FORCE PROTECTION

Air Force Doctrine Document 2-4.1
9 November 2004

This document complements related discussion found in Joint Publications 0-2, *Unified Action Armed Forces (UNAAF)*; 3-07, *Joint Doctrine for Military Operations Other than War*; 3-10, *Joint Doctrine for Rear Area Operations;* and 3-11, *Joint Doctrine for NBC Defense.*

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE DOCTRINE DOCUMENT 2-4.1
9 NOVEMBER 2004

SUMMARY OF REVISIONS

This document is substantially revised. The definition for force protection is updated to reflect new best practices (pages 1-2). It updates the information on command relationships to reflect current best practices of where force protection responsibilities reside in an air and space expeditionary task force (AETF) structure, along with clarifying force protection command relationships in a joint environment (chapter 2). Discussion of the threat to Air Force personnel and resources is updated to describe a threat continuum, replacing the old threat levels (page 15). A new discussion of integrated base defense is incorporated (chapter 5).

OPR: HQ AFDC/DR (Mr Bob Christensen)
Certified by: AFDC/DR (Col Scott Walker)
Supersedes: AFDD 2-4.1, 29 Oct 99
Pages: 50
Distribution: F
Approved by: BENTLEY B. RAYBURN, Major General, USAF
Commander, Air Force Doctrine Center

FOREWORD

The bombing of the Marine barracks in Lebanon in October of 1983 marked the beginning of a period in US military history where force protection against a terrorist enemy rose to take on a prominent role in military operations. From Khobar Towers, where the Air Force was personally bloodied by a terror attack, through the attacks on 9/11, the trend of terror attacks is a growth in frequency and lethality up to this very day. The current level of threats to our people and resources dictates that the Air Force take strong measures to protect our forces, at home and when deployed. Protecting Air Force personnel and resources is critical to our ability to perform our missions. Air and space expeditionary forces are poised to respond to global taskings at any time, and a major effort within that response must be force protection.

The changing methods of attack used by our adversaries require us to consider the nontraditional ways in which we may be attacked and how to counter these elusive threats. Evolving methods of attack vary from standoff to suicide, single to simultaneous, automobiles to boats to airplanes—all designed to catch their victims off guard. Because of ever-changing tactics, we must be increasingly vigilant, using all the various expertise available to out-think our enemies and negate their intentions.

Commanders at all levels must aggressively and effectively execute their force protection responsibilities and programs. Commanders are responsible for protecting their people and the resources used to perform military operations. We are obligated by our past, present, and future to ensure force protection is a part of Air Force culture.

Understanding and applying this doctrine are fundamental elements in the successful protection of our people and resources.

BENTLEY B. RAYBURN
Major General, USAF
Commander, Air Force Doctrine Center

TABLE OF CONTENTS

INTRODUCTION

PURPOSE

This Air Force Doctrine Document (AFDD) establishes doctrinal guidance for organizing and employing force protection capabilities at the operational level across the full range of military operations. It is a critical element of Air Force operational-level doctrine and as such forms the basis from which Air Force commanders plan and execute their force protection responsibilities.

APPLICATION

This AFDD applies to all US Air Force military and civilian personnel (includes Air Force Reserve Command [AFRC] and Air National Guard [ANG] units and members). The doctrine in this document is authoritative but not directive. Therefore, commanders need to consider the contents of this AFDD and the particular situation when accomplishing their missions. Airmen should read it, discuss it, and practice it.

SCOPE

Air Force personnel and resources can be used across the range of military operations at the strategic, operational, and tactical levels of war. This AFDD discusses the fundamentals of organization and employment of Air Force force protection capabilities required to support the operational missions assigned to combatant commanders and carried out by air and space component commanders.

FOUNDATIONAL DOCTRINE STATEMENTS

Foundational doctrine statements are the basic principles and beliefs upon which AFDDs are built. Other information in the AFDD expands on or supports these statements.

- ✪ Agile combat support includes the integrated actions of force protection to protect Air Force personnel, assets, and capabilities throughout the spectrum of peacetime and wartime military operations. (Page 1)
- ✪ Force protection (FP) is an integrated application of offensive and defensive actions that deter, detect, preempt, mitigate, or negate threats against Air Force air and space operations and assets, based on an acceptable level of risk. (Page 1)
- ✪ Every Airman is a sensor. Protecting the force is everyone's duty. (Page 5)
- ✪ Threats, vulnerabilities, and risk drive everything accomplished in FP. (Page 7)
- ✪ Commanders will ensure there is a fundamental emphasis on awareness of force protection challenges. (Page 9)
- ✪ Force protection is an inherent responsibility of command. (Page 11)
- ✪ Centralized control of force protection measures and resources and the decentralized execution thereof are essential to effectively protect our forces against each threat. (Page 11)
- ✪ Clarity in FP responsibilities is a necessity. (Page 14)
- ✪ The essential goal of force protection is to counter threats against Air Force personnel and assets. (Page 15)
- ✪ A commander must know what threat is being confronted in order to devise a means to counter it. Without this knowledge, the commander is acting blindly. (Page 23)
- ✪ Commanders must take deliberate action to implement comprehensive countermeasures to deny an adversary information, access, and influence, thereby deterring him from taking action against friendly forces. (Page 24)
- ✪ Integrated base defense is the integrated application of offensive and defensive action, both active and passive, taken across the ground dimension of the force protection battlespace to achieve local and area dominance in support of force protection. (Page 29)

CHAPTER ONE
FORCE PROTECTION OVERVIEW

The threat of terrorism is real, it is persistent, and it is aimed at us. Yet, recent history has shown that terrorists prefer to attack soft, weak, or unprotected targets. Thus, we cannot let our guard down for a moment. Every Airman must be a sensor, and we must, at all times, ensure that our bases and facilities are hard targets.

—James G. Roche, Secretary of the Air Force, 2004

The 21st Century has, thus far, been characterized by a significant shift in Air Force responsibilities and an increased exposure of its resources to worldwide threats. This point is underscored by the terrorist attacks on Khobar Towers, the USS Cole, the attacks of 11 September 2001, subsequent anthrax attacks, and the ongoing Global War on Terrorism. Today, potential opponents are more unpredictable, capable, and lethal. They leverage the increased availability of high and low technology weapons, including weapons of mass destruction (WMD). US air and space power requires protection from these threats at home, in transit, and abroad, in order to perform its missions.

AGILE COMBAT SUPPORT AND FORCE PROTECTION

Agile combat support (ACS) is the Air Force's distinctive capability under which force protection falls. It is how the Air Force supports its forces; a force poised to respond to global taskings within hours that must also be able to support and protect that force with equal facility. **ACS includes the integrated actions of force protection to protect Air Force personnel, assets, and capabilities throughout the spectrum of peacetime and wartime military operations.**

ACS includes actions taken to create, effectively deploy, and sustain military power anywhere—at our initiative, speed, and tempo. ACS capabilities include provisions and protection of air and space personnel, assets, and capabilities throughout the full range of military operations. For additional information, see AFDD 1, *Air Force Basic Doctrine*, and AFDD 2-4, *Combat Support*.

FORCE PROTECTION DEFINED

Joint doctrine defines force protection (FP) as "actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease." (Joint Publication [JP] 1-02, *Department of Defense Dictionary of Military and Associated Terms*) Force protection is an overarching concept that is inherent to command within all military operations.

The Air Force views the execution of FP as **an integrated application of offensive and defensive actions that deter, detect, preempt, mitigate, or negate threats against Air Force air and space operations and assets, based on an acceptable level of risk.** Key to the Air Force view of FP is the protection of its people, the prime asset of the Service. In addition, in the Air Force perspective, prevention of accidents, along with protection against various forms of disease, especially those induced through hostile action, are elements of FP.

FP involves multi-dimensional protection, providing multi-layered protection of forces and resources. It covers the geographical spectrum; in garrison, in-transit, and at deployed locations; space, air, and surface dimensions. It includes not only the Service members and civilian employees, but also their families, contract employees, and visitors while on an installation. In addition, a broad array of integrated functional expertise facilitates a seamless FP posture. This functional expertise includes intelligence collection; awareness and reporting by all Airmen, on and off duty; detection of chemical, biological, radiological, nuclear, and high yield explosive (CBRNE) agents; physical security enhancements; armed defense; law enforcement liaison; along with numerous others. This multi-layered protection extends our awareness and influence as far out as possible, while providing in-depth protection from that point back to our people and resources. This maximizes our ability to disrupt attacks and provide the earliest warning possible, while ensuring the best protection for our most valuable assets through close-in security. The end result is an Air Force that has the best available protection, adjusted for risk, and ability to conduct its mission, wherever it is.

FP requires a global orientation because of air and space power's worldwide presence and its ability to move quickly across great distances in the pursuit of theater and national objectives. A global orientation is also required due to the proven ability of terrorists to strike worldwide. As a result, Air Force planners must consider the environment at home station, in transit, and at the deployed destination in their planning efforts. Deploying personnel and those traveling for other reasons also need to focus on their changing security environments. For example, they should know the assessed threat at each location they will transit, examine the vulnerabilities associated with the type of transportation scheduled, and develop a personal protection plan.

US Embassy in Kenya after its 1998 bombing

FP practitioners should consider both the threat and existing vulnerabilities, and should not rely exclusively on the assessed threat. Terrorists successfully attacked military targets, such as the USS Cole, Khobar Towers, and the Office of Program Management, Saudi Arabian National Guard, when those locations were in Force Protection Condition (FPCON) Bravo. In addition, non-military targets, such as the US embassies in Tanzania and Kenya and the World Trade Center, were attacked when the country terrorist threat assessment for those locations was moderate, low, or negligible. History supports the idea that the assessed threat is not necessarily an accurate reflection of the actual threat. As a result, identifying our vulnerabilities is critical. Once identified, steps to mitigate the vulnerabilities should be undertaken to increase survivability for Air Force personnel and assets.

Effective FP is more than just a law enforcement, antiterrorism (AT), or security function. Prior to the 1996 bombing of Khobar Towers, the closest term to "force protection" used with any frequency was "antiterrorism," and antiterrorism was often viewed as a law enforcement-only function with some focus on individual protective measures. Since 1996, FP has received greater attention and become more integrated and cross-functional. It has also been routinely confused as being synonymous with antiterrorism, hence the erroneous term "AT/FP." This linkage of AT with FP has led to a mindset that AT and FP are synonymous. FP is much broader in scope, with AT being a subset of FP. Security forces, augmentees, and owner/user personnel (e.g., personnel such as maintenance and operations personnel working in and around a flightline) provide security. Intelligence and counterintelligence contributions provide as accurate a threat picture as possible. In addition, civil engineers develop physical security improvements and provide full spectrum threat response (FSTR) planning, training, and response capabilities to deal with major accidents, natural disasters, hazardous material incidents, and similar events; medical and disaster preparedness personnel conduct presumptive identification for the presence of biological agents; and communications specialists integrate evacuation notification systems.

FP is accomplished through planned and integrated application of intelligence, counterintelligence, risk management, combatting terrorism, force health protection, integrated base defense, information security, operations security, law enforcement liaison and integration, personal protective services, and FSTR activities. Examples of the diverse actions involved include Air Force Office of Special Investigations (AFOSI) threat briefings and maintenance personnel reporting suspicious activity on the flightline.

FP is both an individual and a command responsibility. Individuals should know the assessed threat of their current location, intermediate stops along their route of travel, as well as their destination. They should also know and implement individual protective measures themselves. In addition, individuals should immediately report suspicious activities or occurrences to the nearest security forces, AFOSI, counterintelligence, or local law enforcement officer. Immediate reporting increases the chance intelligence remains actionable. Commanders retain ultimate responsibility for the well-being of their subordinates and ensure FP standards are met.

A key aspect of force protection is a healthy and fit force designed to protect all individuals. An indirect example is receiving annual flu shots to protect individuals and groups from illness, thus preventing lost duty time from naturally occurring viruses. In contrast, an anthrax vaccination is a direct force protection measure to protect individuals from an enemy-introduced threat. FP is directly related to, and is impacted by, force health protection that creates a healthy and fit force. Further information on force health protection can be found in AFDD 2-4.2, *Health Services*.

Safety, as applied via operational risk management (ORM), is a major element of any FP planning, and should be the primary tool used in the risk assessment phase of the risk management process when planning to counter the threat (see chapter 4). The ORM process, from identifying a hazard through implementing risk control measures and supervision and review of the effort, lends itself ideally to planning for FP efforts. Safety has an incontrovertible impact on FP's overall effectiveness.

FP is a task for all commanders. Joint force commanders conduct FP in a similar fashion as movement and maneuver; intelligence, surveillance, and reconnaissance; employing firepower; sustaining operations, operating in a CBRNE environment; and providing command and control during the execution of campaigns, major operations, and tactical engagements. FP actions are intended to be accomplished by the Services, and by joint forces under the multiple levels of command, from the theater, through the operational, and down to the tactical level. FP is an overarching concept and mission responsibility inherent to command within all military operations. It should not be used as a synonymous term with antiterrorism or other supporting task.

FP requires the full dimension of protective measures, including active force protection and passive force protection.

✪ **Active force protection (AFP) consists of purposeful actions taken to mitigate, defeat, or destroy threats against Air Force interests on a continuous or periodic basis.** One example is host nation authorities arresting a terrorist based on information provided by the AFOSI. Other examples include: enhanced owner/user work area security, executing defensive countersurveillance and surveillance detection operations, surveillance of vulnerability points, and defeating a hostile force in a firefight.

Random antiterrorism measures (RAMs) fall under the heading of active force protection. RAMs change the look of an installation's FP program. They are applied periodically and at irregular intervals. From an adversary's perspective, RAMs introduce uncertainty into an installation's overall FP program, help complicate surveillance attempts and make it difficult for a terrorist to accurately predict our actions. RAMs are measures taken from higher FPCON, as well as a variety of other "outside the box" initiatives. Possible RAMs include operating random patrols mandated in FPCON Bravo to check vehicles while in FPCON Alpha, searching every third truck entering the base, conducting random sweeps around a building by the facility's users, or having a military working dog team sweep the command building for possible explosive devices.

AFP measures under the FSTR auspices include activities such as hazard prediction, detection, and identification and marking, which provide commanders with critical information needed to determine protective warnings and tailor protective actions to the specific threats. Early threat detection provides more time to implement immediate appropriate measures.

- **Passive force protection (PFP) measures negate or reduce the effects of hostile acts against Air Force personnel and resources by making them more survivable.** This is proactively accomplished through risk management, training, education, hardening, redundancy, camouflage, concealment, deception, information security, operations security, planning, and coordinating with local community counterparts. Examples of PFP include hardened facilities, immunizations against biological agents, deploying during the hours of darkness, and movement of family members onto or away from a base during emergencies. Pre-mission studies focused on accurately characterizing the threat and vulnerabilities and how to counter them vastly improves PFP effectiveness.

  PFP activities ensure integration of the installation's FSTR programs supporting the passive defense aspects of operational analysis; equipage; accession training; professional military education and training; functional area task qualification; exercises; science and technology; modeling and simulation; and research, development, and acquisition activities.

> *I expect that our combat battalions will be used primarily to go after the VC [Viet Cong] and that we will not be forced to expend our capabilities simply to protect ourselves…. Therefore,…all forces of whatever Service who find themselves operating without infantry protection …will be organized, trained, and exercised to perform the defense and security functions.*
>
> **—General William C. Westmoreland, 1965**

FORCE PROTECTION FUNDAMENTALS

All Airmen need to know the fundamental aspects of FP to safeguard their own lives, those of fellow countrymen, and valuable Air Force resources:

- **Every Airman is a sensor. Protecting the force is everyone's duty.** Whether reporting suspicious activity while engaged in their primary duties or augmenting base defense, all Airmen are responsible for FP.

  ✪ ✪ This responsibility can stress available personnel and resources. In the end, commanders must balance mission accomplishment with FP. It is each individual's responsibility, with commanders ultimately responsible for overall FP of their command.

- **Airmen must always be aware of their surroundings.**

- As demonstrated by the attacks of 11 September 2001, the bombings of Khobar Towers and the USS Cole, and other recent terrorist attacks around the world, **our enemies often strike our interests in a non-combat operational setting.**

- **FP enables the Air Force to execute its operational missions across the spectrum of threats, while retaining freedom of movement.** It assumes enemy action and threatening conditions. FP does not mean the Air Force will be free from attack.

- **FP is built on the concept of full-dimensional protection**, providing multilayered protection of forces and facilities using all available personnel and resources based on the threat, vulnerabilities, and risk analysis.

- **A collaborative, integrated, cross-functional effort supports the FP posture.** Recurring planning meetings involving key intelligence, support, and operations personnel help ensure the effort is collaborative. Additionally, cross-functional participation facilitates integration of various areas of expertise and minimizes duplication of effort. Cross-functional participants should include, but not be limited to, civil engineers, communications, intelligence, counterintelligence, health services, maintenance, operations, logistics, and security forces communities. The joint staff integrated vulnerability assessments; Air Force, major command, and wing-level vulnerability assessments; and major command red teams are examples of collaborative, integrated, cross-functional products. The teams' members represent different specialties, brought together for a common mission. As a result, their findings address the entirety of a vulnerability, rather than examining a vulnerability within specialty stovepipes.

- **Coordination, planning, and preparation across Services, as well as host nation, national, state, and local authorities increase the likelihood of either defeating or mitigating effects of an attack.**

- **Technology advancements are enablers for FP, but should not be considered as replacements.** Technology offers force protectors advantages in speed, range, and effectiveness to assist them in meeting the demands of a changing operational environment. For example, advances in disease identification now allow for accurate assessment of biological attack in minutes, rather than days. Use of small remotely controlled aerial vehicles that extend tactical situational awareness for base defense is one example. None of these technologies is able to stand alone to perform FP, however; FP requires continued vigilance by the members of the force being protected, using technology to enhance their capabilities.

- **Effective command and control is the key to successful FP activities.** It facilitates the collection and dissemination of key intelligence to those who can act on it, rather than intelligence remaining stovepiped within staff functions. Effective command and control also ensures responsibility for FP is clearly assigned. Finally, effective command and control promotes rapid decision-making and response during crisis situations.

- **Effective intelligence, counterintelligence, and liaison efforts are critical to determining the threats to the force.** Identifying a potential threat strengthens the overall FP effort. Threats may be conventional military units, special forces, foreign intelligence agents and services, terrorist groups, riotous civil populations, cyberterrorists, criminal elements, extremist groups or insider threats, and antigovernment and hate groups. These groups may use weapons such as mortars, rockets, man-portable air defense systems (MANPADS), computer viruses, and CBRNE material and agents. Intelligence and counterintelligence personnel need to be capable of analyzing a broad range of threats. Key to the process is the timely and effective dissemination of intelligence to the appropriate commanders at all levels, including the senior commander, mission support group commander, security forces commander, AFOSI detachment commander, and the installation's FP officer/NCO. Constant liaison with host nation forces enhances cooperation and host willingness to conduct timely information sharing. Casual interface is often not sufficient during critical times for crisis-level information sharing with a host. Intelligence that is not acted on is equal in value to no intelligence.

✪ **Threats, vulnerabilities, and risk drive everything accomplished in FP.** Identifying and assessing threats and vulnerabilities are the first steps in FP planning, followed by selecting the appropriate countermeasures through risk management. Threat assessments for FP are optimized when they are done systematically and continuously, to reduce uncertainties concerning the enemy and the battlespace for all types of operations. A FP threat assessment analyzes and assesses the applicable area's land, sea, air and space, and information dimensions. In addition to the typical threat-related areas, threat assessments should include infrastructure, economic, political, and cultural aspects of the particular area of interest or operations.

Khobar Towers

The terrorist bombing attacks on the Office of Program Management-Saudi Arabian National Guard and Khobar Towers in Saudi Arabia (1995-1996) occurred during Threat Condition (now Force Protection Condition) Bravo. This demonstrates the necessity of dealing with both the threat and vulnerabilities in a given area; Bravo was deemed appropriate for the threat, but the vulnerabilities of both locations allowed terrorists to attack with fatal results.

Threat Assessments

Threat assessments should be all-source, fused analytical assessments. All-source assessments include the use of **national-level assets** (Defense Intelligence Agency [DIA]; DIA-Joint Task Force-Combatting Terrorism; DIA-Armed Forces Medical Intelligence Center; National Security Agency; Federal Bureau of Investigation; Bureau of Intelligence and Research, Department of State, etc.), **theater-level assets** (Joint Intelligence Center, AFOSI, Joint Information Operations Center, Air Force Information Warfare Center, Air Force Communications Agency), **in-country assets** (US Embassy, other in-country Service components, etc.) and **local assets** (host-nation military, local law enforcement, etc.). Information and intelligence from these sources should be compiled, compared, evaluated, integrated, analyzed, and assessed by a threat assessment team comprised of cross-functional personnel. The end product, the threat assessment, combined with vulnerability assessments, provides commanders a baseline for conducting **risk assessments** and later for applying the appropriate FP measures to counter the threat. Commanders use the appropriate FP measures that do not preclude mission accomplishment. The risk must be weighed against the impact on mission accomplishment. There are instances, depending on the criticality of the mission, that will require a commander to accept a higher level of risk.

Once the threats are identified, the commander normally employs a vulnerability assessment team with expertise in the following areas: physical security; civil, electrical, and structural engineering; special operations; operational readiness; law enforcement and operations; infrastructure; FSTR; health services; communications; intelligence; and counterintelligence. In many cases, commanders may tailor the team composition and scope of the assessment to meet the unique requirements of a particular activity, however, commanders should meet the intent of providing a comprehensive assessment. The assessment team reveals the vulnerabilities and potential solutions relating to present and future threats. Commanders can augment the team with any personnel possessing the expertise they deem appropriate for the assessment.

RISK ASSESSMENTS

Risk assessments provide commanders with a method to assist them in making resource allocation decisions designed to protect their people and assets from possible threats in a resource-constrained environment while still ensuring mission accomplishment. Chapter Four discusses in detail the FP tools available to commanders to mitigate or counter the threat.

COUNTERMEASURES

At the heart of FP doctrine is the need to counter the spectrum of threats against Air Force interests. Countermeasures, used in both active and passive FP, are those devices and techniques that are designed to impair the effectiveness of the enemy. Countermeasures against one threat are often effective against a variety of other threats. These steps encompass an effects-based approach using tactics, techniques, and procedures, enhanced through application of technology. The end result will support mission accomplishment at the strategic, operational, and tactical levels. Some examples include practicing building evacuations; implementing communications, operations, and information security measures; conducting RAMs; red teaming; and hardening structures to minimize potential blast damage. All personnel, regardless of rank or specialty, should be trained on a recurring basis in basic FP skills needed to survive and operate. These include basic small arms skills; basic ground combat skills (unless personnel are limited by the Geneva Conventions); self-aid and buddy care; chemical, biological, radiological, nuclear, and high yield explosives (CBRNE) defense; antiterrorism; threat awareness; and other essential common skills.

Small arms skills are necessary for force protection

AWARENESS

Commanders will ensure there is a fundamental emphasis on awareness of FP challenges. Awareness programs raise the comprehension by Air Force personnel and their dependents of the continuum of threats and measures that will reduce personal vulnerability. Fundamental knowledge of the threat continuum and measures to reduce personal vulnerability is vital, including awareness of the following areas:

- Threat methods of attack and operations.
- Detecting surveillance by threat groups/agents.
- Individual protective measures.
- Basic hostage survival procedures.
- Threat levels and FPCONS.
- Local threat updates.

Timely threat updates are essential. Everyone, at all levels of command, needs to know about changes in threat information as soon as possible to implement tailored FP measures. All-source intelligence and counterintelligence efforts, along with effective on-site surveillance detection and proactive liaison, are keys to timely threat detection and awareness.

Awareness also ties in with FP resource allocation. FP resource allocations are risk-based and programmatically sustained**;** they are a long-term investment. Force protection resources, including manpower, are properly borne by the system program and are part of the acquisition program baseline. In the past, the United States has increased FP investments only after a devastating event. A cyclical pattern has not worked in the past and it will not work to protect Air Force personnel and resources in the future. Commanders at all levels must change past oversights and shortcomings through a sustained effort for FP.

CROSS-FUNCTIONAL EXPERTISE

Tremendous change has occurred in this area since 1996. At that time, FP was primarily seen as a Security Forces responsibility. Since then, wings have developed FP working groups and executive committees that blend such wide-ranging functions as communications, engineering, and comptrollers. In addition, multifunctional organizations such as the Air Force's contingency response units provide first-in, squadron level FP teams comprised of logisticians, medics, explosives ordnance disposal personnel, logistics readiness personnel, AFOSI and more. This trend of integrating expertise provides bases with a more thorough, systematic FP plan and increases the likelihood of deterring and defeating any adversary.

COMMAND AND CONTROL

Command and control for FP allows commanders to respond to threats and implement tailored countermeasures. Commanders need timely and accurate information and intelligence on threat indicators and changes to make effective risk management decisions to modify FP postures and ensure personnel receive near-real-time threat updates. A unified command and control organizational structure allows subordinate commanders to expedite requests for essential FP resources and additional personnel. Commanders must ensure FPCON changes, threat updates, and risk management decisions are communicated to appropriate levels of command. To enable commanders to make the most effective decisions possible, commanders and all organizational FP monitors should receive specialized FP training. Leadership, as executed through command and control, ensures current threat assessments are passed to forward-deployed and en route assets in near-real time. Commanders must be aware of, adjust to, and be interoperable with civilian command and control systems. For additional information, see AFDD 2-8, *Command and Control*.

CHAPTER TWO
ORGANIZING FOR FORCE PROTECTION

...we can't be the best at building airplanes and submarines and second or third best at protecting our men and women.

—General John Shalikashvili,
Chairman of the Joint Chiefs of
Staff, November 1996

Force protection is an inherent responsibility of command. Accordingly, commanders at all levels must make force protection an imperative. Command and control structures must enable commanders to quickly react to threats with active defensive or offensive operations. Commanders are accountable for FP within their responsible areas. The overarching nature of the FP effort requires it be coordinated and integrated at the highest levels and across all functional areas. One of the greatest challenges for commanders is the integration of all aspects of FP at all levels of command, including interoperability with civilian command and control systems within the United States. **Centralized control of force protection measures and resources and the decentralized execution thereof are essential to effectively protect our forces against each threat.**

COMMAND RESPONSIBILITIES FOR FORCE PROTECTION

Commander, Air Force Forces (COMAFFOR)

A COMAFFOR will serve as the commander of Air Force forces assigned or attached to a joint task force. A combatant command-aligned numbered Air Force (NAF) is typically redesignated as the AFFOR (e.g., 9AF serves as US Central Command Air Force Forces [USCENTAF]). This organizational structure may be tailored by the COMAFFOR to fit specific

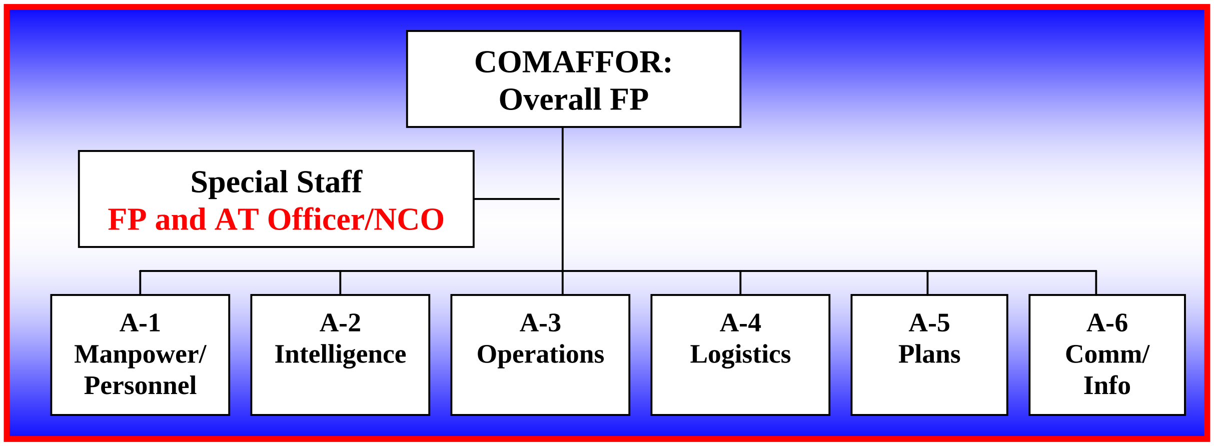


Figure 2.1. COMAFFOR Staff with FP Officer/NCO location identified.

mission needs. The organizational structure represented in figure 2.1 shows one example of how a COMAFFOR may organize the staff. As the joint force commander will normally delegate operational control (OPCON) to the COMAFFOR for all Air Force forces assigned or attached, the COMAFFOR will thereby obtain tactical control (TACON) over those forces, including TACON for FP.

Subordinate Commanders

Subordinate commanders at the wing, group, and installation level face three major FP challenges: planning for FP integration and support as tasked in applicable operational plans, training for FP, and providing FP for those interests within their purview. Air and space expeditionary task forces (AETFs—a notional example of an AETF as a wing is located at figure 2.2) have the added responsibility of accomplishing FP planning for the units identified to deploy to their location during contingency operations. Commanders need to integrate FP personnel into their organizations to establish guidance for, program for, and manage FP requirements for their organizations. **Commanders should also appoint a single FP focal point, an individual trained and versed in FP issues and methodologies with appropriate rank and experience, to act as their advisor on all FP issues.**

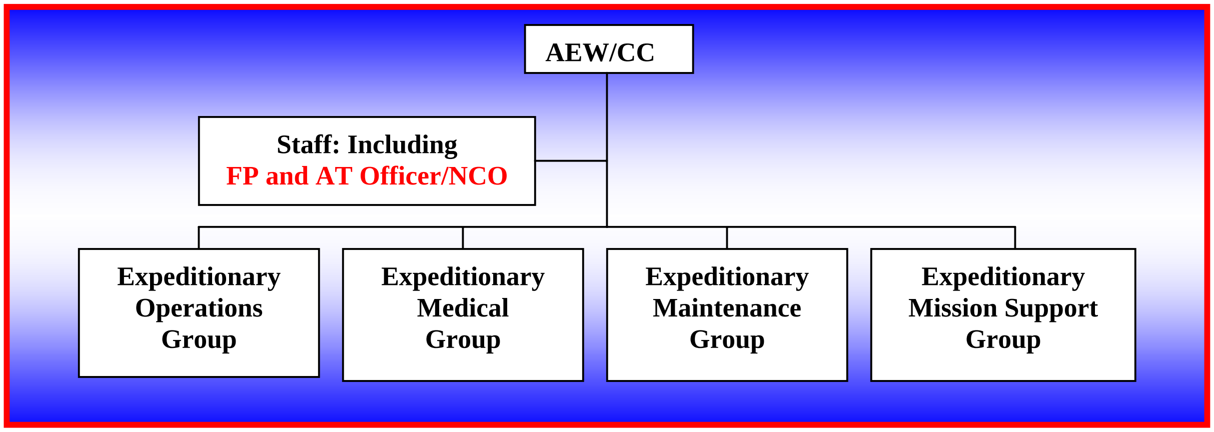

AEW/CC
Staff: Including
FP and AT Officer/NCO
Expeditionary Operations Group
Expeditionary Medical Group
Expeditionary Maintenance Group
Expeditionary Mission Support Group

Figure 2.2. Notional air expeditionary wing structure, with FP responsibility highlighted.

Administrative Control of Force Protection

In addition to the operational responsibilities for FP inherent in the organizational structures commanded by a COMAFFOR and subordinate commanders, there is an administrative control (ADCON) function for FP that resides in Air Force organizations above the COMAFFOR in the Service ADCON chain:

- ✪ Headquarters, US Air Force: The Chief of Staff, United States Air Force (CSAF) provides guidance on how to organize, train, and equip forces. The CSAF exercises control over FP programming, training, staffing, manning, and developing FP policy. The Air Staff's primary function lies in allocating additional forces and funding as needed to fulfill FP requirements.

- Major Command (MAJCOM): MAJCOM commanders organize, train, and equip forces. MAJCOM commanders should integrate FP requirements into every aspect of their activities. They should establish cross-functional coordinating bodies to establish guidance for, program for, and manage all FP requirements and allocated FP resources for the MAJCOM, and to report shortfalls and new requirements to the Air Staff. MAJCOMs should have a designated FP focal point, trained in FP issues and methodologies, to act as their advisor on all FP issues.

- Numbered Air Force (NAF): The NAFs are the Air Force senior warfighting echelons that have, in addition, ADCON responsibilities for FP. They provide representation to the MAJCOM cross-functional staffs for FP or provide inputs on requirements to their MAJCOM FP focal point. They coordinate with joint task force FP representatives, when assigned or attached as an air and space expeditionary task force (AETF). NAF commanders should appoint a single FP focal point, trained in FP issues and methodologies, to act as their advisor on all FP issues.

FORCE PROTECTION COMMAND RELATIONSHIPS IN A JOINT ENVIRONMENT.

The Air Force routinely operates in joint and coalition environments. Because of this, the need for clarity in determining responsibility for FP at a given location is vital. FP is not exclusively a Service responsibility; **geographic combatant commanders have the overall requirement to establish and implement FP in their areas of responsibility (AORs).** This then flows down to all commanders operating within the AOR, and affects all Department of Defense (DOD) personnel in that AOR not under the security responsibility of the Department of State, regardless of whether they are assigned or attached to any organization therein. Transiting personnel fall under the geographic combatant commander's FP requirements as much as personnel assigned or attached to organizations in the AOR; this exercise of TACON for FP is an exception to the normal limitation of commanders in an AOR exercising chain of command authority over transiting forces. **Air Force commanders, therefore, have a responsibility to implement FP measures for all DOD personnel on their installation or within their AOR, regardless of Service or status.**

TACON for FP covers all DOD personnel, regardless of Service, including those tasked for FP duties.

Clarity in FP responsibilities is a necessity. Where FP responsibility lies should be unambiguous. If a joint force commander assigns command of an installation to a specific Service component commander, that commander has TACON for FP over all personnel on that installation, regardless of Service or status. FP is not Service-specific. The Service responsibility of ADCON is used to support various measures of FP, but is not the appropriate command relationship to describe where the responsibility for implementation lies. For example, each Service has an ADCON responsibility to equip its personnel deploying to a hostile fire zone with appropriate body armor, but the requirement to wear that armor, and under what circumstances, is best left to the commander on the ground at the deployed location. As FP flows from geographic combatant commanders, it is normally delegated as a TACON responsibility for implementation. For further information, consult JP 0-2, *Unified Action Armed Forces (UNAAF),* and JP 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense.* TACON for FP is recognized as a specified form of TACON, and is to be used by an installation commander as the command relationship over all personnel assigned, attached, or in transit for the explicit purpose of FP, regardless of Service.

TACON for FP is a specified form of TACON.

CHAPTER THREE
FORCE PROTECTION THREATS

Always presume that the enemy has dangerous designs and always be forehanded with the remedy. But do not let these calculations make you timid.

—Frederick the Great

You will usually find that the enemy has three courses open to him, and of these he will adopt the fourth.

—von Moltke the Elder

The essential goal of force protection is to counter threats against Air Force personnel and assets. Air Force personnel must identify threats, then determine ways to counter them to protect personnel and resources in order to enable mission accomplishment.

THE THREAT CONTINUUM

Threats to Air Force interests occur across the continuum of Air Force operations from peacetime through wartime operations. It is important for commanders to recognize that any given threat may be present at any point along the continuum. **Commanders should consider the effects intended to be produced by the threat, not just the nature of the threat itself.** In this manner, a threat can be small in execution with large-scale effects as the outcome. Experience has shown that threats can occur anytime during peace and war. These threats can undermine mission capability as severely as sabotage or engagement with enemy forces.

Small-scale operations conducted by agents, insiders, saboteurs, sympathizers, partisans, extremists, and agent-supervised or independently initiated terrorist activities present a grave danger to Air Force interests as well. These operations may derive their personnel resources from nation-states or non-state actors, such as the al-Qaeda terrorist organizations. Often asymmetric in nature, these threats may be unorganized or well orchestrated and may take the form of insider threats, demonstrations, riots, random sniper incidents, physical assaults, kidnappings, aircraft hijackings, or bombings.

Intelligence gathering, and the sabotage of air or ground operations conducted by special operations, guerrilla, and unconventional forces or small tactical units are threats that enter the realm of state-to-state combat operations. This threat is often asymmetric in nature. Major attacks by large tactical forces that may use air, space, land, or maritime operations are at the large-scale end of state-to-state conflicts. Attacks may also come from aircraft and theater missiles/artillery armed with conventional weapons and WMD. The Air Force also uses its air and space warfare functions to counter and engage this threat; engagement of these forces takes it out of the realm of FP into combat operations.

FORCE PROTECTION THREAT SPECTRUM

There are a variety of threats, a number of which are discussed below, facing the Air Force. In addition to those threats we know exist, there is the paradox of attempting to counter threats we currently do not know exist. When Khobar Towers was attacked in 1996, one vehicle packed with explosives was used and the attack was conducted to maximize the enemy's survivability. In 2003, three housing complexes in Riyadh, Saudi Arabia, were attacked simultaneously. A vehicle designed to penetrate the compound, followed by an explosive laden vehicle, initiated each attack. The attackers appear to have placed little priority on their own survivability. Therefore, in addition to addressing the threats below, we need to continually think "outside the box" and conduct "what if" scenarios to counter potential future threats we have not seen yet, or have seen executed in a different theater. We must learn from tactics introduced in one theater because, if proven effective, the same tactics can be seen again in other regions of the world. As a result of increased FP measures due to the threat of attack, ongoing operations may be affected. A commander's risk assessment is critical for successful FP measures and successful mission accomplishment.

- ✪ Conventional Threat—Regular military forces supported by a recognized government are categorized as a conventional threat. Included in this threat are tactical air, land, and sea forces.

- ✪ Unconventional Threat—This threat encompasses a broad spectrum of military and paramilitary operations predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape networks.

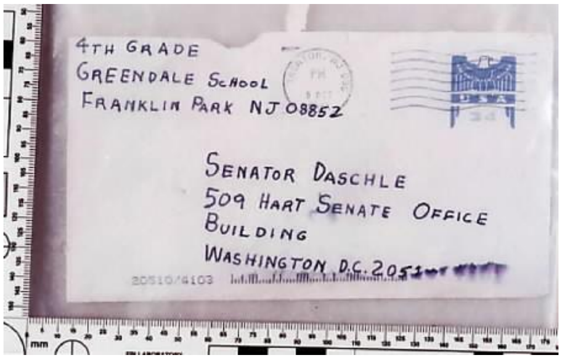
- ✪ Terrorism Threat—This threat involves the calculated use of violence or threat of violence to inculcate fear and is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Acts of terrorism are often planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists, and erode public confidence in the ability of a government to protect and govern the people.

Terrorism is a key force protection issue.

- ✪ Criminal Threat—Criminal activity may help us predict future actions or provide advanced indications and warning of attack. For example, theft of vehicles, military identification cards, passports, or installation entry passes is a potential indicator of pending hostile action. Synthesized analysis of law enforcement and counterintelligence information is necessary to identify indicators of future attacks. Aggressively initiated and continuous liaison efforts are needed for timely information sharing and willing cooperation from host forces.

- ✪ Insider Threat—This threat comes from assigned personnel (military or civilian), host-country nationals (military or civilian), third country nationals (contract employees) or other persons assigned to or transiting the AOR. Any of these groups of people may threaten Air Force interests by disclosing sensitive or classified information, making decisions that favor dissident groups, or by asymmetric attack. They may target individuals, groups, facilities, weapon systems, or information systems. Host country forces may not provide the degree of FP anticipated or agreed to under treaty or coalition arrangements.

- Psychological Threat—Enemy threats target the psychological and physical well being of Air Force personnel. The threat of CBRNE attacks can hinder effective military operations as much as an actual attack. The enemy may also use deception (such as releasing harmless powder) to undermine the mission. Enemy propaganda and potentially biased media sources may also undermine coalition and public support, create civil unrest, and dangerously weaken military morale. Commanders should never underestimate the importance of effective communication to minimize FP risks.



4TH GRADE
GREENDALE SCHOOL
FRANKLIN PARK NJ 08852

SENATOR DASCHLE
509 HART SENATE OFFICE
BUILDING
WASHINGTON D.C. 2051

20510/4103

The threat of anthrax or other diseases can produce psychological as well as physical effects.

- Weapons of Mass Destruction (WMD) Threat—The WMD threat comes from systems that are capable of a high order of destruction or of being used in such a manner as to destroy large numbers of people. WMD can be high explosives or nuclear, biological, chemical, and radiological weapons.

> *A bioterrorist event presents an entirely different scenario, one that is alien to civil authorities. Epidemics of serious diseases such as are anticipated are wholly unknown to American cities. Unlike an explosive or chemical event, the bioweapons release would be silent and almost certainly undetected.*
>
> **—DA Henderson, International Symposium on Respiratory Viral Infections, 3 December 2000**

- Civil Unrest Threat—This threat reflects country-specific concerns of violence by the population related to friendly force operations. The threat can manifest itself during protests, demonstrations, refugee/humanitarian operations, and any other local tensions that may escalate into a direct threat to our forces.

- Information/Data Threat—This threat results from attempts to adversely affect Air Force information systems, information-based processes, and computer-based networks. The enemy and its unconventional supporters may attempt to impact military command, control, communications, and computers, disrupt support activities such as local, military, and civil financial institutions, and interfere with supervisory control and data acquisition systems used to control critical infrastructures. This threat can work in conjunction with all other threats.

- Environmental threat—Air Force assets may be threatened by hazardous waste, unstable infrastructure, inclement weather, disease vectors, unfamiliar culture, and other factors. If ignored, these threats may have serious consequences on an Airman's ability to support the mission, total unit functional capacity, and morale.

THREAT OBJECTIVES AND TYPES OF ATTACK

Threats against Air Force interests are divided into the categories of methods of attack and the objectives those methods seek to accomplish.

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.

—Giulio Douhet

Threat Objectives

There are multiple objectives of methods of attack, designed to cause one or more of the following deleterious actions:

- Injure or kill personnel to create a tactical and/or strategic event.
- Destroy war-fighting or war-supporting capabilities.
- Deny use of war-fighting or war-supporting capabilities through damage or contamination.
- Deny or disrupt military operations through the threat of attack.
- Influence public opinion and/or governmental policies to comply with competing ideologies.
- Force nations deployed on foreign soil to end operations and depart the deployed location.
- Thrust a nation into civil unrest resulting in civil war.
- Force a government agency or corporation to alter its policies.

- Reduce military advantage through theft, destruction, or fraud involving military information or technology.

- Foment criminal activity such as kidnapping, robbery, and extortion likely to be used to finance terrorist operations.

Types of Attack

The forms of attack described below are not mutually exclusive. Any of them can include elements of others; a standoff attack may include a follow-on penetration attack, for example, and a CBRNE attack will invariably include psychological aspects.

Choosing the Targets and Concentrating on the Martyrdom Operations:
The mujahid Islamic movement must escalate its methods of strikes and tools of resisting the enemies to keep up with the tremendous increase in the number of its enemies, the quality of their weapons, their destructive powers, their disregard for all taboos, and disrespect for the customs of wars and conflicts. In this regard, we concentrate on the following:
1. The need to inflict the maximum casualties against the opponent, for this is the language understood by the west, no matter how much time and effort such operations take.
2. The need to concentrate on the method of martyrdom operations as the most successful way of inflicting damage against the opponent and the least costly to the mujahidin in terms of casualties.
3. The targets as well as the type and method of weapons used must be chosen to have an impact on the structure of the enemy and deter it enough to stop its brutality, arrogance, and disregard for all taboos and customs. It must restore the struggle to real size.
4. To reemphasize what we have already explained, we reiterate that focusing on the domestic (US presence overseas) enemy alone will not be feasible at this stage.

—Ayman al-Zawahiri, excerpt from "Knights Under the Prophet's Banner," written shortly before 11 September 2001

- Standoff Attacks—These attacks are carried out at some distance from the intended target such as from outside a base perimeter. Standoff attacks are difficult to counter due to problems in locating the source of the attack.

- Penetration Attacks—A traditional penetration attack is a form of offensive action in which the enemy seeks to break through our defense and disrupt the defensive system. The insider threat may be involved with this form of attack.

- Terrorist Attack—Recent attacks have involved the terrorist use of unpredictable asymmetrical techniques such as suicide bombings or the use of civilian airliners as terror weapons.

- Chemical, Biological, Radiological, Nuclear, and Explosive Attacks—Biological attacks use living organisms (natural or man-made) or their toxic by-products to produce casualties in personnel, animals, or plants and to contaminate food and water supplies. Chemical attacks employ chemical agents to kill, injure, or incapacitate personnel, plants, or animals for a significant period of time. Such attacks deny or hinder the use of areas, facilities, or material. Information on development and use of biological and chemical agents is widely available, as are the supplies needed to create or employ them. Radiation hazard from a nuclear weapon detonation, dirty bomb, or a radiological source could prove devastating in its effects. Large numbers of people can be injured or killed and large geographical areas can be contaminated if drinking water becomes affected.

- Information Operations—Attacks that may target Air Force personnel and infrastructures through psychological operations, propaganda, electronic attacks, and network attacks. Due to the insidious nature of these events. It may be difficult to determine if an attack has occurred or if routine accidents have occurred. These attacks can be as devastating to mission effectiveness as other forms of attack, and can also be precursors to physical attack.

All personnel involved in FP must recognize the need for a thorough understanding of these methods and their objectives. This understanding allows them to properly plan for countering these methods, thereby improving the FP status of their organization and its personnel.

TERRORIST TRENDS

The 11 September 2001 attacks on the United States, though deadlier than any previous terrorist incidents, reflect trends in international terrorism that began years previously.

- Terrorism has become more lethal and transnational.

- Groups have become as great a threat as some states.

- Jihadists and radical Islamists continue their role as a major threat.

- Despite a continued desire to execute large scale, mass casualty attacks, smaller, more frequent attacks are more likely to occur (e.g., suicide bombings, assassinations, low level biological attacks, car and truck bombings, arson attacks).

- Terrorists will continue to innovate in the types of attacks

Terrorists strike soft targets such as the Marriott Hotel in Jakarta, Indonesia.

they conduct, the methods they use, and the targets they select. Historically, terrorists have been more imitative than innovative, but recent attacks prove they are adept at tactical innovation.

- Evolution of loose networks and increased cooperation among terrorist groups is increasing. As the global war on terrorism reduces the ability of terrorist groups to operate, they may begin to share expertise, training, materials, and even participate in each others' operations.

- Reliance on new technologies (e.g., email, the internet, video/audio production) to enhance internal communications and spread their message to enhance recruitment, popular support, and intimidate adversaries continues.

- The United States is a prime target. While many factors contribute to this, our presence in Southwest Asia and continued economic, political, and military dominance are contributing factors.

"Hamas is not just an extremist organization," says Kadura Fares, a member of the Palestinian Legislative Council, "it's also pragmatic. It runs charitable societies for the poor and elderly. They are keen on both images of the fighter and of the benevolent, staying within the political sphere. They cannot alienate themselves at this stage."
Support for Hamas is high and signing up to an Arafat-sponsored ceasefire would alienate a big part of its constituency.
Followers believe suicide attacks are serving an important purpose.
"I support suicide bombings, in the sense that they create awareness among the Israeli people who will put pressure on their government to stop the daily incursions into Palestinian cities. In that aspect they have been very successful," said Mohammed Hussein Romani, a former Hamas operative who spent six years in jail in the 1990s.

—Canadian Broadcasting Corporation News, 16 August 2002

- The persistence of terrorism reflects the number and intensity of conflicts around the world, the attractiveness of terrorism as a weapon of the weak against the strong, and the inherent difficulties of overcoming the tactical advantages that terrorists enjoy. Although terrorism will continue to pose a significant challenge to United States interests around the globe, the incidence of international terrorism will depend to a large degree on the effectiveness of our counterterrorism efforts.

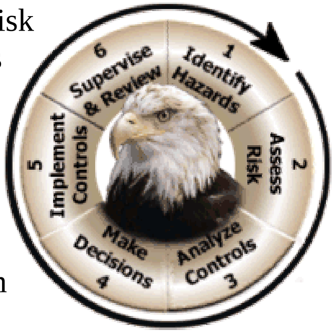
✪ Commanders and policy makers should continue to plan for increases in the volume and lethality of terrorism and for attacks across the entire spectrum of weapons (including CBRNE), tactics, and targets.

CHAPTER FOUR
COUNTERING THE THREATS

This chapter identifies a set of FP tools for commanders to consider when preparing to counter threats in their areas. This begins with the risk management process and proceeds to FP countermeasure planning and implementation.

RISK MANAGEMENT PROCESS

Commanders determine how best to manage risks. This risk management process consists of identifying the potential threats through a threat assessment, analyzing the vulnerabilities through a vulnerability assessment, prioritizing the vulnerabilities by a criticality assessment, then determining the risks acceptable to them for a given operation by conducting a risk assessment. Force protection working groups (FPWG) manage this process for commanders. A safety and risk management focus ensures maximum protection of people and physical resources. This kind of risk-based focus is critical to warfighting success. The Air Force's operational risk management (ORM) process is a readily available tool to perform these assessments.



USAF ORM Process

Threat Assessment

A commander must know what threat is being confronted in order to devise a means to counter it. Without this knowledge, the commander is acting blindly. A threat analysis based on synthesized information can identify indicators of potential attacks. It will review the factors of a threat's existence, capability, intention, history, and targeting, as well as the security environment within which friendly forces operate. This analysis is an essential precursor step in identifying the probability of attack and results in a threat assessment. At the installation level, an element of the FPWG, called the threat working group (TWG), conducts and analyzes the threat assessment and provides recommendations to the FPWG.

Threat assessments fuse information and intelligence from multiple sources (environmental, medical, suspicious activity reports, information/data threat, liaison with local/host nation law enforcement and counterintelligence counterparts) with other information into a cohesive threat picture helpful to FP decision makers. Synthesized analysis of law enforcement and counterintelligence information is important to identifying indicators of future terrorist attacks. Threat assessments are conducted based upon specific criteria and the threat continuum each commander must take into account.

Vulnerability Assessment

Once the threat assessment is complete, commanders need to prepare a vulnerability assessment for their personnel, equipment, facilities, installations, and operating areas. This assessment addresses the broad range of physical threats to the security of personnel and assets.

This assessment considers identified and projected threats against a specific location's or installation's personnel, facilities, and other assets. It should not limit considerations to pre-existing plans, but should allow imaginative thinking in determining vulnerabilities. The assessments should identify vulnerabilities of Air Force interests, prioritized by their criticality to the mission along with ease of exploitation, and propose solutions for enhanced protection.

Risk Assessment

Upon completion of the vulnerability assessment, commanders should have the information needed to make decisions about what level of risk they are willing to accept. Risks to the most critical Air Force interests must be eliminated whenever possible, but it is ultimately the commander's decision about what level of risk to accept.

Once the risk assessment is complete and risk-level decisions made, commanders can use this information to plan a FP course of action to eliminate the risks they are not willing to accept, and mitigate the risks they either cannot eliminate or have accepted. If a mishap occurs, commanders must ensure mishap reporting procedures are implemented.

FORCE PROTECTION COUNTERMEASURE PLANNING

Commanders must take deliberate action to implement comprehensive countermeasures to deny an adversary information, access, and influence, thereby deterring him from taking action against friendly forces. Commanders should incorporate the following countermeasures into their overall defensive and offensive planning.

At the installation level, the TWG provides a threat analysis to the FPWG. The FPWG reviews current and potential threats affecting Air Force facilities, operations, and personnel, and recommends courses of action to commanders to mitigate and/or counter the threat. FPWG membership cuts across multiple disciplines (e.g., intelligence, operations, Security Forces, Civil Engineering, Health Services, communications, AFOSI, etc.), bringing expertise and experience together in one forum to address FP issues.

In the course of planning, commanders should maintain an awareness of legal constraints that may affect operations. Information relevant to the use of force may be contained in international law, US law, host nation law, the laws of war, and established rules of engagement. Together, these laws and rules will regulate the status and activities of forces across the range of military operations.

Deny Information

The Air Force denies an adversary information through a variety of active and passive FP measures. Protecting sensitive unclassified and classified information and associated systems is the key to countermeasure planning. Denying potential adversaries the information necessary to plan and conduct hostile actions is the most effective, but also the most difficult, means to enhance FP. For additional discussion on operations security and denying information to our adversaries, see the AFDDs on Information Operations and Public Affairs.

The following capabilities exist to assist commanders in executing FP responsibilities:

- Counterespionage Programs—These are activities conducted to detect, deter, and neutralize adversary intelligence gathering. They consist of interdisciplinary measures combining personnel security, awareness, and reporting that prompt investigations to neutralize a threat. These programs also employ independent offensive operations to engage adversarial human intelligence (HUMINT) capabilities to deny the adversary's intelligence objectives or influence the adversary's understanding of the environment.

- Technical Security Countermeasure Surveys—These surveys are the means by which adversary technical intelligence gathering capabilities are detected and neutralized. They contain interdisciplinary evaluations of physical security, access control, technical security, and the identification of vulnerabilities specific to those disciplines. The surveys also identify clandestine technical intelligence collection means to be neutralized or exploited.

- Multidisciplinary Vulnerability Assessment—This assessment identifies installation vulnerabilities to information operations to include OPSEC, network, and physical security. This includes information assurance and network vulnerability assessments. Information assurance provides measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. It is an integral part of network defense.

- Information Security—Information security provides guidance for classification, protection, and dissemination of classified national security information processed within any information system.

- Camouflage, Concealment, Deception (CC&D)—CC&D reduces the effectiveness of hostile forces and reconnaissance assets through the principles of hide, blend, disguise, and decoy to protect friendly assets and potential targets with materials and equipment that alter or obscure part or all of their multispectral signatures.

Information security supports FP efforts

Deny Access

The Air Force denies access to adversaries through the application of FP measures. Integrated with measures that deny information to an adversary are measures to deny access if an enemy attempts to collect available intelligence. The objective of denying access is to prevent or deter a hostile action by limiting vulnerabilities of personnel and operations. The following measures can be used to achieve denial of access:

- Surveillance Detection and Countersurveillance—Technical and human sources of information identify potentially hostile surveillance to evaluate it as a threat and recommend countermeasures. Countermeasures may include relocating targeted assets, increasing a security posture, and employing cover or concealment. Countersurveillance operations may also be executed offensively to identify suspected surveillance and disrupt potentially hostile intelligence gathering methods.

- Protective Service Operations—Personal protective operations are undertaken on behalf of high risk or key individuals to reduce the risk of assassination, kidnapping, or other physical harm.

- Protective Threat Assessments and Vulnerability Surveys—Time, location, and threat-specific evaluations of potential individual targets are conducted for the identification of particular vulnerabilities. These assessments and surveys help meet a short-term need to increase the security posture of the facility evaluated or person being protected.

- Combatting Terrorism—Actions taken to protect Air Force personnel and property from terrorist acts and to oppose terrorism throughout the entire threat spectrum. Combatting terrorism includes antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism). Actions may include implementation of random measures to protect Air Force populace from terrorist activities, installation of physical security aids, and education and awareness training. Proactive investigative efforts are used to identify, detect, and neutralize terrorist targets before they strike against Air Force resources.

> *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 equipment.*
>
> **—General Ronald R. Fogleman, CSAF, 1997**

The senior Air Force commander responsible for each air base may delegate authority to conduct air base defense to a subordinate commander. The goal is to enable all Air Force members, support staff, and civilian agencies to contribute to FP while fulfilling their primary functions, thereby ensuring the continuation of air and space operations in any circumstances. The key is integrated base defense (IBD), not ad hoc efforts by different organizations. See Chapter Five for an in-depth discussion of IBD.

Deny Influence

The Air Force denies adversarial influence through force health protection and full spectrum threat response actions. The considered use of the following defensive measures acts as a force multiplier, providing greater survivability for all personnel during routine or emergency situations. The objective of influence denial is to prevent intentional attacks from causing degradation of operational mission capability by assigned personnel.

- Force health protection is a “total life-cycle” health support system that addresses all health-related threats affecting the combat force and the supporting community before, during, and after deployment. It denies influence by:

    - Promoting fitness for enhanced performance, before and during deployments.
    - Assuring healthy and safe food and water.
    - Providing mission-tailored casualty care capability**.**
    - Preventing or controlling infectious diseases, including biological agents.
    - Protecting personnel from hazardous materials, including chemical agents**.**
    - Preventing injuries from combat action.
    - Conducting medical surveillance and information.

For additional information, see AFDD 2-4.2, *Health Services*.

- Full spectrum threat response (FSTR) activities contribute to the overall force protection posture by organizing, equipping, and training the base to respond and recover from natural, accidental, and hostile threasts facing military installations such as major accidents, natural disasters, use of CBRNE by terrorists or in wartime. FSTR actions provide the capability to deny influence by enhancing force survivability and mission continuation through:

    - The dispersal, sheltering, evacuation, or relocation of materiel and people needed for mission accomplishment and recovery tasks.
    - Use of individual protective equipment**.**
    - Mutual support agreements with civilian authorities, local US and DOD agencies, and host nation organizations.
    - CBRNE control, warning, plotting, predicting, and reporting.

Use of chemical detector technology provides additional denial of enemy influence.

✪ FSTR passive defense measures deny influence by improving the capability of personnel to survive and sustain operations before, during, and after an enemy attack. Capabilities include:

✪ ✪ Attack detection and warning**.**

✪ ✪ Reconnaissance after attack.

✪ ✪ CBRNE contamination avoidance/control.

✪ ✪ Damage repair, fire protection, and individual protection.

✪ ✪ Structural engineering, hardening, and infrastructure engineering to increase structural strength and ballistic protection.

✪ ✪ Explosive ordnance disposal to protect personnel and resources from unexploded ordnance and train personnel on unexploded ordnance recognition.

✪ ✪ Individual training in cover and concealment, small arms employment, and personal protection measures.

In summary, the comprehensive measures outlined above are tasks and objectives historically proven to be effective in providing FP when properly implemented. These can prove especially beneficial for air and space expeditionary force operations.

Static aircraft protection embarked on a new phase in 1968 as the Air Force launched a crash shelter construction program…. The protection afforded aircraft by hardened shelters confirmed the soundness of the program…. Seventh Air Force on 3 June 1969 cited two cases in which aircraft parked in shelters escaped destruction by direct rocket hits. On another occasion shelters saved several aircraft from damage or destruction when a nearby munitions storage area exploded. In spring 1970 a USN EC-121 crashed and burned at Da Nang, but adjacent hardened shelters saved three USAF F-4Ds from destruction and two others from major damage. The estimated dollar savings attributed to shelters in these incidents more than paid for the $15.7 million program in [the Republic of Vietnam].

—Roger P. Fox, Air Base Defense in the Republic of Vietnam: 1961-1973

CHAPTER FIVE
INTEGRATED BASE DEFENSE

Every Airman a sensor

If I see a troop walking across tent city and ask him what he or she is thinking about, I expect to hear an alert answer about security and force protection. Every Airman is a sensor.

—General John P. Jumper, CSAF, 2003

One of the most vital tools in countering threats, especially in an expeditionary environment, is integrated base defense (IBD). **IBD is the integrated application of offensive and defensive action, both active and passive, taken across the ground dimension of the force protection battlespace to achieve local and area dominance in support of force protection.**

Integrated base defense requires Air Force personnel to see first, understand first, and act first.

The IBD battlespace encompasses flightlines, priority resources, personnel cantonment areas, base facilities, and accommodation areas, and extends beyond the physical perimeter. The objectives that guide IBD forces seeking to dominate the battlespace are to see first, understand first, and act first. The conditions influencing IBD are points in the operational spectrum defined by the strategic, operational, and tactical situations. While the methods used to achieve battlespace domination will vary depending on prevailing conditions, the enduring components for success are people and technology.

Essential capabilities for IBD are those actions deemed critical to successfully plan, program for, and execute combat support operations. They are shown at Figure 5.1. The application and methods, through which the IBD essential capabilities can be achieved, are variable depending on the prevailing threat, environment, friendly forces available, rules of engagement, and other factors that characterize the battlespace.

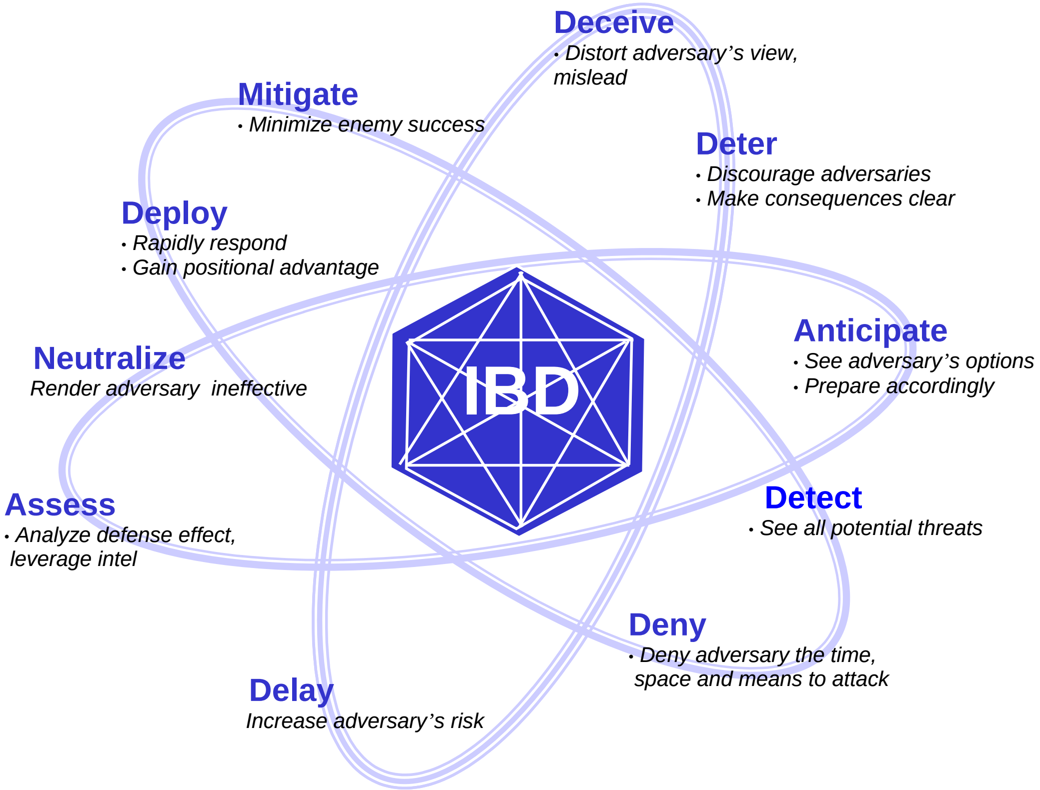

Deceive
• Distort adversary's view, mislead
Mitigate
• Minimize enemy success
Deter
• Discourage adversaries
• Make consequences clear
Deploy
• Rapidly respond
• Gain positional advantage
Anticipate
• See adversary's options
• Prepare accordingly
Neutralize
Render adversary ineffective
IBD
Assess
• Analyze defense effect, leverage intel
Detect
• See all potential threats
Deny
• Deny adversary the time, space and means to attack
Delay
Increase adversary's risk

Figure 5.1. Integrated Base Defense Capabilities.

IBD forces will vary depending on the theater and may include other Services, civilian employees/civil servants, government and law enforcement agencies, civil emergency services, coalition partners, host nations, and friendly communities. The blending of IBD forces' efforts creates unity of effort from which complementary and synergistic effects can flow. The teaming of IBD contributors can create a seamless defense effect that is stronger than the defense efforts of individual contributors.

IBD is viewed as an element of a well-defined, networked command and control architecture and is essential to achieve responsive base defense. This networked architecture permits rapid information exchange and provides a common operating picture to facilitate accurate, effects-based decisions.

As FP is ultimately a commander's responsibility, it is incumbent on an installation commander to protect those assets within his or her responsibility. This means not only providing FP for all personnel and property on an air base, but also protecting aircraft arriving or departing the installation. The surface-to-air missile (SAM) footprint should be considered whenever operations require Air Force personnel to work in an area where this threat may exist. Established rapport and mature relationships are needed with host military and civil forces to mitigate threats and react to incidents appropriately. In addition, the threat of indirect fire weapons from the surrounding vicinity of an installation should be considered. This requires IBD to proactively examine the entire environment surrounding an installation, not just the installation proper. Although the geographic combatant commander has ultimate responsibility for all FP within his or her AOR, Air Force commanders at every level have the inherent responsibility to protect their forces and assets. It is incumbent on them to take all necessary measures to meet the needs of the combatant commander. IBD allows the latter to take all necessary steps to do this.

The base commander on an installation is responsible for the defense of that base and its area of operations. It is incumbent on the geographic combatant commander to identify that area of operations surrounding the installation for which the base commander is responsible. This will allow the base commander to project the necessary force to ensure the security of all personnel and resources. Forces assigned or attached to a base specifically for the purpose of base defense, regardless of Service, should be placed under TACON of the base commander.

Air bases have a unique set of defensive priorities that must be met to ensure the successful employment and sustainment of air and space power. To ensure continued operations, installation commanders must employ or influence the activities of joint/coalition forces within their base security zone (BSZ), the area from which an enemy can launch a standoff attack on the installation based on the local postulated threat. At locations designated a combat zone or where DIA assesses the threat to air and space forces is high, commanders establish an expeditionary operations center (EOC). The EOC provides command and control for operations in support of installation defense as outlined in JP 3-10. An EOC integrates and synchronizes all active and passive force protection efforts under the leadership of the installation commander. The EOC strives to anticipate and counter enemy action by employing joint operations within the BSZ that are deconflicted with the land component commander's ongoing operations. If interdicting the enemy fails, the EOC ensures adequate combat power is available to neutralize an enemy force with joint fires or direct action. The EOC also ensures joint capabilities are brought to bear to mitigate the effects of a successful enemy attack.

CONTINGENCY RESPONSE GROUPS AND BASE OPENINGS

CRG personnel establishing security for an airfield in Kyrgyzstan.

IBD becomes even more vital when the Air Force opens new air bases in uncertain environments, such as the bases in Iraq during Operation IRAQI FREEDOM. For such tasks, a Contingency Response Group (CRG) containing the resources and personnel explicitly prepared for such an operation should be used by the COMAFFOR to perform the mission. **The CRG is the Air Force's "Open the Base" force.**

CRGs provide the seamless transition from airfield seizure, to airbase opening, to force employment and sustainment in concert with follow-on forces across the entire spectrum of airbase operations. Among the FP duties a CRG should be capable of performing are: Establish limited, integrated air base defense; perform airfield assessments; support internment/ humanitarian and relief operations; provide maneuver/mobility sustainment; support airborne, airdrop, air-land, and overland operations; provide confrontation management; perform FP support; establish weapons system security and resource protection; and work issues of interoperability with other Service forces present for FP purposes. While a CRG has multiple responsibilities when deployed to perform its mission, FP is key among them, and is present regardless of the nature of the base opening, whether it is a permissive, uncertain, or hostile environment. A CRG has the responsibility to provide for integrated base defense at any location to which it deploys. This need for FP is important pre-, during, and post-deployment; from base opening to base closure, the CRG's responsibilities in the area of FP remain critical.

At the very heart of warfare lies doctrine…

SUGGESTED READINGS

Air Force Publications

All Air Force personnel should be familiar with the full breadth of Air Force operations. As a beginning, they should read the entire series of the basic, capstone, and keystone operational doctrine documents.

Air Force Doctrine Documents are available online at: **https://www.doctrine.af.mil.**

- AFDD 1, *Air Force Basic Doctrine*
- AFDD 1-1, *Leadership and Force Development*
- AFDD 2, *Organization and Employment of Aerospace Power*
- AFDD 2-1, *Air Warfare*
- AFDD 2-2, *Space Operations*
- AFDD 2-3, *Military Operations Other Than War*
- AFDD 2-4, *Combat Support*
- AFDD 2-4.2, *Health Services*
- AFDD 2-5, *Information Operations*
- AFDD 2-6, *Air Mobility*
- AFDD 2-7, *Special Operations*
- AFDD 2-8, *Command and Control*
- AFDD 2-9, *Intelligence, Surveillance, and Reconnaissance*
- AFDD 2-10, *Homeland Operations*
- Air Force Policy Directive 10-2, *Readiness*
- Air Force Policy Directive 10-8, *Homeland Security*
- Air Force Policy Directive 10-25, *Full Spectrum Threat Response*
- Air Force Policy Directive 10-26, *Counter-Nuclear, Biological, and Chemical Operational Preparedness*
- Air Force Policy Directive 41-1, *Health Care Programs and Resources*

- Air Force Instruction 10-245, *Air Force Antiterrorism (AT) Standards*
- Air Force Instruction 10-2501, *Full Spectrum Threat Response Planning and Operations*
- Air Force Instruction 90-901, *Operational Risk Management*
- Air Force Manual 10-100, *Airman's Manual*
- Air Force Manual 10-2602, *Nuclear, Biological, Chemical, and Conventional Operations and Standards*
- Air Force Tactics, Techniques, and Procedures (Interservice) 3-2.42, *Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Defense Operations*
- Air Force Tactics, Techniques, and Procedures (Interservice) 3-2.46, *Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Protection*
- USAF/XOI, *Postulated Worldwide Non-Nuclear Threat to USAF Installations, Personnel, and Resources*

Joint Publications

- DOD Directive 2000.12, *DOD Antiterrorism (AT) Program*
- DOD Directive 2000.12-H, *Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence*
- DOD Directive 2000.16, *Antiterrorism Standards*
- Joint Publication 0-2, *Unified Action Armed Forces (UNAAF)*
- Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*
- Joint Publication 3-0, *Doctrine for Joint Operations*
- Joint Publication 3-07, *Joint Doctrine for Military Operations Other Than War*
- Joint Publication 3-07.2, *Joint Tactics, Techniques, and Procedures for Anti-terrorism*
- Joint Publication 3-10, *Joint Doctrine for Rear Area Operations*
- Joint Publication 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense*
- Joint Publication 3-11, *Joint Doctrine for NBC Defense*
- Joint Publication 3-13, *Joint Doctrine for Information Operations*

- Joint Publication 3-40, *Joint Doctrine for Combatting Weapons of Mass Destruction*

Other Publications

- Department of State, *Patterns of Global Terrorism*

- Fox, Roger P., *Air Base Defense in the Republic of Vietnam: 1961-1973,* (USAF Office of History), 1979.

- Nolan, Keith William, *The Battle for Saigon—Tet 1968*, (Pocket Books), 1996.

- Shlapak, David A. and Alan Vick, *Check Six Begins on the Ground*, (RAND), 1995.

- Vick, Alan, *Snakes in the Eagle's Nest*, (RAND), 1995.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ADCON	administrative control
AETF	air and space expeditionary task force
AEW	air expeditionary wing
AFDD	Air Force doctrine document
AFFOR	Air Force forces
AFOSI	Air Force Office of Special Investigations
AFP	active force protection
AFRC	Air Force Reserve Command
ANG	Air National Guard
AOR	area of responsibility
ATSO	ability to survive and operate
CBRNE	chemical, biological, radiological, nuclear, and high yield explosives
CC&D	camouflage, concealment and deception
COMAFFOR	commander, Air Force forces
CRG	contingency response group
CSAF	Chief of Staff, United States Air Force
DIA	Defense Intelligence Agency
DOD	Department of Defense
EOC	expeditionary operations center
FP	force protection
FPCON	force protection condition
FPWG	force protection working group
FSTR	full spectrum threat response
HUMINT	human intelligence
IBD	integrated base defense
INFOSEC	information security
INR	Bureau of Intelligence and Research, Department of State
JP	joint publication
MAJCOM	major command
NAF	numbered air force
NBC	nuclear, biological, and chemical

NCO	noncommissioned officer
NSA	National Security Agency
OPCON	operational control
OPSEC	operations security
ORM	operational risk management
PFP	passive force protection
RAM	random antiterrorism measures
SAM	surface-to-air-missile
TACON	tactical control
TWG	threat working group
UNAAF	Unified Action Armed Forces
US	United States
USAF	United States Air Force
USCENTAF	United States Central Command Air Forces
USS	United States ship
VC	Viet Cong
WMD	weapons of mass destruction

DEFINITIONS

active force protection. Measures to defend against or counter a perceived or actual threat and, if necessary, to deny, defeat, or destroy hostile forces in the act of targeting Air Force assets. (AFDD 2-4.1)

area of responsibility. The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. Also called **AOR.** (JP 1-02)

combatting terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. Also called **CBT**. (JP 1-02)

base commander. In base defense operations, the officer assigned to command a base. (JP 1-02)

countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

force health protection. All services performed, provided, or arranged by the Services to promote, improve, conserve, or restore the mental or physical well-being of personnel. These services include, but are not limited to, the management of health services resources, such as manpower, monies, and facilities; preventive and curative health measures; evacuation of the wounded, injured, or sick; selection of the medically fit and disposition of the medically unfit; blood management; medical supply, equipment, and maintenance thereof; combat stress control; and medical, dental, veterinary, laboratory, optometry, medical food, and medical intelligence services. (JP 1-02) [*A comprehensive threat-based program directed at preventing and managing health-related actions against Air Force uncommitted combat power*.] (AFDD 2-4.2){Italicized words in brackets applies only to the Air Force and is offered for clarity.}

force protection. Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called **FP**. (JP 1-02) Because terminology is always evolving, the Air Force believes a more precise definition is: [*An integrated application of offensive and defensive actions that deter, detect, preempt, mitigate, or negate threats against Air Force air and space operations and assets, based on an acceptable level of risk.*] (AFDD 2-4.1){Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

full spectrum threat response. The broad spectrum of planning, response and recovery actions to physical threats facing military installations including major accidents, natural disasters, HAZMAT, terrorist use of WMD, and enemy attack. Also called **FSTR**. (Adapted from AFI 10-2501)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO**. (JP 1-02) [*Information operations are the integrated employment of the core capabilities of Influence Operations, Electronic Warfare Operations, Network Warfare Operations, in concert with specified Integrated Control Enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own*.] (AFDD 2-5) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

integrated base defense. The integrated application of offensive and defensive action, both active and passive, taken across the ground dimension of the force protection battlespace to achieve local and area dominance in support of force protection. Also called **IBD**. (AFDD 2-4.1)

passive force protection. Measures to negate or reduce the effects of hostile acts on Air Force assets by making them more survivable. This can be proactively accomplished through training, education, hardening, camouflage, concealment, deception, information security, and low/zero observable execution. Also called **PFP.** (AFDD 2-4.1)

random antiterrorism measures. Active force protection measures applied periodically and at irregular intervals to change the look of an installation's force protection program. These measures make it difficult for terrorists to accurately predict force protection actions by introducing uncertainty into the overall force protection program. Also called **RAM**. (AFDD 2-4.1)