AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Abandoning the Battleship: The Asymmetric Ground Defense of Air Power

by

Christophe J. DeGuelle, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Lewis Griffith

Maxwell Air Force Base, Alabama

April 2009

| | | | Form Approved OMB No. 0704-0188 |

Report Documentation Page

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Abandoning the Battleship: The Asymmetric Ground Defense of Air Power**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The pre-World War II Navy was centered upon the independent battleship. Much like the modern air base, the battleship was a lethal, heavily armed, and potent symbol of global power projection. The battleship was characterized by its self-sufficiency on the open seas. Nothing could challenge its dominance.1 Unfortunately, the modern air base often times operates as if it too were alone on the open seas with no discernable threat able to encroach on its security zone undetected. Air base security posture frequently ignores the immense capabilities in the civilian community that can be incorporated into base security planning. Just as the U.S. Navy abandoned the battleship, it‟s time the Air Force abandon its battleship mentality of force protection. In an age of asymmetric warfare and terrorism it is important to know thy enemy. In particular, the focus is primarily upon Al Qaeda and those who identify with its ideology (AQAM). We have already historically seen Al Qaeda maintain focus on one target set until it achieves its objectives. The first and second attacks on the World Trade Center exemplify this focus. Through open source reporting we have seen AQAM attempt to attack CONUS installations in New Jersey, Delaware, and Pennsylvania2. Provided AQ, or its believers, have not radically changed their method of operation, we should expect that they will continue to target CONUS military installations. An attack on an air base would have immense strategic value. AQAM has shown that is has the intent to attack US-based installations the question for us is how we can prevent them from obtaining the opportunity and capability to do so.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **42**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

AU/ACSC/DeGuelle/AY09

Table of Contents

Abstract

The pre-World War II Navy was centered upon the independent battleship. Much like the modern air base, the battleship was a lethal, heavily armed, and potent symbol of global power projection. The battleship was characterized by its self-sufficiency on the open seas. Nothing could challenge its dominance.[1] Unfortunately, the modern air base often times operates as if it too were alone on the open seas with no discernable threat able to encroach on its security zone undetected. Air base security posture frequently ignores the immense capabilities in the civilian community that can be incorporated into base security planning. Just as the U.S. Navy abandoned the battleship, it's time the Air Force abandon its "battleship mentality" of force protection.

In an age of asymmetric warfare and terrorism it is important to know thy enemy. In particular, the focus is primarily upon Al Qaeda and those who identify with its ideology (AQAM). We have already historically seen Al Qaeda maintain focus on one target set until it achieves its objectives. The first and second attacks on the World Trade Center exemplify this focus. Through open source reporting we have seen AQAM attempt to attack CONUS installations in New Jersey, Delaware, and Pennsylvania[2]. Provided AQ, or its believers, have not radically changed their method of operation, we should expect that they will continue to target CONUS military installations. An attack on an air base would have immense strategic value. AQAM has shown that is has the intent to attack US-based installations – the question for us is how we can prevent them from obtaining the opportunity and capability to do so.

---

[1] ACSC, JF.

[2] Caudill, Shannon W., *"The Fort Dix Six: Lessons Learned."* Washington, D.C.: Joint Staff. November 2006, 5.

Acknowledgments

I would like to thank my advisor, Dr. Lewis Griffith, for his assistance and guidance. Additionally, I owe a huge debt of gratitude to my fellow graduates of the Federal Bureau of Investigations National Academy who were so quick and willing to help and guide me. I especially thank Arizona Department of Public Safety Commander Dan Wells and Sergeant Ken Morris of the Arizona Counterterrorism Information Center for their invaluable help in showing the advantages of interagency cooperation. The work they do to protect the state of Arizona and its citizens is commendable.

I would also like to thank the senior leaders of the Security Forces community for their faith in my abilities and for releasing me from a critically stressed career field to pursue another professional academic endeavor. I am deeply indebted for this opportunity.

I would also like to thank my wife and daughter for their unending patience, understanding, and support. Without their unconditional support, my career endeavors and successes would not have been possible.

Finally, I am eternally grateful to the brave men and women of the Security Forces career field who bravely fight terrorism and criminality on a daily basis. To A1C Elizabeth Jacobson, A1C LeeBenard Chavis, A1C Jason Nathan, SSgt Travis Griffin, SSgt John Self, SSgt Brian McElroy, and TSgt Jason Norton, all of whom gave the ultimate sacrifice fighting America's enemies, we owe our eternal gratitude.

SECTION 1 – INTRODUCTION

"It is in the nature of cavalrymen to believe in cavalry, bomber generals to believe in bombers, carrier admirals to believe in carriers. When the weapons they believe in become obsolete, generals and admirals usually become obsolete at the same moment, because they will not change their beliefs." - Joseph Alsop[3]

The September 11 attacks on the World Trade Center and the Pentagon marked the opening salvo in what would become the Global War on Terrorism. It also marked a significant change in the tactics used by terrorists in their war against the U.S. and the West – a decided effort to hit America on its own turf. The attacks were symbolic in that the Al Qaeda network attempted to attack the full spectrum of the American instruments of power. In the seven years since the attack, the U.S. has engaged terror networks throughout the world using military, intelligence, diplomatic, law enforcement and financial institutions in an attempt to achieve decisive victory. Despite these efforts, AQAM has still managed to execute deadly attacks in the West and against western interests. Most concerning for military force protection professionals have been attempts to attack military installations located in the continental United States (CONUS).

The Air Force primarily defends its installations through the use of security forces (SF).[4] Unfortunately, the doctrine and guidance which directs the employment of these forces has been slow to evolve to the threat of modern terrorism. Instead it still primarily relies upon installation entry control points and random patrolling. There is an overwhelming tendency for these forces to focus efforts on policing the force versus protecting the force. Furthermore, the response forces tend to be concentrated in the vicinity of high value assets (aircraft, weapon systems, etc.).

---

[3] Alsop, Joseph. "Quotes." www.wisdomquotes.com (accessed on 21 Dec 08).
[4] Security Forces, Military Police, defense forces, law enforcement, policing, base defense, and air power defense are used interchangeably throughout this paper.

In essence, the response force is positioned to engage an adversary once he has already arrived at the resource.

Ground intelligence is similarly lacking. The author's experience with wing intelligence briefs to senior staff has been international focused updates on world crisis spots and far-away enemy capabilities. This information has strategic value but tactically the information does nothing to protect and defend the mission of the installation. Simply put, local ground intelligence is, in the author's experience, lacking. It is further exacerbated by having four separate investigative and intelligence agencies on the installation operating under four different chains of command. The lack of unity of command prevents a common operating picture to properly employ ground-based response forces.

In short, the current U.S. Air Force force protection (FP) efforts at US-based (CONUS) installations are inadequate and need to be dramatically overhauled to match the current nature of modern terrorist warfare. Local civilian law enforcement and intelligence sharing organizations in the communities surrounding our installations already exist, however, lack of active membership, participation and involvement hinders our FP effectiveness. The AF can maximize economy of force through interagency cooperation and partnership.

The purpose of this paper is not to "throw rocks" at the Security Forces, OSI, Intelligence, or Force Protection Officer career fields. There are severe impacts from the operations tempo over the past seven years on the fore-mentioned career fields. Their contributions at home and abroad have been instrumental to the success in the War on Terror. The success in combat however should not distract us from evolving to protect air power in our own backyards.

Significance

The evolutionary study of the ground defense of air power is vital to educating airmen on the dangerous implications of ignoring the vulnerability of assets on the ground. Air bases have historically been attacked as a way of pursuing a broad range of objectives, from the ambitious goal of capturing an airfield to the minimalist goal of harassing air base operations.[5] The USAF experience has typically been void of ground threat to air bases and the asymmetric threat to airmen on the ground in Vietnam and Saudi Arabia were treated as anomalies. The changing nature of war drives reconsideration of this vulnerability to the national ability to project power.

The focus of this research is 'rear area' and CONUS air bases. The preponderance of existing research has focused on the defense of air power in combat zones. The successes of Task Force 1041, operating 'outside the wire,' to secure Balad Air Base showed the efficiency of intelligence-led policing and defensive operations.[6] TF 1041 engaged the local population in the ground intelligence collection program with impressive results. These lessons must be applied to CONUS-based installations. This paper will examine the current security posture at most Air Force installations and examine how that posture reflects the traditional USAF ideology of protection "inside the fenceline" as well as a historical reluctance to participate in ground intelligence operations. This review is necessary to develop and understanding of how ideology and culture affect today's employment of defense forces and a corporate reluctance to operate "outside the wire."

---

[5] Vick, Alan. *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases.* Santa Monica, CA: RAND, 1995, Pg 9.

[6] Palmer, Glenn E. *Air Base Security Operations: An Air Component Responsibility.* Maxwell AFB, AL: School of Advance Air and Space Studies, June 2006 p. 26-30. Task Force (TF) 1041 was an Air Force Security Forces unit charged with dominating the Base Security Zone outside of Balad Air Base, Iraq. The TF employed principles of community policing and engaged the local population in dismounted patrols. The result was an influx of intelligence that was used to identify and apprehend over 100 insurgents. The actions of TF 1041 virtually eliminated the indirect fire attacks on Balad AB.

SECTION 2 – A HISTORICAL RELUCTANCE

The Threat

The invincibility of American air superiority is a given. Conventional and insurgent forces know that they cannot effectively engage US air power in combat without facing devastating losses. This fact leaves them with two options: avoidance or engagement when air assets are most vulnerable. American air power is most vulnerable on the ground. This was noted by early air power theorist Guilio Douhet who 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."[7]

Non-conventional forces have targeted air power in its nest throughout history. The air force of El Salvador "suffered a major blow in January 1982 when 5 Ouragans, six UH-1Bs, and three C-47s were destroyed and another five aircraft were badly damaged on the ground at Ilopango in a raid by one hundred rebel commandos. At one stroke, most of El Salvador's operational combat aircraft were knocked out of action."[8] The United States has also suffered the loss of aircraft on the ground. In Vietnam, the Viet Cong and North Vietnamese army launched attacks that destroyed 99 US and South Vietnamese aircraft. They further damaged another 1,170.[9] During the same period the United States only lost 62 to enemy aircraft.[10] In the current conflict in Iraq, indirect fire killed 14 personnel on air bases, wounded another 25 and damaged one F-16, one UH-60 and three CH-47 helicopters.[11] While the American experiences

---

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

[8] Corum, James S. and Johnson, Wray R. "Airpower in Small Wars: Fighting Insurgents and Terrorists." Lawrence, Kansas: University of Kansas Press, 2003, *334*.

[9] Vick, *Snakes in the Eagle's Nest,* 68.

[10] Chambers, James J., "Force Protection for the 21st Century Expeditionary Aerospace Forces: Security Forces Need for Organic Ground Intelligence." Maxwell AFB, AL: Air Command and Staff College, April 1999, 10.

[11] Palmer, *Air Base Security Operation,* 26

in Vietnam and Iraq were no where near as catastrophic as the almost total destruction of the El Salvador Air Force, it does show that our assets are being targeted.

It is not beyond the realm of possibilities that as war zone targeting remains relatively unsuccessful in deterring air power that adversaries will refocus their efforts on more lightly defended targets. An Al Qaeda inspired organization has already shown intent to attack CONUS-based installations. The "Fort Dix Six" as they are known "planned to storm the base armed with automatic rifles and kill as many soldiers as possible."[12] The cell also conducted surveillance on Dover AFB but chose to avoid that target based on the "assessment that the base was too difficult of a target because of its high security."[13] This is the first publicly known instance in which air power has been targeted domestically. It does however follow an Federal Bureau of Investigations assessment in which a "brand-new form of terrorism" is "focused on targeting of US military bases and events in homeland."[14] The threat to airpower in CONUS should drive the USAF to refocus its counter-terrorism operations and intelligence capabilities. Institutional cultural baggage however can over rule the implementation of more effective tactics, techniques, and procedures.

Operations Outside The Wire

The Air Force became a separate service in 1947 in what could be considered a "nasty divorce." The joint service agreement between the air and ground services "acknowledged their responsibility for defending their own installations. However it did not specify an Air Force ground combat mission, or specifically determine how the Air Force would defend its air

---

[12] Khalil, Lydia. "Threat Analysis Subject: Fort Dix, New Jersey Terror Plot." *NYPD Shield* (May 2007). http://www.nypdshield.org (accessed 26 January 2009), 2.
[13] Caudill, *The Fort Dix Six: Lessons Learned,* 8.
[14] Ibid, 3.

bases."[15] Early experiences further culturally attuned the Army Air Corps and subsequent US Air Force to ignoring the importance of a robust ground combat force to protect air assets on the ground. "Due to the trench warfare that occurred in World War I, no guerillas, insurgents or other irregular combatants disturbed the security of air bases or other rear area installations. Consequently, air base security measures never progressed beyond the venerable interior guard system."[16] The US experience in World War II was remarkably similar as air bases rarely faced ground attacks. In Korea, "although 32,000 to 35,000 North Korean guerillas were operating in United Nations's territory, they ignored air bases as key targets."[17] Thus leading to the conflict in Vietnam, the Air Corps/Air Force never faced the need to defend the base on the ground. It created an institutional bias whereby base defense was focused on preventing pilferage and fights at the club.

The concept of institutional bias against developing a ground combat force that could dominate the entire security footprint of an air base was also deeply rooted in the predominance of the Strategic Air Command (SAC) and service focus on strategic deterrence. SAC and its bombers dominated service culture and the bomber generals commanded the Air Force. Of the 17 senior Air Force generals in 1960, 11 of them came from a bomber background.[18] The SAC/bomber mentality was that air power could be decisively unleashed from lightly guarded air bases far in the rear and away from combat and guerilla action. SAC, and thus the rest of the Air Force, codified the mission of the Security Police in Air Force Regulation 205-5. This regulation "placed a new emphasis on internal reinforced security, with an expanded interior guard system

---

[15] Ditlevson, Jeffery T. "Air Base Defense: Different Times Call for Different Methods." Monterrey, CA: Naval Postgraduate School, December 2006, 15.
[16] Fox, Roger P. *Air Base Defense in the Republic of Vietnam, 1961-1973.* Washington, D.C.: Office of Air Force History, 1979, 1.
[17] Ibid, 6.
[18] Worden, Mike, Col. *Rise of the Fighter Generals.* Maxwell AFB, AL: Air University Press, 1998, 243.

to counter covert threats considered 'inside the wire.' Unyielding AP (Air Police) policy enforcement of these critical areas became possible through the use of strict personnel access control."[19] Thus the focus became protecting air power at the flight line. This inward focused policy was the equivalent of playing defensive football by setting up on the goal line and allowing the opponent full use of the field. It created a mindset for senior Air Force commanders that the SP mission was "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."[20] This policy and mindset would prove disastrous for the Air Force in Vietnam.

Vietnam marked the first US Air Force experience of having air bases targeted. The Air Force initially looked to the Army to defend the security zone outside the fence line. "General Westmoreland, Commander, U.S. Military Assistance Command, Vietnam, was adamantly opposed to this idea. 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."[21] Additionally he ordered air base commanders to develop forces to protect their installations. Even with this guidance the Air Force still "interpreted this to mean their security personnel would continue to apply their air base defense energy on the internal portions of installations."[22] The enemy, realizing that the service would not commit ground forces 'outside-the-wire,' typically resorted to indirect fire attacks hampering air operations, destroying aircraft and equipment, and harming personnel. This would not be the last time American air power was targeted in irregular warfare, however the lessons learned by the

---

[19] Ditlevson, *Air Base Defense*, 18.
[20] Ibid, 62.
[21] Ibid, 4.
[22] Ibid, 4.

Security Police and Office of Special Investigations would be lost and viewed as an anomaly by the institutional Air Force. Vietnam would remain a doctrinal anomaly.

Operation Desert Storm saw a return to the preconceived notions of the secure air base in the rear area. The Iraqi military, outgunned and outmatched, was simply unable to conduct ground operations in the rear area. Terrorist actions in the rear area were also non-existent. Air base defense was again relegated to patrolling the interior lines and relying on the sister services to protect the rear area. "The total success of the military operations in the Gulf War sealed in the minds of the American people and military leadership an invincibility."[23]

In the aftermath of the Gulf War, the United States remained firmly entrenched in the Middle East supporting the containment of Saddam Hussein. Again, the service mindset was security inside the wire. In all fairness, in this case they were also contained by local agreements and Saudi sovereignty. The conceived notion of invincibility from Desert Storm contributed to the deaths of 19 airmen in the 1996 terrorist attack on the Khobar Towers housing complex. The attack eerily resembled the 1983 attack on the Marine barracks in Lebanon. It also served as a notice that airmen and their installations were considered "fair game" by terrorists.

The Air Force mindset of security from "within the wire" has been firmly established by historical engagements dating back to the first use of airpower in conflict. Vietnam should have served notice that protecting air power on the ground should have a higher priority but it did not. It should have served as a call to move "outside the wire" to dominate a base security zone. It was not until after the Khobar incident, that the Chief of Staff, General Ronald Fogleman, stated "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."[24]

---

[23] Chambers, *Force Protection for the 21st Century*, 18.
[24] AFDD 2-4.1, *Force Protection,* 33.

Ground Intelligence

The key to dominating terrain and personnel "outside the wire" is good intelligence. Unfortunately this is another area in which the Air Force has shown a historical reluctance to engage. The primary mission of Air Force intelligence units is to provide support to air combat and forward ground targeting and only limited ground threat intelligence. The Office of Special Investigations (OSI) "is the lead Air Force agency for collection, investigation, analysis and response for threats arising from terrorists, criminal activity and foreign intelligence and security services.[25] OSI is an independent agency and reports to a regional commander, not the installation commander. Security Forces Intelligence and Investigations (S-2) provides the liaison to OSI and IN but are typically untrained in intelligence collection or analysis. This leaves a huge ground intelligence void for the ground Defense Force Commander (DFC).

The lack of ground threats to US installations did not necessitate the building of a ground intelligence capability. In Vietnam, the requirement for good ground intelligence became a vital necessity to the protection and employment of air power. "As a result of the stinging attacks during Tet, Seventh Air Force saw the need for having an intelligence system organic to the base defense role and directed each security police squadron support an intelligence section."[26] This mandate, like many past and current headquarters mandates, was neither funded nor did it provide the manpower authorizations. As a result the positions were filled from existing manpower authorizations within the security police squadrons. The result was the removal of combat power from the frontlines and the filling of intelligence positions with untrained collectors and analysts. This practice is still in effect today.

---

[25] AFI 14-119, *Intelligence Support to Force Protection,* 4.
[26] Chambers, *Force Protection for the 21st Century*, 13.

Ground forces continually used innovative methods to counter the threat to American air power. OSI proved to be an invaluable player in the ground intelligence role outside the wire. The OSI Area Source Program (ASP) was focused on "acquiring information related to the plans and order of battle of the enemy forces within the standoff zones of the Air Force bases."[27] ASP focused on recruiting sources from the communities within the standoff zone. These sources were typically local farmers or laborers who were intimately familiar with the area. The application of investigative and personal interactive skills the agents had developed conducting peacetime investigations to recruit local foreign nationals to provide intelligence on local "bad actors" and pending attacks. ASP proved to be a huge success. "From August 1968 through November 1969, ASP generated 78.3% of all DoD intelligence information and 84.1% of the total items in the report."[28]

The Pacific Air Forces (PACAF) Directorate of Security Police saw the effectiveness of a ground intelligence program in defending the installation and mandated "security police intelligence sections to be responsible for local intelligence from the base to 30 kilometers out."[29] However the PACAF Director of Intelligence non-concurred with this assessment and recommended to the Air Staff that "no changes are required at either headquarters or base level in the intelligence function as related to base defense."[30] Despite the highly effective programs employed by the Security Police and OSI in Vietnam, this one single recommendation doomed any chance of an official Air Force focus on ground intelligence. Subsequently, the end of US involvement in Vietnam and return to a "safe behind the lines" CONUS-base security posture relegated these invaluable lessons to the historical archives.

---

[27] Chambers, *Force Protection for the 21st Century,* 14.
[28] Fox, *Air Base Defense in the Republic of Vietnam* , 142.
[29] Chambers, *Force Protection for the 21st Century,* 15.
[30] Fox, *Air Base Defense in the Republic of Vietnam* , 144.

It was not until after the Khobar Towers attack that the magnitude of the PACAF/IN recommendation came to light.   The subsequent investigation by the Downing Assessment Task Force provided a damning assessment of the service's ground intelligence capabilities. Finding #11 found, "the lack of an organic intelligence support capability in US Air Force Security Police units adversely affects their ability to accomplish the base defense mission."[31] The report further detailed an inefficient intelligence chain of command which focused entirely on the air threat during Operation *Southern Watch*. The OSI had previously noted

> "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"[32]

The historical service focus on solely producing an air intelligence sight picture exposed a soft rear area ripe for enemy attack. The service however continued to view the threat and need for an effective ground intelligence program as an anomaly.   Thus the "battleship" continued to float on unaware of local threats and with little effort to create local tactical intelligence. For CONUS installations, the prevailing perspective was the threat existed "over there."

---

[31] Downing Assessment Task Force. *Force Protection Assessment US CENTCOM and Khobar Towers, Vol 1.* August, 1996, 33.

[32] Record, James, Lt Gen. 1996. *Independent Review of the Khobar Towers Bombing, Part A and B*. http://www.au.af.mil/au/awc/awcgate/khobar/recordf.htm, (accessed 10 May 2006), 32.

SECTION 3 – WHERE WE ARE AND WHERE WE NEED TO GO

"It is not the police; it is not the intelligence services that will defeat terrorism. It is communities that will defeat terrorism."[33] - Sir Ian Blair, Chief Metropolitan Police

Historical biases and perceptions of the role of base defense and policing have relegated the traditional role of the base defense force to a prescribed, static, and highly reactive response capability. Base defense follows the defensive strategy employed by most US government agencies -- defense in depth. "This approach integrates the capabilities of people, operations, and technology to achieve strong, effective, multi-layer, and multi-dimensional protection."[34] Conceptually this concept makes sense and it can be effective. However, the majority of USAF defense forces are dedicated to entry control and near-static resource defense. The "integrated capability" is typically left to the installation defense forces instead of being a whole base effort.

Base patrolling is typically restricted to internal patrol sectors and conducted randomly at the whim of the patrol officer. It is highly subject to being utilized for parking details, loose pet apprehension, and other administrative details that are not focused on the defense of air power. Further compounding the problem, high deployment rates and constant post rotations do not allow patrol officers to become intimately familiar with their beats. The result is an effort that is resource- vice person-focused and distracted by non-defense and policing associated tasks.

Counterterror and policing patrols focus on presence. This is the concept that the presence of a police patrol will have the effect of deterring crime. This conceptualization is faulty. The 1973 Kansas City Preventative Patrol experiment showed "that routine preventative patrol in marked police cars has little value in preventing crime or making citizens feel safe."[35]

---

[33] Peed, Carl R. "The Community Policing Umbrella." *FBI Law Enforcement Bulletin,* November 2008, 24.
[34] Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, DC: Potomac Press, 2004, 81.
[35] Kelling, George L., Pate, Tony, Dieckman, Duane, and Brown, Charles E. *The Kansas City Preventative Patrol Experiment*. Washington, D.C.: Police Foundation, 1974, vii.

Despite the results of this twenty-five year old study, the standard ideology still follows that of the late O.W. Wilson, Chicago Chief of Police who stated, "patrol is an indispensable service that plays a leading role in the accomplishment of the police purpose. It is the only form of police service that directly eliminates opportunity for misconduct."[36] This is not to denigrate the value of patrolling but if it is done blindly it is worthless. Good ground intelligence needs to drive patrol operations.

Installation entry control is the first line of air power defense. "Based on contemporary worldwide threat analyses, installation ECPs [Entry Control Points] represent the most likely venue for adversaries to attempt access to installations to execute vehicle-borne attacks."[37] ECPs serve as "as a vital element in the successive lines of defense (defense in depth) that defend our personnel, resources, and our ability to execute airpower operations."[38] In reality however, ECPs are the weakest link in installation defense. They are typically manned with either entry-level airmen or low-paid contract or government service personnel. Base access policy at many installation results in numerous personnel being granted entry without valid identity verification. Far more focus is paid to those personnel who we have already vetted (servicemembers, etc.) while contractors and delivery personnel are seldom vetted. Exceptions to policy also create a wide gap in front-line defense.

A move toward intelligence-led policing is not currently possible at most installations. The current dissemination of strategic and operational "intelligence" is valuable for identifying the tactics, techniques, and procedures of the current enemy. However, there typically is very little local intelligence provided to response forces. Inter-agency information sharing is

---

[36] Kelling, *The Kansas City Preventative Patrol Experiment*, 1.
[37] AFI 31-101 (draft), *Integrated Defense,* 36.
[38] Ibid, 36.

haphazard and varies widely from installation to installation. A permanent presence by SF, IN, or OSI at local Joint Terrorism Task Forces (JTTFs) or state intelligence fusion centers is almost non-existent. The move to intelligence-led policing is further hampered by a lack of unity of command. The typical USAF installation law enforcement, security and intelligence apparatus is separated into four offices, each under the command of a separate entity, and thus a separate organizational culture and mission focus.

In addition, there has typically been no attempt to physically or psychologically dominate the terrain (base security zone) outside the perimeter fence. Relations with local police and intelligence forces vary widely by installation and are typically personality based. They flourish or diminish with the rotation of commanders and staffs. Relationships with local residents and businesses in the area around the installation are similarly non-existent. Thus, the persons who are likely to first encounter suspicious activity in the base security zone may or may not inform the installation or local police forces. Overall, in order to properly defend air power the current method of operation needs to change to reflect an asymmetric response to an asymmetric threat. The logical move to respond to an asymmetric threat to air power is to implement a patrol and security scheme that is driven by local ground intelligence. This will require a mindset change and a focus on integrating with local police and intelligence agencies on more than an ad hoc basis. It will also require the development of memorandums of understanding with local communities as we seek to dominate the base security zone.

The first step in revitalizing air power defense is to focus on installation entry control procedures. Once the base perimeter is hardened with vehicle denial cabling and perimeter sensors to detect unauthorized entry, the ECP becomes the weakest link in the defense chain. The focus of base ECPs should not be expediency of entry but on the defense of air power.

Policy is the first weakness. A significant amount of time and money is spent to vet military,

civilian and contract personnel who live and work on the installation. Paradoxically, these

individuals receive the most attention and inspection when entering and exiting the installation.

Infrequent visitors and delivery drivers – individuals who are unknown entities to the base

defense forces -- are sometimes permitted unlimited access on the basis of convenience. The

example of the Fort Dix plotters who used a pizza delivery service to conduct surveillance and

targeting shows the travesty of this policy. The suspect knew the installation "like the back of

his hand,"[39] based on his being able to access the installation indiscriminately. Homeland

Security Presidential Directive 12 (HSPD-12) states, "Department and Agency heads must

conduct a background investigation, adjudicate the results, and issue identity credentials to their

employees and contractors who require long-term access to Federally controlled facilities and/or

information systems."[40] While this standard is applied to permanent party and frequent visitors,

a similar standard should be applied to infrequent visitors and guest seeking access to the

installation. At one air base located in a major metropolitan area, all visitors to the base were run

through a basic wants and warrants check. Over the course of a year, over 200 visitors were

identified as having outstanding felony warrants ranging from drug offenses to major violent

crimes.[41] The capability to conduct instantaneous wants and warrants checks at ECPs through

the state or national criminal database should be implemented immediately. Similarly, blanket

approvals for entry to the installation for should be limited and require the approval of the

installation commander.

---

[39] Khalil, *Threat Analysis,* 5.

[40] Bolten, Joshua B. *Implementation of Homeland Security Policy Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.* Washington D.C.: Office of Management and Budget, 5 August 2005, 2.

[41] Wilson, Patrick, Chief Master Sergeant, USAF, Luke AFB, AZ. To the author. Email, 18 March 09.

Installation patrolling and response forces are the next areas that require adjustment. Patrols are currently divided into security response patrols (internal/external security patrols) and law enforcement patrols. The contribution of law enforcement and security to integrated defense should not be understated. However, maintaining an internal focus creates a level of animosity between the security force and the population it is in place to protect. The same people who are asked to be the installation "sensor system." To overcome this potential animosity, the focus should be directed toward "outsiders" and problem-oriented policing used to address internal problems. Doing this we can win the "hearts and minds" of the base populace thereby making them more likely to report activity, thereby becoming, in effect, a secondary "sensor system."

The concept of the Community Liaison Officer (CLO) is not new to the civilian communities. It is relatively foreign to military installations. The CLO is a single patrol officer that is dedicated to high population areas such as housing and community areas. Ideally they have office space in the local community center and have access to a golf cart to "patrol" their assigned area. "Patrol" in this instance is more of a meet and greet function and being a familiar face to local residents. The role of the CLO is to implement a problem-oriented policing solution to reduce criminal activity or nuisances in population area. By being permanently assigned to a "beat," the officer becomes a part of the community and develops an awareness of bad actors in the area and local trends. They assist in developing community based solutions to problems. The CLO should be assigned to the Security Forces Intelligence and Investigations branch and should be a sitting member of the installation intelligence fusion cell.

The protection and safety of personnel is not to be disregarded and there is still an active need and role for traditional law enforcement in base defense. Policing vehicular traffic is a vital cog in an installation safety program. It also provides an opportunity for contact with

offenders. It should be noted that Oklahoma City bomber Timothy McVeigh was caught on a

traffic stop.[42] However, instead of the prescribed 24/7 police patrol, it should be focused on peak

traffic periods with random implementation during non-peak hours. Manpower saved by using

only one patrol for this service can be reallocated a counter-threat patrol.

Counter-threat patrols are permanent teams trained to conduct emergency response, high-

visibility counter threat presence, as well as advanced law enforcement and problem-oriented

policing skills. They should be directed to patrol areas as determined by the installation

intelligence fusion cell and the DFC intent. They maintain a secondary response to incidents

involving high-risk or priority resources. They can also be used to provide presence in the Base

Security Zone to deter perimeter surveillance and conduct Random Anti-Terrorism Measures

(RAMs) on the installation. They must be highly flexible, highly mobile, and highly visible.

Security patrols assigned to protect physical resources should be moved as far out from

the resources as possible and focus on likely avenues of approach. This is should particularly be

considered during hours when maintenance and operations work hours. In essence, the armed

patrols should focus on external threats from likely avenues of approach while maintenance and

operations personnel, close in on the resource, provide the final sensor line. Protection of vital

warfighting air power assets needs to be a community affair.

The overall key to implementing a successful, threat-based, community-oriented patrol

scheme as described above is access to good ground intelligence. The CLO and counter-threat

teams, when properly trained, can become invaluable sources of information to drive operational

patrols. The inclusion of base assets such as the Office of Special Investigations, Intelligence,

and Anti-Terrorism Office into an installation-level intelligence fusion cell (IFC) is vital. The

---

[42] McCormack, William. "State and Local Law Enforcement Contributions to Terrorism Prevention." *FBI Law Enforcement Bulletin,* March 2009*, 6.

IFC should include full-time and part-time representation and report directly to the DFC. This

TACON/OPCON is vital to ensure unity of command. This should not be viewed as "empire

building." Simply stated, the current status of four agencies with four separate commanders

cannot effectively provide the ground intelligence required to drive intelligence-led force

protection operations against an asymmetric threat.

The installation IFC should further be integrated into the local community to ensure they

develop a full-spectrum sight picture. In this instance a clear division of labor between the

installation defense force and OSI needs to be established. The typical OSI detachment simply

does not have the manpower resources to be present at all community organizations, thus a

division of labor is necessary. Off-the-installation representation should be provided at local

detectives meetings, terrorism task forces, and major crimes boards. The purpose, in addition to

gaining a local threat intelligence picture, is to develop strong interpersonal relationships

between individuals and agencies. These relationships can pay huge dividends in times of crisis.

It is also vital that the DFC also be integrated into the local law enforcement and intelligence

communities. Membership *and attendance* at senior law enforcement groups such as the state

Chiefs of Police and local Chief's boards should be mandatory and an IG inspectable item.

The final step in revamping force protection operations beyond the battleship mentality is

to develop a methodology and ideology of dominating the area of influence outside the base

perimeter. This domination should be done physically (where permissible) and psychologically.

It will require a strong partnership between the installation defense force, OSI, and the local

jurisdiction.

Defining and Dominating the Base Security Zone

Defense forces were able to dominate the area "outside the wire" against an asymmetric foe in Vietnam. The application of these principles can be used to defend today's air bases. The area outside the wire is referred to in developing air power doctrine at the Base Security Zone (BSZ). It is defined as:

> "The area outside the base perimeter from which the base may be vulnerable from standoff threats (e.g. mortars, rockets, MANPADS). The base commander is responsible for identifying the base security zone and coordinate with the host nation or area commander for the base security zone to be identified as the base boundary. If the base boundary does not include all of the terrain of the base security zone, the base commander is still responsible for either mitigating (though coordination with the area commander of host nation) or accepting the risks of enemy attack from the area the terrain outside the base boundary. Base security zone is an Air Force-specific term that should be used intra-Service only."[43]

Notionally, the BSZ is the area outside the base perimeter fence line that the commander needs to dominate to ensure unhampered employment of air power. The draft version of Air Force Instruction 31-101 admits that it is "an emerging concept, especially for CONUS and non-contingency OCONUS locations."[44] It leaves considerable discretion to the installation commander and DFC to determine the exact physical delineation of the BSZ as well as how to best dominate the area.

The ability to dominate the BSZ will be largely determined by METT-TC.[45] For most installations, terrain and civil considerations will determine the BSZ domination planning. The overall goal of BSZ domination is to prevent threats to airpower and prevent the "gathering of information about the enemy, the land, the installations, and the neighbors."[46] The first step is to develop a community-based approach to policing the BSZ. In the majority of instances the

---

[43] AFI 31-101 (draft), *Integrated Defense,* 27.
[44] Ibid, 27.
[45] Mission, Enemy, Time, Terrain, Troops available, and Civil considerations
[46] Al-Qaeda, *Military Studies in the Jihad Against Tyrants,* 42. In this case the term enemy refers to enemy of Al Qaeda.

communities surrounding the air base perimeters are permissive environments. Local businesses in the BSZ, many owned and operated by patriotic Americans, provide an untapped source of information of happenings on the base perimeter. The "recruitment" of these businesses as a "first line sensor" could provide information on out of the ordinary persons and vehicles.

The New York Police Department has successfully implemented a civic-based approach to encourage businesses to be on the watch for potential acts of terrorism. It launched an intensive "If You See Something, Say Something" campaign in coordination with Operation Nexus.   The department worked with private business to develop "a nationwide network of businesses and enterprises joined in an effort to prevent another terrorist attack against our citizens."[47] Under this initiative detectives conducted over 25,000 visits to firms and trained owners and employees in recognizing and reporting "suspicious business encounters that they believe may have possible links to terrorism."[48] For air bases, a similar program should be established. This could be done simply by conducting site visits with business owners and employees and providing them with a phone number to call if they see something suspicious. Information provided by persons who are on the installation perimeter for most of the working day and even late night hours can be invaluable to developing an intelligence-led policing (ILP) operations scheme. It "is a useful strategy that can help law enforcement agencies better prepare for and prevent serious violent crime and act of terror. ILP can take advantage of partnerships built through community policing by leveraging the trust between citizens and law enforcement."[49]

---

[47] New York Police Department. *NYPD Shield: Operation Nexus.* https://www.nypdshield.com/secure (accessed 14 January 2009).
[48] Ibid.
[49] Peed, *The Community Policing Umbrella*, 23.

This partnership needs to be developed in coordination with local jurisdictions to ensure an appropriate response but the first call should be to the installation defense force to ensure an immediate visual assessment is conducted. A joint military/civil jurisdiction partnership is also vital to established the BSZ patrolling plan. The local jurisdiction, as well as the local FBI office, needs to be made aware of the installation mission and the importance of that mission to the national defense. This information is valuable to local and national forces as they develop state and national critical infrastructure security planning and patrol allocations. It can also result in the installation being included in the civilian Buffer Zone Protection Program[50]. The integration of military and civilian communities can be a force multiplier in the defense of air power.

---

[50] The Buffer Zone Protection Program is specific to the State of Arizona and is designed to protect the area around the perimeter of critical infrastructure. It is discussed in further detail later in this paper.

SECTION 4 – INTERAGENCY CASE STUDY

There are enormous benefits available to base defense forces through participating in "a cross-jurisdictional partnership, integrating local, state, and federal law enforcement as well as first responders, emergency management and, when appropriate the private sector."[51] The current National Military Strategy of the United States also emphasizes the importance of interagency operations. It states (emphasis added):

> "Commanders must ensure military activities are integrated effectively with the application of other instruments of national and international power to provide focus and unity of effort. *Integration focuses on fusing and synchronizing military operations* among the Services, *other government agencies, the commercial sector*, non-governmental organizations and those of partners abroad."[52]

At the national / strategic level the National Counter Terrorism Center (NCTC) was formed. It was "established to serve as a multi-agency center analyzing and integrating all intelligence pertaining to terrorism, including threats to US interests at home and abroad."[53] State intelligence fusion centers provide this at the operational and tactical level.

The Arizona Counter Terrorism Information Center (ACTIC)

> "In the early morning hours of September 9, 2001, a Maryland State Trooper made a routine traffic stop, pulling over a car headed north on I-95 and issued a speeding ticket. Two days later, the driver of that car, Ziad Jarrah was one of the four hijackers aboard United Airlines Flight 93 when it crashed in western Pennsylvania. The officer who issued the speeding ticket had no idea that Jarrah was on a CIA watch list. If he had, experts say, it is possible he might have prevented, or at least disrupted, the worst terrorist attack in history."[54]

---

[51] Arizona Department of Public Safety, *ACTIC Fact Sheet,* Phoenix, AZ: Arizona Counter Terrorism Information Center, May 2007, 1.

[52] *National Military Strategy of the United States of America.* Washington DC: Department of Defense, May 2004, p. 7.

[53] *The National Strategy for Combating Terrorism*. Washington DC: White House, September 2006, p. 20.

[54] Kaplan, Eben. *Fusion Centers*. Council on Foreign Relations. 22 Feb 07. Downloaded from www.cfr.org/publications/12689, 1.

The aftermath of the September 11th attacks led the law enforcement and intelligence community to relook the way it collected, but more importantly, shared counter-terrorism and criminal intelligence. It was discovered that "no single agency or intelligence function currently maintains all the significant information required to properly defend this nation."[55] One of the results of this internal look was the development of intelligence fusion centers at the state level. As of two years ago, there were 42 of these state fusion centers in operation. The Arizona Counter Terrorism Information Center (ACTIC) is an example of the synergy that can develop when multiple agencies come together with a common goal and understanding.

The mission of ACTIC "is to protect the citizens and infrastructures of Arizona by enhancing intelligence and domestic preparedness operations for all local, state, and federal law enforcement agencies."[56] The center is operated by the Arizona Department of Public Safety and is charged with being an "interagency intelligence operation that is the centerpiece of Arizona's Homeland Security detection and prevention strategy."[57] The center's concept of operations focused on not reinventing the intelligence wheel. Instead it sought to build upon existing criminal intelligence systems already existing within the state of Arizona. It co-located federal, state, and local officers in one location.

There are 44 participating agencies which participate in either a full-time or part-time arrangement. The center combines capabilities to provide counter-terror monitoring, prevention and response in the areas of WMD, computer forensics, facial recognition, and violent criminal apprehension. Participating agencies include police, fire, and emergency services departments from across the state. All participants agree to provide ACTIC access to their criminal and counter terror data bases to all other participating agencies in accordance with law and agency

---

[55] Ditlevson, *Air Base Defense,* 47.
[56] Arizona DPS, *ACTIC Fact Sheet*, 1.
[57] Ibid, 2.

policy.[58] The center is focused around a 24/7 watch center that monitors incidents and disseminates counter-terror and criminal intelligence information.

One of the key training programs run by ACTIC is the Terrorism Liaison Officer program. TLOs are law enforcement officer, firefighters, EMS, and criminal analysts who work for various municipalities, state agencies and federal bureaus. TLOs are trained in an intensive certification course that focuses on fourth generational warfare, CBRNE response protocols, critical infrastructure threat & vulnerability assessments, and processing & handling intelligence.[59] Graduates of the TLO course return to their departments and agencies with a greater knowledge of terrorist operations and the threat to critical infrastructure in their communities. The inclusion of fire and EMS personnel further expand the reach beyond the realm of standard law enforcement operations. Trained to be aware of potential terrorist activities, TLOs in fire and EMS units can apply this knowledge when responding to vehicle accidents and medical emergencies. Their new awareness can alert them to situations of possible terror planning in locations where law enforcement cannot go without probable cause.

At all levels of war, "secure air bases are a prerequisite for airpower operations; ensuring that they are available should therefore be a primary responsibility of USAF leadership."[60] Thus, the state's focus on critical infrastructure protection should be of particular importance for military installations. The Arizona state definition of critical infrastructure "are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their

---

[58] The databases currently available include: ACJIS, ACIC, NCIC, NLETS, IDLP (Interstate Driver's License Photos), SBINet (Secure Border Initiative Project), AZ Computerized Criminal History Interstate Identification Index (III) ,Wanted Person AZ, AFIS, MCSO Mugshots, Stolen Vehicle, AZ MVD Vehicle Registration, Sex Offender Registration, Notification of Stolen Guns, Missing/Unidentified Persons, Identity Theft, Interpol Warrants, Maricopa County Pawn Shop, Maricopa County Jail Management System Convicted Person/Supervised Release Violent Gang/Terrorist Organizations

[59] Arizona Department of Public Safety. *Terrorism Liaison Officer Training Course, February 2009.* Phoenix, AZ: Arizona Counter Terrorism Information Center, January 2009,1.

[60] 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, 77.

incapacitation or destruction would have debilitating effect on security, national economic security, public health or safety."[61] Based upon the Arizona statute, air bases within that state should be classified as critical infrastructure "vital to the United States." The designation of air bases as critical infrastructure would have the added benefit of making them eligible for participation in the Buffer Zone Protection Program (BZPP). "The BZPP assists responsible jurisdictions in building effective prevention and protection capabilities that will make it more difficult for terrorists to conduct site surveillance or launch attacks within the immediate vicinity…"[62] of the installation. The value of the BZPP is it identifies "all applicable law enforcement jurisdictions and other Federal, State, and local agencies having a role in the prevention of, protection against, and response to terrorist threats."[63] It further identifies specific planning and exercises to mitigate threats.

ACTIC also incorporates private businesses as part of its Community Liaison Program. Similar to the NYPD's Operation Nexus, this program offers free training to local businesses, particularly those located in designated Buffer Zones. It makes businesses aware of terrorist tactics, techniques, and procedures and ensures they know who to call if they see something suspicious. In the Fort Dix incident it was an alert video store clerk who alerted law enforcement to disturbing training videos that the members had dropped off to be converted to DVD format[64]. The importance of businesses in the area of critical infrastructure cannot be undervalued in a prevention program. Despite being a relatively new entity, ACTIC has already had several successes in defending the state against terrorist threats.   Its first major success occurred in the lead up to Super Bowl XLII which was held in Glendale, Arizona.

---

[61] Arizona DPS, *ACTIC Fact Sheet,* 2.
[62] Arizona DPS, *ACTIC Fact Sheet*, 4.
[63] Ibid, 4.
[64] Khalil, *Threat Analysis*, 4.

"In December 2007, Glendale Police Department was contacted by Safe Management a security company that provides contract security for the University of Phoenix Stadium. Safe Management had been contacted via email by an individual who was requesting restricted security information including the security Standard Operating Procedures for the stadium."[65]

The Glendale PD contacted ACTIC and investigators from the center along with agents from the JTTF responded. They determined the emails were fraudulent despite the appearance that they were sent by security operators tasked with supporting the Super Bowl. Using the abilities inherent to ACTIC and the JTTF, it was determined the emails were "indirectly connected to a company located in a foreign country."[66] The originators of the emails were subsequently located and detained while attending the Fiesta Bowl "with the purpose of conducting surveillance for an operation they intended on carrying out during the Super Bowl."[67] At this point the "terrorists" identified themselves as members of a Department of Homeland Security (DHS) contractor "red cell" who were validating the Super Bowl security. The success of ACTIC in this operation is significant because it was the 23rd time DHS had conducted "red cell" operations against national-interest events. "Arizona was the only law enforcement community that successfully detected and stopped the operation prior to the 'red cell' accomplishing their intended goal."[68] It should also be noted that Safe Management had participated in the ACTIC Community Liaison Program and its employees had received training in counter-terrorism awareness.

Despite the wealth of access to counter-terror databases and massive response capabilities offered fusion centers such as ACTIC there is very little, if any, representation by Air Force installations. This leaves a huge gap in the ground intelligence sight picture for installation

---

[65] Arizona Department of Public Safety, *ACTIC Successes,* Phoenix, AZ: Arizona Counter Terrorism Information Center, February 2009, 1.
[66] Ibid, 1.
[67] Ibid, 1.
[68] Ibid, 2.

commanders and the defense force commander. Additionally, it leaves gaps in state-wide reporting. According to Commander Dan Wells of ACTIC, "it would be invaluable to have military reporting of personnel who were observing military installations and activities."[69] He also expressed an interest in persons who attempted to enter air bases. The reports on suspicious vehicles and persons could then be analyzed to see if the person had done similar activities at other installations or critical infrastructure sights in the state. Good intelligence sharing and reporting can compromise planned acts and "terrorists will often abandon a project if they suspect it has been compromised. A terrorist who feels he has been compromised will usually inform his group of that information."[70]

Local intelligence fusion cells provide commanders an invaluable opportunity to gain local counter-terror and criminal intelligence with limited investment. Terrorists have already demonstrated interest in attacking military installations and air power where they recognized they have the ability to win. Former National Security Advisor Zbigniew Brzezinski suggests, "every dollar spent on active, preventive intelligence is probably worth more than ten dollars spent on across-the-board but essentially blind upgrading of security at potential terrorist targets."[71] The cost of representation is relatively low when compared to adding additional patrols and hardening of installations. With air power at risk in its "nest," it is vital that air bases have representation at the fusion centers.

---

[69] Commander Wells, personal conversation on 26 Jan 09.

[70] William E. Dyson, "Terrorism Overview" (lecture, FBI Academy, Quantico, VA, July 2005.

[71] Brzezinski, Zbigniew. *The Choice: Global Domination or Global Leadership.* New York: Basic Books, 2004, 23.

SECTION 5 – CONCLUSION AND RECOMMENDATIONS

The USAF must move beyond the "battleship" force protection mentality of using its defense and intelligence forces in an antiquated manner. The key to good home station force protection is having a good home station ground intelligence capability that drives effective force protection operations. In the majority of states, intelligence fusion centers provide this capability. The cost of investment is relatively cheap when compared to the costs of blind patrolling and installation hardening. Furthermore, USAF involvement benefits the local communities in which they reside. To achieve this new paradigm of intelligence-driven policing to defend air power, I provide four recommendations.

Recommendation 1: Enhance interagency relationships. Installation Defense Force Commanders need to be an integral part of the local law enforcement community. Partnerships and personal relationships can be invaluable to base defense operations. To achieve this integration, the DFC should hold membership in local and state groups organized for senior law enforcement and intelligence officials. The West Valley Chiefs of Police, representing the communities on the western side of the Phoenix Metro area, is such an organization. The group "is a partnership of 10 West Valley police agencies with the goal of sharing resources and ideas to provide quality police service….it played a role in collaborating with local, state and federal agencies on issues such as criminal-data sharing and leveraging resources to fight crime more effectively."[72] The relationships developed can open the opportunity for joint training and operations that will serve to protect air power, all at little to no expense to the government.

It is vital that the service invest in the training, education, and development of future DFCs. Education at police administration courses developed for senior civilian law enforcement

---

[72] Arnold, Elias C. "Chiefs Association Honors Saban." *Arizona Central,* 16 May 2008, accessed from http://www.azcentral.com/community/swvalley/articles/2008/05/16/20080516swv-chiefs0517.html on 8 Feb, 2009.

officers, such as the FBI National Academy, the University of Louisville's Southern Police Institute and the Northwestern School of Police Staff and Command should be the norm. These institutions "prepare law enforcement managers for senior positions by combining academic principles with practical applications."[73] While the courses may not have direct application to the application of combat air power and ground defense, it does expose the future DFC to the leaders in local law enforcement and intelligence agencies. That network remains intact throughout the member's career providing an unending world-wide network of capabilities.

Recommendation 2: **Develop a base-level, tactical intelligence fusion cell**. The mission of the cell is to function as the primary integration point with local law enforcement and intelligence agencies. The cell should be composed of SF investigations, OSI counter-threat, and wing intelligence personnel at a minimum. Medical, engineers, and flight safety should have an ancilliary role. The cell should be under the operational control of the Defense Force Commander. This current structure leaves the collection and analysis in the hands of an organization that is not responsible to the commanders who rely on the information to defend air power, thus it violates the principle of unity of command. The DFC is the sole individual responsible for the ground defense of air power. As this research has attempted to prove, good intelligence is vital to good defense. In order to ensure that the correct site picture is being presented to the DFC and therefore the installation commander, the DFC should have OPCON/TACON of this cell.

This would also provide closure to finding #11 of the Downing Commission by creating "an organic intelligence support capability in US Air Force Security Police units."[74] The current construct of using investigators and SF personnel untrained in counter-intelligence and threat

---

[73] Northwestern University. "Center for Public Safety." http://nucps.northwestern.edu (accessed 8 February 2009).

[74] Downing Assessment Task Force. *Force Protection Assessment US CENTCOM and Khobar Towers,* 33.

analysis would cease under this proposal. A true synergistic team under control of the commander responsible for air power defense is the only logical solution to "abandoning the battleship" mentality and ensuring that this lack of capability no longer "adversely affects their ability to accomplish the base defense mission."[75]

        Recommendation 3: Reintroduce the Area Source Program (ASP). The Vietnam-era ASP proved invaluable to defending air bases. The current Eagle Eyes program focuses on encouraging military members to report suspicious activity. This program should be extended into the BSZ. By establishing a positive presence inside the BSZ, the potential exists to recruit businesses and residents to act as "early warning sensors." The United Kingdom's Ministry of Defence Police (MDP) instituted a similar program to defend the base security zones around UK and US installations. The Farm Watch program is billed as "a crucial tool in enhancing our intelligence gathering capability. This is also makes the Farmers feel more secure and involved in protecting their livelihood as well as ours. "Partnership" is the way forward in disrupting, deterring and dispelling terrorist activities."[76] Farm Watch is based on community policing principles. MDP Constables make contact with landowners neighboring the installation. Personal working relationships which benefit the MDP and the land owners are established. According to Sergeant Eileen McAdam, "once the initial contact has been made with the farmer and telephone numbers exchanged, a courtesy call is all that is required as they know they only have to give us a ring with anything they deem suspicious and believe me farmers know what's going on!"[77] The program has been successful in intercepting protestors reconnoitering or

---

[75] Downing Assessment Task Force. *Force Protection Assessment US CENTCOM and Khobar Towers,* 33.

[76] McAdam, Eileen, Sergeant, Ministry of Defence Police, United Kingdom. To the author. E-mail, 24 November 2008.

[77] McAdam, Eileen, Sergeant, Ministry of Defence Police, United Kingdom. To the author. E-mail, 24 November 2008.

attempted to illegally enter the installation. The Area Source Program, similar to Farm Watch, should be implemented in the base security zones at CONUS air bases.

Recommendation 4: Reorganize base defense forces under Operations. The Operations Group serves as the centerpiece of the air base's combat mission. Aircraft and operators in the air and space environments represent the combat capability of the service and serve as keys to national defense strategy. The defense of those national assets is aligned under the Mission Support Group (MSG) combined with human resources, community services, communications, and public works. There is no unity of command for combat power.

Moving base defense forces under the Operations Group would signify an immediate change in the interest in defending national combat assets under a "fighting" commander. More importantly it would refocus the efforts for funding combat and defensive capabilities. Currently, under the MSG, base defense competes for limited Base Operating Support (BOS) funding with service support capabilities such as child care, lodging, and recreation. BOS is also the most likely funding area to be cut, or taxed, during periods of slow funding. The result is equipment, resources, and training vital to the defense of air power are left unfunded.

The defense of air bases, particularly in the "rear areas," has taken on more importance since the 9/11 attacks on the United States. It is thus vital that current force protection and base defense operations be tailored to meet the current threat and move away from an internal looking guard force. Our heritage and history however have been roadblocks to moving in this direction. The historical lack of attacks on air bases in the rear area have led to a popular conception that defense forces should be focused on policing speeders, loud noise complaints, lost animals, and ensuring maintainers are wearing line badges. This historical legacy has the potential to lead to mass devastation to American air supremacy. We know from seized documents and previous

attempts that insurgents have the desire and guidance to attack CONUS-based installations. It is now upon us to abandon the battleship mentality and move to a flexible, responsive defense force guided by ground intelligence and fused with the local communities that host air power installations.

BIBLIOGRAPHY

Ahmad, Eqbal. *"*Terrorism: Theirs & Ours." In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 46 – 52. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

Air Force Doctrine Document (AFDD) 2-4.1: Force Protection, 9 November 2004.

Air Force Instruction (AFI) 10-245. Air Force Anti-Terrorism (AT) Standards, 21 June 2002.

Air Force Instruction (AFI) 14-119. Intelligence Support to Force Protection, 15 August 2007.

Air Force Instruction (AFI) 31-101. The Air Force Installation Security Program, 1 March 2003.

Air Force Instruction (AFI) 31-101 (Draft). Integrated Defense. February 2009.

Air Force Instruction (AFI) 71-101, Volume 4. Counterintelligence. 1 August 2000.

Air Force Policy Directive (AFPD) 31-1. Integrated Defense. 7 July 2007.

Air Force Policy Directive (AFPD) 71-1. Criminal Investigations and Counterintelligence. 1 July 1999.

"The Air Force War on the Ground." Air University Quarterly Review. (Winter 1953-54): 95-110.

Al Qaeda. *"Military Studies in the Jihad Against the Tyrants."*

Alsop, Joseph. "Quotes." www.wisdomquotes.com (accessed on 21 Dec 08).

Arizona Department of Public Safety. *Critical Infrastructure Briefing Paper.* Phoenix, AZ: Arizona Counter Terrorism Information Center, Dec. 16, 2008.

Arizona Department of Public Safety. *Terrorism Liaison Officer Training Course, February 2009.* Phoenix, AZ: Arizona Counter Terrorism Information Center, January 2009.

Arizona Department of Public Safety, *TLO Course Tri-Fold Brochure, Feb 2009.* Phoenix, AZ: Arizona Counter Terrorism Information Center, February 2009.

Arizona Department of Public Safety, *ACTIC Fact Sheet,* Phoenix, AZ: Arizona Counter Terrorism Information Center, May 2007.

Arizona Department of Public Safety, *ACTIC Successes,* Phoenix, AZ: Arizona Counter Terrorism Information Center, February 2009.

Armistead, Leigh. "Information Operations: Warfare and the Hard Reality of Soft Power." Washington, DC: Potomac Press, 2004.

Arnold, Elias C. "Chiefs Association Honors Saban." *Arizona Central,* 16 May 2008, accessed from http://www.azcentral.com/community/swvalley/articles/2008/05/16/20080516swv-chiefs0517.html on 8 Feb, 2009.

Association of the United States Army, *ES2: Every Soldier is a Sensor*, discussion paper, August 2004.

Barker, Brig and Fowler, Steve. "The FBI Joint Terrorism Task Force Officer." *FBI Law Enforcement Bulletin,* November 2008, pp. 12 – 16.

Betts, Richard K. "Fixing Intelligence." In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 459 – 469. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

Bogdanos, Matthew F. "Joint Interagency Cooperation: The First Step." In *Joint Forces Coursebook,* edited by Sharon McBride, 174 – 183. Maxwell AFB, AL: Air University Press, 2008.

Bolten, Joshua B. *Implementation of Homeland Security Policy Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.* Washington D.C.: Office of Management and Budget, 5 August 2005.

Brzezinski, Zbigniew. *The Choice: Global Domination or Global Leadership.* New York: Basic Books, 2004.

Carafano, James J. "Herding Cats: Understanding Why Government Agencies Don't Cooperate and How to Fix the Problem." In *Joint Forces Coursebook,* edited by Sharon McBride, 184 - 189. Maxwell AFB, AL: Air University Press, 2008.

Carter, David L., "The Contemporary Law Enforcement Intelligence Function." Lecture. FBI Academy, Quantico, VA, August 2005.

Caudill, Shannon W., *"The Fort Dix Six: Lessons Learned."* Washington, D.C.: Joint Staff. November 2006.

Chambers, James J., "Force Protection for the 21st Century Expeditionary Aerospace Forces: Security Forces Need for Organic Ground Intelligence." Maxwell AFB, AL: Air Command and Staff College, April 1999.

Chief of Staff US Army and Chief of Staff US Air Force, "Abrogation of Joint Service Agreement 8: USA-USAF Agreement for the Ground Defense of Air Force Bases and Installations", 24 Mar 2005.

Coleman, Richard A. "USAF Air Bases: No Safe Sanctuary." Carlisle Barracks, PA: US Army War College, 1990.

Corey, Frank. "Special Report: Use of Surveillance by Terrorist Groups." Norfolk, VA: Joint Forces Intelligence Command, 16 July 2002.

Corum, James S. and Johnson, Wray R. "Airpower in Small Wars: Fighting Insurgents and Terrorists." Lawrence, Kansas: University of Kansas Press, 2003.

Crenshaw, Martha. "Counterterrorism Policy and the Political Process." In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 450 – 458. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

de Atkine, Norville 2000: 'Why Arabs Lose Wars', in *Middle East Review of International Affairs,* Vol. 4 No. 1 March 2000.

De Wijk, Rob. "The Limits of Military Power." In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 482 - 494. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

Department of the Army White Paper, Ft McClellan, AL: United States Army Military Police School. "Police Intelligence Operations." 1999.

Ditlevson, Jeffery T. "Air Base Defense: Different Times Call for Different Methods." Monterrey, CA: Naval Postgraduate School, December 2006.

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

Downing Assessment Task Force. *Force Protection Assessment US CENTCOM and Khobar Towers, Vol 1.* August, 1996.

Dyson, William E., "Terrorism Overview." Lecture. FBI Academy, Quantico, VA, July 2005.

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

Further Strengthening the Sharing of Terrorism Information to Protect Americans. Executive Order 13388. 25 October 2005.

Gunaratna, Rohan. *Inside Al Qa'eda.* Washington, D.C.: Columbia University Press, 2002.

Kaplan, Eben. Fusion Centers. Council on Foreign Relations. 22 Feb 07. Downloaded from www.cfr.org/publications/12689.

Kelling, George L., Pate, Tony, Dieckman, Duane, and Brown, Charles E. *The Kansas City Preventative Patrol Experiment*. Washington, D.C.: Police Foundation, 1974.

Khalil, Lydia. "Threat Analysis Subject: Fort Dix, New Jersey Terror Plot." *NYPD Shield* (May 2007). http://www.nypdshield.org (accessed 26 January 2009).

Mac Donald, Heather. "Keeping New York Safe from Terrorists: Intelligence sharing and accountability for investigators are the keys." *City Journal* (Autumn 2001). http://www.city-journal.org/html/11_4_keeping_new_york.html (accessed 13 January 2008).

Masse, Todd. *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States.* CRS Report RL31920. Congressional Research Library: May 19, 2003.

Masse, Todd. *A Summary of Fusion Centers: Core Issues and Options for Congress.* CRS Report RL34177. Congressional Research Library: September 19, 2007.

Marquise, Richard A., "Trends in International Terrorism." Lecture. FBI Academy, Quantico, VA, August 2005.

McAdam, Eileen, Sergeant, Ministry of Defence Police, United Kingdom. To the author. E-mail, 24 November 2008.

McCormack, William. "State and Local Law Enforcement Contributions to Terrorism Prevention." *FBI Law Enforcement Bulletin,* March 2009.

Mintz, John. "Homeland Security Employs Imagination," *Washington Post*, June 18, 2004.

National Military Strategy of the United States of America. Washington DC: Department of Defense, May 2004.

The National Strategy for Combating Terrorism. Washington DC: White House, September 2006.

New York Police Department. *NYPD Shield: Operation Nexus.* https://www.nypdshield.com/secure (accessed 14 January 2009).

Northwestern University. "Center for Public Safety." http://nucps.northwestern.edu (accessed 8 February 2009).

Norwitz, Jeffrey H. "Combating Terrorism: With a Helmet or a Badge." In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 470 – 481. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

Palmer, Glenn E. *Air Base Security Operations: An Air Component Responsibility.* Maxwell AFB, AL: School of Advance Air and Space Studies, June 2006.

Peed, Carl R. "The Community Policing Umbrella." *FBI Law Enforcement Bulletin,* November 2008, pp. 22 - 24.

Pillar, Raul. "The Dimensions of Terrorism and Counterterrorism*."* In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 24 – 45. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

Posen, Barry R. "The Struggle Against Terrorism: Grand Strategy, Strategy, and Tactics." In *Terrorism and Counterterrorism: Understanding the New Security Environment,* edited by Howard, Russell D. and Sawyer, Reid L., 429 – 441. Guilford, Conn.: McGraw-Hill/Dushkin, 2002.

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

Sampson, Rana and Scott, Michael S. *Tackling Crime and Other Public Safety Problems: Case Studies in Problem-Solving.* Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, 2000.

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.

Wright, Lawrence. *The Looming Tower: Al-Qaeda and the Road to 9/11*. New York: Vintage Books, 2007.

Williams, Theodore C. "US Air Force Ground Defense System." Carlisle Barracks, PA, Army War College, December 1968.

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

Wilson, Patrick, Chief Master Sergeant, USAF, Luke AFB, AZ. To the author. Email, 18 March 09.

Worden, Mike, Col. *Rise of the Fighter Generals.* Maxwell AFB, AL: Air University Press, 1998.

Young, David T. "Applying Counterinsurgency Theory to Air Base Defense: A New Doctrinal Framework." Monterrey, CA: Naval Postgraduate School, September 2005.