. First, proactive intelligence

[106] HQ Air Force, *31-301*, 4-5.

[107] Poole, *Tactics of the Crescent Moon*, 194.

programs seemed nonexistent, with problems surrounding either a lack of precise intelligence, receiving it in a timely fashion and/or obtaining it from participating host nation forces. Better intelligence programs and information sharing in Vietnam and Khobar Towers may have prevented the destruction of numerous aircraft and the deaths of military personnel. Secondly, there appeared to be no programs or systems in place to not only identify, but primarily to protect critical infrastructure and assets. Aircraft and their associated infrastructure, command centers and vital war fighting resources were routinely destroyed in Vietnam due to their improper placement and inadequate defense. Additionally, a large military barracks, situated too close to the base perimeter despite known threats, continued to house military personnel at Khobar Towers. Finally, the lack of adequate technology, either involving weaponry or detection equipment, proved to be problematic primarily in Vietnam and at Khobar Towers. The use of tactical and automated sensors, infrared or thermal imagery and other technologically advanced security measures may have also prevented or disrupted these enemy attacks. It is clear further examination into these areas is required to ascertain Security Forces' current and potential involvement in these areas. Chapters IV, V and VI will discuss these particular areas in great detail, identifying previous procedural or doctrinal errors made as they relate to air base defense, as well as possible recommended solutions and/or courses of action for future Integrated Base Defense planning.

IV. INFORMATION AND INTELLIGENCE SHARING

A great part of the information obtained in war is contradictory, a still greater part is false and by far the greatest part is of doubtful character.
- Clausewitz 108

The collection, analysis and timely application of useful intelligence are vital in the execution of the air base defense mission. In the past, intelligence producing and/or gathering assets were either non-existent inside Air Force security units or they lacked sufficient emphasis to make them a worthwhile commodity. The lack of focus on a working intelligence program allowed guerrilla/insurgents to operate relatively freely in Korean and Vietnam country sides and overlooked several rather obvious signs of a pending attack at Khobar Towers. This chapter illustrates some of these early doctrinal and procedural errors and describes the importance of a functional intelligence program and the dividends they bestow upon the air base defense mission. In order to appreciate the importance of a well-designed intelligence program, one must first understand the sources of military intelligence and the process in which it flows to the air base defense consumer. This chapter briefly describes that process as well as the way in which this information feeds into several data management and other information sharing programs used by Security Forces in the execution of the air base defense mission.

A. EARLY POLICY ERRORS AFFECTING AIR BASE DEFENSE

Air Force security personnel, responsible for planning, organizing, and conducting air base defense throughout the Vietnam countryside often relied upon the functional expertise of engineers and logisticians, but more importantly, intelligence analysts and their potential information support. However, with clear and seemingly unending gaps in air base defense doctrine, a functional relationship between security and intelligence personnel took several years to develop.

Since the connective requirement was not established early, ground defense and security planners lacked valuable intelligence which they required to set security alert conditions, deploy contingency forces and counter enemy forces moving throughout the

108 Military Intelligence Quotes website, http://www.arrse.co.uk/cpgn2/Forums/viewtopic/t=30797.html February 18, 2005 (accessed on 18 June 2006).

area. Instead of providing support to the air base ground defense mission, intelligence personnel were immersed in providing intelligence updates for air combat missions.[109] After swift and violent stand-off attacks devastated U.S. aircraft on Tan Son Nhut air base during the Tet Offensive, a formal request was made for photo-reconnaissance aircraft to conduct an aerial survey of the entire base perimeter. Upon completion of this important mission, photo interpreters were able to locate 176 enemy rocket/mortar launch sites, along with a labyrinth of bunkers, trenches and associated storage areas.[110] Allied aircraft subsequently pummeled these areas and coordinated sweeps by ground forces seized several rocket emplacements and an enemy base camp. The thrill of victory was short-lived, however, as future requests for aerial reconnaissance and photo interpretation were subsequently denied due to other mission priorities. Ground defense intelligence support was nothing more than sporadic from that point forward.

Relying upon other sources of support for intelligence, base security officials turned to the Air Force Office of Special Investigations (AFOSI or simply OSI) to enhance the base defense posture. Because host-nation security forces lacked adequate training and failed to place an emphasis on offensive operations, OSI developed a program whereby they assisted the VNAF in training and developing Vietnamese sources (usually local farmers or laborers familiar with a specific area) to report information on real or potential threats to the allied air bases in the region. Despite funding and occasional information-validity concerns, this source program became one of the most fertile sources for tactical warning and base defense intelligence. As these local observers would come across insurgents moving through the area, they would attempt to covertly gather as much information as possible regarding their movements and overall intentions. Once information was obtained, it was quickly relayed to the Security Police commander and/or director of base intelligence for immediate ground assault and air strike planning. Use of local farmers and other laborers for ground intelligence also proved to be quite successful. From August 1968 through November 1969, these native

[109] Fox, 139.

[110] Ibid., 140-141.

sources generated 78.3% of all DOD Intelligence Information Reports, accounted for nearly 4,000 captured/killed VC/NVA and 300 confiscated enemy weapons.[111]

While OSI was combing the countryside for informants, Security Police commanders at Vietnam air bases also tried implementing the use of indigenous forces as intelligence sources. They paid Vietnamese civilians with cash or gifts for providing information on VC/NVA movements. While this program scored some initial successes, it never really developed, as the funding source required for paying the informants dried up quickly and was not replenished.

After informant funding sources vanished, a grassroots program called the Civil Action Program (CAP) began operating on air bases in the region.[112] This program was geared towards winning over the local populace by providing goods, services and construction projects for townspeople in hopes they would provide quality information in return. Unfortunately, the quality of reported information was often untimely, inaccurate and/or nonexistent. The Air Force personnel performing this task were untrained and were often 'volunteered' for the duty, forced to perform on their scheduled days off. Despite several significant civic action projects around Bien Hoa and Tan Son Nhut air bases, those bases came under heavy enemy attack in 1968 with no warning from the local populace; a glaring example of the program's overall deficiencies. Needless to say, this program never fully developed as anticipated.

Since lead intelligence agencies and other base defense personnel (such as the Marines) were too preoccupied to provide quality intelligence, and the local populace provided sporadic, often useless information, the SP's, out of necessity, plunged into several internally-created programs to glean the precious knowledge their ground forces were lacking. Security Police units created organic intelligence positions 'out of hide', usually consisting of one officer and one non-commissioned officer responsible for their air base and a designated geographical area surrounding it. However, while these self-generated positions did the best they could tracking enemy positions and preparing weekly intelligence summaries, they lacked the proper intelligence training that would

111 Fox, 142-143.

112 Ibid., 144

have made them efficient collectors and analyzers of local intelligence. It was not until the arrival of the SAFESIDE units that fully trained SP's with intelligence analyst training arrived in country. Unfortunately, it was too little too late, as the bulk of those units arrived just prior to the pullout of U.S forces.

Despite advancements in intelligence collection and analysis techniques, limitations and shortfalls still existed some 20 years after the Vietnam experience. Investigating commissions for the Khobar Towers incident cited the failure of intelligence assets on the ground there to provide specifics on how, when and where an attack may occur as a contributing factor in the tragic 1996 terrorist bombing of the military barracks. Retired General Downing was quoted as saying, "DOD needs to improve intelligence operations. Military officials were warned of terrorist threats to U.S. forces in Saudi Arabia, they had the time and motivation to reduce vulnerabilities, but it was not enough."[113] Downing added that despite the fact intelligence did not provide specific information, a considerable amount of threat information was available that indicated terrorists were operating in the region and that Khobar Towers was a potential target. Downing's report also claimed the Khobar base commander suffered from an inefficient intelligence chain of command, which focused almost entirely on the air threat during Operation *Southern Watch*. Downing also added tactical details were lacking due to a near absence of human intelligence assets. He recommended more people and more money funneled into that program to prevent future terrorist attacks. The Long Commission Report, commenting on the lack of human intelligence capabilities, stated they were "neither precise nor tailored to the commander's needs."[114]

While many of the findings from both the Downing and Record Reports are classified, several were listed in the unclassified version. Finding 9 from the Downing Report stated theater and national intelligence communities were deficient in their abilities to conduct in-depth trend analysis as well as determining the overall intentions and capabilities of terrorist groups operating in the region. Finding 10 cited the misapplication of threat level assessments by both the Department of State and DOD,

[113] Linda Kozaryn, "DOD Releases Report on Khobar Towers Bombing", *American Forces Information Service*, Sept 1996. Available at http://www.pentagon.mil/news/Sep1996/n09181996_9609181.html (accessed on 23 September 2005), 3.

[114] Creamer, 69.

causing confusion for the intelligence consumers at the base level.[115] Specific to Security Police units operating in the area, Finding 11 identified the lack of an organic intelligence support capability within the SP units negatively affected their ability to perform the critical base defense mission. Because Security Police units assigned to Khobar were typically not briefed on the force protection mission and current threats in the region, the Downing Report recommended an organic intelligence asset be provided to SP units performing air base missions.[116] Finding 14 described an available communications network that supported the flow of intelligence through the upper echelons of command, yet field units often lacked the proper clearances to gain access to the required information. Information is useless if the consumer, the one relying upon timely, accurate information, cannot access it due to classification restrictions.

There were also several failures on the part of OSI in relation to threat assessment information. Several OSI special agents (correctly) identified the potential for an attack from outside the perimeter, but these recommendations were never given to the installation commander. Additionally, upon completing an assessment of physical security on the base, one OSI agent recommended the construction of a blast mitigation wall to his supervisor. This information never reached the base commander because the OSI supervisor, believing the blast wall had been discussed and rejected previously; felt it was an unwarranted recommendation.[117]

Finally, while the details of another finding describing host-nation security support are still classified, it is no secret the Saudi security personnel were not only inefficient in the performance of their duties, but generally refused to act upon suggestions/recommendations or potential threat information provided by Air Force security personnel. Saudi officials were quick to point out that security at Saudi installations was inherently their responsibility, and that U.S. personnel were not allowed to extend force protection measures beyond the installation fence line. Security Police members reported numerous suspicious incidents just prior to the Khobar bombing involving reports of surveillance by Middle Eastern men and another incident involving

115 Creamer, 102.

116 Ibid., 102.

117 Record, Appendix 1, 32.

the driver of a vehicle ramming a jersey barrier adjacent to the installation. While the Saudis dismissed these reports entirely, the Security Police unit incorporated numerous internal security measures, including the posting of roof-top sentries at night and updating building evacuation plans. Despite the lack of host nation support, and their apparent disinterest in viable intelligence, it was precisely these security measures that potentially saved the lives of dozens of airmen on the night of the bombing.[118]

Despite numerous findings and recommendations following the Khobar incident, the proposed force protection enhancements discovered during the ensuing investigations never fully developed and the creation of antiterrorism and force protection guidance was slow to mature. Meanwhile, the Air Force relocated their forward operating bases from urban and residential areas to more austere, isolated locations in hopes the increased stand off distance would prevent future terrorist attacks. Yet, it was not until the horrific events of 9/11 that we realized the intelligence problem persisted throughout many military, federal and state channels. This lingering problem demands immediate resolution at all levels. Part of the ultimate solution resides with the gathering of useful and actionable intelligence from known and reliable sources.

B. SEVERAL SOURCES OF INTELLIGENCE FOR AIR BASE DEFENSE PLANNING

Transnational terrorism, rival military aggression, proliferation of weapons of mass destruction and political instability are just a few of the primary threats to our nation, our citizens, our military and our political and economic interests. In order to prepare for and prevent terrorist-related acts, intelligence must be accurate, timely and provide answers for the questions: who, where, how and when. During Korea and Vietnam, the use of informants/host nation forces and other marginal sources of intelligence often resulted in inadequate or untimely (or both) intelligence reporting. Intelligence gathering can no longer be limited to just those sources. The importance of

118 Creamer, 18-19. In his report to the President, Secretary of Defense William J. Perry summarized the event: "Shortly before 10:00 local time on Tuesday, June 25, 1996, a fuel truck parked next to the northern perimeter fence at the Khobar Towers complex. Air Force guards posted on top of the closest building, building 131, immediately spotted the truck and suspected a bomb as its driver fled the scene in a nearby car. The guards began to evacuate the building, but were unable to complete this task before a tremendous explosion occurred. The blast completely destroyed the northern face of the building, blew out windows from surrounding buildings, and was heard for miles. Nineteen American service members were killed and hundreds more were seriously injured." (Perry, 2.)

integrating all-source intelligence and analysis is the key to 'connecting the dots'. No single agency or intelligence function currently maintains all the significant information required to properly defend this nation.[119]

Traditionally (meaning prior to 9/11), terrorism-related intelligence was obtained from sources outside the United States, and typically via intelligence agencies specifically. Meanwhile, federal, state, local and military law enforcement focused on domestic issues, primarily criminal in nature. U.S. intelligence agencies traditionally collect information which is vital to the protection of this nation, while law enforcement agencies initiate arrests and attempt to collect information for criminal indictments.[120] Prior to 9/11, there was no specific or directed intelligence function for most state, local or military police entities. Ultimately, the September 11th attacks fell into uncharted territory, an area that caught both the unsuspecting intelligence and police agencies unaware.[121]

The events of 9/11 changed the rule book, and the hierarchy of traditional intelligence roles is still evolving. Buzzwords around the Pentagon and Department of Justice these days include "information sharing," "intelligence fusion" and "data mining." There are obvious advantages to sharing information, and the DOD has recognized that in recent policy transitions and recommendations for an increased role. At the micro level, and specific to air base defense intelligence planning, Security Forces units must form an unassailable trifecta with the Air Force Office of Special Investigations and the base intelligence office (IN) to ensure timely and worthy intelligence flow specific to their parent air base/surrounding area. However, Air Force base defense planners must also learn to rely upon other outside sources of intelligence in formulating their security defense and response plans. Establishing intimate working relations with federal military, law enforcement and intelligence agencies as well as adjacent police municipalities will also be part of the formula to success.

---

119 *Final Report of the National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission Report)*, (New York, NY: W.W. Norton, 2004), 408

120 Jonathan R. White, *Defending the Homeland, Domestic Intelligence, Law Enforcement and Security* (Wadsworth/Thomson, CA, 2004), 17-19.

121 The 9/11 Commission Report, 263

Leading the charge for the DOD in proactively seeking and obtaining the intelligence required for proper execution of the CONUS air base defense mission is U.S. Northern Command (NORTHCOM).[122] This rapidly developing organization is quickly blending the military into the homeland defense mission. Normally called to action under 'extraordinary' circumstances, NORTHCOM specializes in shooting down hijacked aircraft, explosive ordnance disposal, special military operations and of particular interest to Air Force base defenders, intelligence collection within U.S. borders.

Since its inception, NORTHCOM has developed cooperative, intelligence-sharing relationships with numerous federal, state and local governments. The Pentagon inspector general approved the placement of military special agents (investigators) inside the FBI's Joint Terrorism Task Forces (JTTF) all throughout the country. They are responsible for identifying threats to military communities/air bases within the cities and neighborhoods they operate in. In the formation of joint interagency coordination groups (JIACG), NORTHCOM has partnered with domestic law enforcement agencies such as the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) as well as the Federal Emergency Management Agency (FEMA) and Immigration and Customs Enforcement (ICE) to name just a few.[123] In an effort to expedite intelligence analysis and dissemination across a greater spectrum of agencies and partners, NORTHCOM also participates in a liaison exchange program with the Defense Intelligence Agency's Joint Intelligence Task Force–Combating Terrorism (JITF-CT), the Department of Homeland Security (DHS), National Counterterrorism Center (NCTC), Coast Guard and National Guard Bureau. Through the numerous coalitions NORTHCOM participates in, air base defense planners have access to an exponentially greater volume of useful and actionable intelligence than they did in previous eras. Additionally, through the implementation of expansive technology, intelligence consumers, such as Security Forces, are able to access

[122] Established in 2002 and fully operational in 2003. The first combatant command with sole responsibility for defending the country's borders and providing military assistance to civilian authorities, its primary mission remains deterring, preventing and defeating terrorist threats and/or aggression in the United States.

[123] Harold Kennedy, "U.S. Northern Command Actively Enlisting Partners", *National Defense Magazine*, June 2004, 1.

NORTHCOM anti-terrorism intelligence products on the NCTC's website creating a real-time, nationwide, on-line display of potential threats and vulnerabilities specific to their areas of concern.[124]

While much of the information used to support air base defense planning comes to NORTHCOM via the FBI and CIA, another source of information is the Counterintelligence Field Activity (CIFA). Created in 2002, their charter is to protect Defense Department personnel and infrastructure from terrorism and espionage.[125] Coming as a surprise to some, they collect and analyze intelligence and perform operations not only abroad but also within the United States. Much is not known about this agency whose expenditures and overall size remain somewhat secretive. What once was simply an agency responsible for oversight on military counterintelligence, has become a living, breathing entity consisting of nine directorates and in increasing scope of authority.[126]

CIFA's Directorate of Field Activities is a vital player in demonstrating the growth of Pentagon activity within our borders. In addition to preserving critical military assets via roving patrols and surveillance of threatening personnel inside the United States, they can provide real-time intelligence support in hostile areas around the globe to protect military forces and infrastructure from terrorist threats. Another CIFA directorate, the Counterintelligence and Law Enforcement Center, categorizes and measures potential threats to DOD personnel and infrastructure from foreign intelligence services and clandestine terrorist organizations.[127]

Although their methods may be somewhat controversial, CIFA manages and maintains several critical terror information databases. One such database is dedicated solely to collecting and analyzing Threat and Local Observation Notices (TALONs), which includes information obtained from Security Forces and/or OSI investigators

[124] Timothy J. Keating, Statement before the Senate Armed Services Committee on 15 March 2005, 12. Available at http://armed-services.senate.gov/statemnt/2005/March/Keating%2003-15-05.pdf (accessed on 18 September 2006).

[125] Walter Pincus. Pentagon's Intelligence Authority Widens, Fact Sheet Details Secretive Agency's Growth From Focus on Policy to Counterterrorism. Washingtonpost.com (accessed on 19 December 2005).

[126] Ibid., 1.

[127] Ibid., 1.

involving possible terrorist activity on or around their air bases.[128] Another, somewhat more delicate database, involves a 'data mining' operation consisting of a large data sets of public records, intercepted communications and other 'actionable intelligence'.[129] CIFA's Assessments and Technology Directorate quickly analyzes this information and shares it with federal, state, local and military law enforcement agencies. While the data lists are living, breathing documents, hundreds of foreign terrorist suspects operating inside the U.S. remain in this database.[130] Recently, DOD authorized CIFA to formulate and task domestic investigations and counterintelligence operations to various military services with the purpose of centralizing all counterterrorism intelligence collection activity. This will allow CIFA to designate criminal and counterterrorism missions for over 4,000 Army, Navy and Air Force investigators.

AFOSI, which has increasingly been involved in terrorist threat detection and deterrence, has approximately 2,000 agents home and abroad and routinely partner with Air Force Security Forces units in criminal investigations and anti-terrorism planning.[131] Greater cooperation between intelligence and law enforcement/security allows for not only more proficient follow-up investigation, use of resources/time, but ultimately increases the number of potential intelligence trails each agency can monitor.[132] When AFOSI shares threat information with Security Forces (or vice versa), superfluous information is often eliminated, resulting in more efficient and timely base defense

---

[128] Deputy Secretary of Defense Paul Wolfowitz called for the creation of the TALON program, a DOD reporting mechanism designed to capture raw and non-validated reports of suspicious activity. NewsMax.com, Report: TALON to Gather Suspicious Information for DOD, June 30, 2003. Available at http://www.newsmax.com/archives/articles/2003/6/29/204152.shtml, 1, (accessed on 19 July 2006).

[129] William M. Arkin, "Mission Creep Hits Home; American Armed Forces are Assuming Major New Domestic Policing and Surveillance Roles", *Los Angeles Times*, 23 November 2003, 3.

[130] Ibid., 3.

[131] Pincus, 2.

[132] Rebekah Bina and Caroline Nicolai, *The Legal Framework in U.S. Law for Sharing Law Enforcement and Intelligence Information*, Background Paper from Syracuse University's Institute for National Security and Terrorism (INSCT). Available at: http://insct.syr.edu/Research%20and%20Events/Res&Activities_2004ConfProgram.htm, 7-8, (accessed on 24 July 2006). Additionally, RAND reports 64% of officers surveyed cited more/better intelligence information on threats and terrorist activity in their regions/jurisdictions as what they needed to improve their response capabilities, (Riley, K. Jack, et al, *State and Local Intelligence in the War on Terrorism* (Santa Monica, CA: RAND, 2005).

.

planning. This enhanced partnership is remarkably better than the AFOSI/Security Forces relationship that existed during the Vietnam and Khobar Towers periods.

With a growing emphasis on shared intelligence and participation in intelligence fusion centers such as the NCTC, JTTF's and the CIA's Counterterrorist Center (CTC), it is imperative Air Force Security Forces stand ready to implement policies and directives geared towards accomplishing this new joint mindset. Fusion centers, at state and federal levels, continue to emerge as communities attempt to establish anti-terror coalitions. There are now over 100 JTTF's located across the country, with plans to develop additional centers in the future.[133] With an increasing role of DOD personnel participating in or maintaining positions on several of these fusion centers, the possibility for obtaining timely and valuable base defense intelligence increases dramatically. No longer do the base defense planners have to wait (or pay) for information, typically inaccurate or insufficient, to trickle down to them from paid informants or host nation forces.

The unwillingness to share information or work collaboratively towards a common goal proved quite costly in Vietnam and at Khobar. Today, with Security Forces obtaining much of the intelligence required for base defense planning through both federal and civilian law enforcement/intelligence channels, it is imperative this relationship remain vibrant and openhanded. Security Forces planners should expect an increasing role in the processing, commingling and application of useable intelligence as relationships with these valuable intelligence sources continues to develop. One way in which this merger is evolving is through the use of computer database programs and shared real-time information between consumers. Security Forces and other base defense planners play a vital role in performing this function.

C. THE JOINT PROTECTION ENTERPRISE NETWORK (JPEN) AND SECURITY FORCES' ROLE IN INTELLIGENCE SHARING

The National Strategy for Homeland Security calls for information sharing across all levels of government, particularly through the use of computer databases allowing for all (authorized) agencies to tap into current and developing information as it is collected

[133] Remarks from speech to International Association of Chiefs of Police, John Negroponte, Sept 27, 2005. Office of the Director of National Intelligence website. Available at: www.dni.gov/inter_assc_chiefs_police.shtml, 1 (accessed on 23 September 2005).

and analyzed.[134] The document also recommends "…Homeland security intelligence and information must be fed instantaneously into the Nation's domestic anti-terrorism efforts. Those efforts must be structured to provide all pertinent homeland security intelligence and law enforcement information—from all relevant sectors including state and local law enforcement as well as federal agencies—to those able to take preventive or protective action."[135]

The evolving nature of the terrorist threat and its ability to affect portions of society previously thought to be impermeable has resulted in greater demands for sharing information and intelligence. Developing technologies, capable of exponential information processing are being developed and implemented across all levels of government to help in the terror battle. Simultaneously, methods to categorize and access (data mine) this material are being developed that will combine the strengths of both the intelligence and law enforcement/military communities, and provide the functionality and necessary availability to those "sworn to defend" at every level of government.[136]

Data mining databases have been designed and/or incorporated into mainstream intelligence gathering such as DARPA's Total Information Awareness (TIA) system which was ultimately shelved due to its alleged controversial foundations[137] and DIA's Joint Intelligence Task Force Combating Terrorism database. According to an Associated Press article, police and other government security workers have come in direct contact with over 6,000 suspected terrorists over the past 28 months.[138] Many of these suspected terrorists were identified operating on or near military installations or infrastructure. A list of over 200,000 names containing known or suspected terrorists is maintained by the Terrorist Screening Center (TSC), who serves as an advisor for law

134 George Bush, *National Strategy for Homeland Security*. Washington, D.C.: Office of Homeland Security, July 2002, xi.

135 Ibid., 16.

136 Bert B. Tussing. 2004. Sharing Information for Homeland Security: Overcoming Obstacles of Technology, Process and Culture. Obtained from Internet at http://www.cusa.uci.edu/op3.htm, [19 September 2006], 16.

137 DARPA stands for Defense Advanced Research Project Agency. Critics of the program felt the database reached into areas unrelated to counterterrorism, pervading individual expected rights of privacy.

138 Helena Independent Record, "200,000 People in U.S. Terror Suspect Database, Director Says", *Associated Press*, 15 March 2006, 1. Available at: www.helenair.com/articles/2006/03/15/national/a05031506_01.txt, (accessed on 12 June 2006).

enforcement personnel on managing this type of data and how to engage personnel on the list when/if they encounter them.[139] Managed and implemented effectively and within the boundaries of the law, terrorist databases can play a key role in Security Forces' antiterrorism and IBD effectiveness.

In the past, AFOSI, the base Intel office and Security Forces personnel would find themselves on their classified work stations searching through dozens of websites trying to locate a single piece of interesting and/or useable data. Often when applicable information was finally located, it was compartmentalized (a widely-practiced pre-9/11 phenomenon), and not properly analyzed or distributed to those on the front lines who required it. With technology evolving on both sides of the playing field, it is imperative military leaders/planners are able to quickly 'connect the dots' of air base intelligence, and preferably from a single source.[140]

Effective 1 February, 2006, NORTHCOM mandated the use of the Joint Protection Enterprise Network (JPEN) for all military bases falling under NORTHCOM's chain of command. This web-based interactive tool serves as an intelligence source for all NORTHCOM military installations allowing for the collection and dissemination of suspicious activity reports (SAR) in an effort to deter, prevent and defeat threats and aggression aimed at the United States. JPEN is an interactive web-based network that provides near real-time sharing of invalidated (unclassified) force protection information to all participating DOD installations. The desired end state is for every DOD installation and facility within NORTHCOM's area of responsibility to have access to this system and routinely participate by entering collected SARs into the system.[141] While this section is not intended to be a JPEN user's manual, it is intended to demonstrate JPEN's various capabilities and procedures corollary to existing Security Forces' functions as well as demonstrate the system's potential capabilities in enhancing and executing the IBD mission.

---

139 Helena Independent Record, 1.

140 Elaine Grossman, "Combat Commanders Make Broad Access to Intelligence a Top Priority", *Inside the Pentagon*, 9 February 2006, 1-3.

141 USNORTHCOM/J34, *USNORTHCOM Joint Protection Enterprise Network Concept of Operations, version 2.1*, 23 August 2005, 5. Currently, USAFE and PACAF bases do not have the JPEN system due to funding limitations.

While any military member or civilian, either on or off the military installation, can report SARs or potential threat data, Air Force Instruction 10-245 stipulates the three primary installation focal points for gathering threat data are the Installation Antiterrorism Officer, Security Forces and AFOSI.[142] Coincidentally, these three entities also serve as the primary collection points for JPEN threat data from around the installation and servicing community. The Antiterrorism Officer, working directly for the installation commander, is responsible for collecting and entering antiterrorism/force protection (AT/FP) events from other Threat Working Group (TWG) members from around the installation.[143] Security Forces personnel will enter JPEN data via the terminal located in their Security Forces Control Center (SFCC) which is the equivalent to a civilian 911 dispatch center, and where JPEN is monitored 24 hours a day. Finally AFOSI personnel collect AT/FP observations, including *Eagle Eyes* reports (covered later in this section), and enter them into JPEN as appropriate. Wolfowitz stated TALON reports, initiated by concerned citizens and military members (verified and authored by AFOSI) would include surveillance of DOD facilities/air bases, tests of security and elicitation attempts.[144] The information contained in a TALON report may be incomplete or unverified, but the goal of the program is to provide rapid reporting thereby allowing near real-time access of potential probes or surveillance to authorized participants of the program. On the other end of this process, CIFA collects and analyzes JPEN and TALON information via a daily report for potential networking throughout the counterintelligence community, particularly with JITF-CT.

By providing a database for local and regional trends pertaining to potential terrorism threats and force protection issues, JPEN provides an additional source of information for installation threat analysis.[145] In particular, the Security Forces role in this process is to partner with AFOSI in analyzing JPEN data to determine specific vulnerabilities, trends and possible mitigating factors. Tactical users of the system, such

[142] Air Force Instruction 10-245, *Air Force Antiterrorism Standards* (Washington, D.C.: HQ Air Force, June 2002), 16.

[143] The TWG is the installation commander's primary advisory body for assessing the local threat and recommending courses of action to mitigate potential threats.

[144] NewsMax.com, Report, 1.

[145] Headquarters, United States Air Force, (Air Force Inspection Agency), *Joint Protection Enterprise Network Eagle Look Report* (Washington, D.C.: HQ Air Force, November 2005), 27.

as Security Forces members or contracted security personnel guarding the installation gates can monitor the system at the same time strategic decision makers view the same data. Security Forces-specific information required for JPEN entries include what are called Force Protection Event Categories such as Be On the LookOut (BOLO) and vehicle turn arounds; both primarily handled at installation entry gates. Such a tool, if the technology were available during the Vietnam era, would have allowed for base defense planners to track and identify specific and reoccurring trends involving VC/NVA stand-off attacks and plan countermeasures accordingly.

JPEN would not be a significant or useful tool if its real-time data was not made available to those charged with managing and controlling crisis situations. Therefore, NORTHCOM plans to link JPEN into Department of Homeland Security, Department of Justice and local law enforcement data systems to enhance the information sharing partnership.[146] Additionally, JPEN is intended to assist military commanders in meeting their antiterrorism and force protection (FP) responsibilities by disseminating FP information in a timely fashion both horizontally (with other installations) and vertically (up and down the chain of command).[147]

With the JPEN program and its implementation at NORTHCOM installations a fairly recent requirement, the overall impact of this program remains to be seen. However, in support of NORTHCOM's overall AT/FP mission, JPEN offers an opportunity to share information throughout DOD and other participating agencies unlike any seen in past decades. Competency, accuracy and timeliness of reporting are crucial elements of intelligence sharing and the interface process missing in days past and are required to make JPEN a successful venture for air base defense planners.

D. RECOMMENDATIONS

The information sharing challenges illustrated by intelligence failures in Korea, Vietnam and Khobar Towers, and more recently, by the 9/11 terrorist attacks, illustrate the requirement for faster and more integrated information sharing capabilities between

146 Headquarters, United States Air Force, (Air Force Inspection Agency), *Joint Protection Enterprise Network Eagle Look Report*. The Department of Homeland Security's data network is the Homeland Security Information Network (HSIN), while the Department of Justice's networks include Law Enforcement Online (LEO), Regional Information Sharing System (RISS) and Multi-State Antiterrorism Information Exchange (MSAIE). 31.

147 Ibid., 29.

federal, state and local authorities. In an effort to 'break down the walls' and 'connect the dots', Security Forces commanders, both stateside and deployed, must proactively seek quick and efficient methods of gaining the actionable intelligence required to perform the IBD mission. In an effort to ensure the success of the JPEN program as well as the daily fulfillment of intelligence requirements, SF policy makers and planners should follow several recommendations:

1. An antiterrorism initiative called "Eagle Eyes" was developed by AFOSI and has built foundations all around the world. The program encourages Air Force members and local citizens to report possible terrorist planning activities observed during normal daily interactions. The program also provides for rapid follow-up investigations and information sharing at all levels of Air Force command as well as with interested law enforcement agencies. Recently, OSI detachments and Security Forces squadrons joined together to establish local reporting procedures for effective implementation of this program. Security Forces' participation in this program is vital, as most suspicious activity is reported via the SFCC. The Integrated Base Defense doctrine relies upon 'sensors' or people reporting information, from areas both on and off the air base. Once a call comes into the SFCC, the SF representative must notify AFOSI for possible follow up investigation and/or a joint security response to the scene.

Proper promotion and integration of the Eagle Eyes program (or any similar programs under different names) is also vital to ensure the local community understands the program's reporting criteria. Newspaper articles, leaflets, website information and SF/AFOSI publicity methods make the community aware of the program while simultaneously informing them which types of activities normally qualify as suspicious.[148] Security Forces members would do well to promote this program and its many benefits to the populace occupying the areas around their defended positions. Whether it is a rural area adjacent to a stateside military installation or an urban area located near a remote air base in another region of the world, getting the local populace to report

[148] Typically, Eagle Eyes reporting criteria are very similar to TALON reporting. Surveillance, elicitation, tests of security and other suspicious incidents are commonly reported.

accurate and timely information (something missing from the Korea/Vietnam era) only benefits the air base defense mission.

2. Security Forces members can promulgate an information sharing environment through the use of an effective and well-known crime deterrent method called community policing. Engaging with the younger crowds at the Youth Centers and base sporting events provides an outlet for children/adolescents to report any observed suspicious activities. Additionally, setting up information booths at the Base Exchange during National Night Out and National Police Week provide useful outlets for information dissemination to the base community. By establishing a community policing 'hub' or office within base housing, SF units not only provide a sense of ownership in the crime/terror fighting process, but an environment where base residents can establish a relationship with their base police.

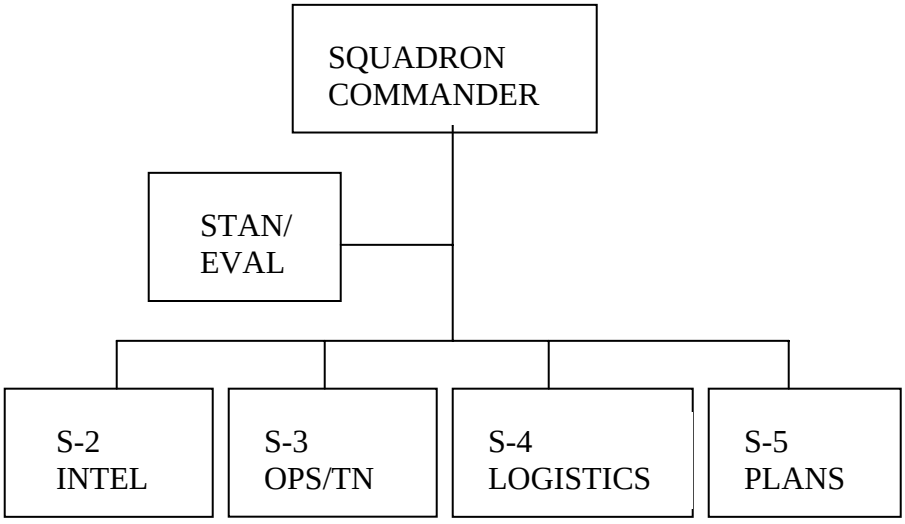
3. Intelligence briefings offered by the wing intelligence unit and/or AFOSI remain constants in the intelligence and information collecting and sharing process. Regularly scheduled intelligence briefings given to both Security Forces leadership and junior enlisted members offer the opportunity for both strategic planning and operational enhancement. While these intelligence briefings typically focus on international events and terrorist planning activity, interpreted data can be incorporated into daily SF functions. SF commanders and leadership owe it to their troops patrolling the perimeter, searching commercial vehicles entering the installation or working the primary installation entry points to provide them with accurate and timely information pertaining to their relative assigned duties (particularly during contingency operations and/or elevated threat conditions.)

4. SF commanders (or a designated representative) should log onto the Secure Internet Protocol Router Network (SIPRNET) on a regular basis to review and potentially acquire threat-related data pertaining to their air base defense mission. Several key sources on the SIPRNET generate daily reports pertaining

to specific areas, several of which could prove to be useful in determining policy or plans to counter potential threats.

5. As of this writing, Security Forces squadrons are in the midst of a reorganization in regards to their overall structure and composition (Figure 2). They have recently received approval to align themselves into the "S" function staff structure. The "S" function configuration potentially standardizes the overall SF structure in both home station and deployed environments. This is yet another example of how SF units can internally manage intelligence data and requirements using organic assets. Although attempted (unsuccessfully) during the Vietnam era, SF commanders must now ensure they utilize this new asset for enhanced collection and dissemination of intelligence related to each unit's overall force protection mission.

Figure 2. Proposed Security Forces Squadron Structure



6. SF commanders must continue to actively participate in and encourage proactive action in various physical security and force protection-related planning groups such as the Threat Working Group, Force Protection Working Group and Installation Security Council. All of these groups are required per Air Force Instructions, yet they are often eyewash and only meet to

satisfy the requirement. SF Commanders and Installation Antiterrorism Officers must promote positive groupthink and the solicitation of potentially groundbreaking methods of securing their installations. During potential or actual contingencies, SF commanders should possess current threat data and intelligence to assist in the development of potential countermeasures and/or to advise the installation commander on potential actions to be taken.

7. While it may not always be logistically of fiscally feasible to maintain a permanent SF presence in many of the fusion centers located around the country, a working, functional relationship should be sought between SF members and those with seats at the fusion centers. If a SF unit is unable physically to send a representative to these fusion centers, SF units should be added to DHS and JTTF mailing lists for their security and information bulletins. At a minimum, SF units should work to develop a strong and functional relationship with both local and federal police jurisdictions within their area of operation (including joint planning, exercises and training.)

Timely and efficient intelligence is critical to determining the overall threats to the air base, its personnel and war fighting components. Working together with their AFOSI and intelligence counterparts, Security Forces play a vital role in a typical AF installation's force protection triad. Thorough integration and active participation in programs such as Eagle Eyes, JPEN and intelligence fusion centers can and do enhance an installation's overall security posture. The old cliché "knowledge is power" is only true these days if it is knowledge shared.

Useful and actionable intelligence is useless unless it is applied quickly and efficiently. One area where base defense planners failed in the past and need to improve upon for the future is applying known threat and associated vulnerability intelligence to the protection of their critical infrastructure (CI) and resources. Possessing actionable intelligence is useless if you do not have the infrastructure and assets to execute offensive and defensive countermeasures. Chapter V explores how mistakes involving CI were made in the past and how Security Forces play a fundamental role in defending these resources, vital to the proper implementation and execution of IBD.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CRITICAL INFRASTRUCTURE PROTECTION

> *The majority of bases do not have a positive approach or active planning program for the protection of their operational assets…There are no criteria established for the construction of air bases in a combat environment.*
>
> *Seventh Air Force Base Defense Study Group, 1967.*[149]

The execution of many war fighting missions relies upon the functionality and availability of critical infrastructure and associated key assets. In the past, base defense planners often overlooked the importance of proper siting and/or sufficient security resources assigned to defend them. With the ongoing mission in the Middle East, air bases are being constructed in some of the most hostile parts of the globe. Closer to home, the threat of violence and attacks on stateside bases remains a constant and ever-present threat. In the midst of all of this, the proper defense of critical military infrastructure and assets remains one of the highest priorities for Security Forces. This chapter describes some of the earlier doctrinal and procedural errors executed during the defense of various critical infrastructures on bases in Korea, Vietnam and at Khobar. It also briefly describes the Department of Defense and Air Force Critical Infrastructure Programs (CIP) and Security Forces' role in executing those important missions within the IBD arena.

A. EARLY POLICY ERRORS AFFECTING AIR BASE DEFENSE

An examination of Air Force air base defense history exposes a doctrine with an apparent short attention span for the protection of air bases and associated critical infrastructure against ground threats, particularly those of an asymmetric or unconventional nature. After Korea and Vietnam, the Air Force reduced security manning and paid little attention to an air base defense doctrine repeatedly found wanting, especially post-Vietnam. As a result, a lack of continuity for security operations developed and carried over into the Khobar attack which ultimately caused an awakening for the protection of both personnel and priority assets and infrastructure at air bases in the far corners of the world as well as those within our own borders.

[149] Fox, 55.

Prior to entering the war in Korea, the Air Policemen mission consisted mostly of preventing thievery, pilferage and trespassing on its stateside bases. Protection of critical assets and infrastructure was not a primary concern for them, and this mission-focus carried over into Korea. Since the Air Force had only recently split from the Army Air Corps, many Air Force leaders felt that since installations were typically located in the Army's defended rear area, it was the Army's responsibility to defend them. A full year into the Korean conflict, the Air Staff and other military leaders were receiving reports from the field that the Air Force still had no viable air base defense doctrine. In the Air Force's first attempt at base defense guidance, *Air Force Regulation 355-4* directed Air Force installation commanders to deny enemy access to buildings, facilities, equipment and other critical infrastructure. While this early attempt to identify and defend key assets sounded good in theory, it called for security response only in emergencies and did not include guidance for "sustained ground defense operations."[150] Air Force security members were fortunate their inadequate base defense doctrine was mostly unchallenged by Korean guerrillas operating in the area. Critical infrastructure, including aircraft, barracks and fuel/weapon storage areas would have undoubtedly been lost during enemy attacks.

After Korea, 'containment' became the buzz word in defense policy. Controlling, or containing communism was the primary objective, and air base defense took a backseat to the prevention of or preparation for massive nuclear annihilation. Security doctrine designed for safeguarding our nuclear stockpiles and associated facilities became the primary focus, and while vital combat equipment and nuclear-related critical infrastructure were well defended, preparation for the defense of peripheral infrastructure, still vital to the mission, remained undeveloped.

In an effort to expedite the introduction of U.S. air assets into the Vietnam region, abandoned air bases, formerly used by the French regime during their occupation and located in densely populated areas, were resurrected and became primary U.S. airfields. Many dwelling areas, located adjacent to base perimeter fences laden with holes and excess vegetation, offered uncontrolled access points and tactical cover and concealment

[150] Headquarters Air Force, *Air Force Regulation 355-4*, 5.

for guerrillas moving about the area. These population centers near the base also prohibited security personnel from deploying landmines, trip flares and other warning mechanisms outside the perimeter fence. The expansion of several air bases also forced the relocation of numerous villagers that previously resided in those areas and who due to their religious customs, required repeated entry onto the air base for various familial or ceremonial rituals. Security personnel, forced to escort these villagers and sweep for mines/bombs after their departure, were unavailable for normal security duties, further exposing infrastructure on base to ensuing enemy guerrilla attacks.[151]

The rapid buildup of forces and assets in the region also saturated the few operational bases U.S. forces had occupied. During the heaviest fighting, 76% of all coalition aircraft and 60% of U.S. aircraft flew sorties from these target-rich air bases.[152] Inadequate placement and protection of munitions and jet fuel, combined with the construction of major military headquarters units on these bases made them even more lucrative targets to the guerrillas operating in the region. The improper siting of these resources ultimately forced the Air Force to dedicate additional security personnel to defend them, an asset already in short supply.[153] Air Force security officials continuously demonstrated a genuine disinterest along with improper planning in the placement of critical infrastructure and other war fighting resources in a combat area. Alternate placement, with collaborative security and manpower considerations, could have simplified security operations and should have been executed.

With air bases defended by indigenous forces early on in the Vietnam conflict, U.S. war fighting assets were often entrusted to host nation forces with limited oversight provided by U.S. military liaisons in the area. Additionally, instead of focusing on the more relevant and pressing counterinsurgency doctrine to defend Vietnam air bases, Air Force security remained focused on the Soviet saboteur threat—concentrating on the interior portions of the air base while host nation forces patrolled the exterior. The host nation relationship with the Vietnamese Air Force (VNAF), tumultuous at best, prevented

---

[151] Fox, 60-63.

[152] Ibid., 63.

[153] At several forward operating bases, fuel tanks and bladders were placed 30-50 feet inside the base perimeter, making them prime targets easily struck by stand-off or small arms weapons.

Air Force security personnel from properly defending their own critical war fighting aircraft, usually parked wingtip to wingtip and laden with war fighting munitions. Instead, this misguided security emphasis left them to focus on non-critical infrastructure and assets. The VNAF exercised ownership rights and control over construction and placement of all new buildings, airfields and infrastructure on Vietnam air bases, often denying or delaying requests. These delays and deviations from original security and logistical planning often caused U.S. forces to develop alternate and typically less secure plans.

With little apparent thought given to their strategic placement, various critical infrastructures, vital to war fighting efforts, were sited in non-tactical locations and/or were often left unprotected. Critical electric power plants and generators, used by command centers and for aircraft navigational aids, were often not assigned designated security personnel, and due to poor planning were typically located in close proximity to one another. Additionally, munitions areas and fuel tanks/bladders were often located and stored on or adjacent to aircraft parking areas, causing the potential for explosive and cataclysmic problems for both personnel and aircraft. Command posts, communication centers, aircraft maintenance and civil engineering control centers, all vital nodes in the war fighting effort, also lacked proper blast and fragmentation mitigation measures. Many key operating facilities and mass-gathering areas also lacked the proper shielding and roof structures required to withstand direct enemy rocket attacks. Finally, critical recovery vehicles such as those used for fires and crash damage control were often left non-dispersed and unprotected in open areas.[154] Continuous enemy attacks on unprotected critical infrastructure led some officials to believe something must be done.

Despite several efforts to shore up physical security using hardened aircraft revetments/shelters, vegetation removal and much-needed perimeter lighting, the 81-mm mortar and recoilless rifle attacks of the enemy continued to wreak havoc on U.S. airfields and aircraft. On April 13, 1966, Tan Son Nhut, a major operating base in the region and the only Air Force air base yet to be attacked, was struck by an enemy mortar

[154] Fox, 64-67.

and rifle barrage. Thirteen minutes and 245 rounds later, 62 aircraft were damaged or destroyed as well as the loss of 34 vehicles, a 420,000-gallon fuel tank and significant portions of the runway.[155]

In total, repeated guerrilla attacks by the Viet Cong and North Vietnamese Army on U.S. air bases led to the overall destruction of 1,269 U.S. and Vietnamese aircraft on the ground, more than were downed by enemy MiGs in air-to-air combat.[156] The majority of these 475 air base attacks involved the enemy's use of stand-off weapons from just outside the perimeter of the air base while Air/Security Police concentrated on less critical infrastructure located in the interior portions of the base.[157] The highly disciplined VC/NVA had found a way to continuously exploit Air/Security Police security doctrine by striking safely from a distance and always at self-imposed locations and frequencies.

Fast forward approximately 20 years and we find the Air Force Security Police fighting a similar kind of enemy in a different part of the world. The tragic bombing of a military barracks at Khobar Towers, located near Dhahran, Saudi Arabia, left 19 servicemen and women dead and another 200 wounded from the enormous blast and exploding debris. Despite selfless acts of professionalism and courage on the part of several Security Police members, numerous operational and planning deficiencies indicate military planners were unaware of the risks posed to U.S. service personnel serving in Saudi Arabia. The brutal attack on Khobar Towers on June 25, 1996 "exposed the risks to U.S. military personnel deployed to foreign countries with various cultural sensitivities for contingency operations."[158]

The Khobar Towers complex, originally designed by Saudi developers to provide shelter to the local Bedouins, was offered up to the Americans by the Saudi government to provide housing and operational areas for military personnel involved in Operation

[155] Hettinga, 43-44. Tan Son Nhut was a command center for a Marine Amphibious unit who provided primary security for the base, while Air Force security patrolled approximately 10% of the base perimeter.

[156] Vick, 68-69. 99 fixed-wing U.S. aircraft were destroyed on the ground versus 62 in the air.

[157] Ibid., 68.

[158] Floyd Spence, Chairman, House National Security Committee, *The Khobar Towers Bombing Incident: Staff Report* (Washington, D.C.: National Security Committee, 14 August 1996), executive summary.

Southern Watch. The location of the complex, deep in the middle of an urban environment and surrounded on all sides by residential and commercial facilities, posed operational security challenges regarding the placement of perimeter fencing and other physical barriers. Security Police officials highlighted this potential vulnerability, yet the perimeter fence adjacent to the largest military barracks in the compound was a mere 85 feet from the building.[159] Yet another perimeter fence, delineating civilian and military housing areas ran directly down the middle of a four-lane highway.

In response to the bombing of the Saudi Arabian National Guard building (killing five Americans) in Riyadh in 1995 and numerous reports of enemy surveillance or suspicious activity, several security enhancements were ordered for Khobar Towers. Concrete barriers were placed along the perimeter of the compound and guards were added to the rooftops of taller buildings. Despite these and other modifications, the base leadership continued to focus on a vehicle-borne improvised explosive device (VBIED) entering the base through a primary installation entry point in a penetration style of attack. Less emphasis was placed on a stand-off or other unconventional type of attack coming from outside the perimeter.

Much like the experience in Vietnam, interaction and coordination with host nation forces was often a daunting and unsuccessful venture. Requests to move the perimeter fence adjacent to the north end of the base and closest to one of the largest U.S. barracks met with Saudi resistance. The Saudi government, renowned for bureaucratic delays, mismanaged processes and non-expeditious action, stated expansion of the fence would limit available parking for a nearby mosque and the stand-off distance was more than sufficient for a car bomb similar to the one used earlier in Riyadh. Challenges arose regarding operational security matters and host nation security action/involvement. The presence of U.S. military personnel tested the cultural and religious beliefs of many local residents. With trees and other vegetation growing along the perimeter fence allowing enemy movements and surveillance, U.S. officials asked the Saudi government to cut it back. Fearing an increased exposure of U.S. servicewomen wearing short pants and/or driving around the compound, the Saudi government refused the request. In response, the

[159] Spence, 3.

U.S. military asked for an increase in external Saudi patrols coupled with random inspections of vehicles outside the perimeter. Once again, the Saudis were indifferent to this request.

Several internal force protection recommendations and countermeasures regarding a potential stand-off attack were also overlooked. Because both the Office of Special Investigation and Security Police threat and vulnerability assessments failed to identify the expansion of the perimeter fence, this measure was not pursued with the sense of urgency it should have received. Similarly, while focusing on the threat of a car bomb penetration attack, the placement of Mylar on barracks' windows and/or the relocation of military personnel housed closest to the perimeter fence were not the primary focus of enhancement efforts.

After the dust settled, policy makers and defense planners in Washington demanded answers. While it is undoubtedly easier to evaluate mistakes or policy implementation errors made after the fact, several committees were swiftly created to investigate potential mistakes and develop after-action reports. The two pertinent reports associated with the Khobar incident were the *Downing Report*, a product of the Downing Assessment Task Force and the follow-up to that report, the *Independent Review of the Khobar Towers Bombing*, conducted by Lt Gen James Record. Their recommendations associated with their list of findings were designed in the hopes of preventing atrocities such as Khobar from happening in the future. In regards to critical infrastructure and its protection, both reports agreed on several findings regarding general and physical security. First, critical military facilities should be located in secluded areas whenever possible and such structures should be physically hardened based on appropriate threats. Next, in regards to large-scale VBIED's and other similar explosive attacks, stand-off distances and blast mitigation measures need to be considered and implemented whenever possible. The reports recommended using enhanced barriers to shield and protect specific critical infrastructure. Finally, vulnerable facilities should be relocated to more secure, U.S. controlled environs whenever possible, and concrete barriers and other obstacles should be employed around vulnerable compounds and structures.[160]

[160] Downing, abstract of findings. Record, 7-10.

As one steps back and examines the policy and procedural errors made during all three periods of time, it is apparent that adequate examination into the vulnerability of critical infrastructure and assets, particularly aircraft, fuel and munitions storage areas were not explored, particularly during the Vietnam conflict, leading to the loss of nearly 1,300 aircraft and other valuable, war fighting equipment.[161] Nor was the continued use of the military barracks at Khobar Towers, located dangerously close to the perimeter fence, a positive example of weighing all available information, including vulnerabilities and the known threats. With the current and predicted expeditionary nature of the DOD, its assets and personnel will continue to be parceled to all corners of the globe. As a result, funding and the requisite security assets deemed necessary for the protection of its critical infrastructure remain a HD/LD problem.[162]

As Shlapak and Vick stipulate, our future adversaries are no match for our military superiority and thus would avoid large-scale conventional attacks on military installations and infrastructure. Instead, our future enemies will undoubtedly continue to use asymmetrical and unconventional methods to attack high-value assets critical to USAF operations.[163] Air Force Security Forces personnel must play a vital role in the defense of critical infrastructure and associated critical assets through both the Defense and Air Force Critical Infrastructure Programs.

B. DEPARTMENT OF DEFENSE CRITICAL INFRASTRUCTURE PROGRAM (DCIP)

Certain infrastructure deemed critical to the defense of the nation, otherwise known as National Defense Infrastructure, such as missile sites, electrical generation plants and military air bases, could cause severe and/or permanent mission degradation if destroyed or incapacitated. The Department of Defense must stand ready to rapidly identify and respond to potential threats to not only the nation's infrastructure, but also infrastructure specific to DOD missions and functions. Additionally, the DOD must stand ready to prevent or limit the overall effects of a terrorist attack and recover from

161 Vick, 68-69.

162 High demand-low density.

163 Shlapak and Vick, 15.

ideally limited numbers of threats or attacks.[164] While denying our enemies any unforeseen advantages, protection of this infrastructure (both domestic and foreign, public and private) also allows for the planning, mobilizing, deploying, executing and sustaining of military operations around the world.

During the Cold War, the U.S. military came to rely on and focus all energies on specific enemies through military or diplomatic measures. This balance of power was able to keep most non-state actors in check for over 40 years. Today, things are dramatically different. Enemies of the U.S., the sole remaining hegemon, know better than to take on our military conventionally in some form of direct combat situation. Rather, through unconventional or asymmetric methods, they seek targets with high symbolic value or those which may garner massive media coverage. As numerous researchers and theorists indicated in Chapter III, military resources (air bases and other assets) clearly have high symbolic value. Destruction or disruption of these assets promotes tremendous support amongst the terrorists' constituency, while perhaps simultaneously hurting the American public's morale. Successful attacks on these targets domestically may also distract war planners and policy makers from ongoing missions in the Middle East.[165]

While complementing other DOD CI programs, the DCIP is designed to provide solutions for identified vulnerabilities within the defense industrial base. This process will be accomplished using a familiar methodological approach of identifying, prioritizing and assessing defense critical infrastructure, while simultaneously developing plans and procedures to minimize any associated and potential risks. Should an attack or event occur, and critical infrastructure within the sector is lost or degraded, the DOD must have procedures in place to restore capabilities and support consequence management.[166]

---

[164] Headquarters, United States Air Force, *Homeland Operations, Air Force Document 2-10* (Washington, D.C.: HQ AF, 21 March 2006), 35.

[165] Hoffman, et al, *Trends in Terrorism*, 16; Shlapak, 15; Drew, 3; Bruce Hoffman, Matthew Levitt and Daniel Benjamin, "The War on Terror in the Shadow of the Iraq Crisis," p. 2-3; Wilkinson, *Terrorism versus Democracy*, 208.

[166] Headquarters, United States Air Force, *Air Force Policy Directive (AFPD) 10-24: Air Force Critical Infrastructure Program (CIP)* (Washington, D.C.: HQ Air Force, 28 April 2006), 2.

Because DOD assets and other military infrastructure remain such lucrative terrorist targets, effective implementation of DCIP is tremendously important. However, in order to exploit the core capabilities of precision engagement and air/space superiority, prioritization of global air base assets remains critical not only to the success of DOD mission, but ultimately for the Air Force's overall mission as well. Yet, without a clearly defined and universally implemented methodology, Combatant Commands (COCOM) and individual service branches could end up going in several different directions. Fortunately, the Air Force CIP closely resembles that of the DCIP, with similar sectors and responsibilities. Security Forces play a crucial role in the execution of the Air Force program, particularly as it relates to the air base defense mission.

C. SECURITY FORCES' ROLE IN THE AIR FORCE CRITICAL INFRASTRUCTURE PROGRAM (AF CIP)

In developing its own CI program, the Air Force is called upon to identify and list particular infrastructure and assets deemed critical to not only the Air Force mission, but also the COCOMs and DOD missions as well. Once these assets and associated vulnerabilities are assessed and identified, remediation and mitigation strategies must be devised and implemented to support the execution of the National Military Strategy (NMS). Yet, the execution of the NMS contains elements of military, strategic and political risk made more prominent by the interconnectedness of its cyber and physical Defense Critical Assets (DCAs). The dependencies and often overlapping functionalities of these assets, while often improving capabilities and overall mission effectiveness, similarly increase the Air Force's risks and vulnerabilities to them, whether from human error, natural disasters, and/or intentional attacks. When assets and capabilities are connected in some fashion, often the destruction or temporary reduction of one can carry negative or lingering implications on others. Viewing the program more from an operational level, Air Force installations/air bases, MAJCOMs and COCOMs must understand these risks as they depend on various critical assets and infrastructures vital to their operational effectiveness and mission execution.

Through the use of structured and somewhat scientific methodologies, the specifics of which are not intended for this research, the AF CIP attempts to determine its

mission essential tasks (METS.)[167] The difficult and often somewhat subjective element of this process is then determining task critical assets (TCAs) and supporting infrastructure critical assets (SICAs) vital to the execution of each identified mission. In generic terms, identified critical assets and infrastructures are assessed for their overall importance to and support of MAJCOM and COCOM missions and day-to-day operations of core business processes and functions.[168] This process not only identifies those assets and infrastructures most vital to war fighting missions, but also provides the identified capability to apply scarce resources (i.e., funding and security manpower) to the most critical assets.

Similar to the National and Defense Critical Infrastructure Plans, the Air Force CIP also developed specific Sector Leads (i.e., public works, health affairs, logistics and personnel) to develop and maintain relationships with other government and civil agencies, as well as the private sector, to address critical infrastructure issues and concerns. Each Sector Lead is responsible for evaluating their individual sectors, using both existing DOD and AF doctrine, to determine whether they adequately address the measures called for by the AF CIP. Ideally, this process should identify risks and vulnerabilities to AF infrastructure within each sector, as well as generate potential tools to help prevent or mitigate them.

Creating and exploring methodologies to determine an asset's overall importance is meaningless if you don't also follow up your findings with various actions. Undoubtedly, one must identify measures to mitigate identified threats, establish redundant or back-up assets/infrastructure, and document all this information in some type of data management system for COCOM and MAJCOM situational awareness. Currently, vulnerability/risk assessment and pertinent infrastructure data is input into

167).Generally, tasks falling into this category are absolutely necessary, indispensable or critical to the success of a COCOM or USAF mission (warfighting, operational or Title 10) or required capability.

168 The level of importance of a particular asset is broken down into four Tiers, with the first two Tiers being the most critical. Tier I capabilities or assets are those that when not assured, will cause the combatant command to suffer mission failure. Tier II capabilities or assets are those that when not assured, will cause a combatant command, Service or sector-specific asset to fail; combatant commander mission accomplishment is degraded, but still achievable. Air Force installations and/or deployed air bases may or may not have designated Tier I or Tier II assets under their control, but will undoubtedly possess assets or infrastructure critical to various Air Force missions at a minimum. Unlike what happened in the past, it is imperative that Security Forces personnel be made aware of the specific base critical infrastructure and assets and be given the appropriate equipment and manpower to properly secure them.

several DOD data systems, such as the Air Force's Critical Assets Management System (AF CAMS). This and other systems allow operational forces and other key players to view crucial data, near real-time, ultimately assisting in timely and more efficient mission execution.

CIP, whether at the National, DOD or Air Force level, is a long-term program, requiring constant attention to changing threats and situations. CIP demands specificity in identification of these threats and vulnerabilities as well as the protective measures selected to counter them. More importantly, CIP requires commitment, from individual Security Forces members, to program managers and senior leaders. We cannot afford to make the same mistakes we have made in the past.

D. RECOMMENDATIONS

The nature of terrorist threats is changing rapidly and will continue to do so for the foreseeable future. The combination of rapidly changing technologies, weaponry and networked organizational styles used by these terror groups creates a volatile situation in which the nature of threats and vulnerabilities may be difficult to assess and even more difficult to predict. If the AF CIP is to be successful, several recommendations should be followed:

1. As directed by AFPD 10-24, it is imperative CIP education and training is inserted into all appropriate command and base level courses in addition to senior staff and senior enlisted professional military education.[169] If Air Force leaders in policy/decision making positions understand the importance of the program and appreciate its utility, they will undoubtedly be inclined to promote the program to junior officers and enlisted members, feeding a much-needed and developing constituency. By incorporating CIP into training exercises, it will help develop an appreciation and awareness of the overall impact of losing various critical assets destroyed or incapacitated through the exploitation of existing or undiscovered vulnerabilities.
2. Incorporation of CIP into MAJCOM and installation-level training exercises. All the guidelines and policies drafted on paper mean nothing if you cannot execute them in reality. Contingency response exercises (terrorist attacks, MARE,

[169] AFPD 10-24, 2.

natural disasters, etc.) are an excellent tool to determine the responsiveness and overall readiness of each responding agency or organization.[170] It is further recommended that installations with critical resources and infrastructure detached from the installation (i.e., JP-8 fuel lines coming from off base), practice joint response scenarios with off-base partners such as local fire and police departments. The time to exchange business cards is not after a major catastrophe.

3. Support the establishment of mechanisms for sanitizing and disseminating data on critical infrastructures such as their associated vulnerabilities, threats and risks. With data management systems such as AF CAMS, COCOM and MAJCOM commanders will gain near real-time situational awareness required for combat effectiveness and readiness. It is imperative critical asset findings and associated information be input correctly and regularly to support the war fighting effort. Additionally, security issues and lessons learned should be shared (as appropriate) with portions of the private sector. Sharing (as well as obtaining) best practices and other innovative security measures will undoubtedly benefit all participants.
4. The creation and incorporation of "Red Cell" teams. Red Cell teams provide a mostly impartial view and method of discovering and dealing with infrastructure vulnerabilities and incidents. Installations can employ these teams as a method of identifying potential new threats and vulnerabilities perhaps overlooked by sentries or other workers who may have developed a level of complacency from working in/around a particular infrastructure for too long.
5. Encourage total base awareness and owner user involvement. With manpower shortages projected in the Security Forces career field due to the high operations tempo, security resources on Air Force installations may be stretched thin. Augmentation programs such as Resource Augmentation Duty (READY) and Security Force Manning Assistance are only temporary gap fillers and often complicate matters by pulling resources away from other areas around the installation, often equally desperate for manpower. Through base awareness

[170] MARE stands for major accident response exercise.

programs, coupled with selective arming programs, installation commanders can effectively augment Security Forces by forcing owner-user involvement. Not every critical asset or infrastructure warrants the same level of protection, and Security Forces cannot be everywhere at once. Owner-user programs would allow for augmented sentries, perhaps more familiar with the associated infrastructure, to participate in securing it, even if only in times of elevated threats.

6. While each installation commander may argue for additional funding or manpower requirements for resources or infrastructure they deem critical, it may not be critical in terms of the overall Air Force, and ultimately, DOD mission set. Computer data programs such as the Vulnerability Assessment Management Program (VAMP) and the Core Vulnerability Assessment Management Program (CVAMP) must be managed properly to identify where the most critical AF infrastructure is located and track various deficiencies and vulnerabilities through closure.
7. As future enemies will undoubtedly operate in an asymmetric manner in employing potential attacks on air bases and military installations, security planners also need to think in an asymmetric fashion to protect their most critical infrastructures from attack. Given the limited resources available for facility upgrades, force protection enhancements and other physical security projects, focus must be directed towards the most critical infrastructures on any given installation. Planners should reconsider preconceived notions of why/how various resources are deemed critical, and continually explore how/if various critical infrastructure are interconnected. The interconnectivity of various infrastructures may make analogous resources more vulnerable than those outlying resources perhaps deemed more critical in previous assessments. During operational planning, a small amount of effort can ultimately lead to a large amount of security if planners examine non-obvious methods of strengthening their critical nodes.
8. Security Forces leadership must stay engaged in Force Protection Working Groups, Threat Working Groups and other force protection advisory and

planning venues for determining, assessing and prioritizing base resources, particularly in determining appropriate levels of protection once a list is developed. Additionally, if SF leadership maintains a working knowledge of current and projected base critical infrastructure, they will be better prepared to establish an appropriate security posture to defend it.

Often times, the implementation of effective intelligence sharing and/or critical infrastructure protection plans would not be possible if it were not for various force protection-enhancing technologies and equipment. As it has been described throughout this work, one of the primary reasons enemy attacks on air bases were successful in the past was the lack or inadequate quality of technology available to security personnel. Troops on the ground often sought improved weapons, vehicles, sensors, remote and handheld detection equipment, yet were often disappointed by the slow or nonexistent delivery of said items. Chapter VI will examine many of these earlier failures, describing how various force protection equipment fell far short of expectations and often left troops on the ground with nothing more than expensive paper weights. This chapter will also describe some of the current and future air base defense technologies/programs and explain Security Forces' role in implementing these technologies in the IBD mission.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. TECHNOLOGY, INNOVATION AND BASE DEFENSE

> *The Department of Defense faces numerous competing priorities and operational demands. However, the committee notes that without a stable long-term investment in basic research and technology development, the recent display of the armed forces' technological advantages, such as precision weaponry, unmanned systems, smart munitions and increased situational awareness, would not have been possible.*
>
> Senate Armed Services Committee, May 13, 2003.[171]

Throughout history, the military has evolved strategically and doctrinally, and perhaps even organizationally, because of continued advances in technology. From muskets to machine guns, strategic bombing runs to precision-guided missiles, history is filled with examples of where a new weapon, improved airframe or enhanced communication system have provided those who possess them some form of advantage on the battlefield. Ever since Western armies first attempted to counter German machine guns with their Mark I tanks, it has depended almost entirely on its technological advances to keep pace with the evolution of war. A continued emphasis on technology appears to be the trend and the basis for prescribing how DOD, and ultimately Security Forces, will operate in the near future and beyond.

Technology can, and often does, benefit the force protection mission. As the Air Force moves forward with new Integrated Base Defense security systems, the structural and procedural integration of this technology will be critical to executing the IBD mission. This chapter will examine prior cases where possessing inadequate equipment and/or failing to obtain various technologies negatively affected the air base defense mission. It will also examine numerous future and current technologies and programs vital to the effective implementation of the IBD mission. Finally, this chapter provides recommendations for air base planners regarding the use and employment of various technologies and associated doctrine.

---

[171] Association of American Universities. Report language in the fiscal year 2004 Defense Authorization Committee Report (108-46). Available at http://www.aau.edu/DOD/quotes.pdf (accessed on 12 August, 2006), 2.

A. EARLY MISUSE OR LACK OF TECHNOLOGY AFFECTING AIR BASE DEFENSE

During the Vietnam War, the United States possessed several computerized models and other quantitative indicators used for analyzing the progress of the war from Washington, D.C. Yet, as war planners seated comfortably in their Washington offices became enamored by this computerization and quantitative analysis, they tended to overlook the more delicate aspects of where the enemy was truly winning. Security personnel in Vietnam relied upon a mixture of tactical support equipment, including various sensors and locating devices in their air base defense mission. Unfortunately, as the stand-off attacks escalated at air bases throughout the region, these electronic and mechanical aids were often rushed into service, many of which were untested and inadequate. Despite the first-ever use of countermortar radar devices at various installations, these surveillance radars had radial scan limitations, usually only covering approximately 40 degrees (out of 360) within a particular sector.[172] Because of these limitations, these devices were often purposely aimed directly at areas deemed most likely as high speed avenues of approach for an enemy attack. These countermortar radars were also mostly ineffective against rockets, allowing for enemy troop movements to launch numerous rockets simultaneously with limited detection capability. Similarly, Da Nang air base paid the price for this limited capability, as insurgents fired 64 rockets onto that air base (and a nearby village) in less than 60 seconds.[173]

Based on an increasing need to detect enemy personnel and vehicle intrusions along base perimeters, the South East Asia Intrusion Detection Equipment Program was started. This program was designed to field test a wide variety of intrusion detection equipment, hastened for battlefield use by skipping normal production line issues and other standard testing procedures. This "buy and try" approach was extremely unorthodox and often led to fielding and operational problems.[174] In another case of an expedited research and development period, approximately 40 specialized rifle sights, designed by Sears Roebuck Company to enhance nighttime shooting were also rushed to

[172] Fox, 104. This siting limitation allowed for the enemy mortar barrage upon Tan Son Nhut air base, in which enemy insurgents shelled the base for over 13 minutes.

[173] Ibid., 105.

[174] Ibid., 105.

the battle zone. With limited instructions and unorganized fielding, these sights were ultimately a bust. Another failed system, the Surveillance and Detection System (SADS 1.5) required a buried seismic sensor line in and around the areas security personnel sought to defend. This system was eventually rejected due to its overall cost and inability to produce sound results in varied climates.[175]

Probably the most complex, yet promising system tested during this period was the Perimeter Detection and Surveillance Subsystem (PDSS.) This system utilized two types of antipersonnel radar and a radio data mechanism allowing for the transmission of triggered alarm data to a fixed receiver panel. This system actually showed early promise, but produced inadequate, unreliable data during inclement weather, with moisture and leakage causing malfunctions within the system.[176] The PDSS, initially thought to generate a manpower savings, actually mandated additional manpower as it typically required numerous sentries to protect the system from VC/NVA units looking to dig up the sensor lines.[177] Air Force security leadership recognized a limited benefit in placing sensor devices outside and away from the base perimeter, yet also realized these sensors were not meant to actually replace security personnel as detection instruments on the base perimeter. Realizing the equipment's limitations, they understood these sensors represented nothing more than an "extension of the sensory capabilities of the sentry," and the "use of these sensors should be governed until much more sophisticated devices are developed."[178]

One of the key elements to executing the air base defense mission is reliable communications. Yet, communication equipment in Vietnam often proved to be inadequate to provide tactical communications for patrolling units and base defense operations centers. Base defenders relied upon 2-channel Motorola radios transmitting from over 300 different locations.[179] As the VC/NVA developed radio jamming

[175] Fox, 105.

[176] Ibid., 106.

[177] Ibid., 106.

[178] Steve Wieman. Vietnam Security Police Association. 1998. Vietnam Operation SAFESIDE Final Report: Letter from Lt Gen William W. Momyer to HQ AF. Available at: http://www.vspa.com/phan-rang-safeside-final-report-1967.htm (accessed on 12 August 2006), 2.

[179] Fox, 152.

capabilities, the radios and the over saturated networks used by U.S. personnel during the Vietnam conflict proved to be non-tactical and clearly inadequate for use in an insurgent environment.

Vehicles used by Security Police mobile patrols were often less than satisfactory. Police units were often called upon to respond to portions of the installation unreachable on foot. This required various vehicle platforms, including the M-151 (resembles the old-style Jeep).[180] The M-151 did not provide the necessary levels of armored protection for responding police units, degrading the response capability of this vehicle. Similarly, Security Police units experienced difficulties with the armored personnel carriers (APC) provided to them for a more protected/hardened response. These vehicles were advertised as being capable of operating through any kind of weather and on any type of terrain. Security Police units at Vietnam air bases soon learned this was not the case. The APC's were extremely heavy, causing them to bog down in wet sand or mud. This made them extremely unreliable in an area certainly not lacking in its annual precipitation.

During combat operations in Vietnam, the one piece of equipment a base defender came to rely on implicitly was his/her weapon. Yet, despite its impressive features, the standard-issue Colt AR15, M-16 rifle often demonstrated the ability to misfire or seize up due to the muck and dust that would often collect in the weapon's gas tubes and chamber. During the Vietnam industrial push, bullet manufacturers issued a new form of gunpowder that often left chunks of calcium carbonate in the weapon's gas tube. These environmental and man-made elements, along with an insufficient spring-loading mechanism, often caused the weapons to jam during intense fighting. Additionally, if the weapons were loaded with 30-round magazines the M-16 would routinely seize up. After experiencing this technical malfunction far too often, occasionally resulting in a fatal error, Air/Security Police on the ground learned to load their magazines with 27 rounds.[181]

---

[180] Fox, 146-147.

[181] Frank Vizard and Phil Scott, *21st Century Soldier: The Weaponry, Gear and Technology of the Military in the New Century* (New York: Popular Science, Time, Inc, 2002), 96.

While some tactical support equipment, such as the starlight rifle scope and various other night vision observation devices, actually performed adequately by partially illuminating enemy ground forces, most items were either impractical, too costly or failed during field testing. In examining the technologies available or implemented during Vietnam, it was clear once again that the Air Force was completely unprepared to execute its underdeveloped and mostly untested air base defense mission.

An examination of available data related to the Khobar Towers bombing indicated a lack of emphasis on improved and integrated technologies to enhance the force protection posture there, despite an increase in terrorist activities and threat messages in the region. In his after action report, retired General Downing and his commission concluded that the DOD needs more money, more people, better intelligence and advanced technology for the force protection mission.[182] The report also stated using advanced technology can help protect U.S. forces, particularly in forward- deployed areas. Downing's task force found "a manpower-intensive approach to force protection that included sentries armed only with binoculars and their weapons on 12-hour shifts in 120-degree-plus heat, bomb dogs with an effectiveness of 15-30 minutes on guard at gates, crude highway traffic control devices used as blast protection barriers." [183] Downing went on to say, during a Pentagon news briefing, that "We can and we must provide our forces with state-of-the-art sensors, blast protectors, automated entry points and cargo inspection devices. We have enough inspectors out there. We have enough people going out and telling commanders what is wrong. We need people to go out and help, to point out deficiencies and then remain and make corrections and help commanders overseas install these advanced systems."[184]

While several of the general findings from Downing's Khobar Towers Assessment remain classified, others pertaining to technology were cited in the version released to the public. Coming as no surprise, Finding #17 cited U.S. forces and facilities in Saudi Arabia and the region were vulnerable to attack. In addressing the physical security aspect of this finding, Downing's group recommended employing improved and

[182] Kozaryn, 1.

[183] Ibid., 3.

[184] Ibid., 3.

integrated technology into the force protection mission. They recommended intrusion detection systems, ground sensors, closed circuit television, day and night surveillance cameras, thermal imaging, perimeter lighting and advanced communications equipment to enhance the security posture for all air bases in the region. Based on the repeated occurrences of explosive-related incidents in the region, the commission also recommended the employment of technology-based explosive detection and countermeasure devices.[185] Finding #25 from the Downing Report stated technology was not widely used to detect, delay, mitigate and respond to acts of terrorism. The commission recommended generic methods for incorporating technology and technical assistance to those in the field who required it.[186] The Record Report concurred with Downing's findings, but stated that the Air Staff should direct Air Force unit deployment managers to review their operational capabilities and ultimate requirements when it comes to the inclusion of high-tech equipment on future deployments. The report also recommended training military leaders on an integrated systems approach for incorporating physical security and force protection technologies.[187]

Terrorism experts mostly agree that there is no silver bullet for stopping all forms of terrorism. The most dedicated, structured and well-financed terrorist groups will undoubtedly find ways to outmaneuver or outwit various forms of sensing and detecting-type equipment and technologies. Yet today, ion scanners, biometric identification cards and cargo crate X-ray devices detect and undoubtedly deter potential terrorists from carrying out their often-deadly acts. However, as history has demonstrated, the absence or ineffective use of force protection technologies contributed to the success of repeated insurgent stand-off attacks and perimeter penetrations in Vietnam and one catastrophic event at Khobar Towers. After-action reports and case studies from both periods determined the availability and ultimate utilization of improved technologies may have prevented some or most of these attacks from occurring.

More recently, it has become evident that increased weapon and information technologies will allow enemy forces to attack air bases often used for the forward

185 Creamer, 104.

186 Ibid., 108.

187 Record, Part A, Finding 25.

deployment of our land-based forces. So, as the Air Force moves forward with its IBD mission, expanding the battlespace and seeking to see, understand and act upon these enemy weapons and technologies first, there will be a tremendous emphasis placed on elaborate and expensive intrusion and detection systems and their appropriate implementation. A continued emphasis on technology appears to be the trend and the basis for prescribing how DOD will operate in the near future and beyond. As the Air Force moves forward with improved equipment and new camera, detection and warning security systems, the structural and procedural integration of this technology is critical to executing the IBD mission.

B. BETTER THAN BEFORE: CURRENT AND FUTURE AIR BASE DEFENSE EQUIPMENT AND TECHNOLOGY

Security Forces personnel, particularly those patrolling the perimeter and controlling the intrusion detection systems, are crucial in the development and enforcement of the new IBD doctrine. Yet security sentries can also occasionally be the weakest link in the process and the primary reason why security fails. Arguably, Security Forces personnel remain the most disciplined career field in the Air Force, yet they still experience those rare occurrences involving patrols or entry controllers being inattentive or simply not focusing on their primary task at hand. Consequently, every security system must have trusted, trained and mission-focused personnel to function properly. There are those who feel advances in technological systems will ultimately replace people, thereby eliminating the 'human nature' factor, the apparent cause of some system failures. However, unlike computers, ground surveillance radar systems and other rigid forms of technology, people are creative, ingenious and often quite flexible. The most effective security equipment and/or systems should be designed to maximize the creativity and flexibility humans provide while simultaneously reduce their inherent limitations. While many software programs and new-age munitions are developed to adapt to environmental and other mission changes, only people can truly alter their response pattern as an enemy attack develops.

It is quite beyond the scope of this chapter to examine all future or recently fielded military technologies, their implementation and associated doctrine and strategy. Yet as threats to U.S. air bases and military infrastructure from insurgent stand-off, IED

and other explosive attacks remains a strong possibility, the U.S. military continues its technological transformation, to acquire new and improved technologies in an effort to subjugate this postulated threat.[188]

The days of placing security personnel in foxholes or entrenched positions in forward areas of the air bases they are defending (listening post/observation post (LP/OP) are seemingly behind us. While the IBD template still calls for detection and assessment of the enemy as far from the air base as possible, this task will now be accomplished primarily through detection and sensing technologies. Replacing security sentries in guard towers along the perimeter are the ground based surveillance radars and motion-tracking cameras. Flight line access gates, often manned by security personnel in the past, can and will be operated from a central location while also functioning through biometric and other personal recognition technologies. As mentioned earlier in this chapter, air base defenders of the past often lacked up-to-date or appropriate weaponry and optical/sensing equipment for their base defense mission. Weapons, detection equipment and personal gear continue to evolve and offer enhanced capabilities in thwarting potential air base attackers.

The standard-issue Colt M-16 rifle, used by U.S. war fighters since 1963, has only recently been replaced by a shorter and lighter M-4 version. The M-4 comes with an optional forward handgrip, advanced opticals and is ideal for short-range combat. Additionally, weapons currently in development and scheduled for deployment as soon as 2009 include the Objective Individual Combat Weapon (OICW), a 12-pound, high-explosive grenade firing workhorse and the Objective Crew Served Weapon (OCSW), a replacement for the esteemed 50-caliber machine gun. Using a two-person crew, the OCSW uses a laser rangefinder for directing 25mm rounds out to distances as far out as 2,000 meters at a rate up to 260 rounds per minute.[189]

With many forward-deployed locations involved in humanitarian or peacekeeping missions and most stateside air bases remaining in close proximity to civilian populations, the military often finds itself operating around and adjacent to large groups

[188] As stated previously, insurgent attacks often do occur on U.S. bases located inside Iraq and Afghanistan. However, the IBD concept has yet to fully develop in those regions.

[189] Vizard and Scott, 105-106.

of civilians. This environment, particularly in forward-deployed locations, carries the potential for a negative set of cascading circumstances. The U.S. military is currently researching and developing a variety of non-lethal weapons for situations that do not warrant lethal force, yet require more than a string of harsh words. Many of these weapons are still in the blueprint or prototype phase, yet several are worth mentioning for their potential utility in the air base defense role. One form of what is called active denial technology is a HMMWV-mounted weapon that emits a directed electromagnetic energy beam that passes through the enemy's clothing and penetrates his skin a fraction of an inch, causing temporary, yet intense heat. The U.S. Marine Corps is currently funding this program and anticipates its potential application as early as 2009.[190] Several other incapacitating-type weapons in development include: electrical shock devices, laser and acoustic directed energy weapons. The focused, high-power noise caused by an acoustic weapon can incapacitate humans from within the stand-off range. So, whether it is a laser beam used to temporarily blind the enemy, or electrical shock weapons used to cause immediate and uncontrollable muscle contraction in insurgent attackers, these less-than-lethal weapons certainly possess some utility in protest, peacekeeping and humanitarian type missions. However, they may also be utilized in forward-friendly or stateside urban areas in the IBD role.

For nighttime combat and air base perimeter observation, security personnel are now equipped with night vision goggles such as the AN/PVS-7. These goggles have two eyepieces but a single lens illuminates the ground in front of the wearer, requiring very little ambient light to do so. With the ability to mount this item on a Kevlar helmet, make adjustments with one hand and incorporate a compass and infrared spotlight lens, these goggles offer many advantages Air Force security personnel in Korea, Vietnam and Khobar Towers did not have or were late in receiving.

Other forms of handheld or mobile detection equipment include thermal infrared sensors, ground surveillance radar units, laser range finders, target designators and a radar flashlight. Thermal infrared sensors detect heat emitted by humans and combustion engines at considerable distances. While they do not typically fare well in precipitation

[190] Vizard and Scott, 116. HMMWV is a Highly Mobile Multi-Wheeled Vehicle, often referred to as a "Humvee".

or dense fog, they can see through obscurants and operate during the daytime. Handheld ground surveillance radar units emit short bursts of electromagnetic energy to detect motion on the battlefield or areas outside air base perimeters. These units are said to be capable of detecting enemy personnel hiding behind cement walls.[191] Laser rangefinders, capable of being placed on individual weapons, use invisible lasers to determine the range from an approaching vehicle or troop formation using GPS technology. When mounted on direct-fire weapons, shooters can incorporate infrared sensing goggles for extreme firing accuracy. Finally, the radar flashlight uses microwave radar with an internal digital processor to detect the smallest of human movements (such as a person's heartbeat or breathing rhythm). This item is so sensitive, it is said to be able to detect human respiration through walls and dense foliage.[192]

While some of these items are still in development, many others continue to crop up with promises to "detect this" and "track that." History has shown that more technology is not necessarily better; however, the right technology for the mission can be worth its weight in gold. Now that we have examined several portable technologies suitable for base defense, all of which are upgrades from previous periods, the focus will now shift to technological security systems that are currently being utilized at Air Force bases around the world.

C. SECURITY FORCES' ROLE IN EXISTING BASE DEFENSE SYSTEMS AND TECHNOLOGY

An examination of the air base defense doctrine implementation and execution from Korea up until the attack at Khobar indicates the force protection mission was often given a low priority. Consequently, considering the DOD fiscal system is typically driven by requirements and priorities, the Air Force force protection, and specifically the air base defense mission, also generally received a lack of appropriate funding. This lack of funding resulted in inadequate or missing technologies mentioned in the previous section.

As Downing and Record have indicated in their investigative findings from the Khobar incident, had there been additional motion, or other forms of detection, sensors

[191] Poole, H. John. *Phantom Soldier: The Enemy's Answer to U.S. Firepower* (North Carolina: Posterity Press, 2001), 209-212.

[192] Ibid., 209-212.

placed around Khobar's perimeter, the terrorist bombers may have been discovered earlier and perhaps even apprehended. After the Khobar tragedy, force protection became a huge priority. In the year following the Khobar attack, the Air Force procured a contract with TRW for the deployment of the Tactical Automated Security System (TASS), an intrusion detection system specifically designed for placement around air base perimeters. The TASS system, "utilizing state-of-the-art technologies, operated on a variety of detection/sensor platforms, from microwave and magnetic, passive and active infrared to plain old fashioned trip wires."[193]

While TASS was certainly an improvement over the pre-Khobar situation, it also had its limitations. TASS sensors could not pinpoint an enemy's exact location within a detection zone and were often prone to nuisance alarms from blowing debris, wildlife or unmanaged foliage. After several nuisance alarms in one particular zone or from one particular sensor, a Security Police controller could become complacent and simply 'acknowledge' future alarms without dispatching a patrol to investigate further. Or, a Security Police patrol, if dispatched numerous times to the same location, may make a command decision that the alarm is once again a nuisance and simply not respond. Both situations represent the 'human nature' factor mentioned previously. To avoid these and other complications, the Air Force conceptualized the development of an integrated security system whereby Security Forces controllers (ideally working out of consolidated first responder Emergency Dispatch Center) would receive a common operating picture for all air base alarms, cameras, and detection and warning sensors and systems.

As a result of intense planning, research and development, the Air Force recently put in motion their Integrated Base Defense Security Systems (IBDSS) contract, designed to upgrade existing TASS capabilities and develop electronic detection, alarm assessment, access control and enhanced communications within a single system. Due to immense program costs, this new system, named Pathfinder, is currently only being designed and installed at a handful of air bases. Andrews Air Force Base, located just outside of Washington, D.C. and the home of Air Force One, was selected in September,

[193] Cheryl Gerber. 2003. Lead Ahead for Force Protection. Military Information Technology: Online Edition. Available at: http://www.military-information-technology.com/print_article.cfm?DocID=232 (accessed on 19 August 2006).

2002, as the first Air Force base to field the Pathfinder system.[194] This elaborate system, designed to enhance the overall effectiveness and performance of the security system at Andrews AFB, was developed using both transformational (leap-ahead) and off-the-shelf technologies.[195] Capabilities of the system include: multi-layered area intrusion detection, tracking and reporting, access control, alarm day/night assessment, integrated 6-screen Command and Control Display (CCD) and delay/denial capabilities. Early detection and delay capabilities were designed around long and short infrared cameras, pan/tilt/zoom (PTZ) and fixed cameras, long and short range ground-based radar and Object-Video (smart video) detection software.[196] Access control to and through sensitive areas is maintained by numerous automated vehicle gates and pedestrian turnstiles, both requiring access cards and 4-digit PIN numbers for entry. Through the use of much of this transformational technology, the system will provide not only early detection and situational awareness (well beyond the air base perimeter), but the ability to monitor and track enemy penetrations through both camera and radar systems. Early detection of potential adversaries in locations outside the air base perimeter (similar to those areas in which stand-off and explosive-related attacks were conducted in Korea, Vietnam and Khobar Towers) provide Security Forces the capability to achieve local and area dominance of their battlespace in support of force protection.[197]

Since the Pathfinder system was designed specifically to augment the Integrated Base Defense mission, the system is primarily operated and maintained by Security Forces members. In regards to the circulation control requirements for the system, Security Forces are responsible for determining security clearance requirements, delegating entry authority and the issuance of restricted area badges to authorized

[194] In an effort to determine overall costs, risks and evaluate the performance of a fully integrated security system, Andrews AFB was selected to receive the first large-scale Pathfinder security system. Several other bases are receiving smaller versions, typically only including immediate flight line areas. Andrews' design will include the entire Industrial Complex/flight line area with designs for SmartGate and installation entry control tie-ins programmed for out years.

[195] The scope of this chapter is not intended to describe every nuance of the Pathfinder system, rather to provide a generic description of some of its detection and assessment capabilities and several general Security Forces-related functions..

[196] Object Video Early Warning software monitors numerous video feeds for unusual or suspicious behavior. Any movement not defined by the program's pre-established parameters will be brought to the attention of the Security Forces Pathfinder Operator (i.e., an individual walking out of some nearby woods or too closely to a plane parked on the flight line).

[197] United States Air Force, *Air Force Tactics, Techniques and Procedures, 3-10.1*, 1.

personnel. The Pathfinder system operator is responsible for: monitoring events at numerous automated crash-rated entry control points and pedestrian gates, including authentication attempts, lockouts, flight line gate operations and duress alarms. Additionally, the operator will monitor the 6-screen CCD, track and report all alarm activations, dispatch appropriate security patrols and up channel incidents involving priority resources. Security Forces patrols, in addition to proactively patrolling the air base and responding to complaints and calls for service, will respond to and assess Pathfinder alarm activations and take appropriate action if required. Improved surveillance of high-speed avenues of approach to and around the air base as well as improved perimeter and flight line sensors are critical so Security Forces personnel can quickly detect and defeat penetration attempts. Other technologies such as in-dash police video, friendly force tracking and state-of-the-art communications systems are also crucial to augment the overall effectiveness of responding security units.

Mostly due to the VBIED threat and its potential impact to air base missions, most, if not all, Air Force bases now have a separate vehicle entry gate, usually situated in a remote portion of the air base, used exclusively for commercial vehicle entry. Several methods for searching commercial vehicles exist and are used by Security Forces personnel. The Technical Support Working Group (TSWG) developed a Vehicle Entry Explosive Search Strategy (VEESS) that most vehicle inspectors reference and often carry in the cargo pockets of their uniforms.[198] In addition to this useful booklet and the thorough hand searches conducted by dedicated security personnel, several different smaller-sized devices are commonly utilized at commercial search gates for examining areas search personnel either cannot explore or could potentially contain explosive material or contraband. Many Air Force bases utilize Ion Scanners or VaporTracer devices for detecting swabbed or vapor samples for traces of explosives and/or contraband.[199] Ion Scanners are typically desktop units requiring a dedicated, climate-controlled workspace, and VaporTracers are handheld, portable units. With proper and

[198] TSWG is a D.C.-based group, established in 1986, that identifies and prioritizes research and development requirements for combating terrorism technologies for the purpose of national security.

[199] VaporTracer is a patented creation of the General Electric Corporation.

regular training, these devices can be extremely beneficial to the commercial search gate as well as for preventing the introduction of explosives and other contraband from entering the air base.

Several Air Force bases have procured large-sized detection devices for bulk explosive detection at their commercial search gates. One of the newer technologies being used today is the Idaho Explosives Detection System (IEDS). Utilizing a state-of-the-art neutron generator along with complex gamma-ray neutron activation analysis systems, these systems are capable of detecting a number of explosive and chemical warfare agents. While this system typically requires a remote operating location, moderate shielding materials and intense operator training, this system is attacking the threat head-on and producing excellent results.[200]

Another example of a larger-sized technology being utilized at search gates and other areas of the air base is the Mobile Search Vehicle (MSV) manufactured by American Science and Engineering (AS&E). This piece of equipment (not considered part of the normal vehicle fleet) generates two types of X-Rays (transmission and a patented Z-backscatter) to process and analyze vehicles of all sizes. As the MSV slowly passes by the target vehicle, it processes an image, similar to that of a normal airport x-ray, for the MSV operator to examine and analyze. Narcotics, explosives and other items can be easily identified on one of several large monitors located inside the MSV control room. The MSV requires a 3-person crew and an almost perfectly flat surface to operate, but can locate metallic and organic items located in hidden compartments, in the undercarriage of vehicles or other places not visible to the naked eye.

Security Forces personnel supporting the IBD mission have recently begun conducting airborne surveillance utilizing their Force Protection Airborne Surveillance System (FPASS). The primary FPASS vehicle, aptly named Desert Hawk by current Air Force Chief of Staff General Michael Moseley, is small, lightweight and easy to operate. The Desert Hawk is a miniature UAV capable of flying pre-programmed missions for up to an hour on a single battery charge. The flight plan of the Desert Hawk can also be

[200] Ernesto Cespedes. 2005. Explosive Detection and Testing. Idaho National Laboratory website. Available at: http://www.inl.gov/nationalsecurity/factsheets/docs/explosives_testing.pdf#search=%22remote%20explosive%20detection%20system%22 (accessed on 22 August 2006).

altered mid-flight with a few simple keystrokes on the system's laptop computer. FPASS was designed specifically for Security Forces personnel to operate within close proximity of its assigned air base, providing real-time visual assessment of the surface-to-air missile footprint.[201] Unmanned aerial vehicles such as the Desert Hawk do have some limitations however. They cannot simultaneously monitor every square foot of the battlefield or areas adjacent to the air base perimeter. They also typically cannot penetrate triple canopy vegetation; detect enemy movement below ground, beneath dense foliage or inside buildings. Additionally, legal limitations prevent the use of such items over civilian populations, allowing for future foes to potentially operate near U.S. controlled areas undetected by this form of surveillance. Yet, this crucial surveillance tool, equipped with thermal and night vision cameras, extends the range Security Forces personnel can monitor outside and away from air base perimeters without jeopardizing the forces or placing them in harms way. FPASS is primarily utilized at forward-deployed air bases such as Tallil Air Base in Iraq. Here, the Desert Hawk interdicts enemy avenues of approach, weapons caches and anti-aircraft weaponry outside the air base perimeter, playing a vital role in the overall IBD mission.

D. RECOMMENDATIONS

In examining military history, one finds that as war fighting methodologies evolved, new technological developments or innovative tactical approaches evolved right along with them. As technologies develop to counter the often unpredictable and seemingly ever-present threat of terrorism, they must focus on the critical areas of detection, networked communications, targeting/assessment and deterrence to benefit the air base defense mission. The following basic recommendations apply to Security Forces members utilizing various technologies in the performance and execution of the IBD doctrine:

1. Upon the acquisition of new technological gear or actual systems, it is imperative that those using the equipment/systems receive proper training, either from the manufacturer of the equipment or the procurement agency (such as Electronic Systems Center/ESC). Recurring training

[201] John Pike. 2005. Desert Hawk. GlobalSecurity.org website. Available at: http://www.globalsecurity.org/intell/systems/desert-hawk.htm, (accessed 22 August 2006).

programs should be considered in out-year budgeting forecasts, as well as 'train the trainer' programs to allow for in-house development and proper continuity. Similarly, those procuring these new systems and equipment should plan/budget for necessary future upgrades. Often equipment or operating systems become obsolete after the initial contract expires, leaving the system/equipment owner with the responsibility of funding necessary upgrades.

2. Ensure the systems or equipment acquired is capable of integrating with existing infrastructure or at the very least not have negative cascading effects upon one another when being utilized. In the past, newly acquired items have negated or partially degraded an existing item/system's capabilities.

3. Ideally, portable gear carried by security personnel should be easily managed (in regards to storage and inventory), receive scheduled periodic maintenance by those trained to perform it and most importantly, function properly when called upon to do so. If gear is easily pilfered or lost and does not receive the appropriate cleaning and/or maintenance required to function, it will not.

4. Users of this equipment or these systems must learn to not become solely reliant upon the technology and relax on previously developed tactics, techniques and procedures. While many of these 'gadgets' may in fact improve upon or increase overall awareness, systems and equipment fail and can often produce false positives or incomplete/inadvertent data. Inspector General (IG) and self-inspection checklists should account for procedures during system failures and these common tasks should be exercised regularly.

5. Similarly, advancements in various technologies can and often do provide force enhancement, yet they do not always offer force replacement opportunities. While infrared and thermal imaging devices may free up Security Forces personnel from several of their static or non-mobile posts, they still require a Security Forces member to monitor them and dispatch a response unit in the case of an alarm or intrusion. Technology can therefore assist in the force

protection mission, but Security Forces members (and other uniformed personnel) are still required to accomplish the mission.

6. Often, the naked eye or older technologies serve as the back-up assessment tool when primary systems go down. Planners should anticipate system failures and develop redundancies incorporating either replacement technologies or additional manpower/posts as required to fill the existing void.

7. Security Forces leadership should remind air base leadership to remain flexible as new air base defense technologies come on line. As pop-up barriers, SmartGate systems, proxy card readers and other systems are incorporated, delays can be expected. Vehicles and personnel may be redirected or take additional time when entering various locations, and these delays should be explained and advertised as necessary.

8. Security Forces leadership or appropriate unit personnel should continue to keep in close contact with the Security Forces Battlelab and other producers of air base defense technology (such as TSWG) for prototype units which are often available to the requestor at little or no expense to the unit. Often these agencies are seeking a testing environment for their equipment and will place the equipment and monitor it for results and little/no cost to the unit. Planners should not accept any/all equipment, but only that which may be necessary to fill an existing void in air base defense mission execution.

9. Base defenders in Vietnam were often given gear or equipment upgrades they neither felt were necessary nor desired. While a few of these "upgrades" were moderately beneficial, most only required additional training or were simply ill-suited for the Vietnam climate. It is imperative that Security Forces commanders and acquisition planners take into account the needs and requirements of the security personnel on the ground performing the IBD mission. The latest and greatest gadget should not be simply thrust upon them because it is new and shiny. Ease of integration, overall effectiveness and level of utility factors should all be weighed with overall cost when considering new air base defense technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

> *If you joined the Air Force not long ago and became a security forces person, you would have spent a lot of your time guarding missile silos, guarding bombers, alert fighters, guarding gates, or at least being at a gate. But after we stood up 50 expeditionary bases in the Arabian Gulf and after we've had attacks on the bases, after we have had rockets and mortar attacks on the bases, after we've had aircraft hit on arrival and departure with surface-to-air missiles and small-arms fire, and after we've looked at what does it take to secure an airfield in an expeditionary sense, this security force business takes on a whole different light. . . . Get outside the wire with the Office of Special Investigations folks . . . and begin to think about what's a threat to this airfield. What do we have to do to defend it so we can operate 24 hours a day, seven days a week, in a true joint sense, and in a true combatant sense, so that there are no threats to this airfield that we haven't thought about?*
>
> General Michael T. Moseley, Chief of Staff of the Air Force[202]

In the past, the Air Force mistakenly neglected numerous doctrinal and procedural deficiencies directly connected to their air base defense mission. While the Air Force painstakingly and often begrudgingly developed its own base defense doctrine, enemy forces lurked undetected in the shadows wreaking constant and costly havoc to forward deployed air bases. Between undefined forward and rear areas, uncooperative host nation forces and an incorrect/industrial focus on defending only the innermost portions of its air bases, the Air Force's primitive air base defense capabilities suffered early defeats in both Korea and Vietnam. Air Force casualties from Vietnam alone are staggering; 155 servicemen were killed with over 1,700 others wounded in action.[203] Despite the casualties and the continued successes of enemy stand-off attacks, the Air Force's air base defense mission remained relatively unchanged after Vietnam and remained so for nearly another twenty years.

---

[202] Robert H. Holmes, et al., "The Air Force's New Ground War: Ensuring Projection of Air and Space Power through Expeditionary Security Operations," *Air & Space Power Journal*, (Fall 2006), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/fal06/holmes.html (accessed on 14 November 2006).

[203] Fox, 207.

Over the last several decades, security and force protection planners have seen an obvious shift in the global security state of affairs. Replacing the Cold War threats of nuclear sabotage and communist air base infiltration are the unconventional enemies forming insurgencies and fighting more asymmetric methods of warfare. The attack on Khobar Towers, and more recently the insurgent uprisings in Afghanistan and Iraq, are perfect examples of this recent trend. The Khobar attack brought to the forefront several of the force protection policy deficiencies and execution errors that remained unchecked and mostly unchanged from the Cold War period and beyond.

A thorough examination of air base attacks during these earlier periods indicated an improper focus on several policy and procedural areas. Vital programs such as intelligence collection and analysis, critical infrastructure protection and implementing effective force protection technologies led to far too many successful enemy air base attacks in the past, and ultimately the loss of too many precious lives and war fighting assets. As the Integrated Base Defense mission evolves, specific attention must be paid to improve upon these critical areas to avoid a repeat of those operational and doctrinal mistakes made in the past.

One of the primary lessons learned from the hundreds of attacks in Vietnam and one explosive attack at Khobar was that ground combat operations lacked a functional intelligence program to support the force protection mission. Attempts to utilize indigenous sources, create organic SF intelligence positions and/or develop functional programs with outside agencies lacked functionality or fell short of mission operability. Today, fusion centers, real-time data networks and other information sharing programs are essential in executing the IBD mission. More importantly, the coalition of Air Force intelligence, AFOSI and Security Forces, organizations that currently coexist on air bases both home and abroad, must develop a cohesive and efficient information sharing system to enable commanders on the ground to make sound and often timely force protection decisions. Proper collection, rapid analysis and thorough dissemination of threat information are necessary to support the IBD mission.

All available literature on air base attacks over the past 60 years indicates the vast majority of attacks were conducted by insurgent or guerrilla ground forces targeting

aircraft or war fighting assets with a desire to impact both the American military's ability to fight as well as the American public's political will to support the fight. Today's enemies still know they are no match for U.S. military dominance, and therefore have and will continue to choose unconventional methods to attack our operational and strategic military infrastructure. However, the protection of this critical infrastructure is often quite challenging for a number of reasons. First, during threat and/or vulnerability assessments, the tools used by working groups and force protection planners to determine a particular infrastructure's vulnerability or subjectivity to risk are often quite subjective. Additionally, increasing the security posture for a specific infrastructure through various force protection measures often leaves other, only slightly less critical infrastructure, more vulnerable. Finally, with many nodes and/or networks of war fighting infrastructure meshed together across various air bases, Major Commands and Combatant Commands, an attack upon one portion may have a cascading effect upon the others. What is quite clear from the available literature on previous air base attacks is that the protection of critical infrastructure was not given proper emphasis. Force protection planners, and ultimately commanders on the ground, need to ensure this infrastructure, whether proprietary or networked, is protected at all costs, and that contingency plans exist for the implementation of redundant systems when and if the need arises.

Due to exponential modern advancements in technology today, cameras, radars and other high-tech sensors used in the execution of the force protection mission are often only as good as the operators who use them. Yet in the cases presented in this research, technologies, when they were available, were often inadequate, inappropriate and mostly ineffective against deterring the enemy's stand-off attacks. Had many of these technologies been properly field tested for the environments for which they were planned, upgrades and modifications to these systems may have provided the required technological support the ground forces needed. Despite their tremendous upside, force protection technologies are certainly not the sole solution for disrupting or better yet, deterring enemy stand-off attacks. However, they do represent a tremendous upgrade from the Security Forces member's naked eye, a pair of muddy/cracked binoculars or some antiquated TASS equipment similar to those available in earlier periods. Today, ground forces utilize enhanced technologies to enlarge their battle space and identify

potential enemy targets and their activities before they approach the air base perimeter. In order to exploit this strategic advantage, the IBD mission will require continued advancements in force protection technologies that detect and assess enemy movement in the stand-off zones. However, detecting enemy movements on radar or a camera monitor are only half the battle. The overall IBD objectives of "see", "understand" and "act" first will also require that Security Forces members put "boots on the ground" outside the air base perimeter.

Base defense forces must proactively seek to not only get inside the enemy's planning cycle through quality intelligence and high-tech sensors, but also actually maneuver into his operating areas by launching preemptive patrols and countermeasures. Similar to the SAFESIDE missions conducted in Vietnam, the Air Force recently instituted Operation DESERT SAFESIDE in Iraq and achieved tremendous results. After over 400 stand-off attacks rocked U.S. air bases in Balad, Security Forces members deployed in the region began a 60-day operation seeking to deter future enemy aggression and prevent additional stand-off attacks. Security Forces patrols outside the air base perimeter resulted in the eventual capture of 17 high-value targets, over 100 insurgents and a number of weapons caches. More importantly, this team was able to virtually eliminate enemy stand-off attacks in that area.[204] Brief execution of SAFESIDE missions in Vietnam, as well as more recent attempts in Iraq, proves Security Forces men and women are more than capable of defeating the insurgent stand-off threat. History has demonstrated that as long as our enemies were allowed to operate freely within the stand-off range of our forward-deployed air bases, they continued to wreak havoc through violent and repeated attacks. The execution of IBD must prevent the enemy such proximity at all costs.

With the expectation of irregular types of threats to continue, coupled with our enemy's increasing desire to conduct calamitous and symbolic violence, air bases, regardless of their location, remain a constant target. Additionally, the seemingly expanding Global War on Terror and the Security Force's associated expeditionary ground defense role place these war fighters at air bases increasingly in harms way. With

[204] Holmes, et al., 3.

forward-operating air bases cropping up in remote regions of the world, initial fielding/siting and other security considerations remain a growing concern of air base defense planners. With vast expenditures on force protection enhancements and other detection equipment following the 9/11 attacks and subsequent budgetary windfall, air bases are better prepared to detect and defend against VBIEDs and other penetrating attacks now than in days past. However, as the experts cited in Chapter III predict, future attacks on air bases will probably not involve the enemy's use of conventional methods, but rather replicate the attacks seen during Korea and Vietnam through the use of mortars, rockets and other stand-off weapons. In fact, during the first two years of Operation Iraqi Freedom, U.S. air bases in Iraq have been targeted over 1,500 times, mostly via mortar and rocket fire attacks.[205] The successful and repeated enemy attacks on Iraq air bases prompted General Ronald Keys, Air Combat Command Commander, to pronounce air base defense one of the top five unsolved critical problems facing the U.S. Air Force today.[206]

As the DOD and the Air Force continue to evolve technologically, tactically, and strategically to match future challenges and missions, so to do the Security Forces. Security Forces members defending forward-deployed air bases can expect successful enemy attacks to have potentially devastating effects on aircraft, war fighting logistics and troop living quarters. Security operations, including early detection and deterrence of the stand-off areas around air bases, remain critical to the success of the overall IBD and force protection missions. Security Forces must also look to expand their battle space and control the standoff footprint through the use of improved intelligence, integrated sensor systems and other technologies. Former Security Forces Director, Brigadier General Robert Holmes, called this a "refocus on how Security Forces will train and fight." He goes on to say, "We're not in the Cold War anymore; we have to alter our mentality and practices for today's reality…we owe it to our Airmen, fighting the global

[205] Forward-deployed air bases in Iraq have experienced over 1,500 stand-off attacks since Operation *Iraqi Freedom* began in March of 2003 (Holmes, et al., "The Air Force's New Ground War", 3).

[206] D.T. Young, Security Forces Transformation: Why, What For? Air Force Print News Today, 27 January 2006, p. 1. Available at http://www.minot.af.mil/news/story_print.asp?storyID=123018665 (accessed on 23 September 2006). General Keys made this proclamation in 2004.

war on terror, to provide training, equipment and resources to be effective."[207] In a recent speaking engagement, current Security Forces Director, Brigadier General Mary Hertog stated,

> The war on terror has forced us to rethink how we defend our air bases, both home station and deployed. We can no longer stay inside the perimeter manning static posts and let the threat come to us and rely on another service to take care of that threat. We must integrate more with Joint Forces, with technology…and promote the evolution of force protection culture across our Air Force—everyone in the Air Force needs to be a warrior and involved in base defense.[208]

Air bases continue to face a full-spectrum of terrorist threats, and Security Forces cannot anticipate and defend against them alone. Air base defense, particularly as it applies to defending against enemy ground attacks, has traditionally been viewed within the USAF as a Security Police problem. Yet, as long as the execution of the national military strategy continues to rely heavily upon airpower's contributions, every man and woman in uniform must maintain a heightened sense of awareness and participate in the air base defense mission.[209] Through increased training and awareness, everyone must develop a basic force protection skill set and assist in the defense of an air base when/if attacked. Specifically, Security Forces members, from the newest airman all the way up the chain of command, play a vital role in managing effective intelligence, executing an appropriate critical infrastructure plan and utilizing the latest in force protection technologies

As the Security Forces career field strives to become a significant, war fighting capability, providing security operations for deployed commanders, the doctrinal and operational changes surrounding Integrated Base Defense must evolve quickly and efficiently. History has shown us that earlier attempts to thwart the enemy's stand-off attacks through air base defense were mostly futile. With the attack methodologies of current and future enemies mirroring those of the insurgents ground forces faced and mostly failed at stopping before, we can no longer afford doctrinal and procedural errors

[207] J.G. Buzanowski, "Security Forces Transformation: More Than Meets the Eye," *Air Force Print News*, 2 January 2006, 1.

[208] Mary J. Hertog, Speech given at the Annual Security Police Association Meeting, Arlington, VA, on September 2006. Taken from *Tiger Flight* 15, No. 6, November/December 2006, 4-5.

[209] Headquarters, United States Air Force, Air Force Doctrine Document 2-4.1, 4.

to limit our air base defense capabilities. Today's enemies have proven they are capable of much, much more, and we need to stand ready to defeat them. It is clear now, more than ever before, that different times call for different methods.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arkin, William M. "Mission Creep Hits Home; American Armed Forces are Assuming Major New Domestic Policing and Surveillance Roles," *Los Angeles Times*, 23 November 2003.

Association of American Universities website. The Case for Defense Science and Technology Funding. Obtained on Internet at http://www.aau.edu/DOD/quotes.pdf, [accessed 12 August 2006].

Bean, Michael. "United States Air Force Security Forces in an Era of Terrorist Threats." Master's Thesis, School of Advanced Airpower Studies, Maxwell AFB, AL, 1999.

Bina, Rebekah and Nicolai, Caroline. "The Legal Framework in U.S. Law for Sharing Law Enforcement and Intelligence Information." Background Paper from Syracuse University's Institute for National Security and Terrorism (INSCT). Obtained on Internet at http://insct.syr.edu/Research%20and%20Events/Res&Activities_2004ConfProgram.htm, [accessed 24 July 2006].

Bradley, Omar. Speech given on May 14, 1951 to the Senate Committee on Armed Forces and Foreign Relations, The Military Situation in the Far East, Senate Hearings. Obtained on Internet at http://education.yahoo.com/reference/quotations/quote/18185;_ylt=AvVKPJJVA6QiiLvS74Ou_2pcCc0F, [accessed 28 July 2006].

Bush, George. *National Strategy for Homeland Security*, Washington, D.C.: Office of Homeland Security, July 2002.

Buzanowski, J.G. "Security Forces Transformation: More Than Meets the Eye," *Air Force Print News*, 2 January 2006.

Carlson, A.C. "Air Base Defense." Master's Thesis, Maxwell Air Force Base, AL,: Air Force, 1952.

Cespedes, Ernesto, Dr. Explosive Detection and Testing. Idaho National Laboratory website, 2005. Obtained on Internet at http://www.inl.gov/nationalsecurity/factsheets/docs/explosives_testing.pdf#search=%22remote%20explosive%20detection%20system%22, [accessed 22 August 2006].

Christaldi, S.J. Operation Safe Side. Obtained on Internet at http://www.vspa.com/phan-rang-christaldi-safeside-1967.htm, [accessed 24 June 2006].

Cohen, William S. "Personal Accountability for Force Protection at Khobar Towers," Washington D.C., 31 July 1997). Obtained on Internet at: http://www.au.af.mil/au/awc/awcgate/khobar/cohen.htm, [accessed 12 September 2006].

Creamer, Robert Jr. and Seat, James C., "Khobar Towers: The Aftermath and Implications for Commanders," Research Report, Maxwell Air Force Base, AL: Air War College, April 1998.

Damphousse, Kelly R. and Smith, Brent L. When Terrorism Hits Home. Santa Monica, CA: RAND, 17 November 2004, p. 108. Obtained on Internet at www.rand.org/news/press.04/11/17.html, [accessed 23 July 2006].

Delaney, William, "USAF Force Protection, Do We Really Care?" Research Report, Maxwell Air Force Base, AL: Air Command and Staff College, 1998.

Department of Defense. *Directive (DODD) 3020.40, Defense Critical Infrastructure Program (DCIP*) Washington, D.C.: OSD, 19 August 2005.

Dickey, Clifton. "Air Base Defense for the Air Expeditionary Force: More Than Defending the Redline." Masters Thesis, Maxwell AFB, AL: School of Advanced Airpower Studies, June 1998.

Douhet, Giulio, *The Command of the Air*. Washington, D.C.: U.S. Air Force Office of History, 1983.

Downing, Wayne A. *Force Protection Assessment of USCENTCOM AOR and Khobar Towers, Report of the Downing Assessment Task Force*, Washington, D.C.: Department of Defense, 30 August 1996. Obtained on Internet at http://www.fas.org/irp/threat/downing/unclf913.html, [accessed 12 April 2006].

Drew, Dennis. "Airpower in the New World Order." Research Report, Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, 1993.

Final Report of the National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission Report), 1st ed. Vol 1. New York, NY: W.W. Norton, 2004.

Fox, Roger P. *Air Base Defense in the Republic of Vietnam*: *1961-1973*. Washington, D.C.: Office of Air Force History, 1979

Gerber, Cheryl. Lead Ahead for Force Protection. *Military Information Technology: Online Edition*, 2003. Obtained on Internet at http://www.military-information-technology.com/print_article.cfm?DocID=232, [accessed 19 August 2006].

Grossman, Elaine. "Combat Commanders Make Broad Access to Intelligence a Top Priority." *Inside the Pentagon*, 9 February 2006.

Headquarters, Air Mobility Command (AMC). *Integrated Base Defense Concept of Operations (CONOPS).* Scott AFB, IL: HQ AMC, 17 February 2006.

Headquarters, United States Air Force. *Air Force Regulation 355-4, Defense - Local Ground Defense of Air Force Installations.* Washington, D.C.: HQ Air Force, 3 March 1953.

Headquarters, United States Air Force. *Air Force Instruction 10-245, Air Force Antiterrorism Standards*. Washington, D.C.: HQ Air Force, June 2002.

Headquarters, United States Air Force. *Air Force Doctrine Document 2-4.1: Force Protection*. Washington, D.C.: HQ/Air Force, 1999.

Headquarters, United States Air Force. *Air Force Policy Directive (AFPD) 10-24: Air Force Critical Infrastructure Program (CIP)* Washington, D.C.: HQ Air Force, 28 April 2006.

Headquarters, United States Air Force. *Air Force Instruction 31-301, Air Base Defense*. Washington, D.C.: HQ Air Force, 15 May 2002.

Headquarters, United States Air Force. *Air Force Tactics, Techniques and Procedures 3-10.1, Integrated Base Defense.* Washington, D.C.: HQ Air Force, 20 August 2004.

Headquarters, United States Air Force (Air Force Inspection Agency), *Joint Protection Enterprise Network Eagle Look Report,* Washington, D.C.: HQ Air Force, November 2005.

Headquarters, United States Air Force. *Homeland Operations, Air Force Document 2-10*. Washington, D.C.: HQ AF, 21 March 2006.

HelenaIR Website. 200,000 People in U.S. Terror Suspect Database, Director Says, Associated Press, *Helena Independent Record*, 15 March 2006. Obtained on Internet at www.helenair.com/articles/2006/03/15/national/a05031506_01.txt, [accessed 12 June 2006].

Hertog, Mary J. Speech given at the Annual Security Police Association Meeting, Arlington, VA, September 2006. Taken from *Tiger Flight* 15, No. 6, November-December 2006.

Hettinga, Benjamin E., "The Defense of Tan Son Nhut Air Base, 31 January 1968: A Study in the Nature of Air Base Security." Masters Thesis, Ohio State University, 2001.

Hoffman, Bruce, Peter Chalk, Anna-Britt Kasupski, and Robert Reville. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act.* Santa Monica, CA: RAND, 2005.

Hoffman Bruce, Matthew Levitt, Daniel Benjamin. "The War on Terror in the Shadow of the Iraq Crisis."
PolicyWatch, no.690, 12 December 2002, p.2. Obtained on Internet at www.iraqwatch.org/perspectives/winep-pw690-121202.htm, [accessed 24 April 2006].

Holmes, Robert, et al. "The Air Force's New Ground War: Ensuring Projection of Air and Space Power through Expeditionary Security Operations." *Air and Space Power Journal*, Fall 2006. Obtained on Internet at http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/fal06/holmes.html (accessed on 14 November 2006).

Hoover, Karl. "Air Base Ground Defense, the Training Controversy." Research Report, Randolph Air Force Base, TX: History and Research Office, Air Training Command, 1991.

Keating, Timothy J. Statement before the Senate Armed Services Committee on 15 March 2005. Obtained on Internet at http://armed-services.senate.gov/statemnt/2005/March/Keating%2003-15-05.pdf [accessed 18 September 2006].

Kennedy, Harold. "U.S. Northern Command Actively Enlisting Partners." *National Defense Magazine*, June 2004.

Kozaryn, Linda. "DOD Releases Report on Khobar Towers Bombing," *American Forces Information Service* news article, September 1996, Obtained on Internet at http://www.pentagon.mil/news/Sep1996/n09181996_9609181.html, [accessed 23 September 2005].

Lehrer, Jim. "Germany arrests two suspected of planning Sept 11-related attack." Online NewsHour-Combating Terrorism, 2002. Obtained on Internet at http://www.pbs.org/newshour/terrorism/combating/index.html, [accessed 14 April 2006].

Lesser, Ian, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini. *Countering the New Terrorism*. Santa Monica, CA: RAND, 1999.

Military Intelligence Quotes website, Obtained on Internet at http://www.arrse.co.uk/cpgn2/Forums/viewtopic/t=30797.html, [accessed 18 June 2006].

Negroponte, John. Speech given on 27 September 2005 to the International Association of Chiefs of Police. Office of the Director of National Intelligence website: Obtained on Internet at www.dni.gov/inter_assc_chiefs_police.shtml, [accessed 23 September 2005].

NewsMax.com website. "Report: TALON to Gather Suspicious Information for DOD." June 30, 2003. Obtained on Internet at http://www.newsmax.com/archives/articles/2003/6/29/204152.shtml [accessed 19 July 2006].

Perry, William J. Perry. *Report to the President on the Protection of U.S. Forces Deployed Abroad*, 15 September 1996. Obtained on Internet at www.fas.org/irp/threat/downing/report_f.html, [accessed 12 June 2006].

Pike, John. 2005. Desert Hawk. Obtained on Internet at http://www.globalsecurity.org/intell/systems/desert-hawk.htm, [accessed 22 August 2006].

Pincus, Walter. *"Pentagon's Intelligence Authority Widens, Fact Sheet Details Secretive Agency's Growth From Focus on Policy to Counterterrorism.*" Obtained on Internet at Washingtonpost.com, [accessed 19 December 2005], p.1.

Poole, H. John. *Tactics of the Crescent Moon: Militant Muslim Combat Methods*. North Carolina: Posterity Press, 2004.

Poole, H. John. *Phantom Soldier: The Enemy's Answer to U.S. Firepower*. North Carolina: Posterity Press, 2001.

Purser, Wayne. "Air Base Ground Defense: A Historical Perspective and Vision for the 1990's." Research Report, Maxwell Air Force Base, AL: Air War College, 1989.

Record, James, Lt Gen. 1996. *Independent Review of the Khobar Towers Bombing, Part A and B.* Obtained on Internet at http://www.au.af.mil/au/awc/awcgate/khobar/recordf.htm, [accessed 10 May 2006].

Riley, K. Jack, et al. *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: RAND, 2005.

Ruppe, David. 25 January 2006. Report Encourages Pentagon to Focus More on Homeland Defense. Obtained on Internet at http://www.govexec.com/dailyfed/0106/012506gsn1.htm, [accessed 13 May 2006].

SAFESIDE Association. 2005. OPERATION SAFESIDE: History of the Combat Security Police. Obtained on Internet at http://safesideassociation.org, [accessed 26 June 2006].

Santayana, George. 2006. Obtained on Internet at http://www.wisdomquotes.com/002322.html., [accessed 24 April 2006].

Security Forces Transformation Newsletter, Security Forces Pentagon Edition 1, no. 1, March 21, 2006.

Shlapak, David A. and Alan Vick. *Check Six Begins on the Ground: Responding to the Evolving Ground Threat to U.S. Air Force Bases*. Santa Monica, CA: RAND, 1995.

Spence, Floyd, Chairman, House National Security Committee, The Khobar Towers Bombing Incident: Staff Report (Washington, D.C.: National Security Committee, 14 August 1996).

Tirpak, John A. To Provide for a Powerful Force, *Air Force Magazine Online*, 81, no.6 (June 1988). Obtained on Internet at http://www.afa.org/magazine/june1998/0698force.asp, [accessed 16 August 2006].

Turse, Nick. 2005. Bringing it All Back Home: The Emergence of the Homeland Security State. Global Policy Forum. Obtained on Internet at www.globalpolicy.org/empire/terrorwar/liberties/2005/0127emergence.htm, [accessed 18 October 2005].

Tussing, Bert B. 2004. Sharing Information for Homeland Security: Overcoming Obstacles of Technology, Process and Culture. Obtained from Internet at http://www.cusa.uci.edu/op3.htm, [19 September 2006].

USNORTHCOM/J34. *USNORTHCOM Joint Protection Enterprise Network Concept of Operations, version 2.1*. Colorado: Peterson Air Force Base, 23 August 2005.

Vick, Alan. *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases*. Santa Monica, CA: RAND, 1995.

Vizard, Frank and Scott, Phil. *21st Century Soldier: The Weaponry, Gear and Technology of the Military in the New Century*. New York: Popular Science, Time, Inc, 2002.

Website for Technical Surveillance Countermeasures (TSCM). Obtained on Internet at http://www.tscm.com, [accessed 20 March 2006].

White, Jonathan R. *Defending the Homeland, Domestic Intelligence, Law Enforcement and Security*, Belmont, CA: Wadsworth/Thomson, 2004.

Wieman, Steve. Vietnam Security Police Association website. 1998. Vietnam Operation SAFESIDE Final Report: Letter from Lt Gen William W. Momyer to HQ AF. Obtained on Internet at http://www.vspa.com/phan-rang-safeside-final-report-1967.htm, [accessed 12 August 2006].

Wilkinson, Paul. *Terrorism versus Democracy: The Liberal State Response*. Portland, OR: Frank Cass Publishing, 2000.

Young, D.T. "Security Forces Transformation: Why, What For?" *Air Force Print News Today*, 27 January 2006, p.1. Obtained on Internet at http://www.minot.af.mil/news/story_print.asp?storyID=123018665, [accessed 23 September 2006].

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California