The Source for Antiterrorism Information

SPRING 2011 | Volume 13 | Issue 1

The GUARDIAN

Antiterrorism Journal

A Joint Staff, Deputy Directorate for Antiterrorism/Homeland Defense, Antiterrorism/Force Protection Division Publication

The Pentagon, Room MB917 | Washington, DC 20318

Historical Antiterrorism Quotes

March 2010

"Force protection is now a watchword for our nation—not just an obscure program managed by security or law enforcement professionals."

—Brigadier General Jonathan H. Cofer, in his article "Force protection at the joint staff level," from *Military Police*, March, 2002. Cofer had been the J-34 deputy director since July 2000. He has held a variety of positions during his distinguished 29-year career with the MP Corps.

January 2010

"Leaders at Fort Hood had anticipated mass casualty events in their emergency response plans and exercises. Base personnel were prepared and trained to take appropriate and decisive action to secure the situation. The prompt and courageous acts of Soldiers, first responders, local law enforcement personnel, DOD civilians, and healthcare providers prevented greater losses… The tragedy, however, raised questions about the degree to which the entire Department is prepared for similar incidents in the future—especially multiple, simultaneous incidents."

—"Protecting the Force: Lessons from Fort Hood," Report of the DOD Independent Review, January 2010.

The Guardian

The Guardian is published for the Chairman of the Joint Chiefs of Staff by the Antiterrorism/Force Protection Division of the J-34 Deputy Directorate for Antiterrorism/Homeland Defense to share knowledge, support discussion, and impart lessons and information in a timely manner.

Guardian readers,

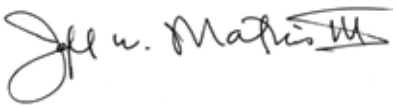
It is with great pleasure that I introduce the Spring 2011 issue of *The Guardian*. Over the past several months, we have experienced an increase in article submissions, and that has helped us better illuminate the latest concepts and advancements in the antiterrorism (AT) community. If you want more information or would like to see certain topics covered in future issues, please let us know. *The Guardian* will only remain relevant as long as it stays abreast of global terrorism issues and covers topics that are relevant to the men and women in the field.

To be sure, 2010 was not an ordinary year for terrorist activity, especially in the homeland. Through clever stings and helpful tips from concerned citizens, US law enforcement foiled a number of homeland terrorist plots in their embryonic stages. Several cases involved enthusiastic terrorists who were given fake explosives. One such case involved a US citizen who parked what he thought was an explosive-laden vehicle in front of a recruiting center near Baltimore. Others have been indicted for allegedly trying to go to Somalia to support al Shabab operations or attempting to attack subway systems in New York City and Washington, DC. And we must not forget the two most prominent cases of 2010: the attempted bombing of New York City's Times Square in May and the interception of two cargo planes with hidden explosives in October.

This year marks the 10th anniversary of al Qaeda's attacks on 11 September 2001, and the 15-year anniversary of the attack on Khobar Towers on 25 June 25 1996. We have come a long way since those days in terms of our tactics and resources, but as you will see in the following articles, much remains to be done. Here is a snapshot:

- **Force Protection and Antiterrorism: Industry Brings Commercial Off-the-Shelf Technology to the Fight:** Discusses the evolution of the Force Protection Equipment Demonstration that began in the wake of the Khobar Towers bombing.
- **Joint Antiterrorism Doctrine Update:** Highlights some of the recent changes to Joint Publication 3-07.2, Antiterrorism.
- **Khobar Towers and the Birth of Modern Antiterrorism:** Reviews lessons learned from the attack on Khobar Towers and where we stand today.
- **Army AT Awareness in Contracting:** Introduces the Army's program for integrating AT awareness with the contracting process.
- **An Out-of-the-Box Proposal: Countering Active Shooter Attacks on DOD Installations:** Discusses alternative ideas for dealing with an active shooter threat.
- **Raising the Focus on Man-Portable Air Defense Systems:** Reminds us of the threat of MANPADs to commercial aviation.

Again, we sincerely appreciate your feedback. If you have a story, share it. If you have new ideas, test them in your units and write down what you learn. As General (Ret.) Wayne Downing noted after the attack on Khobar Towers, "The Department of Defense can more effectively protect our men and women around the world." The Joint Staff shares this belief, and *our* improvement relies on *your* criticism.



JEFF W. MATHIS
Major General, USA
Deputy Director for Antiterrorism/Homeland Defense

FPED VIII

FORCE PROTECTION AND ANTITERRORISM

US Navy photo by PH1(AW) Bart A. Bauer

Industry Brings Commercial Off-the-Shelf Technology to the Fight

By Major Carl White, USMC (Retired), Media Liaison, FPED VIII

FPED VIII will take place at Northern Virginia's Stafford Regional Airport, 17–19 May 2011. This year's event will feature the products of more than 575 exhibitors.

The upcoming eighth Force Protection Equipment Demonstration (FPED VIII) will bring together thousands of military and civilian authorities responsible for FP planning/employment and put them in contact with representatives from companies that may have equipment or systems that meet their unique security needs. FPED VIII is an opportunity to see and learn about the very latest in equipment and systems for saving lives by countering continually emerging FP and terrorism threats.

The first FPED was held in September 1997. In response to the June 25, 1996, bombing of Khobar Towers in Dhahran, Saudi Arabia, the Secretary of Defense appointed retired General Wayne Downing to conduct an assessment of the facts and circumstances surrounding the incident. A key finding in the Downing Report stated: "Technology was not widely used to detect, delay, mitigate, and respond to acts of terrorism." In response, the Chairman of the Joint Chiefs of Staff created the FPED. The first FPED hosted 187 vendors and demonstrated more than 400 products.

FPED VIII will take place at Northern Virginia's Stafford Regional Airport, 10 miles south of Quantico, May 17–19, 2011. This year's event will feature the products of more than 575 exhibitors demonstrating more than 3,000 technologically advanced commercial off-the-shelf (COTS) products in 20 equipment categories (for details, see http://www.fped8.org).

The 20 equipment category types at the FPEDs encompass a broad range of systems capable of highly flexible surveillance missions.

Products to be demonstrated include cargo inspection systems capable of being used in domestic settings within the United States and allied nations as well as in combat zones.

As it did in the early years, the FPED continues to identify solutions to the challenges of terrorism by highlighting COTS equipment and systems. When the Chairman of the Joint Chiefs of Staff established guidance for the first FPED, he listed demonstration of COTS-only products as a priority. The FPED mission has remained the same: Provide leaders and decision-makers from within the Department of Defense, other federal departments and agencies, and selected state and local law enforcement, first-responder, and corrections agencies opportunities to see, and become familiar with, COTS physical security and FP equipment. Today, in addition to the DOD, other federal agency security personnel and city, county, state, and regional security planners across the United States, and their counterparts in allied nations, face very similar AT and related security concerns.

The upcoming eighth Force Protection Equipment Demonstration (FPED VIII) will bring together thousands of military and civilian authorities responsible for FP planning/employment and put them in contact with representatives from companies that may have equipment or systems that meet their unique security needs. FPED VIII is an opportunity to see and learn about the very latest in equipment and systems for saving lives by countering continually emerging FP and terrorism threats.

This iterative interaction between users and manufacturers has created a certain synergy between government and industry, highlighting opportunities for improvements in existing products and development of new ones. Due to the variety of the equipment types demonstrated, it is not unusual for someone seeking preventives to one specific type of threat to discover solutions in equipment produced for another type of vulnerability. As the US community of FP professionals grows and becomes more broadly aware of "what's out there," this valuable type of cross-fertilization of ideas will pay substantial dividends.

In the 14 years since the first FPED, acts of terrorism and attempted terrorist attacks on US and allied troops in combat zones, as well as against civilians in domestic settings, have increased significantly, with a corresponding increase in the variety of technologies and tactics. Authorities today face expanded threats from improvised explosive devices, car bombs, explosives aboard commercial cargo and passenger aircraft, suicide bombers, and direct small-arms assaults. Meanwhile, the list of targets needing protection has grown.

Companies selected for participation in FPED are asked to present functional demonstrations of equipment or systems from among the following categories:

- Automated entry control systems/equipment
- Armored and utility vehicles
- Biometrics
- Blast protection/mitigation (including structural building materials, new or retrofit)
- Cargo inspection devices (including under-vehicle inspection devices)

Though designed for military missions, much of the equipment demonstrated at the FPED may be employed in homeland defense operations by federal, state, and local law enforcement and first-responder agencies.

The equipment and systems demonstrated at the FPEDs are performed by COTS products that must be available for purchase and testing within 90 days after the event.

- Chemical and biological detection, mitigation, and protective equipment
- Communications equipment (including personnel alerting systems)
- Delay and denial technology (including fences, barriers [active, passive, portable, and fixed], and locks)
- Explosives detection (including hand-held, static, and underwater)
- Explosive ordnance disposal equipment
- Fence sensor systems
- Individual protective equipment
- Night-vision and optics devices
- Non-lethal weapons and technology
- Physical security equipment sensor and surveillance systems (interior, exterior, perimeter, and tactical)
- Robotic vehicles and systems
- Unattended ground sensors
- Unmanned aerial vehicles
- Vulnerability assessment/analysis software tools
- Waterside security equipment.

In addition to US companies, firms from around the world have responded to the FPED call for products. Past demonstrations have included international vendors, including companies from Australia, Canada, Denmark, France, Germany, Israel, Korea, South Africa, and the United Kingdom.

As future threats grow and change, the demand for new and improved FP systems and equipment will continue to grow. Advances in robotics, enhanced communications, sensor technology, and a growing list of counterterrorism applications for nanotechnology are examples of how industry continues to push for solutions. At the same time, bombs once made using washing machine timers are now being made with more sophisticated equipment using better technology, such as cell phones, digital clocks, and watches. And bombs are now being hidden in underwear, sneakers, body cavities, and a range of other places. The chase continues and industry continues its hot pursuit.

A goal of the exposition is for commanders and others responsible for security to become better acquainted with the latest technologically advanced products that may be purchased and deployed almost immediately. In contrast, many products exhibited at military trade shows are still in research and development and are months or years away from possible fielding. And most military trade shows are commercial ventures. Neither a trade show nor a commercial venture, the FPED is a federally sponsored demonstration.

The DOD Physical Security Equipment Action Group (PSEAG), administered by the Office of the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs/Nuclear Matters

The expansive venue for FPED VIII is Northern Virginia's Stafford Regional Airport, just off Interstate-95, 40 miles south of the Pentagon and 10 miles south of Quantico.

(OATSD[NCB/NM]), is directing and sponsoring FPED VIII. Additional sponsors include the US Department of Energy and DOD's Technical Support Working Group. The US Army Product Manager, Force Protection Systems located at Fort Belvoir, Virginia, will handle overall coordination and execution.

FPED VIII is open only to civilian and military members of the DOD; members of other federal agencies responsible for security; members of foreign military services who are sponsored by US government personnel; federal, state, and local government agencies involved in law enforcement and security; corrections agencies; and the press.

JOINT ANTITERRORISM DOCTRINE UPDATE

DOD photo by Cherie Cullen

AT and FP are enhanced with changes to JP 3-07.2 *Antiterrorism*

By LCDR Christopher F. Hill, USN

When the members of the military and civilians know what to look for, they can contribute immeasurably to our nation's security.

In the wake of the 1996 bombing of the Khobar Towers in Saudi Arabia, the Joint Staff oriented itself to synchronize the military's AT and FP efforts. Joint Publication 3-07.2, *Antiterrorism*, remains a core element of that effort. In fact, it is our foundational document.

The Joint Staff released the latest edition of JP 3-07.2 on November 24, 2010, after the publication went through several revisions and working groups. This article introduces a few of the changes, including the definitions of terrorism and antiterrorism, as well as the practice of surveillance detection. See Figure 1 for a summary of changes.

How does joint doctrine affect you?

The AT community's most important professional customer is the AT officer (ATO). Any change in doctrine must keep the ATO in mind, as the ATO is the engine behind unit AT readiness and is in direct communication with the commander. For doctrine, the ATO is our soldier in the trenches, the eyes and ears of what works and what does not. With this in mind, JP 3-07.2 contributes to AT knowledge and awareness by tackling big-picture concepts and definitions so that Service-specific and AT publications can go straight to the guts of what to do on a day-to-day basis with tactics, techniques, and procedures relevant to ATOs and their units. Moreover, AT doctrine is designed to provide guidance and unity of effort for commanders in operations, education, and training.

We would also like to think that this publication allows the AT community to step outside its ordinary routine and to reevaluate the big picture: What is our threat, why does he do what he does, how is he organized, and

Changes to JP 3-07.2

- Removes all "For Official Use Only" information and keeps it "Unclassified"
- Revises the definitions of "terrorism" and "antiterrorism" and explains the difference between "terrorism" and "insurgency"
- Provides greater depth on terrorist structures, categories, and affiliations; discusses the concept of "lone terrorists"
- Updates the capabilities and functions of several intelligence and law enforcement organizations, including resources for obtaining intelligence relevant to the commander
- Adds a discussion on "Countering Terrorist Attack Planning," including details on "the terrorist attack planning cycle," "surveillance detection," and "surveillance awareness"
- Combines four separate risk-management–related appendices into one Risk Management Appendix
- Removes five other appendices with information that is better covered and more up to date in other publications, including "Sample Barrier Plan," "FPCON System," "Homeland Security Advisory System," "CBRN Planning Considerations," and "JAT Program Manager's Guide"

Figure 1. Summary of Changes

how should we organize to protect our forces? We start our big-picture evaluation by defining our core business term: terrorism.

Terrorism

There is no universal definition of *terrorism* nor will there ever be. *Terrorism* is an emotionally charged term that is often used pejoratively, that is, we tend to use it as a slur to accuse people, whether or not their tactics cause fear, or whether or not their violence is illegal. Furthermore, how do we distinguish between "freedom fighters" and "terrorists" when the tactics look the same?

The fight over defining the word *terrorism* is a constant academic exercise; indeed one study showed that there are more than 109 definitions for the word.[1] The United Nations has tried for years to define it and has consistently failed to do so. Our challenge in this publication revision was to ensure that the word *terrorism* would remain free of bias and anchored to its etymological roots.

This is what we know: Terrorism involves fear (from its Latin root *terrere*). Terrorism involves violence or the threat of violence (where violence involves death or injury to humans) and is considered illegal. And terrorism is used for political purposes. By "political" we imply that no matter what motivates or inspires a terrorist to commit violence (e.g., religious fervor, economic disparity, revenge, nationalism, Marxism, anarchy, separatism, animal protection) the end goal is something that involves a better political power position for the so-called terrorist. In some cases a terrorist may just want an audience to respond to his grievance. More often these goals include separation from a majority power, establishment of a caliphate, or ousting of an occupying force, just to name a few.

> *We are continuing this policy in bleeding America to the point of bankruptcy … We, alongside the mujahedeen, bled Russia for 10 years until it went bankrupt and was forced to withdraw in defeat. … All that we have to do is to send two mujahedeen to the furthest point east to raise a piece of cloth on which is written al Qaeda, in order to make generals race there to cause America to suffer human, economic and political losses without their achieving anything of note other than some benefits for their private corporations.*[2]
>
> —Osama bin Laden (2004)

> *We have a track record of attacking high-profile economic targets and financial institutions such as the City of London. The role of bankers and the institutions they serve in financing Britain's colonial and capitalist system has not gone unnoticed. … It's essentially a crime spree that benefits a social elite at the expense of many millions of victims. … The IRA is not unwilling to talk, in fact there needs to be talks … however, talks need to deal with the root cause of the conflict, namely the illegal British occupation of Ireland.*[3]
>
> —Real IRA statement (2010)

The old DOD definition for terrorism was revised because it suggested that one of the goals of terrorism could be purely religious (see Figure 2) and, thus, something that does not involve politics. Drawing upon this confusion, one of our concerns was that we did not want Islamic extremism to hijack the term, especially given that terrorism is a systematic tactic used by a number of otherwise secular extremists groups (i.e., Tamil

Old DOD Definition of Terrorism
The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

New DOD Definition of Terrorism
The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.

Figure 2. Old and New DOD Definitions of Terrorism

Tigers). No doubt a function of the shock of what looks like senseless killing of civilians after terrorist attacks, many writers also talk of terror as a means to its own end—that is, "terror for terror's sake." But this neglects the strategic logic of terrorist violence used to achieve political goals,[4] and it is no different than saying that we wage war because we like waging war. Certainly, there may be a few insane people in our midst who like to hurt people for sport, making it difficult to distinguish between terrorists and lunatics, but a deeper exploration of common terrorist groups will show that their goals are more often plainly political.

Furthermore, this publication is neither a legal document nor a solution to the lunatic-terrorist dilemma. This is why this definition of terrorism is different than the definitions used by the Federal Bureau of Investigation (FBI) and the Department of State (DOS), which are in the business of deliberately labeling suspects or states under careful legal pretenses (see Figure 3). Our definition of terrorism, however, is designed to teach and inform Service members so that we can properly penetrate the minds of our enemies and defeat them.

Antiterrorism

The doctrine working group also made a small but notable modification to the definition of *antiterrorism* (see Figure 4). The term *antiterrorism* still involves defensive measures to reduce vulnerabilities, but instead of involving "limited response and containment," it now says "rapid containment" by forces. This change was a function of several lessons learned, most notably the Fort Hood incident, where the immediate response needed to be rapid to contain the situation before more people were killed. In this incident, local law enforcement responded in swift fashion, as one DOD review noted in January 2010:

> The Fort Hood response to the shooting was a result of local commanders training their people before the crisis occurred. First responders used active shooter tactics and procedures to stop the attack one-and-a-half minutes after arriving on the scene. These new tactics, originating in civilian law enforcement, focus on neutralizing the threat as quickly as possible.[5]

Contrast this with the Columbine High School massacre in 1999 where police waited 3 hours before going into the school.[6]

Insurgency

This publication is not responsible for the term *insurgency*, but it briefly discusses why insurgency is often used interchangeably with *terrorism*, rightly or wrongly. Continuing this article's exploration of the term *terrorism*, one can argue that terrorists target unarmed civilians or off-duty military using any number of tactics spanning the spectrum of threats of force, to poisoning food supplies, to skyjacking, to the use of weapons of mass destruction (or potential use). We also find that a lot of tactics used in terrorism overlap with tactics used by insurgents or guerilla fighters. We expect insurgent forces to target government military forces, though they sometimes resort to terrorism, especially in the early stages of their development. As it is defined in Joint Publication 3-24, *Counterinsurgency Operations*, insurgency involves "the use of subversion and violence by a group or movement that seeks to overthrow or force change

FBI Definition of Terrorism:
The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

—28 C.F.R. Section 0.85

Department of State Definition of Terrorism:
Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.

For purposes of this definition, the term "noncombatant" is interpreted to include, in addition to civilians, military personnel who at the time of the incident are unarmed and/or not on duty.

—Title 22 of the United States Code, Section 2656f(d)

Figure 3. FBI and DOS Definitions of Terrorism

of a governing authority." Although both insurgents and terrorist seek political aims, terrorism is always unlawful and intended to cause fear to achieve these aims. As insurgencies develop, they tend to move beyond terrorism to more organized military units and may even build air forces.

The bottom line is this: We acknowledge that these terms do not fit together like pieces of a puzzle, much the same as Force Protection and Antiterrorism are not perfectly integrated terms. Indeed, this publication will never be able to constrain the nuance and beauty of the English language, but JP 3-07.2 provides a starting point for objective, informed discussion within the AT community.

Old DOD Definition of Antiterrorism
"Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces."

New DOD Definition of Antiterrorism
"Defensive measures used to reduce the vulnerability of individuals and property to terrorists acts, to include rapid containment by local military and civilian forces."

Figure 4. Old and New DOD Definitions of Antiterrorism

Surveillance Detection

The largest addition to JP 3-07.2 involves a deep discussion on how to counter terrorist surveillance activities. One criticism of DOD's AT efforts has been that it is too defensive oriented—too much "defend" and not enough "defeat"—which flies in the face of how we were taught to defeat our enemies. The response to this criticism is that we already have an offensive arm in our overall Combating Terrorism strategy: counterterrorism. Still, there remains a perceived gap in coverage between antiterrorism (defensive measures) and counterterrorism (active measures). Within this gap many in the AT community are exploring expanded use of surveillance detection (SD).

SD takes us beyond protective "wires" and front gates to hitting the streets and determining if the enemy is conducting surveillance against us. SD does not involve killing the enemy, but it may involve active operations by individuals who are otherwise oriented to the AT role (e.g., security, policy). SD is not countersurveillance. Countersurveillance is the task of professional operators who may initially incorporate SD in their operations but then attempt to exploit, counter, or defeat the surveillance through a variety of measures.[7] SD is more like a million watchful eyes.

To be sure, the watchful eye is the secret to SD success. And it takes more than just the eyes of security, law enforcement, and other AT professionals. It takes the active observation of ordinary citizens. SD asks us to examine our surroundings and to know what is out of place, suspicious, or abnormal and to report it. The Fall 2010 issue of *The Guardian* contains two articles that discuss this universal approach much more eloquently than I can.

We can learn a lot from another government agency that deals with terrorism every day. The DOS has a robust, integrated SD program that was born—as are many security efforts—out of lessons learned, in this case as a result of the Nairobi and Dar es Salaam chancery bombings in 1998. Al Qaeda operatives had conducted extended pre-operational surveillance of both locations, but there were few US government assets in place to detect it.[8] Therefore, the DOS created SD teams composed of local nationals, contractors, and other security professionals under the Diplomatic Security Service. With more than 200 such teams operating worldwide, the DOS has foiled a number of terrorist plots, many of which ended up in the news, and many of which fortunately did not.[9]

According to the Defense Intelligence Agency (DIA), the most critical portion of a terrorist group's activities

SD takes us beyond protective "wires" and front gates to hitting the streets and determining if the enemy is conducting surveillance against us.

"is the 1 percent of time spent developing and pursuing a specific terrorist attack."[10] The logic goes like this: Instead of building bigger walls and heavier vehicles to counter the later stages of the terrorist attack cycle, why don't we disrupt their entire terrorist operation by rendering them useless and frustrated in the earliest stages of their planning. DIA's comment also implies that it would be an extraordinary event to catch a terrorist doing surveillance if it is such a small part of their planning.

Nevertheless, we do sometimes catch people conducting surveillance, although it is admittedly hard to tell if a tourist is taking casual pictures of an ornate government building or taking pictures of security cameras. In the National Capital Region, for example, it is not unusual to have a handful of suspicious activity events each month where individuals are caught or observed taking pictures of security systems, testing security with fake devices, or making bomb threats via phone or the Internet. The good news is that many of these events are initially reported by ordinary citizens who simply do not like what they see and do something about it. This is where surveillance awareness converges with SD and gives us one of the least expensive and most widely dispersed surveillance systems around: a million critical eyes.

SD strikes at this 1 percent of terrorist planning and produces results that are not measurable. We cannot measure how many times a terrorist decided to avoid attacking a target because it was rendered undesirable by active AT efforts. But this does not dissuade an AT specialist from doing what his country asks him to do.

For more information on changes to antiterrorism doctrine, please download JP 3-07.2, *Antiterrorism.*

Digital copies are available on the Antiterrorism Enterprise Portal on Army Knowledge Online/Defense Knowledge Online. It is an unclassified document.

---

1 Schmidt, Alex P., & Albert I. Jongman. *Political Terrorism.* Piscataway, NJ: Transaction Publishers, 1988; p. 5–6 . These authors break down the frequency of words such as *fear, violence, threat, and political* that are used in the 109 definitions.

2 Al Jazeera. "Bin Laden: Goal Is To Bankrupt U.S." CNN, November 1, 2004. Available at http://articles.cnn.com/2004-11-01/world/binladen.tape_1_al-jazeera-qaeda-bin?_s=PM:WORLD

3 McDonald, Henry. "Real IRA Says It Will Target UK Bankers." Guardian.co.uk, September 14, 2010. Available at http://www.guardian.co.uk/uk/2010/sep/14/real-ira-targets-banks-bankers?intcmp=239

4 A good book on the logic of suicide terror is Robert A. Pape's *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005).

5 "Protecting the Force: Lessons from Fort Hood." Report of the DOD Independent Review, January 2010.

6 Morales, Tatiana. "Columbine Today: Tears, Anger. Many Still Ask Could It Have Been Prevented?" CBSnews.com, April 20, 2004. Available at http://www.cbsnews.com/stories/2004/04/20/earlyshow/main612726.shtml

7 Uninformed observers may confuse surveillance detection with spying. For an example of this phenomenon, see "U.S. Embassy in Reykjavik Monitoring Icelandic Citizens." *Ice News*, November 9, 2010. Available at http://www.icenews.is/index.php/2010/11/09/u-s-embassy-in-reykjavik-monitoring-icelandic-citizens/

8 Haag, David R. "The Terrorist Threat: Are United States Diplomatic Facilities Overseas Safe?" Unpublished paper, Army War College, Carlisle, Pennsylvania. April 7, 2003.

9 Ibid.

10 "Terrorism Analysis: A Primer in the Art for DIA Analysts and Consumers." Defense Intelligence Reference Document [restricted, copy available to author].

KHOBAR TOWERS AND THE BIRTH OF MODERN ANTITERRORISM

DOD photograph taken 6/26/96, photographer unknown

A seminal moment in the DOD AT world

By MA1 Mark T. Robbins, USN, Leading Petty Officer and Antiterrorism Officer, Naval Security Forces Detachment Federal Health Care Center, Great Lakes, Illinois

Many of DOD's AT standards—including programs to deter, detect, mitigate, and respond to and recover from terrorist attacks—stem directly from Khobar Tower lessons.

On the evening of June 25, 1996, Air Force Security Police (SP) sentries stood watch on the roof of Building 131 of the Khobar Towers apartment complex in the city of Khobar, on the eastern coast of Saudi Arabia. The complex contained living quarters for various coalition forces enforcing Operation Southern Watch, the no-fly zone over southern Iraq. Building 131 housed US Air Force personnel. At approximately 9:49 p.m., the SPs observed a tanker truck enter a parking lot outside the northern perimeter, approximately 80 feet from their building. The tanker truck parked near the fence, then two individuals jumped out of the truck, raced to a waiting car, and sped away in great haste. The SPs, who were immediately aware of the danger, left the roof and began notifying building residents by knocking on doors. At approximately 9:55 p.m., the tanker truck exploded, laying waste to the entire northern face of Building 131 and killing 19 US personnel.

This was one of the most significant attacks against US forces since the bombing of the Marine Barracks in Beirut, Lebanon, in 1983. The Khobar Towers bombing, a watershed moment for the DOD AT community, helped facilitate the birth of modern DOD AT efforts. Indeed, many of the DOD's AT standards—including comprehensive programs to deter, detect, mitigate, and respond to and recover from terrorist attacks—stem directly from Khobar Tower lessons.

This article examines the first three of these efforts—to deter, detect, and mitigate—and evaluates how 1996-era AT policies failed the residents of Building 131.

Building 131 and Parking Lot

Profile of Khobar Towers

Khobar Towers was on the eastern coast of Saudi Arabia, in the US Central Command (CENTCOM) area of operations, and was built by the Saudis in 1979. The living quarters were mainly high-rise apartments up to eight stories tall, with some office space and administrative facilities. The perimeter of the US, French, and British area was surrounded by a fence and a row of concrete Jersey barriers. Buildings 131 and 133, the buildings most severely damaged during the bombing, were eight-story apartment complexes facing the north perimeter. The parking lot outside the north perimeter was adjacent to a park and a small group of houses. The perimeter fence was a chain-link fence approximately 7–8 feet high, with three strands of barbed wire or one row of concertina along the top. Its fence was surrounded with Jersey barriers. There were no surveillance cameras, sensors, or alarms, and lighting was very limited.[1]

Goal 1: Deter

Deterrence includes measures to intimidate or dissuade a would-be attacker from striking a particular target. In this instance it would include the presence of SPs, random security measures, and a variety of physical security safeguards (e.g., lights, alarms, barriers, fencing).

The Air Force unit at Khobar Towers, the 4404th Wing (Provisional), was less prepared than it should have been to counter the threat, especially with a 10 percent personnel turnover every week. While most personnel rotated through on 120-day tours, SP commanders, Air Force Office of Special Investigations (AFOSI) personnel, and Wing intelligence officers rotated every 90 days.[2] Additionally, as a result of personnel shortfalls, Security Police could not implement sufficient security measures to maintain Threat Condition CHARLIE, the second-highest state of an installation's security alert.[3] As task force members noted in the Downing Report:

> At the small unit level, the Security Police do not have the opportunity to develop the teamwork critical to security operations in a high threat environment. They currently man observation posts and entry control points primarily as individuals, but do not have the time or manpower to develop the unit skills needed for patrolling, escort duties, or response to a penetration of the perimeter. The frequency of individual rotations into the Security Police Squadron means that the squadron always has a wide mix of experience and knowledge. It never stabilizes long enough to conduct training and develop unit cohesion.[4]

The task force also noted that there were no consistent, uniform FP practices in the region. In many instances, site commanders used their own personal experience and that of their staff or Service-specific (Navy, Air Force, Army) guidance to implement security measures.[5]

These limiting factors did not manifest themselves so far as to present a "soft" target to terrorists—indeed, as we shall see, security was dramatically improved at Khobar Towers in the weeks preceding the bombing. Rather, these indications show that FP measures at this site were considerably strained and conditions were not optimal for mission success.

Goal 2: Detect

Deterrence may not always persuade a terrorist to seek "softer" targets. Thus, the ability of a unit to detect terrorist attacks *before* they happen is of utmost importance. This is primarily an intelligence function, that is, to sift and weigh information and paint a coherent picture of an environment for the commander. The assessment of intelligence capabilities in this particular area was bleak.

First, the 90-day turnover of intelligence and counterintelligence personnel had an adverse impact on intelligence collection. Experienced hands from the region stated that it took at least a year to develop effective relationships with local authorities.[6]

Second, the 4404th had little capability to conduct long-term trend analysis of terrorist intentions and capabilities. This was not just a local failure—the Defense Intelligence Agency (DIA), for example, had 40 analysts assigned to "terrorism" at the time of Khobar Towers, but only seven of them were engaged to provide detailed assessments due to "other commitments."[7]

Third, it was difficult to get timely intelligence to units. In some cases commanders at the field level could not access the information because they did not have the secure means to access it and store it.[8]

Although intelligence did not provide an exact date,

Ground Zero at Khobar Towers. (DOD image taken 6/26/96. Photographer unknown.)

time, place, and method of potential attack, there was a large volume of information pointing to terrorists having both the capability and intention to strike US assets in Saudi Arabia in general and Khobar Towers in particular. The Air Force Inspector General report on the bombing listed a series of suspicious surveillance incidents 90 days prior to the bombing, including the suspected ramming of a Jersey barrier on the east perimeter (the attack occurred on the north perimeter).[9]

In the months leading up to the attack, an increasingly threatening operating environment emerged. In November 1995, terrorists detonated a 250-pound vehicle bomb adjacent to a government building in Riyadh, Saudi Arabia, killing seven Americans who were there to train Saudi military personnel.[10] Moreover, a local AFOSI agent briefed the Commander of the 4404th Wing, Brig Gen Terryl J. Schwalier, on the possibility of terror activity during and after the Haji (annual pilgrimage to Mecca), which took place from April 19 to May 17, 1996. This agent specifically mentioned the threat of a vehicle-borne explosive device, but admonished the command that this specific "information is sensitive and cannot be released down the chain of command."[11]

On April 4, 1996, an AFOSI agent prophetically described the carnage to come in a memo to his home office:

> Security measures here are outstanding, which in my view would lead a would-be terrorist to attempt an attack from a position outside the perimeter. ... If a truck parks close to the fence line, and the driver makes a quick getaway, I think the building should be cleared immediately.[12]

This information was communicated to the command. The main problem, as Senator Arlen Specter related, was that "there was no failure of intelligence, but a failure to use intelligence."[13]

Goal 3: Mitigate

After *deter* and *detect*, we know that the unit must work to *mitigate* the threat. This requires a review of potential adversaries' capabilities, a self-assessment of how terrorists might exploit security shortfalls, and a plan to close the gaps in vulnerabilities as necessary. In this third category—to *mitigate*—Khobar Towers' security fell short.

Lack of Clear AT Standards

The DOD had no physical security standards for fixed facilities, only suggested measures. Thus, commanders were "left to a subjective determination of what is safe or unsafe." Amazingly, the Downing Report found that in

many cases military commanders throughout CENTCOM did not know the *DOD Antiterrorism Handbook* (O-2000.12h) even existed.[14]

Military units, at least those that were aware of the *Handbook*'s existence, were required to do a vulnerability assessment of their installation on a "regular" basis, but there was no established standard for frequency, format, or content.[15] There was no process for formal, higher headquarters–level review of these assessments, if they were even conducted.

Furthermore, there were no AT standards pertaining to design, material, or construction of new and existing buildings; building standoff requirements; or warning systems. The Downing Report noted that "expedient and even long-term upgrades to buildings to enhance force protection are often based solely on the experience of the construction engineer and the availability of funds."[16] There were also no formal standards to mitigate the effect of an explosive blast, specifically regarding windows. In 12 of the 19 deaths at Khobar Towers, flying glass played a significant factor.[17]

Today's doctrine asks us to examine a wide range of possible means of attack and rate their probability of occurrence (based on terrorist presence, intentions, and capabilities) and the severity if such an attack did occur.

Due to a lack of standards, the result was an uneven mix of solutions that varied considerably from one installation to the next, depending on the caliber of the security planners and the politics of the individual commands. Even worse, FP was given low priority for funding. After all, mitigation strategies cost money.

The Scapegoat

Given the breadth of deficiencies that contributed to this disaster, where should the blame lie? Should it have been with Brig Gen Schwalier of the 4404th, who was assigned much of the blame? Or perhaps with the DOD in general, for allowing forces to be forward deployed without adequate FP standards? It is not the intent of this paper to malign the general—who was denied a second star and retired the year after the bombing—but rather to examine the mitigation strategies that were employed and gauge their effectiveness *given the DOD standards in 1996*.

The Downing Report was extremely critical of Brig Gen Schwalier, stating "the Commander, 4404th Wing (Provisional) did not adequately protect his forces from a terrorist attack."[18] The Air Force, however, concluded Schwalier was not derelict in his duties in protecting his personnel.[19] The Air Force inspector general likewise determined Schwalier performed his duties appropriately.[20] However, the Secretary of Defense sided with the Downing Report, declaring that the Air Force reports did not "reflect a thorough, critical analysis of all of the facts and issues, nor, in many instances, do they arrive at conclusions fully supported by the facts." Instead, he announced, "[Brig Gen] Schwalier's actions with respect to force protection did not meet the standard required for a Major General."[21]

To get to the truth of this matter, let us explore the mitigation strategies employed at Khobar Towers. Officials from the 4404th toured Khobar Towers with Royal Saudi Military Police. A colonel from the 4404th asked the Saudis if the northern fenceline could be moved back "10 to 15 feet." The Saudi liaison said he had to ask civilian officials for permission. This liaison later said he was never officially asked to move the fence.[22] This was a contentious issue because the truck bomb was later detonated at this precise location.

The main criticism leveled at the 4404th after the bombing was not that they failed to provide protection but that they were protecting against the wrong threat. The Downing Report noted that the 4404th Wing (Provisional) had extensive FP measures in place but focused on a bomb threat penetrating the interior of Khobar Towers and thus did not take adequate measures against other viable threats, such as stand-off weapons or bombs, kidnappings, and so forth.[23]

The failure in this case was poor security planning. Today's doctrine asks us to examine a wide range of possible means of attack and rate their probability of occurrence (based on terrorist presence, intentions, and capabilities) and the severity if such an attack did occur. The different attack means are thus ranked, with both probability and severity a factor. An installation can then initiate mitigation strategies based on the most *likely* threat (refer to DOD O-2000.12h). At Khobar Towers, the security planners had tunnel vision—they were envisioning another moving vehicle bomb reminiscent of the Marine Barracks in Beirut. The SP Commander, Lt Col James Traister, moved energetically to protect his forces from just this sort of attack. Indeed he was specifically asked by the general to look into what he would do to prevent a car bomb from entering the complex and he made this his primary focus.[24]

Specific security measures included (1) Jersey barriers against the fenceline to stop a vehicle from crashing through (which was exactly what happened in Beirut); (2) establishing a secondary entry control point beyond the first, existing one; (3) installing serpentine barriers before the first vehicle gate to force all vehicles to slow prior to entry; (4) multiple M-60 machine-guns in reinforced bunkers between the two checkpoints; and (5) two large trucks continuously manned, positioned behind the checkpoints to block potential gate-runners.[25] It is safe to assume no truck could have run such a gauntlet and survived.

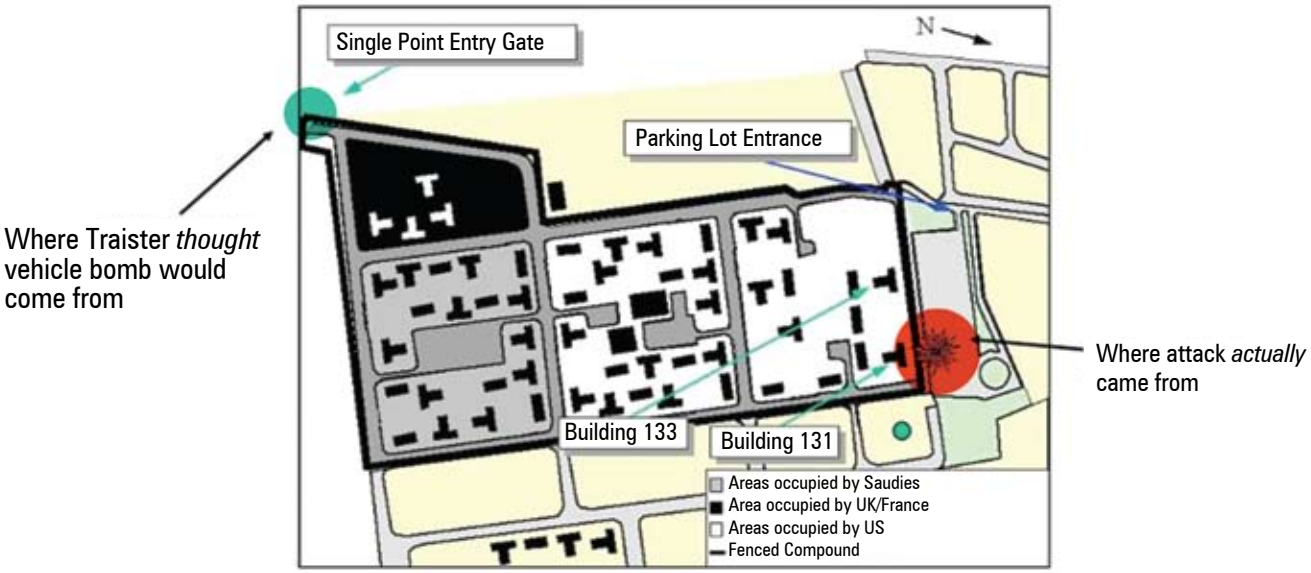


Figure 1: Khobar Towers Complex

As indicators of increased surveillance and terrorist activity mounted, the Command formed FP committees at various levels to discuss mitigation strategies. However, there was no effort to coordinate or share these concerns or any overarching guidance to do so. Lt Col Traister jotted down this revealing observation: "There is a lack of follow-up on projects, the leadership are [sic] unaware of problems until too late."[26]

Brig Gen Schwalier was criticized for a variety of vulnerabilities that were not corrected. The January 1996 vulnerability assessment identified the lack of window glazing as a concern and recommended Mylar film be applied to the windows. Schwalier made the decision to defer the Mylar based on a "variety" of factors, including cost, other security enhancements, and lack of a requirement for Mylar.[27] This goes back to the lack of DOD physical security standards for buildings. However, it is difficult to reconcile why some specific mitigation strategy designed to cope with flying glass was not considered, especially if they had credible intelligence—and they did—that they were facing an explosive vehicle threat.

Much has been made about standoff for the northern fenceline, from whence the explosion came. There was 80 feet between the fence and the northern face of Building 131. The January 1996 vulnerability assessment contained a blast analysis by an Air Force Explosive Ordinance Disposal technician, in which he recommended a 300-foot perimeter to mitigate a vehicle blast of 220 pounds of explosives. The Downing report related, "There is no evidence that any action was taken regarding this aspect of the assessment by the Commander."[28] Evidently, Brig Gen Schwalier was expected to have extended the fenceline.

Within the constraints of security classification guidelines, this author may safely state the standoff at Khobar Towers would still be acceptable in the DOD today. However, once again, if the 4404th had credible, specific intelligence that indicated Khobar Towers was being targeted—and they did—why was nothing done?

The Secretary of Defense and the Downing Report condemned Brig Gen Schwalier for assuming the explosive threat to Khobar Towers would be similar to the 220-pound vehicle bomb used in the earlier attack against the Office of the Program Manager–Saudi Arabian National Guard (OPM-SANG) in November 1995. However, this would be an acceptable assumption in the DOD today, that is, to assume device size based on similar attacks in the region.

Of particular concern were the Air Force Security Police. They had no specific training on the threats they were facing, and they did not conduct terrorism exercises. They also had no specific rules of engagement. Instead, they used general law enforcement doctrine on use of force. The SPs did not conduct weapons training, and their rifles were not zeroed or fired. Downing Report task force members even went so far as to say the SP weapons were "dirty and ill-maintained."[29]

Moreover, as noted earlier, the Security Police were insufficiently manned. Lt Col Traister never submitted a request for additional SPs in the 3 months he was in command. This may be the reason the 4404th did not go to Threat Condition CHARLIE in April 1996 when threats and intelligence reports escalated.[30]

The Secretary of Defense and the Downing Report reserved their harshest criticism for the lack of evacuation exercises in Khobar Towers. The Secretary of Defense, in particular, lambasted the evacuation procedures as "primitive." It is hard to disagree. Their procedure consisted of a complex-wide "Giant Voice" system, which was frequently inaudible, and people running down hallways banging on doors. In comparison, the British

contingent billeted elsewhere in the complex practiced monthly.[31] Additionally, no FP exercises had been conducted with local Saudi forces.[32]

Despite the harsh criticism of Brig Gen Schwalier in the Downing Report, the former Consul General to Dhahran, David Winn, a 25-year DOS veteran of the Middle East and a frequent visitor to Khobar Towers, observed that Schwalier's efforts "were so stringent, so draconian, so professional that I thought he almost had overreacted." Winn also stated that the security measures at Khobar Towers were so impressive that Khobar Towers was "in a league by itself" in comparison to other facilities in the region.[33]

Conclusion

The bottom line is this: The 4404th, and Brig Gen Schwalier in particular, were the victims of an inferior AT program that had no definitive standards and relied on practices that conferred an unacceptable degree of latitude to commanders to determine what security risks to accept. In short, Schwalier was set up for failure. The Khobar Towers tragedy was merely the opening salvo of a new type of terrorism that the post-9/11 world knows all too well. Schwalier was not guilty, as the Downing Report claimed, but he was responsible.

Each new tragedy brings more recriminations, more lessons learned reports, and more "what-if" scenarios. Wherever the fault lies, students of history have the luxury of sitting in their armchairs, reading critiques of the commander's decisions, and passing judgment on patriotic men and women who did what they thought best at the time. We should not forget that.

After Khobar Towers, everything changed in the DOD AT world. We have established physical standards for fixed installations; dedicated terrorist threat assessments for installations or forward-deployed areas; DOD-wide anti¬terrorism building standards for construction, standoff, and so forth; and regular FP exercises held at military installations around the world annually. The DOD AT program is robust, effective, and growing stronger each day. It took the deaths of 19 Airmen for this to happen.

Each new tragedy brings more recriminations, more lessons learned reports, and more "what-if" scenarios. Wherever the fault lies, students of history have the luxury of sitting in their armchairs, reading critiques of the commander's decisions, and passing judgment on patriotic men and women who did what they thought best at the time. We should not forget that.

---

1 Downing Assessment Task Force. "Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad." Report, 1996; p. 69–70. Available at http://www.fas.org/irp/threat/downing/report.pdf. On June 28, 1996, the Secretary of Defense appointed retired General Wayne Downing, the former Commander, US Special Operations Command, to assemble a task force and make an assessment of the circumstances surrounding the Khobar Towers bombing.

2 Ibid, p. 18–19

3 Ibid, p. 69.

4 Ibid, p. 18–19

5 Ibid, p. 29.

6 Ibid, p. 40.

7 Ibid, p. 50–51.

8 Ibid, p. 55.

9 Air Force Inspector General and Judge Advocate General. "Khobar Report." Report, June 25, 1996. Available at http://www.au.af.mil/au/awc/awcgate/khobar/tableof.htm

10 Cohen, William S. "Personal Accountability for Force Protection at Khobar Towers." Report, Secretary of Defense, 1997. Available at http://www.au.af.mil/au/awc/awcgate/khobar/cohen.htm

11 Supra 1, p. 65–66.

12 Ibid, p. 65.

13 Specter, Arlen. "Senate Intelligence Committee Chairman Finds Khobar Towers Bombing 'Not the Result of an Intelligence Failure.'" Press release, 1996. Available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB55/ssci.pdf

14 Supra 1, p. 32–33

15 Ibid, p. 33.

16 Ibid.

17 Ibid, p. 34.

18 Ibid, p. 71.

19 Record, James F. "Independent Review of the Khobar Towers Bombing." Report, 1996. Available at http://www.au.af.mil/au/awc/awcgate/khobar/recordf.htm

20 Supra 9.

21 Supra 10

22 Supra 1, p. 72.

23 Ibid, p. 64.

24 Ibid, p. 73.

25 Ibid.

26 Ibid, p. 74.

27 Supra 19.

28 Supra 1, p. 77–78.

29 Ibid, p. 79.

30 Ibid, p. 79–80.

31 Ibid, p. 81, p. 83.

32 Supra 10.

33 Supra 19.

ARMY AT AWARENESS IN CONTRACTING

U.S. Marine Corps photo by Curtis Lambert/Released

The risk of terrorists targeting Army contracts is very real

By Office of the Provost Marshal General, Antiterrorism Branch, United States Army

The Army AT and contracting communities are working closely together to increase AT awareness in the contracting process.

"Antiterrorism Awareness in Contracting," the Army AT theme for the second quarter of fiscal year 2011 (2Q/FY11), focuses on heightened awareness and understanding of the relationships and shared responsibilities of AT program requirements and contract management processes. By integrating AT awareness throughout the contracting process, the Army, as a community, is better protected from terrorists. The Army AT and contracting communities are working closely together to increase AT awareness in the contracting process. This article is offered to improve discussion of similar programs throughout DOD.

Why Is Increasing AT Awareness in Contracting So Important?

The risk of terrorists exploiting or targeting Army contracts is very real. One does not need to look long or hard to find repeated examples of undocumented or unsuitable individuals gaining access to DOD installations in the continental United States (CONUS). It is entirely reasonable to expect that terrorists will seek to take advantage of the same vulnerabilities that allowed these incidents to happen to gain access to Army sites. Overseas, we have seen that repeated terrorist attacks against host-nation and third-country-national contractors can have a significant impact on US military operations and a chilling effect on local perceptions regarding security and the capabilities of the host government.

The Army employs large numbers of contractor personnel in a variety of mission environments, including peace-time garrison locations and the combat zone. When our nation prepares for and goes to war, contractors provide Army customers with a wide range of goods and services, many of which are critical to mission accomplishment. Although the use of contracting can provide significant benefits to Army forces, it also can result in significant risks to Army personnel and missions. The lack of effective AT and contracting integration can increase the risk of attacks against Army personnel and assets, including contractors and their supporting capabilities, by personnel given access to our bases and installations.

The potential risks associated with terrorism and the use of contracting support can range from low to extremely high. The actual risk depends on many variables including the operational environment, the unit mission, the local threat level, the makeup of the contractor work force, the scope of the contract requirement, and the effectiveness of local security procedures. Managing this risk requires everyone involved in the AT and contracting process to be aware of the problem and then to take appropriate actions. AT officers, contracting officers, contracting officer's representatives, security personnel, and staff officers at the unit, installation, and higher headquarters must work together to ensure that risks are identified and managed.

Although the use of contracting can provide significant benefits to Army forces, it also can result in significant risks to Army personnel and missions.

Headquarters, Department of the Army AT and Contracting Process Action Team

In April 2010, the Army established the Headquarters, Department of the Army (HQDA) AT and Contracting Process Action Team (PAT) to meet requirements established in the Army AT strategic plan, entitled, "Tempering the Weapon, Strategic Goal 5D - Build AT considerations into all Army contracting and logistics." The HQDA AT and Contracting PAT was a joint effort between the Office of the Provost Marshal General (OPMG) AT Branch and the Deputy Assistant Secretary Army (Procurement) [DASA(P)].

The HQDA AT and Contracting PAT meetings succeeded in bringing together more than 35 representatives from 20 different Army organizations. These participants included representatives from the AT and contracting communities at the unit and installation levels and up through the Army Staff. The PAT membership formed three working groups to develop detailed solutions in specific mission areas:

- The Training/Awareness Working Group identified issues and recommended solutions to establish and/or improve the training and awareness of the primary stakeholder groups: Requiring Activities, AT Officers, Contracting Elements, and Contractors.
- The Doctrine/Tactics, Techniques, and Procedures Working Group identified issues and recommended solutions to establish and/or improve the specific procedures and products used to integrate AT and contracting.
- The Defense Federal Acquisition Regulation Supplement (DFARS)/Policy Working Group identified issues and recommended solutions to establish and/or improve the overarching regulatory and policy guidance directing the integration of AT and contracting.

The working groups identified issues and proposed solutions to the PAT for approval. A number of these solutions have been approved and are being implemented throughout the Army. Following are some specific examples:

- A strategic communication engagement campaign increased awareness. This campaign included designating AT awareness in contracting as the theme for 2Q/FY11 and mass distributing awareness products down to Army AT Officers (ATOs) and contracting elements.
- Army AT training was revised:
  - Level II ATO training tasks include an AT risk assessment of contract requirements.
  - Level III AT training for garrison commanders highlights the importance of the integration of the AT and contracting processes.
- The AT in Contracting Desk Reference provides:
  - Format and procedures for an AT risk analysis of contracts
  - A standardized listing of potential AT security measures for use in contracts
  - A contracting process mechanism that requires an ATO review before a contract will be processed (i.e., the contract cover sheet).
- Army doctrinal guidance was updated to integrate AT and contracting in FM 3-37.2, *Antiterrorism*, and ATTP 4-10, *Operational Contract Support*.

A "Trojan Horse" has come to mean any trick that causes a target to invite a foe into a securely protected bastion or place.

An "Achilles Heel" has come to refer to a hidden weakness or vulnerable area that has not been discerned.

AT and Contracting Roles and Responsibilities

Requiring Activities

The primary responsibility for identifying and reducing any terrorist risks associated with a contract requirement lies with the requiring activity. The requiring activity is the actual organization that identifies the contract requirement and receives the contracted support. Requiring activities can include varied organizations such as an Army installation or deployed infantry battalions. Requiring activities should include AT considerations in the planning process for all types of contracts (whether a request for services, supplies, construction) at all locations (both within CONUS and outside CONUS).

The requiring activity should complete an AT risk assessment, as described in Appendix 8 of DOD 2000.12-H, *DOD Antiterrorism Handbook*, when the provisions of the proposed contract or services provided could affect the security of Army elements, personnel, or mission-essential cargo, equipment, assets, or services.

Particular attention should be paid to contracts that require contractor personnel to be given routine access to federally controlled space and access to federal information systems.

Some specific AT considerations should be addressed in the requiring activities' risk assessment:

- "Trojan Horse" vulnerabilities result from contractor personnel being granted access to Army personnel, locations, and materials. Terrorists could seek to gain access to our bases either by becoming contractor employees or by posing as members of the contract workforce.
- "Achilles Heel" vulnerabilities result from terrorist attacks directed against contractor personnel as the "soft target" or "weakest link." Commanders should consider the operational impact of losing the contracted support if contractor personnel are the targets of terrorist attacks.

TIPS FOR COMMANDERS • • •

- Review the AT and contracting integration procedures contained in Appendix 8 of DOD 2000.12H, DoD Antiterrorism Handbook, and the requirements for Army AT Standard 18, AT Measures for Logistics and other Contracting.
- Be familiar with contractors' personnel identity verification requirements and procedures used to determine the suitability of contractors who will be allowed to have unescorted access to the installation:
  - Implement law enforcement screening of contractor personnel using National Crime Information Center and terrorist screening databases.
- Ensure all contract requirements generated by subordinate units or activities include an AT risk analysis.
- Ensure that local security measures are considered and any additional contract-specific AT security measures are identified before the requirements package is sent to the supporting contracting officer.
- Ensure that the organizational AT officer and operations security officer review performance work statements prior to submission to the supporting contracting office.
- During staff calls or AT working groups (ATWGs), review contracts to ensure—
  - Contractor workforce complied with all personal identity verification requirements
  - Reason for access has been validated by the requiring activity
  - Type of access and privileges are appropriate
  - Period of access is specified
  - Access badges and credentials are being controlled
  - Requiring activity contracting officer's technical representatives are evaluating contractor compliance with local security requirements.
- Ensure that representatives from requiring activities as well as the supporting contracting office attend ATWGs.

Commanders and supervisors that request contract support for their units or organizations are responsible for ensuring that AT considerations are included in the contracting process. The challenge lies in striking the right balance between security and cost: Too little consideration given to AT could put the unit at risk and too much could increase contract costs. Commanders should use the risk assessment process and staff coordination to help ensure that appropriate AT security measures are included in the contract requirement.

Supporting Contracting Organizations

It is the supporting contracting office's responsibility to ensure that the contract is prepared in accordance with appropriate contracting regulations and guidance. At a minimum, the supporting contracting office should ensure that all contracts that require routine access to federally controlled space and/or access to federal information systems comply with personnel identity verification (PIV) and E-Verify requirements. Any contract that will require the contractor to accompany the force into a contingency environment should include the appropriate AT training clause. Contracting organizations should not accept contract requirements packages unless the requiring activity can show that it has completed an AT risk analysis.

Contractors

Contractors can help themselves by being aware of and fully compliant with contractual clauses covering PIV and E-Verify requirements. Contractors should also be familiar and in compliance with all local security procedures that govern their access to the base or installation where they work. Contractors should anticipate that they may have to accommodate random schedules, access and/or search requirements, and changes in the local threat level. During heightened force protection conditions, for example, contractor personnel may be directed to enter the installation only through designated access points and only at specified times so they can be identified and searched. Under some conditions, contractor personnel may be prohibited from accessing certain areas of the work location and their activities could be more closely supervised or even curtailed for a period of time. In general, contractors providing goods and services in significant- or high-threat environments or in areas with mission-critical personnel, equipment, and facilities should anticipate additional security and AT requirements.

Way Ahead

Much work has been done and much effort still remains for the Army to increase AT awareness in contracting. The HQDA AT and Contracting PAT will continue to pursue the implementation of solutions that were identified by the working groups. In the near term, the Army highlighted the importance of AT awareness in contracting at its annual AT conference held January 31 through February 4, 2011. The OPMG AT Branch and DASA(P) Policy and Support Directorate are currently developing a handbook for unit and installation activities that will provide detailed procedures and tips for integrating AT and contracting. AT and contracting integration will be a topic of interest during HQDA Protection Assessment Team visits beginning this fiscal year. Longer-term fixes include revising DFARS clauses and improving policy guidance.

The *AT Awareness in Contracting Desk Reference* is available at the Antiterrorism Enterprise Portal at Army Knowledge online.

The Army has posted supporting information, products, and tools for use by Army Command, Army Service Component Command, Direct Reporting Units, Army National Guard commands, and local Army community leaders on its Antiterrorism Enterprise Portal at Army Knowledge Online (https://www.us.army.mil/suite/page/605757). Some of the following products have been posted to support this quarterly AT awareness theme:

- AT and contracting awareness posters (two are included)
- A sample AT and contracting risk assessment
- A sample AT and operations security review cover sheet
- A listing of AT security measures
- The *AT Awareness in Contracting Desk Reference* containing the specific sample products identified above
- Tips and FAQs for commanders, AT officers, and contracting officers
- The recently published *Unit Antiterrorism Officer (ATO) Handbook* (September 2010) discussing the integration of AT and contracting (Annex F)
- The soon-to-be-published *Army AT Field Manual* (FM 3-37.2) including a discussion regarding AT measures in operational contract support.

Antiterrorism Awareness in Contracting

U.S. ARMY ARMY STRONG®

Ensure antiterrorism security considerations are incorporated into contract requirement package

- Consider antiterrorism risk assessments when developing contract requirements – Antiterrorism Officers can assist.
- Consider the impact of random antiterrorism measures and access control when developing performance work statements
- Consider the need for contractor personnel screening
- Ensure all required antiterrorism security measures are in place prior to the start of the contract
- Conduct periodic inspections to ensure adherence to access control and other security procedures

Identify • Screen • Control • Protect

Always Ready, Always Alert

Because someone is depending on you

https://www.us.army.mil/suite/page/605757

Integrate Antiterrorism Awareness into Contract Execution

U.S. ARMY ARMY STRONG®

Contractor Screening

- Screen contract companies
- Conduct background checks
- Process for replacing workers
- Limit contractor work areas

Access Control

- Develop access rosters
- Conduct personal identity verification
- Conduct personnel/vehicle searches
- Develop badge systems

Circulation Control

- Limit work & travel areas
- Implement identifiable badge and vehicle systems
- Use contractor escorts
- Limit/deny access at increased Force Protection Conditions

Special Security Concerns

- Consider alternatives to meet contract requirements
- Ensure contractor antiterrorism training and suspicious activity reporting
- Ensure host nation agreements allow security for logistics operations

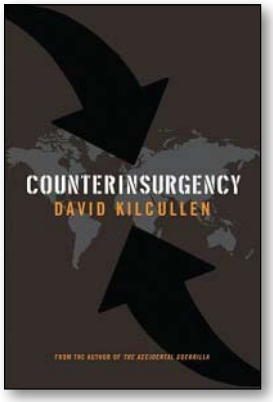
Identify • Screen • Control • Protect

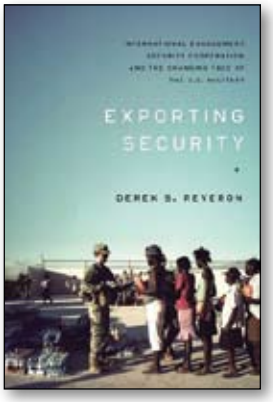
Always Ready, Always Alert

Because someone is depending on you

https://www.us.army.mil/suite/page/605757

Book Review





Counterinsurgency
by David Kilcullen. Oxford University Press, 2010

Exporting Security: International Engagement, Security Cooperation, and the Changing Face of the U.S. Military
by Derek S. Reveron. Georgetown University Press, 2010

Review by J. Furman Daniel III

In two excellent works, David Kilcullen and Derek S. Reveron demonstrate just how far the debates on the uses of American military power have come since the end of the Cold War. Both start with the assumption that threats from failed or failing states are and will continue to be the primary challenge facing the US military. Expanding on this common theme, these works diverge and provide a valuable discussion of different elements of this broader problem. Kilcullen uses his knowledge and experience to provide insights into counterinsurgency theory, and Reveron analyzes the increasing use of the American military to provide security cooperation, economic development, and foreign engagement.

Kilcullen's work, a follow-up to his 2009 *The Accidental Guerilla*, is a collection of essays and chapters from his doctoral dissertation with some additions and annotations. Despite the somewhat disjointed nature of the work, theoretical principles are solidly articulated and supported with a real-world experience that shines through. Of these essays, Kilcullen's "Twenty-Eight Articles: Fundamentals of Company-level Counterinsurgency," is a particularly welcome revision and expansion of his unfinished manuscript that became a viral phenomenon within American military circles in 2006. This chapter is written in Kilcullen's gripping, no-nonsense style, designed to appeal to junior officers engaged in counterinsurgency operations. Like the rest of the book, it succeeds because it provides an actionable plan for practitioners without getting overly involved in theoretical paradigms. Other chapters provide metrics for analyzing operations in Afghanistan, a discussion of the Indonesian insurgency, a theoretical survey of insurgencies across time, and a plan for countering global insurgencies through a combination of network theory and deeper cultural understanding. In each of these chapters, Kilcullen writes with considerable authority yet provides an accessible and engaging text for many different audiences.

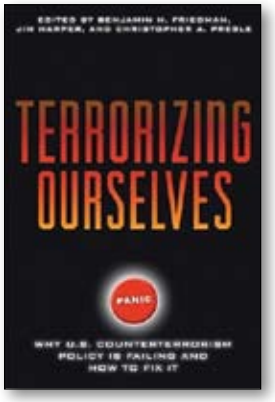
Reveron's work addresses the phenomenon of the use of American power in noncombat roles and does so in a more comprehensive and scholarly style. Despite the academic format, this work is provocative and engaging. According to Reveron, the use of the American military in noncombat roles such as nation building and security cooperation has dramatically increased in the decades since the end of the Cold War. The growth is a consequence of many factors including the lack of a conventional competitor, the shift from coercive diplomacy to military engagement, the unique ability of the military to provide security and assistance in dangerous regions, and the rise of subnational security threats. Many within the American military who would prefer to focus on either conventional firepower dominance or more modern high-tech transformation find this trend threatening. Reveron claims that the advocates of counterinsurgency and irregular-warfare approaches are more attuned to these new missions because of their more expansive views of security and their superior ability to perform nonmilitary political functions. Although Reveron does not advocate the dismantling of more traditional military capabilities, he claims that the US military will likely expand these new security functions and that this trend will have a powerful impact on the future American defense landscape.

Three common themes run throughout these books. First, the current strategic environment is extremely complex and challenging, and the US military will need to continually adapt its force structure, doctrine, training, and cultural understanding to meet the challenges of the coming decades. Second, these new roles require in-depth engagement with indigenous military and civilian groups because bottom-up efforts to build local security and civic involvement are typically more successful than top-down attempts to change government structures or transform entire regions. Finally, local security is an absolute must for any American efforts abroad and should be the first priority of any future mission.

In sum, both of these works are successful because they highlight the complex and evolving nature of the American military efforts around the globe and will provide insight for practitioners, policymakers, and academics alike.

J. Furman Daniel, III holds a PhD in International Relations and Security Studies from Georgetown University. His research focuses on international security, statesmanship, and military history.

Book Review



Terrorizing Ourselves: Why U.S. Counterterrorism Policy Is Failing and How to Fix It

by Benjamin H. Friedman, Jim Harper, and Christopher A. Preble (editors). CATO Institute, 2010

Review by Kerry S. Fray
Antiterrorism Specialist, Washington Headquarters Services

In *Terrorizing Ourselves*, the contributing authors seek to peel apart many of the notions, assumptions, and politics that have guided US counterterrorism (CT) efforts over the last decade. The main thesis is that US CT efforts have missed the mark in establishing and maintaining an efficient, informed system that addresses the threat of terrorism.

The authors of *Terrorizing Ourselves* thoughtfully analyze a variety of players and trends in terrorism and CT. The authors' strong research methodologies enable them to build fascinating cases against policies, false preconceptions, and poor spending strategies. In some cases, they build on truisms: We cannot protect every potential target; the Transportation Security Agency's procedures have raised the cost of air travel and likely would not have prevented the hijackings on 11 September 2001; and labeling US efforts "the Global War on Terror" is a technically incorrect piece of political rhetoric. In others essays, the authors present ideas in a new light that is contrary to oft-cited assumptions, notably, that individuals do not become terrorists because of a perfect storm of root causes that remains the same over a period of time such as economic status, mental state, and opportunity. Rather, it is suggested that terrorism is caused by an ever-changing relationship over time between individuals, organizations, and environments. In fact, the data provided even showed that terrorists tend to have an above-average socioeconomic status relative to the rest of their countrymen.

For those in the Department of Defense, the chapter entitled, "Don't You Know There's A War On?" by Paul Pillar and Christopher Preble, provides thoughtful analysis of what has historically been, what can be, and what should be the military's role in CT efforts. The authors conclude that the US military response to terrorism has been less effective, although more politically powerful, than nonmilitary responses. Other chapters advocate a reevaluation of the threat of terrorism in general, the ability of terrorists to obtain nuclear material, and the ways in which we consider risk and vulnerability.

Among the most compelling chapters is Veronique de Rugy's "Economics of Homeland Security," in which she analyzes spending on CT specifically and the Department of Homeland Security more generally relative to the threats they seek to dispel. The result of this analysis is a question: Why spend so much money on terrorism when any given person is thousands of times more likely to suffer death or injury as a result of violent crime?

For all of the critiques that *Terrorizing Ourselves* offers, it is not without potential solutions. What makes this book a particularly interesting read is that each author, in addition to posing a problem, offers concrete, actionable policy recommendations to reduce the problems that US CT policy, the media, and American culture and bureaucracy have created. Improvements include the development of clearer messages about terrorism that are not loaded with the hype of fear.

No reader will agree with absolutely everything that the authors contributing to Terrorizing Ourselves posit and offer, but the text provides an incredible jumping-off point for readers to reevaluate their education and previously acquired knowledge of terrorism and CT policies. To effectively do so in a mere 253 pages makes the book extremely succinct compared with the heavy tomes that decorate bookstores' shelves. In the end, this text should not be passed up.

AN OUT-OF-THE-BOX PROPOSAL

COUNTERING ACTIVE SHOOTER ATTACKS ON DOD INSTALLATIONS

Lone-wolf attacks require immediate neutralization

By Eric F. McMillin

The DOD should follow the majority of states and allow concealed carry of handguns to those who may face another "Fort Hood" where they live and work.

"Overseas you are ready for it. But here you can't even defend yourself."

— Spc Jerry Richard, survivor of the Fort Hood shooting[1]

On 5 November 2009, 13 individuals were killed and 43 were wounded or injured at the Soldier Readiness Center at Fort Hood, Texas, by a lone wolf shooter.[2] Terrorism experts in the United States believe future terrorist attacks in the United States, especially those perpetrated by individuals affiliated or sympathizing with al Qaeda, will likely come in the form of lone wolf shooting attacks like Fort Hood. Another possibility is a coordinated team attack similar to the Mumbai attack that that took place 26–29 November 2008. DOD installations are attractive targets for these attacks and, perhaps more troubling, may even be easy targets. A little out-of-the-box thinking—that is, allowing DOD civilians and military to carry concealed handguns—might help take DOD installations out of the "easy pickings" category.

Nature of the Threat and the Problem

Lone wolf (also known professionally as "active shooter" or "lone terrorist") attacks, whether terrorist or criminal, tend to follow a certain template. An armed perpetrator carrying large amounts of ammunition goes to a crowded or symbolic area and shoots as many people as he can until he is either shot down himself or is hemmed in by law enforcement and decides to commit suicide. Very few may surrender when they realize they can no longer continue the killing. Brutal math rules these attacks: People continue to die until the shooter is stopped. The longer it takes to stop him, the more people

die. Although most of those working and living inside the fences of stateside installations consider themselves safe, the Fort Hood shooting casts doubt on that assumption.

When Seconds Count, the Police are Only Minutes Away

The DOD report on the Fort Hood shooting indicates that Fort Hood civilian police officers Sgt Kimberly Munley and Sgt Mark Todd ran to the sound of the gunfire and shot and incapacitated the attacker approximately one and a half minutes after they arrived at the scene.[3] Most reports, however, indicate that the shooting began approximately 8.5 minutes prior to the police arriving.[4] Officers Munley and Todd arrived 2 minutes and 40 seconds after the first 911 call.[5] The brutal math of the Fort Hood attack is that 4.3 people were killed or wounded for every minute the attack lasted. One of those killed was CPT John Gaffaney, who was mortally wounded while trying, unarmed, to subdue the attacker.[6] In the wake of a spate of lone wolf shootings

Terrorism experts in the United States believe future terrorist attacks in the United States, especially those perpetrated by individuals affiliated or sympathizing with al Qaeda, will likely come in the form of lone wolf shooting attacks like Fort Hood.

and recognizing the potential for more, US Department of Homeland Security has distributed a poster, "How to Respond When an Active Shooter Is in Your Vicinity." One section of the poster advises:

Take Action

- As a last resort and only when your life is in imminent danger.
- Attempt to incapacitate the active shooter.
- Act with physical aggression and throw items at the active shooter.[7]

Throw Items at the Active Shooter

Some of the best things to "throw" at an active shooter are handgun bullets. The best time to throw them is as soon as it becomes clear you have an active shooter. Remember the brutal math. Response time for law enforcement is measured in minutes, and an active shooter could conceivably shoot hundreds of rounds before the police arrive. Given current DOD regulations and policies, a 21-year-old soldier has a better chance

The brutal math of the Fort Hood shooting:

4.3 people killed or wounded for every minute the attack went on.

Response time for law enforcement is measured in minutes. An active shooter could conceivably shoot hundreds of rounds before the police arrive.

of defending himself against an active shooter incident in Killeen, Texas, the town just outside the gate of Fort Hood, than at Fort Hood itself, despite the fact that Fort Hood is home to tens of thousands of combat troops and billions of dollars of weapons. In Killeen, a soldier, a DOD employee, or any other Texas resident with a clean record can obtain a Texas concealed handgun license and legally carry a loaded, ready, and concealed handgun. At Fort Hood, if the same soldier carries a loaded, ready, and concealed handgun or even carries a gun in his car, that soldier is committing a crime. The DOD does not recognize either the Texas concealed handgun license or the carry permits (generically known as "Carrying a Concealed Weapon" permits) of any other states. Services or local commanders severely restrict, to the point of effectively prohibiting, the carrying of privately owned firearms on DOD installations. This issue was noted in the report of the DOD independent review on Fort Hood

The DOD does not recognize either the Texas concealed handgun license or the carry permits (generically known as "Carrying a Concealed Weapon" permits) of any other states. Services or local commanders severely restrict, to the point of effectively prohibiting, the carrying of privately owned firearms on DOD installations.

in January 2010: "Finding 3.8: The Department of Defense does not have a policy governing privately owned weapons. Recommendation 3.8: Review the need for DoD privately owned weapons policy."[8]

It was not always easier for soldiers, spouses, or DOD employees to defend themselves outside Fort Hood. On 16 October 1991, a deranged man crashed his pick-up truck into Luby's Cafeteria in Killeen, about eight miles away from Fort Hood, and shot and killed 23 people

in the restaurant.[9] One of the dead was LTC Steven Dody from Fort Hood.[10] Another was Al Gratia, who, similar to CPT Gaffaney at the Fort Hood shooting, was mortally wounded while trying, unarmed, to rush and subdue the shooter. Gratia's wife, Ursula, was shot in the head and killed as she cradled her dying husband in her arms. Gratia's fatal charge caused the shooter to turn and continue his attack in a different direction. Gratia's daughter, Suzanne, immediately escaped the restaurant through a broken window and survived. Her Congressional testimony recounting the incident is must-see viewing for anyone hoping to understand the dynamics of an active shooter event.[11] Suzanne Gratia had routinely carried a handgun in her purse but, following the Texas concealed handgun law at that time, had left it in her car when she and her parents went into Luby's.

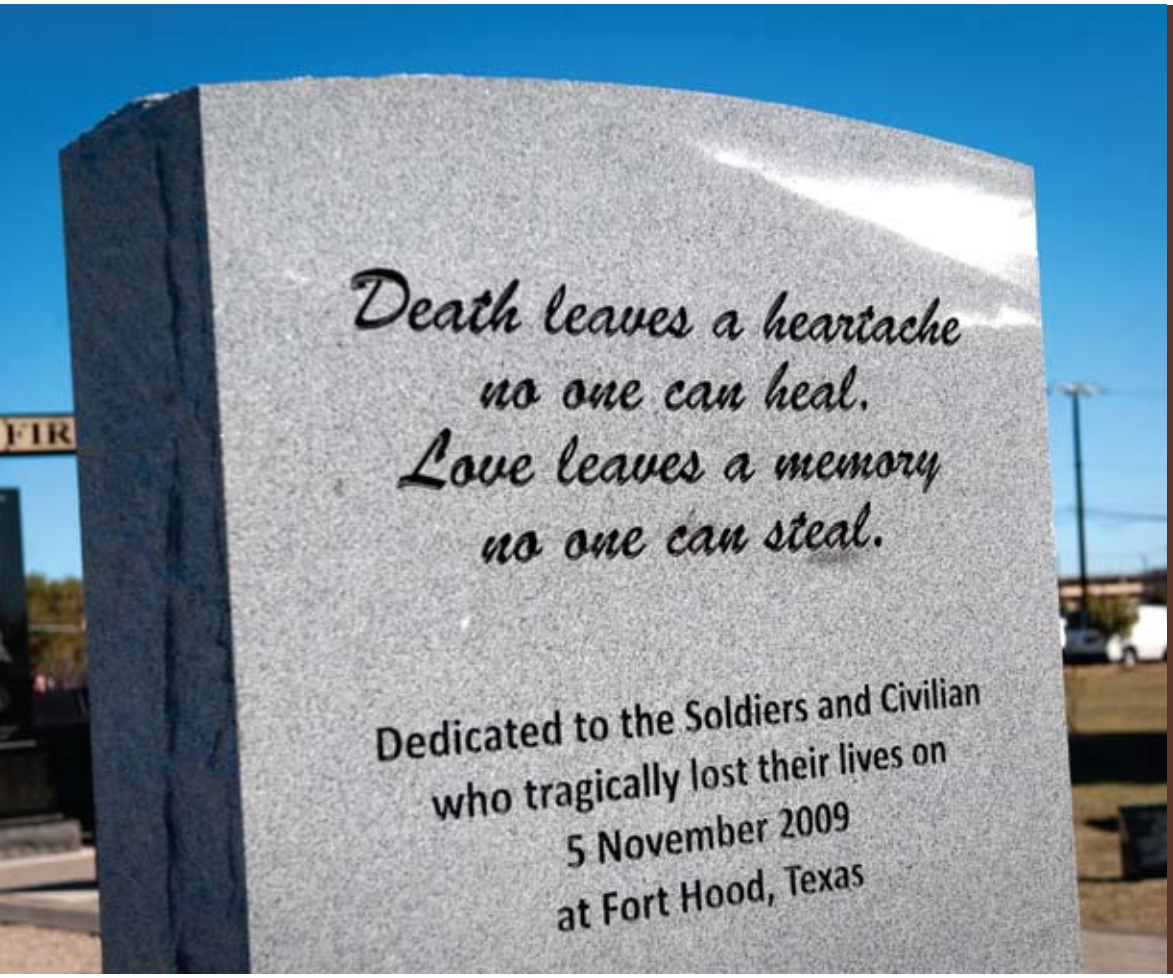
In reaction to her loss, Suzanne Gratia Hupp (her married name) spearheaded a campaign to pass legislation in Texas to allow concealed carry permits for those Texans who have clean records and appropriate training. After she successfully ran for the Texas legislature, Hupp was able to push this legislation through, and then-governor George W. Bush signed it into law in 1995.[12]

The Out-of-the-Box Approach and Risks Versus Benefits

The DOD should strongly consider recognizing state-issued concealed carry permits and making appropriate provisions to allow permit holders to carry concealed handguns on military installations. Most of us who have been around the military and the federal government suspected that the institutional reaction to the Fort Hood shooting would be a predictable set of restrictions on privately owned firearms on military installations.[13] Some of these restrictions, such as requiring soldiers to register weapons even if stored off the installation, went so far that some members of Congress introduced legislation to prohibit commanders from implementing such policies.[14]

Statistically, both law enforcement officers and holders of concealed carry permits are significantly less likely to commit crimes than the overall population.

Firearm rights have always been an emotional issue in this country. Certainly, a proposal that recommends



A memorial stone dedicated to US Soldiers and civilians who lost their lives 5 November 2009, was unveiled during a ceremony on Memorial Field, at Fort Hood, Texas, on the one-year anniversary. (US Army photo by D. Myles Cullen/ Released)

allowing Service members to carry concealed weapons on military installations to counter active shooter threats will stir even more emotion. Some will say that "the last thing we need is Joe running around the barracks with a gun!" This proposal, however, merits rational, unemotional analysis of the risks and benefits. Violence is a very complex phenomenon that requires layers of examination. Some believe that the private ownership of firearms leads to more violence; others believe it deters violence and lowers crime rates. The reality in the United States is difficult to pinpoint. There seems to be no correlation in terms of crime rates between states with extensive firearm restrictions and those with few restrictions; some with heavy restrictions have high levels of violent crime, whereas others do not, and those with few restrictions also span the spectrum of violent crime rates from low to high.[15]

A particular fear involves crimes of passion, where someone legally carrying a gun turns a verbal altercation into a shooting. To be sure, this has happened; some civilians with concealed carry permits commit crimes, as do some sworn law enforcement officers. Statistically, though, both law enforcement officers and holders of concealed carry permits are significantly less likely to commit crimes than the overall population. In Texas in 2007, for example, 1.2 percent of the population (228,909 people) were active concealed handgun license holders,[16] but license holders represented only 0.26 percent of those convicted of a crime.[17]

Rational analysis points to some legitimate concerns in recognizing state concealed carry licenses on DOD installations. First, a combination of firearms and alcohol in the barracks is never a good mix. Second, there is the possibility of accidental discharges in the workplace with greater numbers of people carrying weapons, although the rate of such mishaps over several years would still not likely compare to 13 killed and 43 wounded or injured in 10 minutes at the Soldier Readiness Center at Fort Hood.

A Question of Competence

If anyone outside of the law enforcement community is competent enough to defeat an active shooter, it seems like that ought to be a member of our Armed Services. Some members of the DOD, both military and civilian, are every bit as competent with firearms and the justified use of deadly force as the average law enforcement officer, especially in this era of persistent conflict and multiple deployments. There are also many people in the Armed Services, as well as many DOD civilians and family members, who have little experience with weapons. The training most states require to receive a concealed carry permit is focused on the legal aspects of concealed carry, with a range portion to demonstrate safe handling and operation and, perhaps, a very basic

Lone wolf attacks tend to follow a certain template. An armed perpetrator carrying large amounts of ammunition goes to a crowded or symbolic area and shoots as many people as he can until he is either shot down himself or is hemmed in by law enforcement and decides to commit suicide. Very few may surrender when they realize they can no longer continue the killing.

level of marksmanship. It is reasonable to expect that installation commanders would require an additional level of competence before allowing holders of state-issued concealed carry permits to carry concealed handguns on the base.

Additional requirements might include—

- Matching concealed handgun competency qualifications with those of law enforcement officers serving at the installation
- Passing a written exam on the legal aspects of use of deadly force
- Training on active shooter response.

Fratricide, or a "blue-on-blue" incident, is always a concern in responding to an active shooter situation. The Fort Hood shooter was allegedly wearing the Army advanced combat uniform, as were many of his victims. The DOD would also have to consider how to minimize the risk of a mistaken exchange of gunfire between concealed carry permit holders and responding law

enforcement officers. Some commanders will balk at the resources required to run a concealed carry permit certification program. It is likely, though, that most installations will find more than enough highly qualified active or retired Service members or DOD civilians willing to volunteer their time to run such a program. Installations would only need to supply a range and range supplies, a classroom, and completion credentials and to maintain a database of those who complete the requirements.

An Idea Whose Time Has Come?

Law enforcement cannot be everywhere, and given looming cuts in the defense budget, this situation is not likely to improve. However, the active shooter threat is not likely to go away. Active shooters continue to kill until armed responders shoot them down or hem them in. The longer the "good guy" takes to respond, the more people die. Forty-eight American states have provisions to issue concealed carry permits. Thirty-seven states, including the states that are home to most large military installations, have "shall issue" laws. These laws require state authorities to issue concealed carry permits to citizens who have clean records, take the required training, and apply. The DOD should follow this overwhelming majority of states and provide this level of trust and capability to those who may face another "Fort Hood" on the installations where they live and work.

Law enforcement cannot be everywhere, and given looming cuts in the defense budget, this situation is not likely to improve. However, the active shooter threat is not likely to go away. Active shooters continue to kill until armed responders shoot them down or hem them in. The longer the "good guy" takes to respond, the more people die.

Shortly after the Fort Hood attack, CNN interviewed Private Joseph Foster, who had been shot and wounded in the attack, and his wife, Mandi. Despite his wound, Private Foster was confident that he would still be able to deploy to Afghanistan on schedule with his unit. At the very end of the interview, CNN's John Roberts asked Mandi how she felt about Joseph deploying. She replied, "At least he's safe there and he can fire back, right?"[18]

Eric McMillin is on the faculty of the United States Army Command and General Staff College at Fort Leavenworth, KS. He is a retired Army officer with command and staff assignments in Armor and Cavalry units and he served as an Army Foreign Area Officer in Israel, Jordan, and Iraq.

SWAT team members approach a building with the and 29 more wounded in the attack. (U.S. Army photo

Note: The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Joint Staff, DOD, or any other agency of the federal government.

1 Associated Press. "Many Questions Follow Fort Hood Shooting Rampage." Stars and Stripes, 5 November 2009. Available at http://www.stripes.com/news/many-questions-follow-fort-hood-shooting-rampage-1.96203

2 US Department of Defense. Protecting the Force: Lessons from Fort Hood. Report of the DOD Independent Review, January 2010, p. 1. Available at http://www.defense.gov/pubs/pdfs/DOD-ProtectingTheForce-Web_Security_HR_13jan10.pdf

3 Ibid.

4 Ibid.

5 Ibid.

6 Zoroya, Gregg. "Witnesses Say Reservist Was a Fort Hood Hero." USA TODAY, 24 November 2009. Available at http://www.usatoday.com/news/military/2009-11-24-fort-hood-hero_N.htm

7 US Department of Homeland Security. "How to Respond When an Active Shooter Is in Your Vicinity" [poster]. Available at www.dhs.gov/xlibrary/assets/active_shooter_poster.pdf; similar recommendations can be found in CJCS Guide 5260, *Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism*, October 2002.

8 Supra 2, p. 32.

9 Burnett, John. "Hard Lessons From Two Mass Killings in Texas." NPR, November 20, 2009. Available at http://www.npr.org/templates/story/story.php?storyId=120542319

10 "Some Victims in Texas: A Colonel, an Ex-Teacher and 'Dr. G.'" *New York Times*, 17 October 1991. Available at http://www.nytimes.com/1991/10/18/us/some-victims-in-texas-a-colonel-an-ex-teacher-and-dr-g.html

11 The account of the Luby's massacre is taken from Suzanne Gratia Hupp's testimony to a the US Senate subcommittee. "Gun Control Witness." Available at http://www.youtube.com/watch?v=pnBXQxoIw5A&feature=related

12 Campoy, Ana. "Duel Over Gun Safety in Texas Capitol." *Wall Street Journal*, 8 February 2010. Available at http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704197104575051181299172168.html

13 US Army. *Installation Security Update*. Fort Hood website. Available at http://www.hood.army.mil/incident.security.aspx

14 "Inhofe Introduces Gun Bill To Protect Second Amendment Rights Of Soldiers, Employees Of Department Of Defense" [press release]. Washington, DC: Office of Senator James M. Inhofe. Available at http://inhofe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=b6ea0755-802a-23ad-47a4-2a293618ec1a

15 California has some of the most restrictive gun laws in the United States and in 2007 had a violent crime rate of 522.6 incidents per 100,000 inhabitants; Texas has some of the least restrictive gun laws and had a violent crime rate of 510.6 incidents per 100,000 inhabitants. Rhode Island has restrictive gun laws and had a violent crime rate of 227.3 incidents per 100,000 inhabitants in 2007; in the same year, New Hampshire, with some of the least restrictive gun laws, had a violent crime rate of 137.3 incidents per 100,000 inhabitants.

16 Texas Department of Public Safety. "Concealed Handgun Licensing: Reports & Statistics." Available at http://www.txdps.state.tx.us/administration/crime_records/chl/demographics.htm

17 Texas Department of Public Safety. "Concealed Handgun Licensing." Available at http://www.txdps.state.tx.us/administration/crime_records/chl/convrates.htm

18 CNN. "American Morning, Aired November 9, 2009" [transcript]. Available at http://edition.cnn.com/TRANSCRIPTS/0911/09/ltm.02.html.

Recommended Reading

To assist in the professional military education and development of the AT/FP community, J-34 has compiled a reading list on topics related to antiterrorism.

Benjamin, Daniel, and Steven Simon. *The Age of Sacred Terror: Radical Islam's War Against America*. New York: Random House, 2003.

Clark, Laura, and William E. Algaier. *Surveillance Detection: The Art of Prevention.* Cradle Press LLC, 2007.

Coll, Steve. *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001.* New York: Penguin, 2005.

Hoffman, Bruce. *Inside Terrorism, 2nd ed.* New York: Columbia University Press, 2006.

Horne, Alistair. *A Savage War of Peace: Algeria,1954–1962*. New York: NYRB Classics, 2006.

Joes, Anthony J. *Resisting Rebellion: The History and Politics of Counterinsurgency.* Lexington, KY: University Press of Kentucky, 2006.

Lewis, Bernard. *Crisis of Islam: Holy War and Unholy Terror.* New York: Random House, 2004.

Nagl, John. *Learning to Eat Soup With a Knife: Counterinsurgency Lessons from Malaya and Vietnam.* Chicago: University of Chicago Press, 2005.

National Commission on Terrorist Attacks. *The 9/11 Commission Report*. New York: W.W. Norton & Co, 2004.

Oren, Michael. *Power, Faith, and Fantasy*. New York: W. W. Norton & Co., 2007.

Pape, Robert. *Dying to Win: The Strategic Logic of Suicide Terrorism.* New York: Random House, 2006.

Sageman, Marc. *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press, 2004.

Scheuer, Michael. *Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America.* Dulles, VA: Potomac Books, 2002.

Guardian readers are encouraged to submit articles with analysis that expands on or critiques AT-related topics covered in these books. Send submissions to guardian@js.pentagon.mil.

RAISING THE FOCUS ON MAN-PORTABLE AIR DEFENSE SYSTEMS

U.S. Marine Corps photo by Sgt. Benjamin R. Reynolds/Released

Countering shoulder-fired missiles is key to protecting high-profile targets

By Mr. Charles Simon

Terrorists use MANPADs outside active war zones to reach foreign enemies without having to travel internationally.

Introduction

On 28 November 2002, two Grail surface-to-air (SA-7) missiles were fired on an Israeli Arkia Airlines Boeing 757-300 in Kenya.[1] Although these missiles did not affect the aircraft, their use outside of an active war zone demonstrated the proliferation of MANPADs and terrorist use of SA-7s to reach a foreign enemy without having to travel internationally. Despite this attack, shoulder-fired missiles, also known as man-portable air defense systems or MANPADs, have been underestimated in our efforts to secure our nation's skies. We must increase attention and support for systems that can counter MANPADs and not let the development of these systems be hindered by the commercial airline industry's fear of potential costs. Terrorists seek publicity, and passenger airliner attacks remain a dramatic source of attention. Attacks on airliners create fear among the general public that ordinary lives could be disrupted and that no aircraft is safe. The airline industry (including related industries such as hotels) suffers from loss of the aircraft, human and insurance costs of lost passengers,

Figure 1. DHL aircraft attacked over Baghdad in 2002.[2]

lost revenue from any system or regional shutdowns, and lower ridership as citizens travel by other means. Additionally, a government can be portrayed as powerless and unable to safeguard passengers.

Identifying the Vulnerability

With increased security inside airports and aircraft, external attacks on aircraft are more attractive methods for terrorists seeking to murder large numbers, yet the airline industry and our government have been slow to address this emerging threat.

External attacks have become more cost effective in terms of access and security, even if the weapons required are more sophisticated than a bomb, a gun, or a knife. A gun can be bought and a bomb can be made, but getting those weapons onboard an aircraft is a major barrier. MANPAD systems, although not as common as guns, are available to terrorists. An estimated 500,000–700,000 MANPADs exist throughout the world, most commonly the American Stinger and the Russian Strela and Igla.[3] Stingers were famously passed to insurgents in Afghanistan to fight the Soviet military, and hundreds of those weapons are still unaccounted for. The Strela's most common variants are the SA-7 Grail and SA-14 Gremlin. Russian SA-7s and other missiles were found in Taliban caves during US operations in Afghanistan.[4] Because of the number of sites that manufacture cheap copies, the SA-7 is the most prevalent threat: An SA-7 can be bought for as little as $5,000.[5] Bulgaria, China, Egypt, Hungary, North Korea, and Pakistan all manufacture SA-7s.[6] MANPADs stored in factory conditions have long shelf lives (some 22 years or more), although the launcher's battery requires frequent replacement.[7] With proper missile storage, replacement batteries, and training, any of the more than 30 groups thought to have MANPADs could successfully strike an airliner.

Shoulder-fired missiles, also known as man-portable air defense systems or MANPADs, have been underestimated in our efforts to secure our nation's skies. We must increase attention and support for systems that can counter MANPADs and not let the development of these systems be hindered by the commercial airline industry's fear of potential costs.

Although MANPADs may not always cause the immediate destruction of an aircraft, they are used when the aircraft is close to the ground (e.g., on takeoff or landing) and therefore more vulnerable to an attack that might be recoverable at higher altitude. In Baghdad, on 22 November 2003, two SA-14 Gremlin missiles were fired on a German DHL A300B4 aircraft that was flying at around 8,000 feet.[8] While the aircraft was still in the takeoff phase of flight, one of the missiles hit, causing a fire and instant catastrophic damage to the aircraft's hydraulic system. This damage resulted in a loss of flight controls, leaving the crew to steer by varying the engine thrust.[9] The aircraft recovered safely, but the damage was severe.

Figure 2. The Left Wing of the DHL Airbus After Suffering a SA-14 Hit.[10]

MANPADs require basic training and skill for a successful hit. The attack in Kenya likely failed due either to operator error or to mechanical failure in the missile or the launcher.[11] The SA-7 requires the operator to track the target or "command-to-line-of-sight," making use more difficult than a "fire-and-forget system."[12] Background clutter, which the guidance system could mistake for the target, should be minimized, and if the range is too short, the missile may not have room to adjust its flight path; the attacker can be up to 500–5,500 meters away for an SA-7 and 1,000–8,000 meters away for the Stinger.[13]

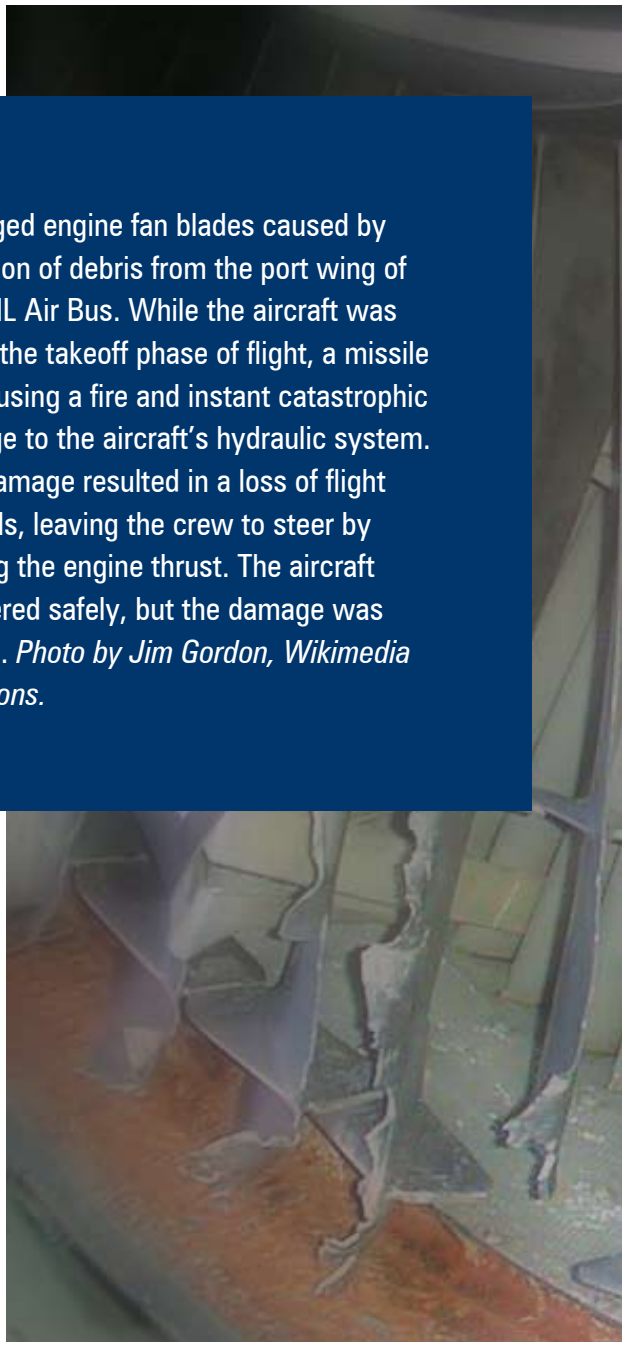
Impact and Why It Requires Increased Attention

A successful attack on an airliner would have a massive economic impact and could even contribute to the collapse of the airline industry. Airport security, including metal detectors, secondary checks, terrorist "no-fly" lists, and locks on cockpit doors all protect passenger aircraft from within but do not extend past an airport's perimeter.

The attacks of 9/11 were successful because the terrorists found a weakness in the security system and exploited it.[14] With the many post-9/11 security increases, the weakness has shifted outside of the airport. Terrorists could use MANPADs to reach beyond the range of security.

The deliberate destruction of an aircraft and the murder of its passengers and crew would create an international event, with psychological, economic, political, and diplomatic repercussions. This situation is very appealing to terrorist groups such as al Qaeda that aim to diminish US economic and political influence.

Terrorists derive their strength from fear through surprise and shock. Attacks on American airliners strike everyday citizens, regardless of social standing, political views, or financial class. Although tourists, business travelers, or ethnic groups may favor a particular route, city, or national carrier, the public would view the victims as mirror images of their own air travel and would curtail their (at least immediate) air travel. This fear of future destruction forces Americans to change their daily lives and the government to enact and enforce intrusive security practices. This reaction is expected and is a goal of the terrorists because the reaction can create financial and political losses beyond the primary event. Destruction of a passenger aircraft by a shoulder-fired rocket would surely involve some shutdown of the commercial and civil aviation industry, and potential passengers would travel more by car. Ironically, this shift results in more deaths because of the higher automotive accident rate.[15]



Damaged engine fan blades caused by ingestion of debris from the port wing of the DHL Air Bus. While the aircraft was still in the takeoff phase of flight, a missile hit, causing a fire and instant catastrophic damage to the aircraft's hydraulic system. This damage resulted in a loss of flight controls, leaving the crew to steer by varying the engine thrust. The aircraft recovered safely, but the damage was severe. *Photo by Jim Gordon, Wikimedia Commons.*

Terrorists derive their strength from fear through surprise and shock. The deliberate destruction of an aircraft and the murder of its passengers and crew would create an international event, with psychological, economic, political, and diplomatic repercussions. This situation is very appealing to terrorist groups such as al Qaeda that aim to diminish US economic and political influence.

Economic repercussions of a MANPAD attack include the initial damage, the impact of a system shutdown, and travel industry losses. The initial damage of one aircraft destroyed is $1 billion.[16] This amount includes the cost of the aircraft ($200–250 million) and the loss of 300 people ($2–2.5 million in compensation per person).[17] Following an attack, there would likely be a system shutdown while authorities determined whether future attacks were imminent. The shutdown and lost revenue would occur not only at the victim airport but also potentially throughout the region because inbound aircraft would be forced to divert and cancel flights into the area.

Other cities would likely suspend operations to look for possible attackers, causing a systemwide ripple effect. The RAND Corporation estimates the cost of a shutdown as $1.4 billion per day and $15.8 billion per week.[18] As corporations, the airlines would suffer from the lost revenue, resulting in layoffs and reduced purchases of new aircraft, fuel, and other operating components. The travel industry would suffer from reduced business travel, hotel stays, vacations, and related purchases. MANPAD attacks (e.g., the DHL attack in Baghdad) also hinder commerce. As companies add the increased insurance costs to the potential loss of lives, equipment, and goods that affect their operating expenses, they may not trade or provide services to high-threat areas. This restriction would limit economic growth in areas with emerging economies, some of which may rely on this

trade for postconflict recovery and counterterrorism efforts.

The successful downing of a commercial airliner raises the perceived potency of a terrorist or a group. Airline crashes are media events, even when terrorism is not involved. The added attention of a terrorist attack would focus tremendous attention on the suspected perpetrators or any group that claims the attack. Even a previously unknown group would be seen as a legitimate threat and would gain recognition.[19] Previously, terrorist attacks on aircraft involved taking hostages to negotiate for ransom or a prisoner exchange, gaining international publicity for the terrorists in the process. Al Qaeda and its inspired transnational terrorist movement have focused more on killing large numbers of people in a public manner. Religious or doomsday terrorist groups generally have fewer constraints with regard to mass murder than a political group seeking legitimacy.[20] Even political groups or state-sponsored terrorists may find an external attack useful if it meets their goals or shows resolve. Libya, for example, supported the Pan Am 103 bombing partly as revenge for America's Operation EL DORADO CANYON airstrikes. The biggest hurdles for a MANPAD attack are acquisition of weapons and training in their proper use, but state-sponsored terrorism may provide these means to a proxy group. Airlines are also symbols of national origin. As seen in the Kenya attack on the Israeli passenger aircraft, terrorists can attack a symbol of a foreign nation from a local base of operations. This approach reduces the need to smuggle weapons or personnel internationally.

Diplomatic missions would suffer because attacks on dignitaries and other Americans in developing areas hinder the ability of nongovernmental organizations to build relations (which support counterterrorism missions). Although not a missile attack, the April 2009 mortar attack on US Representative Donald Payne's plane while it was taking off from Mogadishu, Somalia (and al Shabab's claim of the event), will weigh on the minds of politicians and State Department officials considering future visits.[21] Because the Congressman had met with Somalia's president that day, the attack highlighted the struggling nation's inability to protect foreign leaders.[22]

Currently, the Department of Homeland Security (DHS) has two systems competing to protect aircraft from missiles, but those systems have not gained much widespread public attention. The public perception of airline safety is measured by the length of security lines, which will not prevent a MANPAD attack. Understanding these DHS systems and supporting their development is crucial.

Despite the noble nature of arms control, it is inherently based on cooperation between nations. State sponsors of terrorism, states that find the agreements too intrusive, and rogue nonstate elements (criminal, insurgent, or terrorist) will not be hindered by these efforts.

Proposals for Prevention

Three methods will lower the chance of a successful MANPAD attack: (1) Minimize weapon availability, (2) isolate potential attack areas, and (3) take missile countermeasures. A comprehensive defense requires each of these methods to be addressed, although only postlaunch missile countermeasures, or counter-MANPADs (C-MANPADs), could save lives once a missile is fired.

Because of their portability and widespread manufacture, MANPADs have proliferated across the globe. Arms control efforts have focused on export controls, safe storage, and destruction of excess missiles in military arsenals. Members of the Wassenaar Agreement adopted the Elements for Export Controls of MANPADS agreement in 2000, the first multinational agreement of its kind.[23] The safe storage and export controls outlined in this agreement (which was expanded in 2003) required suppliers to ensure that their purchasers store missiles and launchers separately, maintain 24-hour surveillance, and conduct 100 percent physical inventories every month.[24] In 2006, the Organization for Security and Co-operation in Europe released a best practices guide on stockpile management; additionally, several nations have assisted others with their stockpiles, including the destruction of more than 21,000 obsolete and excess missiles.[25] Some nations will still produce these weapons, but efforts that make it tougher for terrorists to acquire MANPADs are worthwhile. To be successful, terrorists need to train with MANPADs; therefore, one missile is less of a threat than several missiles used as practice rounds in a training camp.

Extending the security around an airport is extremely troublesome. Airports are frequently surrounded by industrial zones and high-crime neighborhoods, neither of which helps law enforcement. Any residential or commercial area could be bought and assimilated into the airport, but this would be exorbitantly expensive. Isolating airports to prevent missile attacks is not feasible. Aircraft fly extended paths during their approach to landing and departure phases, both of which offer large areas of vulnerability. Examining these patterns at Los Angeles International Airport, an SA-7 could be fired from anywhere inside 870 square miles, a range that increases to 4,600 square miles for an SA-18.[26] One bright spot is that many airports are near bodies of water (to make use of regular wind patterns, to mitigate flight noise, and to reduce potential crash damage). Although water also aids terrorists by providing a clear line of sight, a water exclusion zone can be invoked. This zone can then be patrolled and monitored for suspicious activity to reduce attacks.

C-MANPADs are the last defense once a missile has been fired. Commercial airliners should have C-MANPAD devices similar to those seen on military aircraft. Costs are significant but can be mitigated by equipping only high-capacity aircraft traveling in threat areas, along with other randomly chosen aircraft. The use of random aircraft is similar to the assignment of air marshals; by playing a security shell game, terrorists can never be sure which aircraft have these systems. Although C-MANPADs are not a guarantee of protection against all attacks, they complicate terrorists' planning and could hinder attacks or leave a trail for intelligence and law enforcement to identify.

Countermeasures fall into three categories: flares, laser jammers, and high-energy lasers (HELs). Flares defend against first- and second-generation missiles by producing a heat signature that overwhelms the missile's infrared guidance sensor.[27] Because terrorist attacks are unexpected, flares are deployed after an onboard (optical or radar) sensor has detected a missile. Flares are not very useful against command-guided (radiofrequency, optical, or laser beam riders) missiles.[28] Missile-warning sensors must be combined infrared/Doppler to minimize

the chance of a false alarm, which could cause ground fires. Ground-based warning has limited range and requires reliable instant wireless communications for the aircraft to launch flares in time.[29] The main benefits of flares are their immediate availability and strong performance against older (and more widely proliferated) missiles such as the SA-7.[30,31] Laser jammers, also known as directed infrared countermeasures (DIRCMs), work well against early missiles by using a directed beam to overwhelm and then divert a missile.[32] Laser jammers are a more appropriate defense because commercial aircraft cannot be expected to perform the highly evasive maneuvers needed to maximize the effectiveness of flares; however, because undermounted laser jammers fire downward, they require strong warning systems to avoid damage to personnel on the ground. Jammers are also unable to protect against command-guided missiles. The third type of C-MANPAD is a HEL. HELs are unlike the two previous systems because they destroy the missile. Northrop Grumman's Hornet HEL is palletized but has a limited range of around five kilometers; multiple Hornets would be required to cover flight paths.[33] HELs have two major drawbacks: (1) they are still in development (estimated to be at least 3 years from production) and (2) they involve classified systems, which would constrain them to limited deployments, especially to high-threat foreign airports.[34]

Of these options, laser jammers provide the best overall defense. They are designed to protect against the most likely type of missile. Although their ability to engage multiple missiles is not instant because of slew time, it is unlikely that terrorists would be able to fire multiple shots simultaneously; such a complex barrage would only occur from an advanced multiple-missile launcher system. Two leading laser jammer systems are BAE's JETEYE and Northrop Grumman's Guardian, both of which have been tested onboard commercial airliners.[35,36] The 2008 testing involved attaching these systems to actual passenger aircraft to determine operational and cost impacts.[37] American Airlines, which tested them on its Boeing 767-200s, is "not in favor" of these C-MANPAD systems due to the expected costs and lost profits.[38] Our nation must increase support for these systems and not allow financial decisions by an already struggling industry to prevent a layered defense.

Drawbacks and Limitations

Cost is the biggest detraction of C-MANPADs. Commercial airlines are struggling financially, and adding more costs may increase burdens unnecessarily for a rare threat. It would cost an estimated $11 billion to install laser jammers on the approximately 6,800 commercial aircraft, including research and development and manufacturing costs.[39] The life cycle costs are estimated to be $40 billion over 10 years (including $2.1 billion per year for operations and support), although if DHS maintenance reduction goals are met, this amount decreases to $25 billion.[40] For each aircraft, the cost is $300,000 per year, including added fuel to compensate for increased drag and weight, maintenance and delays from maintenance, and technology sustainment.[41]

The airline industry denounces these programs as a "vendor intent on selling C-MANPADs" and estimates the added operating cost at $365 per flight, subtracted from their claimed best-case profit of $600 per flight.[42] To compensate for this thin profit margin, the airline industry could receive additional federal support (some of which already funds Federal Aviation Administration safety and DHS security requirements).

It is difficult to precisely judge the monetary value of deterrence. Although attacks have been relatively rare (and these efforts would reduce them further), airline travel's strong safety record makes any additional cost seem wasteful. This difficulty would be exacerbated if the system were installed but failed to prevent a missile attack. Following an attack, installation of C-MANPADs may have little effect on passenger confidence and would result in costs combined with lost revenue.[43] The government, however, will be seen as paralyzed if it does not install these systems.

If only examining costs, counterproliferation may seem the most reasonable option. Despite the noble nature of arms control, it is inherently based on cooperation between nations. State sponsors of terrorism, states that find the agreements too intrusive (including those for which the arms industry is important to their economy), and rogue nonstate elements (criminal, insurgent, or terrorist) will not be hindered by these efforts. Although reducing the number of MANPADs could limit their spread, models such as the SA-7 can be manufactured in large enough quantities to overcome any gains from destroying missiles in cooperating nations' stockpiles.

A psychological drawback is that vocal support for these systems may raise public fear and reduce air travel, particularly if political posturing is used to force these systems on the airline industry. Describing the vulnerability could highlight it as a viable tactic for terrorists; however, if we avoid action for this reason, we are denying a problem that terrorists will choose eventually.

Conclusion

After completing DIRCM tests onboard commercial aircraft, the United States cut funding for C-MANPADs onboard commercial aircraft in 2010.[44] Recognizing that we are in a period of tight federal budgets, the US government must still fully support and even accelerate the deployment of laser jamming systems, even if only on high-threat routes. Research and development costs, including efforts to reduce maintenance requirements and weight and drag impact, should be seen as a technological investment in our safety. Funding these key

steps after a MANPAD attack will result only in higher costs as the United States tries to make up for lost time. As laser jammers are integrated, airlines will adapt their business model for this new requirement in the same manner as any new flight requirement. Corporate risk decisions accept more damage than the government, and the airline industry's profit concerns should not outweigh the price of human lives. Nonproliferation and airport perimeter security can reduce the chance that a terrorist could acquire and use a missile, but eventually this tactic will be successful against a US airliner. We must raise the focus on terrorist use of MANPADs against airliners before these weapons achieve catastrophic results.

Charles Simon is a former naval aviator who flew aircraft carrier–based combat support flights over Iraq and is a holder of a Federal Aviation Administration commercial pilot license. He currently works in the national security industry.

---

1 "Israeli Airliner Safely Arrives in Tel Aviv After Failed Kenya Attack." Voice of America News, 28 November 2002. Available at http://www.voanews.com/english/archive/2002-11/a-2002-11-28-2-Israeli.cfm

2 Photo credit: Jerome Sessini, courtesy of pdnonline. "DHL A300 Airbus Demonstrates How Serious the Terrorist Threat Is." Talking Proud, December 2007.

3 Center for Strategic and International Studies. "Defending Airborne Commercial Jets from Terrorists." Transnational Threats Update, 1 (2003, July).

4 Chow, James, Chiesa, James, Dreyer, Paul, et al. "Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat" [occasional paper]. Santa Monica, CA: RAND Corporation, 2005. p. 5. Available at http://www.rand.org/pubs/occasional_papers/2005/RAND_OP106.pdf

5 "Proliferation of MANPADS and the Threat to Civil Aviation." Jane's Security News, 13 August 13 2003.

6 "The Threat From Portable Missiles," BBC.com, 29 November 2002. Available at http://news.bbc.co.uk/2/hi/africa/2527645.stm

7 Hunter, Thomas B. "The Proliferation of MANPADS." Jane's Security News, 28 November 2003.

8 "DHL A300 Airbus Demonstrates How Serious the Terrorist Threat Is." Talking Proud, December 2007.

9 Ibid.

10 Supra 2.

11 Supra 5.

12 Ibid.

13 Ibid.

14 Byman, Daniel. *The Five Front War: The Better Way to Fight Global Jihad*. Hoboken, NJ: Wiley, 2008. p. 68.

15 Ibid, p. 50.

16 Supra 4, p. 7.

17 Ibid.

18 Ibid, p. 10.

19 Hoffman, Bruce. *Inside Terrorism*. New York: Columbia University Press, 2006. p. 255.

20 Ibid, p. 239.

21 Ibrahim, Mohamed. "Mortars Threaten U.S. Congressman's Plane in Somalia." *New York Times*, 13 April 2009. Available at http://www.nytimes.com/2009/04/14/world/africa/14somalia.html

22 McCrummen, Stephanie. "Plane of U.S. Lawmaker Fired Upon." *Washington Post*, 14 April 14 2009. Available at http://www.washingtonpost.com/wp-dyn/content/article/2009/04/13/AR2009041300671.html

23 Bevan, James, and Schroeder, Matt. "Man-Portable Air Defence Systems (MANPADS)." In James Bevan (ed.), *Conventional Ammunition in Surplus: A Reference Guide*. Geneva: Small Arms Survey, Graduate Institute of International Studies, 2008. p. 125. Available at http://www.smallarmssurvey.org/files/sas/publications/b_series4.html

24 Ibid.

25 Ibid., p. 125–126.

26 Supra 4, p. 14.

27 Ibid, p. 17.

28 Ibid, p. 18.

29 Ibid.

30 Ibid, p. 19.

31 Supra 6.

32 Supra 4, p. 19.

33 Ibid, p. 21.

34 Ibid, p. 22.

35 "Northrop Grumman Wins Commercial Aircraft Anti-Missile System Contract" [press release]. Rolling Meadows, IL: Northrop Grumman, 25 August 2004. Available at http://www.irconnect.com/noc/press/pages/news_releases.mhtml?d=62954

36 "BAE Systems Counter-MANPADS JETEYE System Takes Flight on Commercial Airliner for Department of Homeland Security" [press release]. Fort Worth, TX: BAE Systems, 10 November 2005. Available at http://www.baesystems.com/Newsroom/NewsReleases/2005/press_10112005.html

37 Hall, Mimi. "Passenger Jets Get Anti-Missile Devices." USA Today, January 4, 2008. Available at http://www.usatoday.com/news/nation/2008-01-04-anti-missile-jets_N.htm

38 Associated Press. "American Airlines to Test Anti-Missile System on Commercial Jets." FoxNews.com, 5 January 2008. Available at http://www.foxnews.com/story/0,2933,320489,00.html

39 Supra 4, p. 24–25.

40 Ibid, p. x.

41 Ibid, p. 26–27.

42 Air Transport Association of America. "Counter MANPADS Deployment – What's the Debate About." ATA Issue Brief, October 2006.

43 Supra 4, p. 11.

44 Magnuson, Stew. "No Further Funding for DHS Shoulder-Fired Missile Program." *National Defense*, August 2009. Available at http://www.nationaldefensemagazine.org/archive/2009/August/Pages/NoFurtherFundingforDHSShoulder-FiredMissileProgram.aspx

Strategic Event Assessment

By LCDR Christopher F. Hill

EVENT: Stuxnet Virus

The Stuxnet computer virus discovered in July 2010 may be capable of controlling industrial systems and causing damage. It allegedly affected a number of industrial facilities including an Iranian uranium enrichment facility.

STRATEGIC SIGNIFICANCE:

The DOD AT community continues to debate whether or not terrorist attacks can occur through a cyber medium. As an asymmetrical strategy used by individuals or groups, terrorism involves the threat or acts of violence to instill fear in a populace and is often motivated by political goals. *Violence* and *fear* are the operative terms in terrorism.[1] For a cyber attack to be considered an act of terrorism, per DOD standards, it would need to maim human beings or create fear of maiming. This narrow definition is distinct from cyber attacks that disrupt computer networks, exploit identities, steal government secrets, or siphon money from banks—all of which have been perpetrated by known terrorists.

U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Nicolas C. Lopez/Released

Until recently, there has been scant evidence that cyber attacks alone could directly threaten life and limb. As news of the potent Stuxnet virus allegedly emerged in Iran in 2010, however, it became evident that if similar sophisticated viruses were exploited by terrorists, these cyber "cruise missiles" could cause the sort of violence and fear consistent with an act of terrorism and, thus, be considered "cyberterrorism."

The Stuxnet virus is a new cyber worm designed to infiltrate and commandeer computer systems that control machinery in nuclear power plants, factories, and other industrial control systems. It can hide itself from programmers and, in theory, sabotage a system so it can be remotely controlled and destroyed, possibly killing people as a result. This worm is believed to have infected several systems around the world, though primarily in Iran. The Iranians have acknowledged the existence of a virus that targeted centrifuge machines at the Natanz uranium enrichment facility, which the United States suspects is part of a weapons program.[2]

The creator of the Stuxnet virus is unknown. Many experts have suggested that the resource requirements necessary to create and control a super virus like Stuxnet point to nation-state involvement. Nevertheless, the complexity of the virus should not suggest that terrorists will not attempt to obtain such a capability. Terrorists have long been known to use the cyber world to advance their goals, through Internet recruitment and training, online magazines (see the Fall 2010 issue of The Guardian Antiterrorism Journal), and credit card and identity theft. It is reasonable to speculate that a new type of threat may emerge where terrorists leverage skilled cybercriminals to take over computer systems with the intent of harming people or shutting down governments. For Antiterrorism Officers, this highlights the need to consider including cyberspace security and robust information access control procedures in unit Antiterrorism Plans.

QUOTES:

"Stuxnet is the first in so many different areas. It's amazing. Basically, this could well be a turning point in how we view cyber…. It can hide how your equipment works in your plant, and it can hide those changes from you so that you won't even see that there is code."

— Liam O Murchu, researcher for Internet security company Symantec, September 2010 (http://abcnews.go.com/Technology/stuxnet-worm-cyber-weapon-targets-power-plants-factories/story?id=11713921)

"What we're seeing with Stuxnet is the first view of something new that doesn't need outside guidance by a human—but can still take control of your infrastructure…. This is the first direct example of weaponized software, highly customized and designed to find a particular target…. It's the type of threat we've been worried about for a long time. It means we have to move more quickly with our defenses—much more quickly."

— Michael Assante, former chief of industrial control systems cyber security research at the US Department of Energy's Idaho National Laboratory, September 2010 (http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant/(page)/2)

"Despite this growing threat, training to counter these attacks has failed to increase in response."

— Cyberterrorism Defense Analysis Center (part of Department of Homeland Security's Federal Emergency Management Agency; http://www.cyberterrorismcenter.org/)

"[Iran's enemies have] been successful in making problems for a limited number of our centrifuges, with software they had installed in electronic devices…. Fortunately, our experts have discovered the origins of the problems, and today they are unable to repeat these acts."

— Mahmoud Ahmadinejad, President of the Islamic Republic of Iran, *Washington Post Foreign Service*, 29 November 29 2010

"[Cyberterrorism is] real and ... rapidly expanding… [Terrorists] will either train their own recruits or hire outsiders, with an eye toward combining physical attacks with cyberattacks."

— Robert S. Mueller III, Director, FBI, 4 March 4 2010 (http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html)

"If a virus could attack [in Iran], then there is every reason to suppose that a virus could be used to attack air-traffic control systems, water plants, or telecoms systems, too."

— Jamie Shea, NATO Deputy Assistant Secretary-General, Emerging Security Challenges Division, December 2010 (http://www.defensenews.com/story.php?i=5274241&c=FEA&s=INT)

1 Per the latest version of JP 3-07.2, *Antiterrorism*, 24 November 2010, terrorism is defined as "the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political."

2 Thomas Erdbrink. "Ahmadinejad: Iran's Nuclear Program Hit by Sabotage." *Washington Post Foreign Service*, 29 November 2010.

DD AT/HD
Joint Staff, J-3 Operations Directorate
Pentagon
Room MB917
Washington, DC 20318-3000

Note: If your copy of the Guardian has been damaged in shipping or is unreadable, please contact us at guardian@js.pentagon.mil. We will send out an electronic pdf to replace it.