Camp Dobol, Bosnia.

55th Signal Company (Eduardo Guajardo)

Changing the Mindset—Army Antiterrorism Force Protection

By RONALD F. ROKOSZ *and* CHARLES H. HASH

In 1995 and again in 1996 terrorists breached force protection measures for U.S. personnel located in Saudi Arabia. The November 1995 attack on the Office of the Program Manager/Saudi Arabian National Guard, which killed 6 and wounded 40, was a sign of deadly events to follow. In June 1996 at the Khobar Towers housing complex a tanker truck loaded with explosives was detonated next to the northern perimeter fence killing 19 U.S. airmen and injuring hundreds more. As Secretary of Defense William Perry stated at the time, "The Khobar Towers attack should be seen as a watershed event pointing the way to a radically new mindset and dramatic changes in the way we protect our forces deployed overseas from this growing threat." Accordingly, DOD launched an aggressive effort to protect all its personnel and their family members.

Brigadier General Ronald F. Rokosz, USA (Ret.), and Major Charles H. Hash, USA, served together in the Operations, Readiness, and Mobilization Directorate at Headquarters, Department of the Army.

The Downing Report

To establish an antiterrorism force protection (AT/FP) baseline and corrective action plan after the Khobar Towers bombing, Perry immediately

asked General Wayne Downing, USA (Ret.), a former commander in chief of U.S. Special Operations Command, to examine the circumstances surrounding the attack. In late August 1996 the Downing Assessment Task Force made some sweeping recommendations. The report submitted by the Secretary to the President on *The Protection of U.S. Forces Deployed Abroad*, which appeared the following month, declared that the Downing report was "an important contribution to changing our entire approach to force protection and provides evidence of the need for changes in the way we do business. We have taken the following actions. . . . [We will]:

- issue DOD-wide standards for providing force protection
- give local commanders operational control with regard to force protection matters
- designate the Chairman . . . as the principal advisor and the single DOD-wide focal point for force protection activities
- move force protection responsibilities from the Department of State to the Department of Defense where possible
- improve the use of available intelligence and intelligence collection capabilities
- establish a workable division of responsibilities on force protection matters between the United States and host nations
- raise the funding level and priority for force protection and get the latest technology into the field and into the Department of Defense."

The Chairman then named the J-34 deputy director for Operations, Combating Terrorism, as single point of contact on the Joint Staff for antiterrorism/force protection. Moreover, he recognized the need to appoint a technical and field agent for AT/FP. That role was given to the Defense Special Weapons Agency (formerly the Defense Nuclear Agency) which functions in conjunction with J-34 to provide technical expertise and assessments. That agency established Joint Staff integrated vulnerability assessment teams which were assigned the AT/FP mission based on experience in conducting facility vulnerability assessments, weapon-target interaction computations, and multidisciplinary threat assessments.

the danger to military personnel comes primarily from unconventional means

The Threat

The danger to military personnel comes primarily from unconventional means because our conventional military capabilities are unrivalled. Foreign states, groups, and even individuals can avoid our military strengths and attack our vulnerabilities through asymmetrical warfare. In simple terms, this warfare pits one's strengths against an enemy's weaknesses.

Command and control nodes, airfields, and work areas are often hardened and difficult for terrorists to enter. However, barracks outside of work areas can house many soldiers and provide soft targets. Domestic terrorists looking to strike a blow may attack an accessible Federal office building as opposed to a hardened, guarded military installation.

Such attacks are asymmetrical and unconventional, but they accomplish their objective—to generate casualties and garner media attention. The broader the exposure and more spectacular the attack the better. The potential for terrorists to inflict high casualties has increased with advanced technology and larger bombs and the availability of weapons of mass destruction such as chemical and biological agents. Attacks like the bombing of the Oklahoma City Federal office building and the sarin gas attack on the Tokyo subway system could become all too common.

Casualties are a center of gravity. American values are based on the sanctity of human life, and public opinion is easily swayed by fatalities televised on CNN. That was demonstrated after the bombing of the Marine barracks in Beirut and the death of Army rangers in Somalia. Enemies are willing to capitalize on American sensitivities and are not restricted by political or ethical rules. Casualties at Khobar Towers confirmed this phenomenon and led us to quickly refocus our efforts to protect U.S. forces in the region.

The Army and AT/FP

The U.S. policy of "engagement and enlargement" finds itself supporting operations across the broad spectrum of conflict in every corner of the world. The Army has proven to be one of the forces of choice to execute these security missions. On any day it has over 100,000 soldiers and civilians forward deployed and another 35,000 temporarily deployed to 86 countries in support of contingency operations and exercises. These personnel make the Army a target of opportunity for terrorist acts. Our soldiers around the world must be proactive in protecting themselves, their unit members, and their families.

Although the Army has had a viable, focused AT/FP program for years, following the Khobar Towers bombing, General Dennis J. Reimer, the Chief of Staff, U.S. Army, directed the Deputy Chief of Staff for Operations and Plans to establish a task force to assess force protection. Major Army commands (MACOMs) focused on the adequacy of AT/FP in the areas of doctrine, policy, training, and resourcing and appraised program execution and recommendations to improve the protection of personnel, information, and critical resources.

Closed circuit security camera.

U.S. Air Force (Shonna Ridings)

As directed, MACOMs reviewed their AT/FP posture and helped to develop task force findings and recommendations. Once the results of the assessment were reviewed, the Chief of Staff sent a message to Army activities on July 26, 1996 outlining the findings of the task force and areas of emphasis. It directed commanders to ensure that key AT/FP initiatives were being followed, including efforts to:

the Army approaches AT/FP along three axes—doctrine and training, operations, and intelligence

- review and revise Army regulation 525-13, the Army combating terrorism program, and ensure responsibilities and required actions are being followed
- emphasize AT/FP training at all levels of command
- ensure AT/FP assessments are part of leader recons in conjunction with deployments
- guarantee AT/FP requirements are given a high priority in budgets
- ensure AT/FP is an area of special emphasis for inspection and review relevant doctrine and supplement it with recent lessons learned.

Army initiatives were systematically being worked by the Army staff and commanders at all levels concurrent with a DOD-wide review of force protection directed by the Secretary of Defense.

What is AT/FP?

It may help to define what Army force protection is and is not. It is not a new program for the Army. AT/FP is the security portion of a much larger operational concept known as force protection. AT/FP synchronizes select security programs into comprehensive defensive measures to protect personnel, information, and critical resources against asymmetrical threat attacks. AT/FP targets foreign and domestic terrorist threats, as well as those criminals, violent protesters, saboteurs, and foreign intelligence agents who support terrorism, promote conditions beneficial to the conduct of terrorist operations, or otherwise mount operations to further their own agendas at the expense of the Army and its mission. According to a draft of Army regulation 525-13, antiterrorism force protection is defined as:

A security program to protect personnel, information, and critical resources from asymmetrical attacks. This is accomplished through the planned integration of personal security, C^2 Protect [command and control protection], *physical security, and law enforcement, all supported by the synchronization of doctrine, training, operations, intelligence, and resources.*

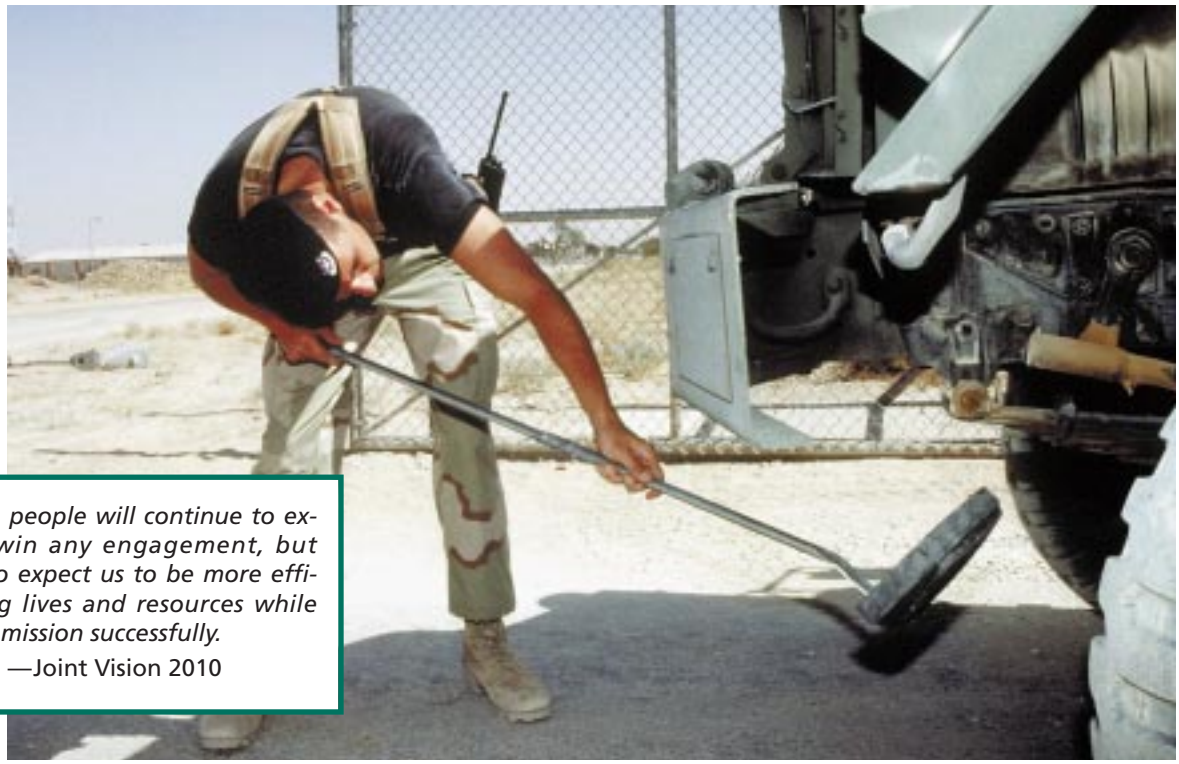
General Reimer has described AT/FP as a holistic program with four pillars: physical security, C^2 Protect, personal security, and law enforcement operations. Moreover, he urged that Army personnel: "Keep focused on force protection. It is a primary leader task and an inherent part of all operations (home station or deployed) to protect soldiers, family members, Army civilians, and resources."

Headquarters, Department of the Army, is responsible for both AT/FP policy and requirements. MACOMs further define policy, provide resources for critical requirements, and oversee subordinate command AT/FP programs. Both installation and unit commanders are responsible for implementing this policy and for allocating resources to maintain the protective posture of installations/units based on local threats and vulnerabilities. Commanders are ultimately responsible for AT/FP. That includes individual and unit antiterrorism awareness training prior to deploying outside the United States, its territories, and its possessions. U.S. Army Forces Command and U.S. Army Europe continue to ensure that all troops deploying to Bosnia are aware of threats and are ready to counter them.

The Army approaches AT/FP along three axes—doctrine and training, operations, and intelligence—which drive resourcing and policy and define the overall program.

Doctrine and Training

The doctrine and training axis is the institutionalization of the program. It is the catalyst for changing the Army's institutional mindset. We must not allow antiterrorism force protection to be a peaks and valleys program. With continued command emphasis, training can ensure that AT/FP is embedded in all operations and activities much like the Army safety program.



U.S. Air Force (Richard M.Heileman)

The American people will continue to expect us to win any engagement, but they will also expect us to be more efficient in protecting lives and resources while accomplishing the mission successfully.

—Joint Vision 2010

The foundation of our training program comes from 15 security related courses taught by the U.S. Army Military Police School (USAMPS), Intelligence School, Corps of Engineers, and the John F. Kennedy Special Warfare Center. USAMPS volunteered for the mission to develop the CJCS level I, II, and III AT/FP training programs. A training task force was formed with each member carefully selected for instructional expertise and experience. The task force condensed 18–24 months of course planning and development to less than three to meet training implementation deadlines.

Level I training provides antiterrorism awareness and specific area of responsibility threat information to all soldiers, Army civilians, and family members deploying or traveling overseas. The purpose is to reduce their vulnerability to terrorism through increased and constant awareness and to reemphasize personal protection measures. This level is divided into two subsets based on threats in the destination country. Low/negligible threat deployments require only the viewing of the Army's individual protective measures video, issuance of Joint Staff Guide 5260 (*Personal Protection Guide*), a wallet-sized card, "Security While Traveling," etc. Medium and higher threat areas require viewing of additional videos and training by a qualified level II instructor. USAMPS has developed level II formal training entitled "The Force Protection Unit Advisors Course." Students representing each unit, battalion and above, will be certified as unit level I trainers and advisors. Level II training prepares individuals to manage unit force protection programs and provide AT/FP expertise to commanders. The trainee can also serve as the level I trainer. This two-pronged program provides commanders with enhanced expertise and will integrate AT/FP into every mission.

The awareness of commanders must also be enhanced to complement level II training. The level III program accomplishes that mission. It provides battalion and brigade commanders with knowledge and skills to ensure unit combat power preservation. This two-hour training support package has been integrated into pre-command courses, including those for garrison and installation commanders. Army schools will energize the package with branch-specific tasks. Required tasks are also getting a technology boost through CD–ROMs which put AT/FP data at one's fingertips.

Level IV training is an executive tier seminar conducted three times a year in the Washington area. It is directed at senior colonels, flag officers, and equivalent level Army civilians to explain their roles in developing programs, address issues, and spotlight information sources to assist in integrating functional aspects of AT/FP. It also offers a forum for exchanging ideas on a host of AT/FP

subjects, better understanding the terrorist, and examining technology to enhance the program. It employs updates, briefings, guest speakers, panel discussions, and a tabletop wargame.

The Army is combining resident schools, exportable training packages, and mobile training team programs with greater command emphasis to institutionalize AT/FP awareness across the board. In addition, Headquarters, Department of the Army, and U.S. Army Training and Doctrine Command (TRADOC) are collaborating on the revision of AT/FP doctrine. The intent is to field a stand alone publication to provide commanders with tactics, techniques, and procedures to implement viable AT/FP operations or integrate them into extant operations field manuals.

new standards and policy will synchronize separate force protection elements

Operations

The Army operations axis is command emphasis on awareness and synchronized efforts to protect people and critical assets. Establishing threat-based standards and revising Army policy are critical to founding baseline requirements for an aggressive and pervasive AT/FP mindset that is embedded in all soldiers and part of every process from mission planning through execution to the after action review.

While commanders are ultimately responsible for providing security for people and assets, other key players include G-3 (operations), G-2 (intelligence), resource manager, provost marshal, staff judge advocate, engineer, and public affairs officer. G-3 integrates all staff efforts.

Policy is being updated through a rewrite of AR 525-13 on the Army program to combat terrorism. The revision includes new DOD and Army standards and policy and will synchronize separate AT/FP elements for a seamless deterrent to terrorists, criminals, spies, and saboteurs. The new regulation embodies the overarching nature of antiterrorism force protection.

The Army recognized that it needed a force protection baseline before fully implementing a program. The tool to assess the Army AT/FP posture was Headquarters, Department of the Army, Force Protection Assistance Team (FPAT) assembled in January 1997. It represented the best from the fields of physical security/law enforcement, special operations, training, structural engineering, information operations, counterintelligence, chemical/biological, medical service, and risk management/safety. Its charter is to assess the health of the program, establish standards, and provide a tool for commanders to measure their force protection posture.

Khobar Towers.

FPAT completed 16 visits in early 1997 to include Army component headquarters of unified commands, MACOM headquarters and installations, and the Reserve components. Commanders received a bonus from the FPAT visits: an assessment of their overall security posture and recommendations on further site enhancements.

> *America has global interests and responsibilities. Our national security strategy for protecting those interests and carrying out those interests requires deployment of our forces to the far reaches of the globe. There will be future terrorist acts attempted against U.S. military forces. Some will have tragic consequences. No force protection approach can be perfect, but the responsibility of leaders is to use our national resources, skill, and creativity to minimize them.*
>
> —William J. Perry

FPAT coordinated with Headquarters, Department of the Army, to resolve issues from the field and recommended initiatives to improve AT/FP. This feedback is critical in tracking trends and indicators that will allow us to measure improvement. The staffed recommendations were brought to the AT/FP Steering Committee Board of Directors for action.

Additionally, the results of the FPAT review were briefed at the Senior Leaders' Training Conference in July 1997. Although FPAT completed its charter, this effort will continue with MACOM assessments of subordinate commands and installations, inspector general oversight of MACOM programs, and Joint Staff integrated assessments of Army installations scheduled by MACOMS and coordinated through Department of the Army.

The board, chaired by the director of Operations, Readiness, and Mobilization at Headquarters, Department of the Army, is the integrating agency for Army AT/FP initiatives. Its inner circle includes representatives from TRADOC, the U.S. Army Intelligence and Security Command, and Army staff elements with responsibility for training, counterintelligence/human intelligence, information operations, resource management, etc. Its outer circle includes key advisors whose areas of expertise sharpen our focus and facilitate key technical initiatives within their areas of specialization. Board oversight ensures that requirements are identified, tracked, and completed. It also develops and allocates tasks based on terrorist threats, Joint Staff team input, intelligence data, and CJCS guidance. The committee is currently reviewing initiatives designed to facilitate and implement the AT/FP program. Two critical initiatives are resourcing programs and developing, acquiring, and installing physical security equipment.

DOD

Exercise checkpoint.

1st Combat Camera Squadron (Paul R. Caron)

Since the Khobar Towers bombing the Army has reviewed resourcing for AT/FP with an emphasis on antiterrorism. The initial review was completed in time for the submission of critical force protection initiatives in the FY97 congressional supplemental budget and the FY98–03 program objective memorandum relook. One major initiative is the acquisition and fielding of AT/FP equipment to the troops.

Properly equipping soldiers is vital to AT/FP. In 1997 $155 million was spent specifically on protecting personnel. Major funding included $86.4 million for up-armored, high-mobility multipurpose wheeled vehicles (HMMWVs), $11.3 million for body armor, $9.8 million for ballistic blankets, and $7.2 million for other physical security equipment. The Army received approval for program enhancements in the amount of $58.1 million in the FY97 supplemental budget. It included $37.6 million for the Army Central Command Saudi relocation and $7 million to implement the land information warfare activity command and control-protect (C^2-P) mission. The remainder was added to the current Army program for activities related to antiterrorism force protection.

Since AT/FP is embedded in most Army activities, it is difficult to determine exact amounts programmed or expended towards that mission, but at the core of the program are the physical security equipment, law enforcement, antiterrorism, installation counterintelligence, and criminal investigations management decision packages. Some 85–90 percent of the personnel were military, Army civilian, or contract guards. Technological initiatives to supplement or replace the manpower-intensive guard force are being solicited for investment funding priority.

The Army's physical security equipment (PSE) program is a pivotal component of the operational axis and brings the latest in technology to counter the threat. Headquarters, Department of the Army, funds critical equipment based on MACOM PSE priorities. The most widely used intrusion detection systems are the joint service interior system, commercial systems, integrated commercial systems, and the alarm monitor group.

The Army has also taken the lead in preparing a DOD physical security and AT/FP technology guide which will be available to commanders in 4th quarter FY97. Commanders on all levels will use it to identify and purchase PSE. The Army PSE program is vital to the overall AT/FP posture of a command. Threat and vulnerability assessments are conducted and reviewed for all installations on a continuing basis. We rely heavily upon Army intelligence assets to help define the threat to personnel and installations. Once it is identified PSE must be applied.

Intelligence

The intelligence axis, specifically counterintelligence, drives the collection, analysis, and dissemination of terrorist threats. Army counterintelligence provides commanders with a predictive analysis tool to counter asymmetrical threats and identify potential terrorist attacks against soldiers and installations. Good intelligence facilitates training and applying resources to harden activities.

Counterintelligence (CI) support covers a range of functions by assisting in vulnerability assessments, advice and assistance to AT/FP and other security programs, liaison with local and national agencies, and CI force protection source operations overseas. Army CI elements collect and report military and military-related foreign intelligence and CI information on foreign terrorist activities and other specified areas. Army CI elements report that information to the Defense Intelligence Agency and provide information copies to the Army Counterintelligence Center (ACIC). Immediate threats are reported to commands and supporting provost marshals.

ACIC conducts analysis and production of strategic CI information. All echelons with CI staff capability conduct analysis and production to meet local needs. Strategic CI production may include worldwide assessments of organizations, personages, sites, funding, training, operations, capabilities, and when possible the intentions of terrorist groups. Local CI elements may use these products and analyze the local situation which affects supported units, installations, or activities.

the threat is no longer limited to the extremist willing to carry out a suicide bombing

The intelligence community, though limited by executive order from collecting information about U.S. persons, can effectively support AT/FP. There is a considerable difference between what CI elements can do for a commander in Bosnia and in CONUS. Federal, state, and local law enforcement agencies have primary responsibility for gathering information to protect U.S. forces in this country. Commanders work with these agencies through garrison provost marshals. Army intelligence personnel may collect, retain, analyze, and disseminate force protection-related data on Americans in CONUS only when DOD has determined they are an actual or potential threat to DOD personnel, installations, or matériel.

The nature of the threat is evolving. It is no longer limited to the foreign-based extremist willing to carry out a suicide bombing. We face domestic dangers from radical militia groups, separatist organizations, and individuals with agendas that include violence.

Threats include assaults on information systems. DOD systems worldwide experienced over 250,000 attacks in 1996 alone, ranging from adolescent hackers to foreign intelligence services. The information highway poses great opportunity and risk for the Army. Additionally, the Internet has become an excellent source for detailed information on bomb making and sabotage. A terrorist or disgruntled employee on a tight budget has easy access to a wealth of information at little or no cost, which may seriously harm Army personnel, information, and critical resources.

The Army vision for the future is simple: AT/FP must be integral to everything we do and plan. To accomplish this we must continue to educate all soldiers, Army civilians, and family members. It is an individual and unit responsibility that requires a dramatic change in outlook.

The Army mindset will be changed through initiatives designed to avoid the periodic peaks and valleys of interest in terrorist acts. We must permeate the operational environment with antiterrorism force protection initiatives and recognize that the best measures are proactive, not reactive. We must also continually update policy and doctrine and ensure that every soldier, civilian, and family member is educated on the subject. Finally, we must adhere to common standards, apply resources based on the threat, and continue to oversee protection through both deterrence and defense. JFQ