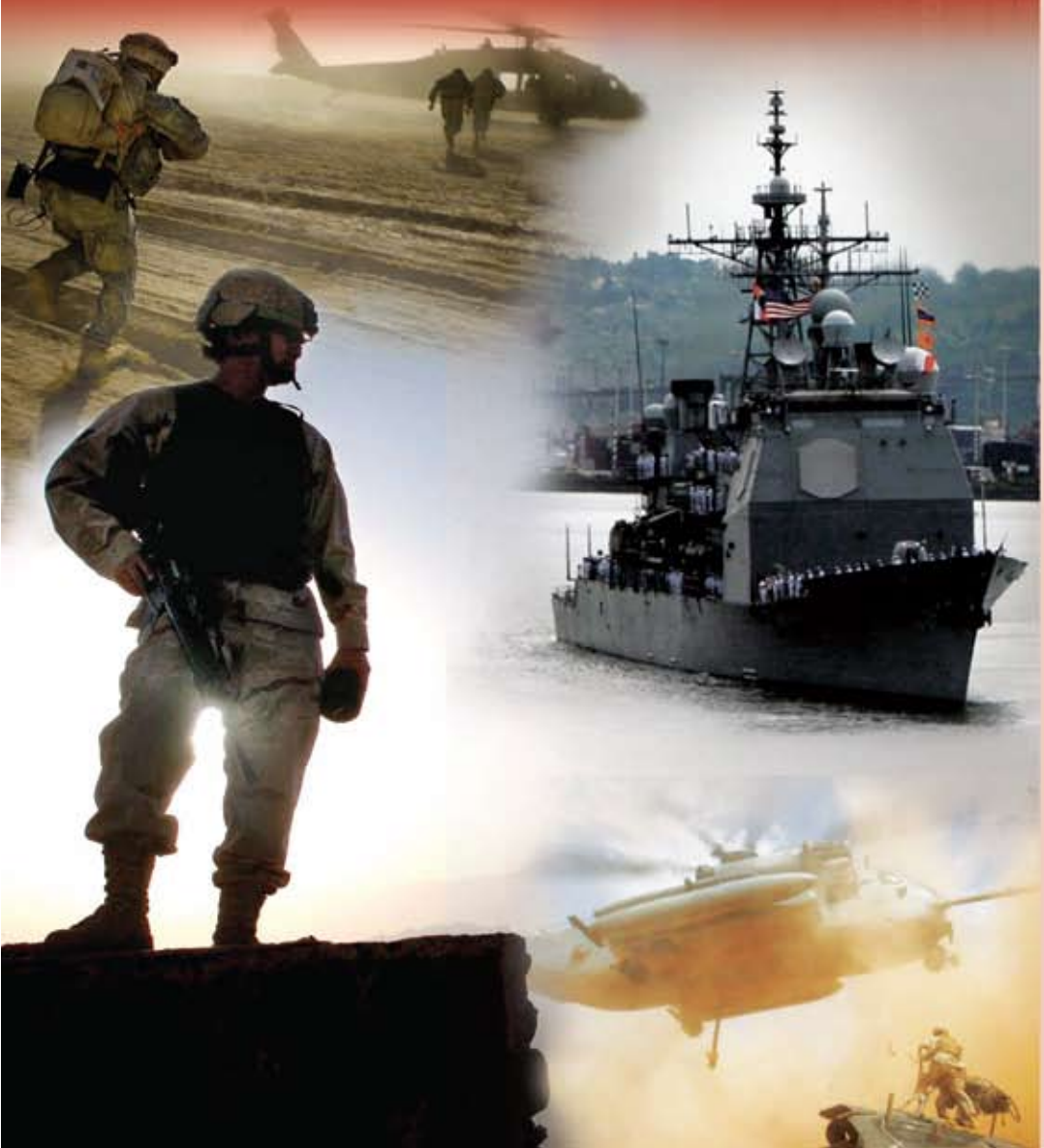
Volume 10
Number 2

The Guardian

The Source for Antiterrorism Information



In This Issue

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

The Pentagon, Room MB917
Washington, DC 20318

"The fight against terror and extremism is the defining challenge of our time. It is more than a clash of arms. It is a clash of visions, a great ideological struggle. On the one side are those who defend the ideals of justice and dignity with the power of reason and truth. On the other side are those who pursue a narrow vision of cruelty and control by committing murder, inciting fear, and spreading lies.

This struggle is waged with the technology of the 21st century, but at its core it is an ancient battle between good and evil. The killers claim the mantle of Islam, but they are not religious men. No one who prays to the God of Abraham could strap a suicide vest to an innocent child, or blow up guiltless guests at a Passover Seder, or fly planes into office buildings filled with unsuspecting workers. In truth, the men who carry out these savage acts serve no higher goal than their own desire for power. They accept no God before themselves."

—President George W. Bush
May 15, 2008

"A drawdown of US forces in Iraq is inevitable over time—the debate here in Washington is now principally about pacing and timing. But the kind of adversary we face today—violent jihadist networks untethered from nation states—will not allow us to remain at peace. What has been called the "Long War" is likely to be many years of persistent, engaged combat all around the world in differing degrees of size and intensity. This generational campaign cannot be wished away or put on a timetable. There are no exit strategies. To paraphrase Leon Trotsky, we may not be interested in the long war, but the long war is interested in us."

—Secretary of Defense Robert M. Gates
May 5, 2008

"I don't like to even bring up Afghanistan without talking about Pakistan, because I think they are linked. And I think we need to make sure our strategy includes not just Afghanistan, but also Pakistan. We have a heavy focus on the FATA, and I think that is right. Clearly, if I were going to pick a place where the next attack is going to come from, that is where al Qaeda is, that is where al Qaeda leadership is, and we are going to have to figure out a way to resolve that challenge."

—Chairman of the Joint Chiefs of Staff ADM Mike Mullen
April 17, 2008

Editor's note on "Special Even Antiterrorism Risk Assessments: Leveraging Doctrine" (Spring 2008 edition): The FPCON graphic should have read, "CHARLIE—Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. DELTA—Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent."

I'm dedicating this edition of *The Guardian* to the memory of a former J-34 Action Officer, LTC James Walton, USA, who died in combat in Afghanistan in June 2008. While on the Joint Staff, Jim worked tirelessly to counter the Improvised Explosive Device threat. He had a passion for doing everything possible to protect our troops in harm's way. Jim's efforts helped save lives through the advent of new technology, tactics, and collaborative efforts across the DOD. LTC Walton's leadership and initiative made a difference in the lives of many. He will be missed.

This past Independence Day, I reflected on our American heroes who, like LTC Walton, left their homes, businesses, farms, and families and took up arms for the ideals espoused by our forefathers in the Declaration of Independence. These ideals are not lost on the men and women who leave behind those same things to wear the cloth of our Nation today. I truly appreciate all you do to protect our American values. The loss of LTC Walton serves as a reminder to us all that our work, initiatives, and collaboration make a profound difference in the Global War on Terror and the protection of our American homeland. We must redouble our efforts and strive to break the shackles of old thinking, stale doctrine, and self-defeating paradigms.

LTC James Walton

Several issues ago, I mentioned the need for an "all-hazards" approach to protection. A holistic, synergistic approach ensures there are no gaps and that resilience is maintained across the mission areas. In my view, all-hazards protection extends beyond the traditional concept of antiterrorism/force protection into force health protection, consequence management, border security, physical security, defense critical infrastructure protection, cybersecurity, counternarcotics, threat detection, access control, and law enforcement. The majority of these mission areas are interrelated, and positive effects in one area can bring positive second- and third-order effects in another.

I have challenged my staff to write about their programs, discuss important initiatives, and share their perspectives on ways to improve how the DOD protects our nation and service members. The fruits of that effort can be found in this edition, which is heavy with J-34 authors. I applaud their work. I ask you, the readers, to continue to contribute to *The Guardian*. Your opinions, lessons learned, and best practices greatly assist our efforts to share information, benchmark successes, and move toward a common goal of better protecting our nation and defeating the efforts of terrorists and insurgents worldwide.

The price of freedom is eternal vigilance.
—Thomas Jefferson

Peter M. Aylward
Brigadier General, US Army
J-3, Deputy Director for Antiterrorism/Homeland Defense

The Guardian newsletter is published for the Chairman of the Joint Chiefs of Staff by the Antiterrorism/Force Protection Division of the J3 Deputy Directorate for Antiterrorism/Homeland Defense to share knowledge, support discussion, and impart lessons and information in an expeditious and timely manner. *The Guardian* is not a doctrinal product and is not intended to serve as a program guide for the conduct of operations and training. The information and lessons herein are solely the perceptions of those individuals involved in military exercises, activities, and real-world events and are not necessarily approved as tactics, techniques, and procedures.

SUBMITTING NEWS & ARTICLES

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. The editors invite articles and other contributions on antiterrorism and force protection of interest to the Armed Forces. Local reproduction of our newsletter is authorized and encouraged.

Securing the Force Protection Advocate: Challenges, Choices, and Requirements

By Michael Adams, Antiterrorism Plans Senior Analyst, CACI, with contributing authors Kevin Reese, Project Manager, CACI, and Carolyn Emery, Antiterrorism Officer, Army Reserve Command

How effective is the military's overall force protection (FP) program? In this article we present two initiatives that may lead to improvement. First, create formal recognition for uniformed members to make FP or antiterrorism a highly desirable assignment. Second, establish an FP advocacy program. Included are some suggestions for development of the initiatives as well as suggestions to address the whispered or unspoken concerns about the FP of DOD's "soft targets" within the homeland.

Among Those Who Know the Need

Full-time and "additional duty" antiterrorism (AT) and force protection (FP) officers, managers, contractors, and others attended the 2008 Army Antiterrorism Conference in Orlando, Florida. There were experienced, dedicated presenters and attendees from headquarters to "boots on the ground" locations. Relatively few occupied an authorized-personnel position, and more of those full-time professionals were civilians than uniformed military. Attending the conference were active-duty personnel, Army Reserve, National Guard, and other government agencies.

First Initiative: Recognize Antiterrorism and Force Protection Practitioners

One of the presenters in uniform has directed FP on a full-time basis in a constant front-line threat environment. LTC Stephen St. Clair is a Military Police officer who retired from active duty in the early 1990s and was recalled last year to become Chief, Force Protection Office (FPO), Combined Joint Task Force 82, Afghanistan. He received applause and positive comments when he said, "Force protection and antiterrorism needs to be a Military Occupational Skill (MOS) or an Additional Skill Identifier (ASI)." In a short hallway conversation, LTC St. Clair acknowledged that this was not his original idea but agreed to being quoted, since in his view, it is obvious. It is time to formalize the process of identifying the practitioners in some way beyond receipt of a training certificate. Our installations will be safer, and deploying units will be better protected as they prepare for leave, arrive at, and perform missions.

Many of the changes brought on by AT are easy to see, and perhaps AT seems to catch attention faster than FP. Regardless of your preferred term for the program, you probably agree that positive, measurable efforts have been taken, systems and technologies developed and employed, and funding applied to the AT/FP program since the abrupt awakening of our nation to the reality of terrorism. For

the most part, the military accepted adjustments that would probably have been viewed as inconveniences prior to losing so many so dramatically on 9/11. Formerly "open" installations have closed the back gates, erected defined entrances, and placed guards who stop all traffic, check identifications, and follow routines specified by the Force Protection Condition (FPCON) and the associated written measures.

On Army installations, staff members other than the AT officer (ATO), such as the provost marshal and physical security specialist, are involved in FP. The G3 or S-3 is usually responsible for the program and most of the FP staff. An intelligence officer is probably in a separate staff section. The future will probably bring additional dedicated staff, such as critical infrastructure specialists for some places. Army Regulation 525–13, Antiterrorism, currently under revision, also requires at least two FP groups or committees at the staff and executive levels, bringing in members to steer the command's AT and FP programs. At the center of the installation's program are the ATOs, assigned not to the garrison but to each of the battalions (and above), pulling, pushing, evaluating, assessing, documenting, and planning. There, uniformed members are expected to be trained and on written orders.

Regardless of the number of staff, where they are assigned, and full-time ATOs or persons performing FP as an additional duty, there must be well-researched, developed, coordinated, and exercised plans that are scalable and proportional to changes in the local threat and operational capability.

Improvements have been made in training for all of the Armed Services. Added to the list of annual training requirements is AT Level I. AT principles are included in precommand courses. ATO Level II has evolved into two parts, and the content has been updated. The course developers seriously applied the Training and Doctrine Command (TRADOC) Systems Approach to Training (SAT), and the resulting instruction bears witness to their focused efforts.

Most of us agree that the military's FP program has improved since 9/11. AT Strategic Goal 7, Objective 7B, is integration of AT into all officer, noncommissioned officer (NCO) professional military education (PME), and civilian training to ensure long-term development of knowledge and skills. Simplistically, this embodies synchronization and unification of effort. Embedding AT in all activities is a strategic initiative that has already paid off. Further measurable strides have been made in formal training for all the Armed Services. But as we have moved forward, the enemy has neither gone away nor remained static. We must do even more if we are to stay ahead of the insidious thoughts in a terrorist's mind. Now is the time to capitalize on established procedures and strategic initiatives and create an advocacy program.

What's in a Name?

The FP (or AT, if it goes that way) advocacy program could mirror the success of the Army Values program, where "LDRSHIP," complete with posters and pocket cards, is used to help soldiers remember the values.

"Force protection and antiterrorism needs to be a Military Occupational Skill (MOS) or an Additional Skill Identifier (ASI)." — LTC Stephen St. Clair

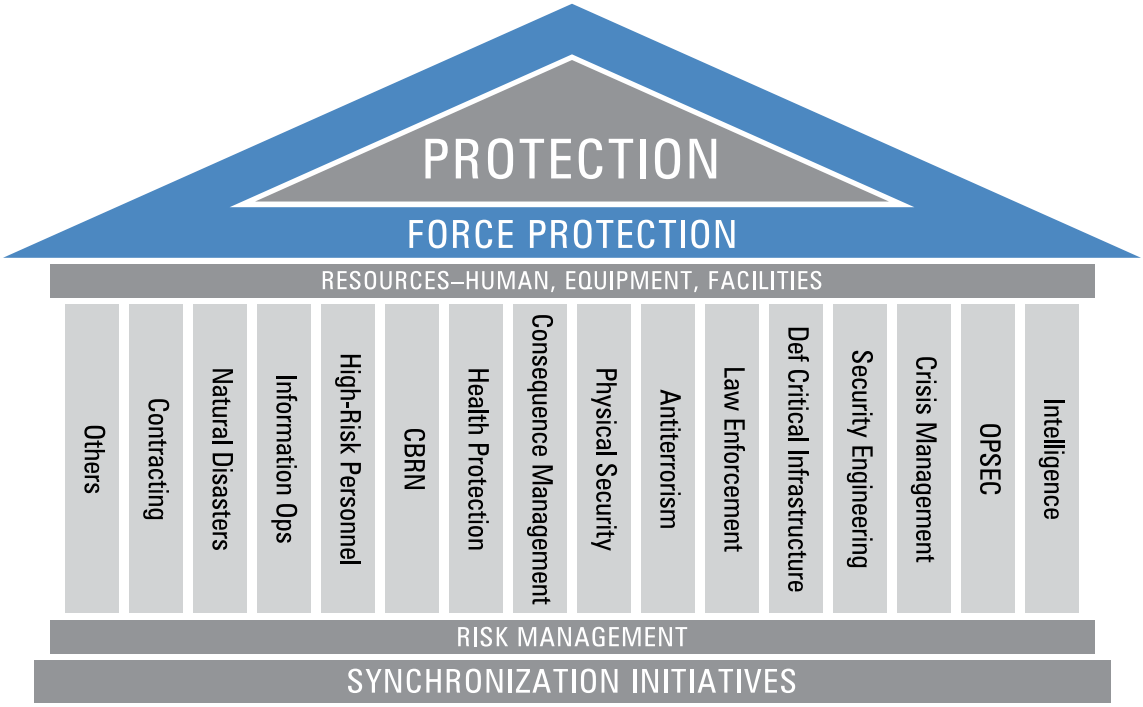
We will defer the actual memory words to the selected proponent (although we do like "Vigilant"), if anyone takes this initiative and moves it forward. Maybe an incentive award could be offered to the person, group, or organization with the best words for a memory jogger. A proponent is preferred in order to maximize resources. It makes little sense for organizations with the same needs and sparse resources to devote effort to the creation of similar programs that all can benefit from. While filling at least a portion of the protective-posture gap for off-installation facilities, this program could also benefit the additional duty ATOs within units on installations.

Second Initiative: Advocacy Program

Immediately following 9/11, citizens and particularly the military were gripped with an internal drive to do something. As never before, we experienced outrage over the incident and a range of emotions as we asked how could this have happened and what we can do to avenge and prevent another such strike. Our imaginations turned toward something akin to reveries of vigilance and fidelity. The subsequent "suspicious white powder" incidents fueled the fire for a while, but as time went on, there was an inevitable tendency to return to "normalcy." As a nation, we simply have not come to grips with the reality of terrorism.

The military departments have aggressively moved forward to establish protection programs. So why is it that we still have much more to do? This may be a reflection of the traditional approach to growing programs, sometimes displayed on a diagram of an FP building with a series of columns, and sometimes with a greater span representing a system of systems.

Although the FP castle concept is good as a starting point, we have yet to see the level of synchronization needed to achieve necessary efficiencies in funding, training, reporting and



sharing of information. Synchronization needs to go beyond the five traditional security program areas: Information Operations, Physical Security, Antiterrorism, Intelligence Support, and High-Risk Personnel Security. To maximize operational and fiscal efficiencies it also requires full synchronization with other related or supporting protection programs, including Continuity of Operations, Operations Security, Homeland Security and Emergency Preparedness, logistics and other contracting processes, construction, environmental assessments, prioritization of Mission Essential Functions (MEF), Organizational Inspection Program (OIP), and others. Without synchronization the columns are more accurately described by the term "stovepipes." Regardless of the efforts put into developing programs, synchronization is done by people, including people at the field level who do not have visibility of and coalitions within adjacent programs.

A potential weak link in the chain of FP program elements is the human factor, one of which may be a newly assigned, untrained, and overcommitted ATO; another is the lack of any actual on-the-ground, dedicated FP advocate at off-installation facilities. We consider the concept of an ASI to be one possible entryway to building a program that will be needed for the known future.

The ASI H3 Physical Security Specialist is underrated. Revamping and renaming the ASI needs to be given serious consideration. It may ultimately maximize effectiveness of training and improve protection of assets both here and in the overseas hot spots. While critical for units engaged in a war zone, where soldiers must carry the primary responsibility for FP, the ASI concept also has merit for soldiers in units preparing for deployment. Why is this important? It allows the commander to quickly locate and interview or select a trained and dedicated AT expert who serves as an advocate.

In presenting this concept, we have chosen the term "FP advocate" to identify the persons who intentionally or by default carry the FP mission. It is unlikely that a full-time, Level II–trained ATO is resident at the majority of these facilities. The nearest authorized ATO may be at a higher command or at a regional command in another state. There are thousands of separate facilities to protect, including the multiservice Armed Forces Reserve Centers (AFRC), Reserve Component Centers and Facilities, National Guard installations and armories, Corps of Engineers facilities, and recruiting stations. Only a very few are 24-hour operations; usually the facility commander is not full time; and has a sparse staff to maintain operations in support of the missions of the drilling Service members in residence on training weekends.

As we examine this initiative, we point out that civil service members and contractors have their part, particularly in stateside installations and facilities. But it is critical for deploying units to arrive at their assignments with a trained and experienced FP officer or ATO. So how do we establish the mechanisms to make FP and/or AT one of those highly sought-after, desired areas with not only due recognition but stability and effectiveness? In uniform or out, on the largest installations or at off-installation facilities, the need exists for advocacy beyond the ATO, other associated authorized staff, appointed (designated officials), and commanders.

Start With What We Have

Only on installations or bases and large commands is there at least one individual who occupies a position designated as ATO. Battalions and above are required by regulation to have an appointed ATO, but that individual may be performing other assigned duties. There cannot be an AT/FP program without a plan, and development of a plan has a human factor—the essence of the advocacy program. Today, a focal point for all of this is the individual designated to serve as the commander's FP program lead. Another of the many "Commander's Programs," AT is almost always coordinated and managed by the operations directorate. In theory, the provost marshal, intelligence, and security officers advise and support the operations officer, and by regulation, there is an ATO at battalion and above operating in a separate command structure. The program should then be drilled down by training initiatives to all unit members. In our view, one of the most important things we can do is establish and practice information exchange and test alert rosters.

Together with specific training, the broader application of education is perhaps one of the most important FP program elements we can do something about right away. Intelligence indicates that terrorists are currently looking for "soft targets," those places that are not expected to have strong physical security measures in place. Particularly where there is no full-time ATO, we should ask what assets the terrorist might target and why. Look at ease versus value and softness versus hardness.

An effective AT program requires integrating every soldier, civilian, and family member into the team. We start with common program goals: deter incidents, employ countermeasures, mitigate effects, and conduct incident recovery. When we eventually "defeat" terrorism, or, more realistically, prevent or minimize severity of the next attempt, we can still expect there to be other forces demanding our attention, including terrorist, criminal, or environmental threats. Our best efforts for performing operational missions while minimizing risk are through education, awareness, and universal involvement—in simple terms, the human factor.

Everyone must be an advocate, but the program still needs identified, proclaimed champions! This is not the commander; it is the commander with front-line representatives who are trained, motivated, confident, empowered, and recognized to initiate actions in accordance with approved plans. Soon others will see the value and say, "I'd be good at that!" Being the advocate champion, both in name and award through training, could parallel the obvious benefits that are associated with a sought-after ASI to those in uniform.

Various Real Challenges

Regardless of the best efforts and sustained heightened awareness of the possibility of additional attacks on homeland soil, our military is still unacceptably vulnerable to a destructive blow. The term *"unacceptably vulnerable"* suggests that data could be produced as validation. It is beyond the scope, intent, and security classification of this article to provide details of every time and place the authors have conducted or reviewed results of vulnerability assessments that have led us to that conclusion. Rather, we ask that you accept the possibility that the premise is correct and that further improvements can be made. It does not take much imagination to describe possible scenarios of wheeled vehicles running gates or of small, private aircraft flying over the "Almost Anywhere" National Forest to crash into a barracks, housing complex, headquarters building, or water treatment facility. The predictable and unpredictable consequences of losing 100 sons and daughters in basic military training on US soil are sobering.

Our best efforts for performing operational missions while minimizing risk are through education, awareness, and universal involvement—in simple terms, the human factor.

Plans are in place to increase authorized AT-personnel positions. But what does this really mean in precluding a terrorist incident? Picture the after-effects of a Fort Dix Six–type of operation planned and executed against a recruiting station. Imagine a community-friendly AFRC, with few if any of the FP standards developed for military installations in place, on a training weekend with several hundred Service members in residence. In a nightmare scenario, there is even a unit in the last hours of preparation for deployment, with military and civilian officials, a band, the American Legion, and family members lined up to wish their local heroes a safe departure and return from performing their duty to the nation; some of the community-friendly military facilities scattered across the nation do have fences and working gates, but without 24-hour operations, no one saw the bundle left under the reviewing stand at 0200 the night before.

In the years prior to the Global War on Terror, in an effort to enhance community relations and improve recruitment, some of the Reserve Components removed perimeter fences and relaxed procedures that are an inherent part of FP. There was little to no concern for stand-off distances, protection of utilities, access control, or the other basic tenets of FP. "Hometown, USA" is not immune from terrorist

threats; further attacks on the homeland are a real possibility.

Sometimes Reserve Component Service members are the only military presence that citizens in a community see on a regular basis. On training weekends, some Reserve Component facilities support more than 300 occupants—the number usually used to define an installation. It is not always apparent how to transform existing community-oriented facilities into hardened targets. What would we do with accurate CARVER or MSHARPP findings if we had them? Strict application of Unified Facilities Criteria may be either impossible or may simply not be considered cost-effective given the absence of threat and vulnerability assessments measured against the value of the assets.

At one DOD site, we watched a vendor drive through the open main gate and park next to the facility. More than 300 people were in the building at the time.

When There Is No Antiterrorism Officer

Assets in Northern Command area of operations are likely to transition to an all-hazards approach to FP, affecting staff positions and much more. Even the Core Vulnerability Assessment Management Program (CVAMP) is preparing to add the ability to report additional benchmarks. But whatever the modifications are and evolve to be, the FP program is an immutable, critical component. DOD-owned, -leased, or -managed facilities are now required to have an official who has FP responsibility for the DOD occupants and areas within the facility. "Designated official" (DO) is the term used for the individual with this responsibility. By reasonable inference, if someone is responsible, he or she is also accountable. But a DO will not have the training, experience, staff, and support infrastructure that the commander of a fortified power-projection installation does. What is absolutely necessary are plans that maximize all existing support elements and define triggers for realistic and rehearsed response.

An Installation's Program Is Not a Facility's Program

As we have pointed out, a potential weak link in this chain of FP program elements is the human factor. Often the lack of planned staffing, even for simple access control, leaves an off-installation facility wide open during work hours and unwatched after hours.

Not all off-installation assets have fences around the entire property or even around the more critical portions, and those that do may have decorative fences in order to blend into the community.

At one DOD site, we watched a vendor drive through the open main gate and park next to the facility. More than 300 people were in the building at the time.

During work hours there are simple procedures that could reduce but not eliminate the risk of unauthorized entry, but the message has either not been received or not been heeded. Without doubt, local law enforcement officers must be involved in the after-hours protection of these DOD facilities.

Unfortunately, there are many weak areas in the current state of preparedness. Providing FP at soft targets, such as stand-alone facilities, presents challenges. There are so many different types, purposes, and locations. Even conducting

At off-installation facilities, open access is typical.

vulnerability assessments—necessary not only for compliance with regulations and guidance but also to compete for resources by delineating requirements in CVAMP—is a challenge. Joint Staff Integrated Vulnerability Assessments (JSIVA) teams do not reach that far down into the unit or facility inventory. There is no secure communications system to allow input of assessments and requirements. Creating a term such as "DO" allows bypassing of the regulatory training requirements for an ATO (US Army Military Police School is the only source for this training). Thousands of DOs could be on a waiting list for AT Level II or other FP training that is still, at best, installation-centric—

and don't forget the "additional duty as assigned" reality.

As a rule, facility managers receive extremely valuable training and are often highly qualified for their traditional duties, but from an FP standpoint, the training is no more relevant than FPCON without site-specific barrier plans. Facility managers usually have links with the community, including fire departments and local police. They certainly know where the closest hospital is located. What they might not have is a written, higher headquarters–approved plan that addresses what to look for, report, and respond to: methods and mechanisms to prepare for any number of possible threats to their location and what can, should, or must be done when bad things threaten or occur.

What is needed for these critical individuals is an aggressive, progressive, enhancing, and realistic training program. Much training already exists, such as the Federal Emergency Management Agency's Community Emergency Response Team (CERT) training. Northern Command requires those assigned to take certain enhancing courses that could be included in the DO and ATO career development plan. Career development tied to grade increase, salary increase, and awards is a great motivator. More important, these FP practitioners deserve them.

Continuity of Operations or Other?

Depending on the local assets and unit missions, there may be good cause to lock the doors and go home in a elevated threat condition or incident aftermath. However, some of our most critical units are located in the Reserve Components, and not all of those units are housed in what could be considered fundamentally secure facilities. With the shift of competencies among Army components and among Defense departments, there is likely to be a mission-essential need to execute a continuity of operations (COOP) move or to quickly harden the facility. But creating and sustaining minifortresses in urban, suburban, and rural America to accommodate even a small percentage of the critical assets would also divert funding from other critical defense needs.

Even given enough funding, it is clear that not all existing off-installations could be hardened by applying current physical security and AT standards. Further, if the facilities were occupied and guarded 24/7, how would this affect such factors as communities, civil–military relations, and media coverage?

A possible alternative that has not received much attention is to prepare a portion of selected, nonsecure facilities to be hardened if and when necessary. Compartmentalization of information is a basic security measure, and it also makes sense for critical assets to be isolated from each other. The Corps of Engineers already employs the Modular Design System (MDS) when constructing new Reserve Component facilities, and AT construction standards are now a must for new construction. But what about the multitude of existing facilities for which even stand-off is not achievable? What if a "safe room" were designed for existing off-installation facilities? It may be possible and reasonable to create a place where, with little warning, the occupants could assemble, lock down, and alert local police and higher headquarters. Tiering the facilities based on assets housed, with well-thought-out but simple plans of action for characteristic threats, training and empowering the DO and key individuals, and testing communications, will go a long way toward improving our protective posture at off-installation facilities.

Summary

The fundamental issue is whether we are less vulnerable to the effects of criminal minds, terrorism, accidents, old or poorly planned infrastructure, or nature's whims than we were in the past. For now, we have to confront the possibility that we can be hurt, that it could happen anywhere, and that our best efforts to establish and maintain an effective program include a human factor. That we will benefit from having the right person functioning effectively where the next bad thing occurs is indisputable.

In presenting these concepts, we do not discount the heroic actions of individuals who are in the right place at the right time to prevent or lessen the impact of plans by an enemy that operates by rules foreign to our Western way of thinking and living. Strapping explosives around one's body or going up in flames with a vehicle bomb reflects a radical departure from how we believe humans should act. But America has always bred individuals who would lay down their lives for a greater good. What we have investigated and described in this article are enabling measures in the form of better training and support systems. What we need are realistic plans specific for the assets.

We proposed two initiatives with some suggestions for implementation: (1) Create an ASI for uniformed members serving as ATOs, elevating FP into a desirable assignment with continuity; and (2) establish a Force Protection Advocacy Program, supplementing commanders' guides and strategic plans, providing a common-sense solution for eyes and ears at off-installation facilities. These FP practitioners will be the ones who can name the "full spectrum of threat capabilities," from demonstrations to terrorist weapons of mass destruction and everything between, while expanding on what actions have been taken to protect the assets at their unit or facility. Is this everything needed for FP program maturation? Of course not. And yes, resources are involved. But these initiatives are obvious, necessary next steps and part of the way ahead to overall FP program effectiveness.

Transforming DOD Law Enforcement

By Lt Col Shannon W. Caudill, USAF, and Lt Col Bryan Keeling, USAF, Joint Staff, J-3

Military interventions are actually police functions, although warlike operations often ensue.

—US Marine Corps, Small Wars Manual[1]

Law enforcement (LE) expertise is a growing requirement in support of the Global War on Terror (GWOT) and an enabler to the warfighter in stability, security, transition, and reconstruction (SSTR), counterinsurgency and other combat operations. *The National Strategy for Combating Terrorism* states that LE is an instrument of national power on par with the traditional diplomatic, information, military, and economic (DIME) elements of American power.[2] Although not the federal lead for LE, DOD must integrate and support LE as a critical plank in the US effort to combat terrorism and as a growing enabler for combat operations in Iraq and Afghanistan. The problem, however, is that DOD has not designated a "top cop" with the vested authority to establish LE policy, to integrate and synchronize dispersed DOD LE operations, and to improve DOD's interagency coordination and cooperation within the federal LE enterprise.

DOD recognized this shortfall in 2006. Although the Department began establishing working groups to develop a DOD-wide suspicious activity reporting (SAR) process, a glaring vulnerability stood out to all involved: There was no one person who could speak authoritatively for DOD's LE community, develop and approve DOD-wide LE policy, and synchronize DOD's LE effort both within and outside the Department through the federal interagency LE construct. Recognizing this seam in DOD policy and operations, Deputy Secretary of Defense (DepSecDef) Gordon England tasked the Under Secretary of Defense for Intelligence (USD[I]) in October 2006 with facilitating the identification of a DOD LE Principal Staff Assistant (PSA).[3]

In January 2007, DOD's Office of the Secretary of Defense (OSD), Director, Administration and Management (OSD-DA&M), accepted the DOD LE PSA initiative from USD(I) and then conducted a July 2007 DOD-wide study of the current LE enterprise. OSD-DA&M is expected to make a recommendation on LE PSA assignment to DepSecDef England in 2008.

An examination of the challenges within the DOD LE enterprise reveals the need for an LE PSA. Services and other DOD LE agencies currently establish their own LE policies and use their own forms and documentation. DOD agencies, Services, and combatant commands have different LE procedures, databases, training standards, and processes. Each Service has a "stovepiped" LE data system, and none talk to the others or share database information with other federal or local LE agencies. Efforts to integrate DOD LE operations into the federal LE enterprise and

to improve interagency cooperation is ad hoc because there is no single point of contact for LE matters within DOD.

DOD LE enablers include, but are not limited to, skill sets supporting expeditionary forensics, law and order missions, sectarian violence investigations, foreign police training, and interagency LE integration and information sharing. LE is becoming a critical function supporting counterterrorism (CT) operations globally. The Army and Marine Corps Counterinsurgency Field Manual, FM 3–24/MCWP 3–33.5, specifically mentions using military police as foreign police trainers for the following skill sets: weapons handling, small-unit tactics, special weapons employment, convoy escort, riot control, traffic control, prisoner and detainee handling and processing, police intelligence, criminal intelligence, criminal handling, and police station management. Operationally, the Counterinsugency Field Manual envisions LE personnel as enablers of operations by "pushing human intelligence (HUMINT) or LE personnel to the battalion level and below" to "improve target exploitation (TAREX) and document exploitation (DOCEX) by tactical units," by conducting security operations, and by operating prolonged detention activities.[4] In short, commanders increasingly view LE expertise as a critical enabler of the warfighter and necessary to support the growing interagency effort to combat terrorism at home and abroad.

DOD LE must transform to maximize its impact on current DOD combat operations and to fully integrate into the US government interagency LE effort to defeat terrorism. Without an LE PSA, who will challenge traditional DOD LE capabilities and transform the DOD LE enterprise to improve its support to the warfighter? One National Defense University study on stabilization and reconstruction operations concluded:

> Does the United States need a new type of military police capability? The question is outside the scope of this study but deserves serious consideration. Other countries field national police forces that bridge a gap between their civilian and their military forces. The United States fills that gap with military police that are organized, trained and equipped to accompany military units to establish security in environments that range from quiet to hostile. However, they do not focus mainly on civil law enforcement missions.[5]

At home, DOD LE expertise and interagency coordination are key enablers to homeland defense and other mission areas of the US Northern Command (USNORTHCOM). The appointment of a DOD LE PSA will do much to improve service interoperability, federal LE integration, and interagency planning. DOD LE support includes the execution of the following in support of USNORTHCOM missions and operations: receiving, fusing, analyzing, and disseminating accurate, relevant, and timely LE threat information; planning and coordinating the employment of Defense Criminal Investigative Organizations (DCIOs) and other DOD LE organizations (to include military police and security forces); and executing required engagement and coordination with DOD and non-DOD LE agencies.[6]

The Stakeholders

DOD has a diverse and disjointed LE community, made more confusing by a variety of terminology to describe its various police entities. The US Army and Marine Corps refer to their LE patrolmen as *military police,* while the Air Force refers to police functions as *security forces;* the Navy calls them *masters-at-arms*. There are also civilian DOD police agencies providing LE services at various military installations and activities, including the Pentagon Force Protection Agency, which protects the Pentagon and other DOD sites in the National Capital Region.

Criminal investigations have even more diversity and varied jurisdictions. Within DOD, there are four federal LE agencies: the DOD Office of the Inspector General's (DOD IG's) Defense Criminal Investigative Service (DCIS), the United States Army Criminal Investigation Command (CID), the Naval Criminal Investigative Service (NCIS), and the US Air Force Office of Special Investigations (AFOSI). AFOSI and the NCIS are full-service investigative agencies, similar in function to the Federal Bureau of Investigation (FBI), with differing jurisdictions; they conduct criminal, counterintelligence, and counterterrorism operations and investigations. The Army bifurcates their investigative responsibilities between CID and Military Intelligence (MI). Army CID focuses on criminal investigations, whereas the MI component

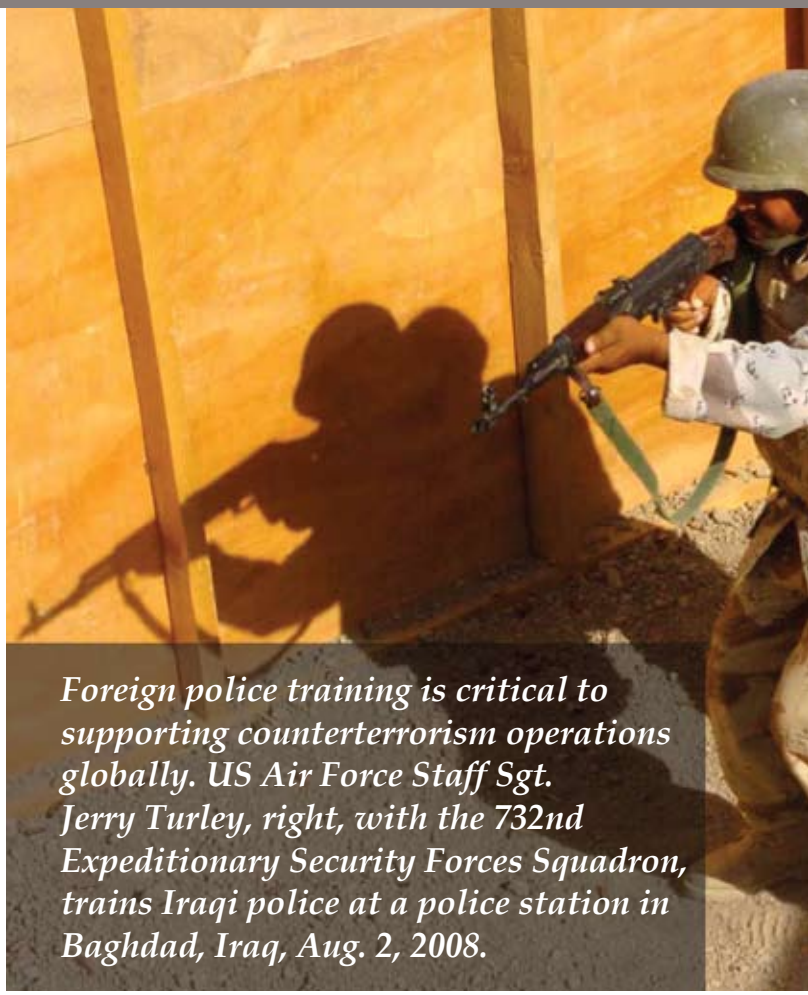
Iraq Police Day Ceremony

Iraqi Police Day is a new holiday in Iraq that was established to recognize the sacrifices of the Iraqi police in building a new democratic society and to celebrate the creation of a new Iraqi Police Service.

is responsible for counterintelligence and counterterrorism operations and investigations. Army MI is not a designated federal LE agency and has limited investigative authority as applied to counterintelligence and terrorism. The DOD IG's DCIS is primarily responsible for investigating DOD-level fraud, but since 9/11, it has expanded into other areas, including membership in select Joint Terrorism Task Forces. Specifically, they investigate large-scale defense contractors and fraud in ongoing DOD programs and operations that span two or more Services.

Excluding Title 18 of the US Code and Service-level criminal investigative policies, the Inspector General Act of 1978 is the only DOD-level document governing all DOD criminal investigative actions. Specifically, the act designates that "the Inspector General of the Department of Defense ... be the principal adviser to the Secretary of Defense for matters relating to the prevention of fraud, waste, and abuse in the programs and operations of the Department."[7] The law requires the DOD IG to report "fraud and other serious problems, abuses, and deficiencies" to the US Congress.

Additionally, each of the seven DOD combat support agencies maintain small elements of police, security, and criminal investigators who have LE authority and responsibility for maintaining law and order and investigating criminal acts within or against their respective agencies.[8]



Foreign police training is critical to supporting counterterrorism operations globally. US Air Force Staff Sgt. Jerry Turley, right, with the 732nd Expeditionary Security Forces Squadron, trains Iraqi police at a police station in Baghdad, Iraq, Aug. 2, 2008.

The Challenges

There are many challenges and opportunities for an LE PSA. Starting with the basics, there is currently no accepted DOD definition for "law enforcement."[9] DOD does define a "law enforcement agency" as an agency "*outside* [author's emphasis] the Department of Defense" that is "chartered and empowered to enforce US laws in the following jurisdictions: The United States, a state (or political subdivision) of the United States, a territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a host nation."[10]

The DOD LE study initiated by OSD-DA&M queried the Joint Staff, unified combatant commanders, Services, and other DOD entities with LE equities or interests, but the OSD-DA&M did not seek to develop a common definition of DOD LE. John F. Awtrey, Director, Office of LE Policy and Support, Office of the Under Secretary of Defense (Personnel and Readiness), has worked informally with the Services on a draft definition of DOD LE. While not definitive, the Joint Staff (J-34) provided an amended version of Awtrey's definition to OSD-DA&M to assist in conducting their LE PSA research:

> DOD LE is defined as crime prevention, detection, and response, criminal investigation, forensics analysis, apprehension and detention, pretrial and post-trial release, collection and maintenance of case files (prosecution and adjudication), correctional supervision or rehabilitation of accused and convicted persons, and collection, storage, and dissemination of criminal history record information and criminal intelligence, performed under federal (including the UCMJ), state, and local law, by authorized agencies/organizations, in order to protect the public safety. LE includes enforcing federal and state law, issuance of federal citations, detaining suspects, motor vehicle traffic management, traffic investigations, apprehension and restraint of offenders, and crowd control. This includes development of policy and plans for the training and employment of LE personnel, emergency response, and apprehension of persons who commit crimes, and confinement of pretrial and Level One offenders.[11]

Although certainly not inclusive of every aspect of LE skill sets and mission areas, Awtrey's definition provides a sound starting point for defining the parameters of LE for the new PSA. In addition to the

above definition, J-34 sent the following text to OSD-DA&M as part of the LE PSA study for consideration of the transformational issues affecting the DOD LE enterprise:

"LE is a key enabler to the Global War on Terror and includes deployable units performing law and order missions in a wartime environment, deployable forensics assets supporting the warfighter, threat information sharing, police training supporting security and stability operations, and investigations activities which provide criminal justice expertise to combat commanders.[1"2]

The need for a transformative, expeditionary DOD LE capability has become more critical as the GWOT has matured. A 2007 article in *Joint Force Quarterly* highlighted the need for DOD attention to LE capabilities in support of the GWOT:

> Even leaving aside the complexities of stabilization and reconstruction, addressing the direct threat requires the expertise and technological capabilities of law enforcement agencies, both in the conflict arena and great distances, in order to terminate or restrict support to terrorism. Moreover, the effective utilization of law enforcement capabilities requires cooperation of networks of not only law enforcement organizations but also military organizations across the globe.[13]

Lack of DOD LE Policy

Since DOD LE is undefined and has yet to be codified by any overarching DOD policymaker or guidance, it will undoubtedly result in friction with existing authorities, programs, and policies from other DOD offices. Programs with LE elements include Antiterrorism, Force Protection, Security, Counterintelligence, Counterespionage, Homeland Defense, Suspicious Activity Report, High-Risk Personnel, and the DOD polygraph program.

All of the aforementioned programs have codified DOD or joint definitions and/or have program authority vested in an appointed PSA or other designated policymaker who will certainly guard his or her areas of authority and parameters of jurisdiction. Developing a new DOD LE construct will be a challenge as the PSA establishes policies and budget authority for DOD LE programs on behalf of the OSD. It may also require analysis of existing portfolios and a study on whether some should migrate to the new LE PSA. For instance, does it make sense that the Under Secretary for Defense for Intelligence (USD[I]) is the PSA for physical security, a mission area that is heavily dependent on the use of LE expertise? Joint Publication 3–0, Joint Operations, states, "Functions *in physical security include* facility security, law enforcement, guard and patrol operations, special land and maritime security areas, and other physical security operations like military working dog operations or emergency and disaster response support."[14] These functions would seem to fit more squarely with an LE PSA than with an organization primarily focused on intelligence matters. Regardless, these types of policy and portfolio issues will need to be addressed in a thorough and thoughtful manner to ensure the LE PSA is vested with the proper authority to be effective.

Information Sharing

> We will continue to improve law enforcement capability, including greater and more effective collection and reporting of intelligence, without encroaching on the privacy and civil liberties of Americans, to interdict terrorists before they strike the Homeland.
>
> —White House, *9/11 Five Years Later: Successes and Challenges*[15]

DOD lacks an interoperable LE database to improve information sharing within the Department and among agencies. This absence creates a seam in which criminals and potential terrorists can operate. Currently, the Army uses the Centralized Operations Police Suite (COPS), the Air Force uses the Security Forces Management Information System (SFMIS), and the Navy uses Consolidated Law Enforcement Operations Center (CLEOC). Each of these programs provide the respective Service's police with a system for creating and maintaining police reports, incident management reports, and traffic violations. Additionally, each DOD criminal investigative agency independently maintains and operates case management systems to document investigations and leads, track evidence, and support trials for their

Services. None of the aforementioned systems can talk to the others. Terrorists and criminals can potentially navigate this seam by performing similar surveillance activities and committing criminal acts at multiple installations without other Services being aware of related police reports. DOD LE databases must be shared and interoperable.

Although all of the aforementioned LE information systems in DOD report through the Defense Incident-Based Reporting System (DIBRS) for uniform crime reporting (UCR) purposes to the FBI, UCR is used for crime analysis, not immediate "case solving." In order to fill this interoperability gap, there is an emerging effort to leverage the Navy's success with their Law Enforcement Information Exchange program to create an LE Defense Data Exchange (D-DEx). The first step for D-DEx will be to interactively link the four DCIOs. Once that step is successful, the other LE record management systems will be brought into D-DEx. At the same time, D-DEx will be molded into DOD's portal for consolidated criminal information sharing with the LE National Data Exchange (N-DEx).

Since DOD LE is undefined and has yet to be codified by any overarching DOD policymaker or guidance, it will undoubtedly result in friction with existing programs and policies from other DOD offices. Programs with LE elements include Antiterrorism, Force Protection, Security, Counterintelligence, Counterespionage, Homeland Defense, Suspicious Activity Report, High-Risk Personnel, and the DOD polygraph program.

Joint Training and Interoperability

DOD must improve the interoperability of DOD LE assets. Military police and investigators are high-demand, low-density assets in the GWOT. The US Army has utilized Air Force and Navy military police to fill its own manpower shortfalls in Iraq, placing a strain across the Services—a shared price in the GWOT.

A synthesis between military and police-trained units could significantly enhance the efficiency of stability operations.

—John F. Kennedy School of Government, Harvard University, and the US Army Judge Advocate General's Legal Center and School, *Implementing the Rule of Law and Human Rights in Stability Operations*[16]

An opportunity to improve interoperability can be found in streamlining and standardizing LE forms. The Services each have their own versions of a witness statement that, when compared, are essentially the same form in a different format. Standardized forms also enable a standardized data management system by establishing the same required data fields. Services provided in lieu of forces had to receive training on the use of Army forms so that the data could be entered into the Army's COPS data system. This redundant training, driven solely by a different form, can be overcome through the Services utilizing one form. This is not unprecedented, as DOD utilizes standardized forms for prisoner and detainee transfers.

The criminal investigative agencies have seen successes in joint training and interoperability, but most of the programs are linked to the DOD's intelligence apparatus, which historically limits LE potential due to the separation of LE and intelligence activities. Specifically, AFOSI, NCIS, and Army MI have benefited from joint counterintelligence and LE training under USD(I)'s Counterintelligence Field Activity (CIFA) Joint Counterintelligence Training Academy (JCITA). Additionally, AFOSI and NCIS are full interagency partners in using the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia. This common interagency training is serving as a foundation for future task force–type relationships that will pay large dividends for combatant commanders' mission execution of the GWOT.

The best, but relatively unknown, example of a predominantly DOD LE program that successfully combines joint and interagency training is CIFA's Defense Academy for Credibility Assessment (DACA). Since 1996, DACA (formerly known as the DOD Polygraph Institute) has served as the executive agent for all federal government polygraph training and certification.

Doctrine

Review, revision, and approval of new doctrine is critical to fully utilizing the operational capabilities and skill sets of DOD LE personnel. Joint doctrine

focuses military police and provost marshals on traditional roles and responsibilities. Since 9/11, building a DOD construct for LE operations and interagency integration has been ad hoc and done by trial and error.

Some Herculean efforts have been undertaken, but none has been codified with major changes to joint doctrine to capture how to best organize combatant commander LE expertise or to cement an interagency approach. The Joint Interagency Task Force–South (JIATF-South), for example, "provides a model of an interagency construct that fuses military, law enforcement, and intelligence operations into a unified organization under one leader."[17] The Joint Interagency Coordination Group (JIACG) provides another template from which to "closely align" the "US diplomatic, law enforcement, financial control, and intelligence sharing endeavors" and "establish a 'limited' JIACG capability in each combatant command."[18] An LE PSA–led effort to examine current LE-related doctrine will ensure combatant commands are organized effectively prior to a wartime crisis and will avoid the shortfalls produced by minimal interagency integration, as documented by a National Defense University Case Study:

> The law-enforcement community, however, enjoyed no formal relationship with Central Command (CENTCOM) prior to JIACG. In large part, this was because of the command's concerns about violating either the Posse Comitatus Act or intelligence oversight restrictions. The task, therefore, within multiple interagency environments and while still maintaining the tactical synergy achieved in Afghanistan, was to transform the combat-tested JIATF–Counterterrorism into a JIACG capable of developing the operational depth to coordinate theater-level planning and the strategic reach to shape national-level planning.[19]

The key to the long-term effectiveness and institutionalization of DOD and interagency LE expertise into combatant commands is the approval of doctrine that provides a template and an interagency framework that works prior to major operations occurring.

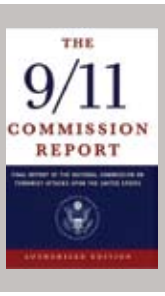
DOD Forensics

DOD has traditionally employed forensics to establish facts for criminal justice actions for use in a court of law or Uniform Code of Military Justice (UCMJ) proceeding or to identify human remains and determine manner of death. The GWOT has produced both legal and operational needs for forensics across the spectrum of combatant operations. Emerging warfighter requirements, however, transcend traditional forensics roles and provide the Joint Force Commander with a powerful tool in identifying enemy combatants and terrorist networks and other roles that enable his protection of the force through a greater understanding of his operating environment. DOD must maximize its use of forensic functions and capabilities to fully enable JFC on the battlefield. Despite the apparent value of a programmed forensic capability, neither the required capabilities nor the responsibilities to source these capabilities have been identified or validated, resulting in an ad hoc, incremental, and disjointed approach.

The majority of DOD forensics expertise and infrastructure comes from the LE community. The DOD Biometrics Community has supported and developed a forensics Capabilities-Based Assessment (CBA) and Concept of Operations (CONOPS) in an effort to kick-start a more comprehensive and integrated DOD approach supporting warfighter needs. Even though there is some overlap in areas like latent fingerprints, the DOD Biometrics Office recognizes that forensics is not a component of biometrics because forensics includes a whole suite of forensic science and LE expertise outside the scope of biometrics. In February 2008, OSD Acquisition, Technology and Logistics created a Forensics Executive Steering Group with three supporting working groups to begin work on improving and integrating the DOD forensics enterprise. Biometrics leadership acknowledges that a forensics PSA may be needed or that it may be appropriate for the LE PSA to include forensics in his portfolio of PSA responsibilities. This is certainly an important issue to the LE community because the core and enduring DOD forensics capability will remain in the LE community regardless of peacetime reductions of expeditionary forensics capabilities.

The 2007 DOD Forensics Workshop Report, published in September 2007 by the Army's Office of Provost Marshal, stated, "Finding 1: The failure to identify someone who performs functions like those of a Principal Staff Assistant or Executive Agent for forensics inhibits the development of policy, doctrine, uniform standards, training programs, planning, integration, coordination, prioritization, programming, budget execution, and acquisition; it also inhibits standardization across Service lines." The appointment of an LE PSA could provide the necessary leverage and management for the DOD forensics enterprise to fully develop forensics capabilities. As stated by Mr. Tom Dee, Director of the DOD Biometrics Office, "Forensics does not equal biometrics." This point is repeated by the DOD Biometrics leadership as they shepherd the forensics effort with the goal of handing it off to a PSA with forensics authority.

The GWOT has produced both legal and operational needs for forensics across the spectrum of combatant operations. DOD must maximize its use of forensic functions and capabilities to fully enable the Joint Force Commander on the battlefield.



Information procedures should provide incentives for sharing, to restore a balance between security and shared knowledge.

– The 9/11 Commission Report[20]

The Need for Interagency Integration

DOD LE must integrate into a common framework with the federal LE enterprise by sharing information, training, and expertise on multiple levels. Within legal limitations, the LE PSA's efforts must challenge old paradigms about DOD's integration and coordination with outside LE agencies at the international, federal, state, local, and tribal (American Indian) levels. This should include updating DOD Directive (DODD) 5525.5, DOD Cooperation with Civilian Law Enforcement Officials, last updated in December 1989.[21] The world has changed since the end of the Cold War, and the events of September 11, 2001, necessitate a complete reevaluation of DOD LE policy, just as has been done across the rest of the federal LE enterprise.

DOD LE entities must work with federal, state and local LE through Joint Terrorism Task Forces (JTTFs), for example, to maximize interagency information sharing and coordination within the United States. Joint Publication 3–0, Joint Operations, states that "a cooperative police program involving military and civilian law enforcement agencies is essential" to force protection efforts.[22]

According to the FBI, JTTFs are small cells of highly trained, locally based investigators, analysts, linguists, and other specialists from dozens of US LE and intelligence agencies. As of 2005, JTTFs were established in 100 cities nationwide, with 56 field offices and more than 3,723 members, including 2,196 special agents, 838 state or local LE officers, and 689 professionals from other government agencies (e.g., Department of Homeland Security, Central Intelligence Agency, Transportation Security Administration).[23] The DOD has more than 75 special agents and counterintelligence specialists assigned to 50 JTTFs around the nation.

The lack of an LE PSA is readily apparent to interagency partners. In January 2007, the Department of Justice's (DOJ) National Gang Intelligence Center (NGIC) released a controversial report entitled, *Gang-Related Activity in the US Armed Forces Increasing*.

General officers and a Senior Executive Service civilian representing the Army, Air Force, and Navy criminal investigative Services wrote a united letter to the Director of the FBI disputing some of the assertions and analysis. A major concern for the Services representatives was the lack of staffing prior to release of the report; however, without an LE PSA, other federal partners are left to wonder who they should staff LE matters to in DOD and who represents the true position and concerns of the DOD LE community.

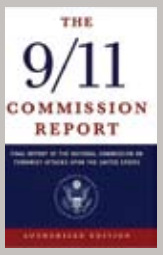
DOD must not only integrate its efforts operationally with other agencies but also with the larger federal LE database management and information-sharing effort. The national LE community has invested billions of dollars in database management and stores records in many different formats and technology platforms. To respond to this problem, the DOJ and the FBI's Criminal Justice Information Services (CJIS) division set the goal of creating N-DEx, a standard LE information-sharing system.

N-DEx is intended to enable timely and accurate LE information sharing across jurisdictional boundaries and to provide an advanced investigative tool in the fight against crime and terrorism. This system promises to provide nationwide connectivity to local, state, tribal, and federal LE systems, allowing users to search, link, analyze, and share information on a national basis. N-DEx will allow participating agencies to detect critical relationships between key evidence and information and will enable users to link data across jurisdictions. The ability to data mine the system for relevant facts and information will allow LE agencies to collaborate on an unprecedented scale. When an N-DEx user searches a person's name in the system, for example, N-DEx will automatically provide relevant links to information throughout the N-DEx user database and make correlations between "people, places, and things." All LE information shared through N-DEx will originate from local, state, tribal, and federal systems and will include incident and arrest reports, case files, booking reports, incarceration records, criminal histories, and other pertinent data.

Increment I of N-DEx became operational on March 19, 2008, and offers an estimated 50,000 users basic search-engine and correlation capabilities. DOD has executed a memorandum of understanding (MOU) with the FBI CJIS for N-DEx, and AFOSI is now DOD's first N-DEx user. In February 2009, Increment II is projected to double the number of users and to implement advanced research and analysis features. Increment III will increase the number of users to 200,000 and will implement a fully redundant system with full, advanced analysis tools linking databases to a wide range of criminal justice entities, including probation and parole databases.

> The development and deployment of N-DEx will provide nationwide capability to share information derived from incident, arrest and event reports. This will expedite coordination across law enforcement so that we can remain one step ahead of the criminals and terrorists despite jurisdictional boundaries.
>
> —Federal Bureau of Investigation[24]

The LE PSA has the opportunity to forge a new information-sharing alliance with federal, state, and local LE agencies, which will improve interagency cooperation and the overall protection of DOD installations and personnel. N-DEx offers DOD an opportunity to leap ahead in LE technology to ensure a common interface and information-sharing system for its LE database management. It provides the platform for DOJ and local LE information sharing. If fully exploited, it would ensure a common operating picture across the spectrum of LE surrounding a military installation. By migrating to a common LE database, a new N-DEx–based system would facilitate law-and-order and antiterrorism operations in the combatant commander's area of operation.



It is hard to "break down stovepipes" when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own.

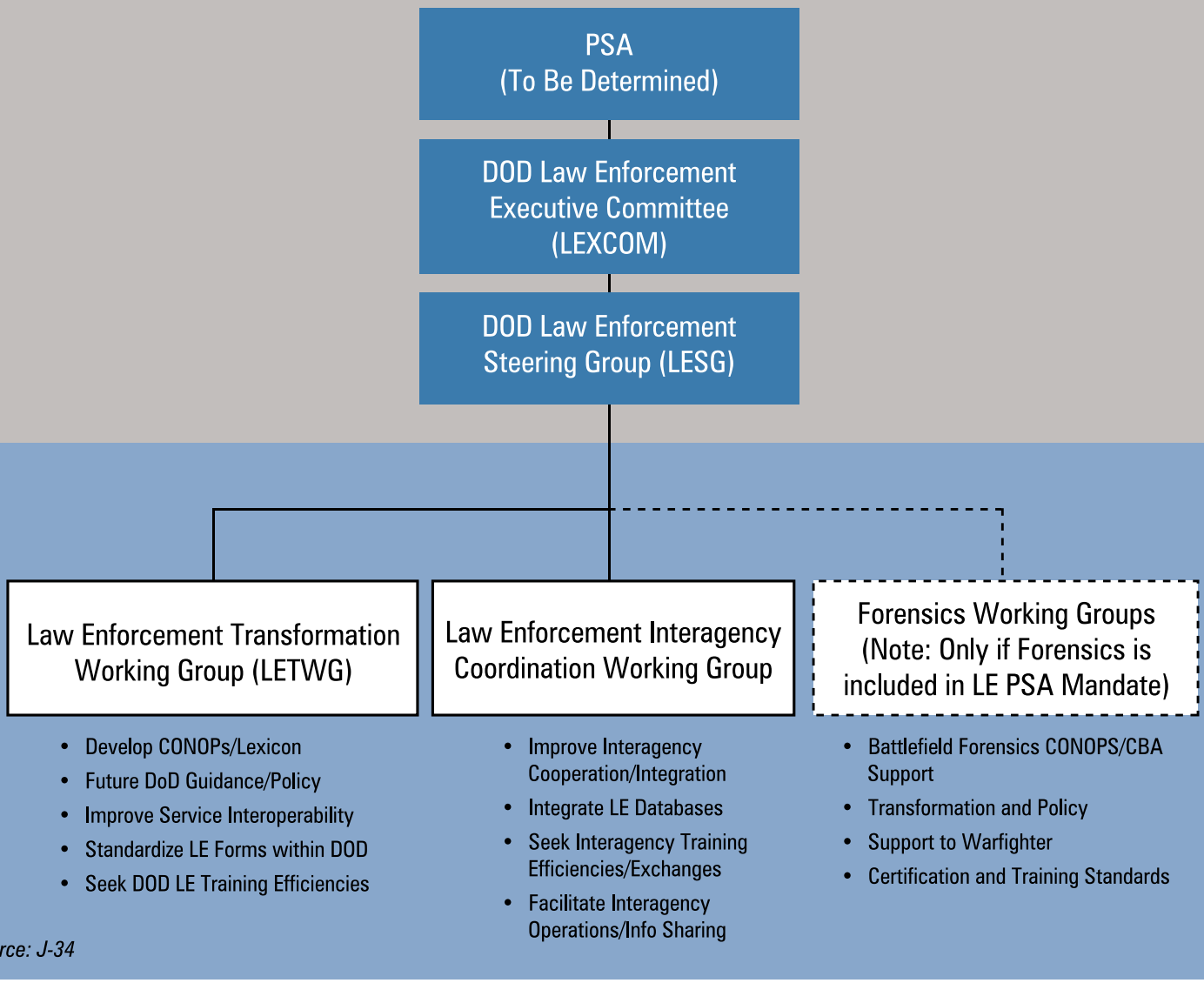
—*The 9/11 Commission Report*[25]

Cultural Barriers

LE agencies received a great deal of criticism in the wake of the 9/11 terrorist attacks regarding their failure to share information across the federal LE and intelligence enterprise. LE culture, outdated information-sharing protocols, and misunderstandings about federal intelligence statutes all contributed to this failure.

DOD LE culture shares many of the same traits as other federal and state LE organizations. LE personnel are very protective of their jurisdictions and distrust those outside their own organizations, even those in sister LE agencies. As a result, bureaucratic and jurisdictional rivalries create an environment in which cooperation becomes difficult and is typically based on informal professional relationships. An LE PSA will no doubt find that the various LE-related organizations in DOD share these same cultural traits and will resist efforts to forge a new DOD LE construct.

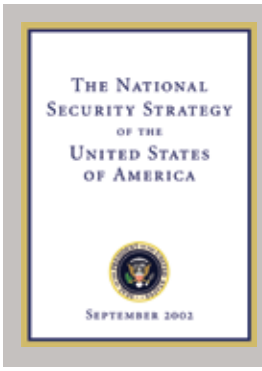
Proposed DOD Law Enforcement Management Infrastructure



Source: J-34

Moving Forward: Road Map for the New LE PSA

Once established, the DOD PSA should move quickly to establish a DOD LE governance structure. This will leverage LE expertise across the DOD LE enterprise and ensure compliance with proposed solutions sets and processes. J-34 proposes the management structure shown above as a notional template for the PSA to begin deliberations on a road-ahead strategy. It addresses policy issues through an LE Transformation Working Group and highlights the need to fully integrate with the federal LE establishment by standing up an LE Interagency Coordination Working Group. Additionally, it provides a means of incorporating the existing forensics working groups into the structure if forensics is indeed part of the LE PSA's mandate. Forensics Executive Steering Group members could be incorporated into either the LE Executive Committee or the LE Steering Group to ensure forensics equities are properly represented.



To defeat this threat we must make use of every tool in our arsenal—military power, better homeland defenses, *law enforcement* [author's emphasis], intelligence, and vigorous efforts to cut off terrorist financing.

—National Security Strategy of the United States, 2002

Summary

The appointment of a DOD LE PSA is a transformational necessity to strengthen DOD's LE enterprise; to fully exploit its LE expertise and skill sets in the GWOT, both overseas and in defending the homeland; to build a fully networked LE data system; and to support the warfighter. The appointment of an LE PSA holds promise in many areas. An LE PSA will ensure that DOD can deliver its considerable LE expertise to defeat terrorist networks, to better support the warfighter, and to increase information sharing with interagency and international partners.

Now is the time, in advance of the appointment of the DOD LE PSA, to identify the most pressing issues and to ensure a successful launch of this important work. It is critical to fully integrate DOD LE capabilities and expertise into the GWOT, both overseas and in the homeland. While there are many challenges to synchronizing and improving DOD LE operations, the fruits of this effort will integrate DOD both internally and externally into the larger national LE effort to win the GWOT.

1 US Marine Corps. FMFRP 12–15, Small Wars Manual, 1940. Available at: http://www.au.af.mil/au/awc/awcgate/swm/full.pdf

2 White House. *National Strategy for Combating Terrorism.* February 2003. Available at: http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism/counter_terrorism_strategy.pdf

3 Gordon England. "DOD Integrated Threat Reporting Working Group" [memorandum]. October 12, 2006.

4 Army Field Manual 3–24/Marine Corps Warfighting Publication 3–33.5, Counterinsurgency. December 2006. Available at: http://usacac.army.mil/cac/repository/materials/coin-fm3-24.pdf

5 Binnendijk, Hans, and Johnson, Stuart (eds.). "Transforming for Stabilization and Reconstruction Operations." Center for Technology and National Security Policy, 2004. Washington, DC: National Defense University Press. Available at: http://www.ndu.edu/ctnsp/S&R_book/S&R.pdf

6 USNORTHCOM. *Concept Of Execution: Law Enforcement Support Requirements.* July 20, 2006.

7 Title 5, Appendix, of the Inspector General Act Of 1978, 5 USCA Appx § 1 (2001) § 1. Available at: http://www.dodig.mil/IGInformation/igact.pdf

8 DODD 3000.06, Combat Support Agencies. July 10, 2007. Available at: http://www.dtic.mil/whs/directives/corres/pdf/300006p.pdf

9 Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms. April 12, 2001; amended October 17, 2007. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

10 Ibid.

11 John Awtrey. Personal e-mail to J-34. August 1, 2007.

12 Shannon Caudill. Personal e-mail to OSD-ODA&M. August 2, 2007.

13 Bowman, M.E. "Law Enforcement Technology, Intelligence, and the War on Terrorism." *Joint Force Quarterly,* 3rd quarter 2007. Available at: http://www.ndu.edu/inss/Press/jfq_pages/editions/i46/4.pdf

14 Joint Publication 3–0, Joint Operations. September 17, 2006; Change 1, February 13, 2008. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf

15 White House. *9/11 Five Years Later: Successes and Challenges.* September 2006. Available at: http://www.whitehouse.gov/nsc/waronterror/2006/waronterror0906.pdf

16 John F. Kennedy School of Government, Harvard University, and the US Army Judge Advocate General's Legal Center and School. "Implementing the Rule Of Law and Human Rights in Stability Operations" [workshop]. September 25–26, 2006. Available at: http://www.hks.harvard.edu/cchrp/pdf/September2006_RuleofLaw_ConferenceReport.pdf

17 Gorman, Martin J., and Krongard, Alexander. "A Goldwater-Nichols Act for the US Government; Institutionalizing the Interagency Process." *Joint Force Quarterly,* 4th quarter 2005. Available at: http://www.ndu.edu/inss/press/jfq_pages/editions/i39/i39_essaywin_02.pdf

18 US Joint Forces Command, Joint Warfighting Center. "Doctrinal Implications of the Joint Interagency Coordination Group (JIACG)." *Joint Doctrine Series,* Pamphlet 6, June 27, 2004. Available at: http://www.dtic.mil/doctrine/jel/other_pubs/jwfcpam6.pdf

19 Bogdanos, Matthew. "Transforming Joint Interagency Coordination: The Missing Link Between National Strategy and Operational Success,"*Case Studies in National Security Transformation,* Number 9. Available at: http://www.ndu.edu/jrac/docUploaded/NDU-Transforming%20IA%20Ops.pdf

20 The 9/11 Commission. *The 9/11 Commission Report.* July 22, 2004. Available at: http://govinfo.library.unt.edu/911/report/911Report.pdf

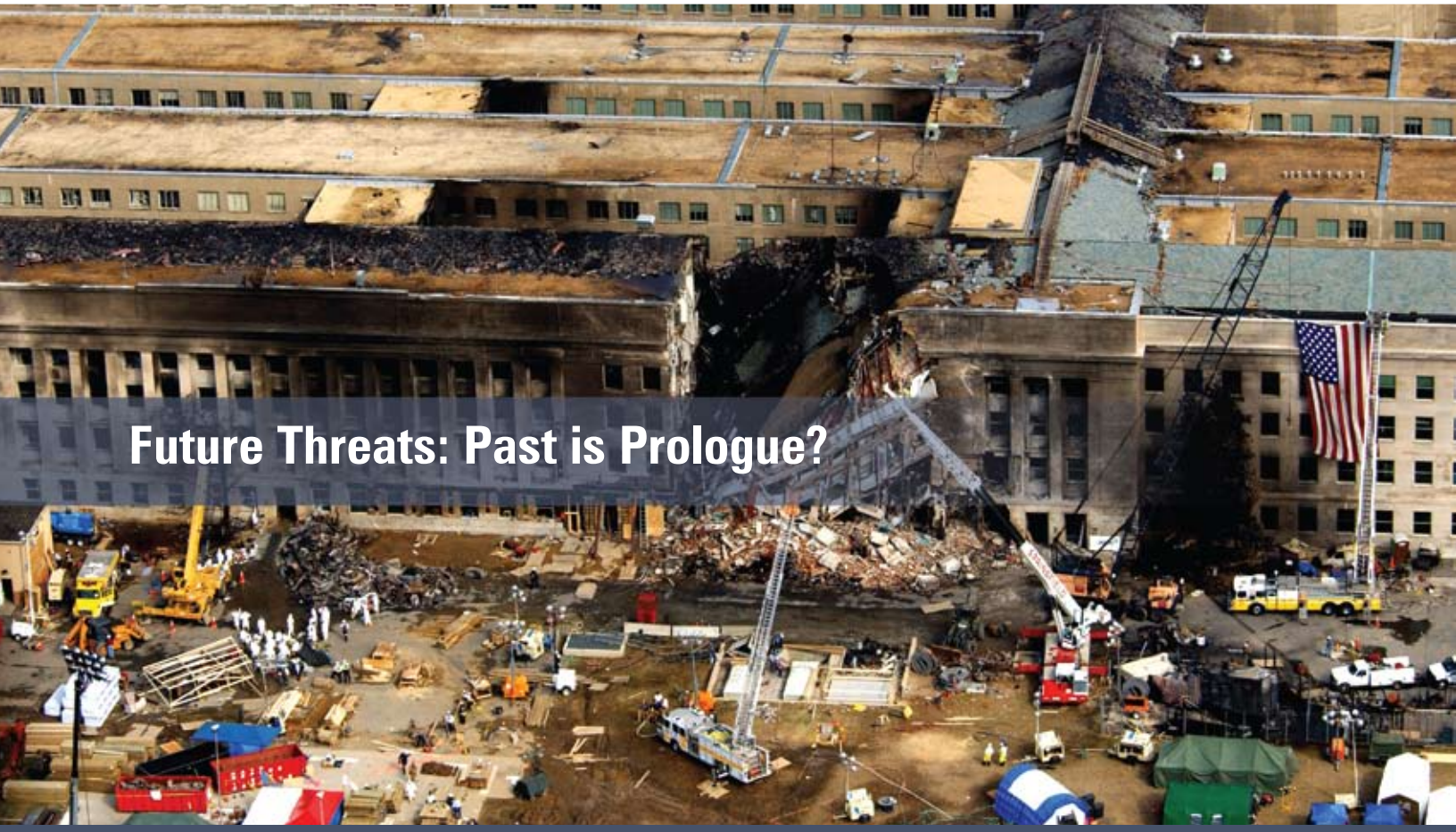
21 DODD 5525.5, DOD Cooperation with Civilian Law Enforcement Officials. December 20, 1989. Available at: http://www.dtic.mil/whs/directives/corres/pdf/552505p.pdf

22 Joint Publication 3–0, Joint Operations. September 17, 2006; Change 1, February 13, 2008. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_0.pdf

23 Federal Bureau of Investigation. *Protecting America Against Terrorist Attack: A Closer Look at the FBI's Joint Terrorism Task Forces.* December 1, 2004. Available at: http://www.fbi.gov/page2/dec04/jttf120114.htm

24 Federal Bureau of Investigation. "FBI Announces Contract Award in Information Sharing Program" [press release]. February 16 , 2007. Available at: http://www.fbi.gov/pressrel/pressrel07/ndex021607.htm

25 *Supra* at 20.



Future Threats: Past is Prologue?

By CDR Taylor Thorson, Joint Staff, J-3

On September 11, 2001, the threat of terrorism jumped to the forefront as the premier national security threat. Two major combat operations ensued as well as several smaller military ventures into places such as the Philippines and East Africa. The increased attention to force protection (FP) and antiterrorism (AT) brought large amounts of money to procure and support FP efforts for DOD forces and installations. An analysis of past attacks against DOD personnel and emerging tactics of terrorists around the world suggests that these resources might not be countering the correct threat.

This article will briefly discuss the historic threat to DOD. It will also provide examples of recent, successful terror attacks that occurred outside the continental United States (OCONUS) and that are outside the "norm" of typical threats perceived against DOD installations. Examples from Iraq and Afghanistan are also included to highlight the threats from suicide bombers and vehicle-borne improvised explosive devices (VBIEDs). Through this lens, the future threat to DOD installations, particularly those within the continental United States (CONUS), will be analyzed. A brief description of the Main Gate Paradox will be followed by a discussion of the continuing threat to off-post DOD personnel. The conclusion will highlight important questions for the AT/FP community to consider as it determines future resource allocation.

The Historic Threat

The overwhelming majority of attacks against DOD since 1960 have taken the form of kidnappings, assassinations, or bombings that target DOD personnel off installation.[1] Four horrific attacks, however, dominate the protection psyche: 9/11; the attack on the USS COLE; the Khobar towers bombing; and the 1983 attack on the Marine barracks in Beirut, Lebanon. From a strictly DOD perspective, the 1983 attack produced the most casualties, while the 9/11 attack on the Pentagon was the most damaging in terms of psychological and financial harm.

The DOD defines *terrorism* as "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."[2] It is important, however, to keep in mind that the governments and societies that are intimidated may not be within the targeted demographic. It can

be argued, for example, that the 9/11 attacks had multiple intended audiences, and not just the United States. These intended audiences include the "West" writ large, Muslim governments and societies, and

Khobar Towers VBIED Crater

Source: www.defenselink.mil

other terror groups. Some terrorist organizations merely need to complete an attack to affect a completely separate constituency and gain further funding or increase credibility or leverage. The West will not ordinarily be coerced by terror; therefore, it is important to truly be cognizant of the intended audience when examining terror attacks. Not every terror attack is against a symbolic or high-value target. Similarly, the body of evidence supports the theory that an attack will not normally produce massive casualties; many times, the images of the attack and its aftermath produce the desired effect. Recent terrorist attacks in Algeria and Russia bear this out.

Preparing rockets to be fired into Israel

Source: http://www.weaponsurvey.com/missilesrockets.htm

Security improvements have focused on implementing long-standing Force Protection Condition (FPCON) measures that are personnel intensive while constructing long-term barriers for traffic and personnel flow. In addition, efforts are underway to be able to identify every person that enters a military installation. To save personnel cost and to reduce risk to security forces, myriad efforts are being undertaken to introduce robotic vehicles, remote weapons, and sensor arrays to detect infiltration. Clearly, the emphasis is on protecting forces inside the perimeter of the installation, both inside CONUS and OCONUS, despite the historical precedents.

Recent Attacks

In a new twist, the Fort Dix Six were going to take advantage of the seam of protection between off-base and on-base by targeting DOD personnel as they entered the base. The terrorists then planned to enter the post to cause further casualties. This technique was not new and was demonstrated in 1993 in an attack against Central Intelligence Agency (CIA) employees in Langley, Virginia. The Fort Dix Six group was going to take the carnage to a much greater level. Few current efforts would have reduced this threat, short of greater manpower and firepower at the front gate of the installation.

In May of 2002, al Qaeda operatives launched a MANPAD at a US fighter operating out of a Saudi Arabian air base.[3] There have been multiple attempts using various MANPADs against allied aircraft in Iraq and Afghanistan. Attacks against civilian aircraft include a missile strike on a DHL cargo aircraft in 2003[4] and an attempted missile strike on an Israeli airliner in 2002.[5]

Spectacular attacks against Israeli forces offer a window on the future threat. On December 12, 2004, terrorists destroyed an Israeli outpost after digging 800 yards and placing 1.5 tons of explosives under the outpost.[6] The many attacks against Israeli mass transit, as well as the London 7/7 bombing, also prove worrisome.

State-sponsored groups such as Hamas that continually use Qassam rockets against Sderot, Israel, and Hezbollah's bombardment of northern Israel during the brief Israeli incursion into Lebanon in 2006 also may augur further attacks against DOD facilities and personnel.

Iraq and Afghanistan

The insurgency in Iraq has presented two unique terror phenomena: the use of chlorine VBIEDs and indirect fire (IDF; primarily mortars) on DOD installations. The remainder of the attacks in Iraq are primarily the same techniques used prior to 9/11: kidnappings, small arms, and explosives used against DOD personnel off installation. Direct attacks using large VBIEDs against Joint Security Stations and other buildings in Iraq are similar to the 1983 Beirut attack, but because of the design of the facilities and proactive rules of engagement (ROE), the attacks have not produced the same levels of casualties.

The situations in Iraq and Afghanistan are different from threats against forces in other countries and in the United States. The tactics, techniques, and procedures learned by the terrorists from this and other conflicts can, however, be easily adapted for attacks against DOD personnel.

The Future Threat Against DOD Installations

Current FP efforts are tailored primarily to one type of threat: the design basis threat (DBT), which is centered around detecting and mitigating the VBIED. While this may be the most likely threat against DOD installations, it is not the only threat to DOD personnel and facilities and it is not the most damaging. Overall, the terrorists have not sought to affect the continuity of operations for DOD; they have sought to produce the kind of horrific, symbolic attack that maximizes casualties and furthers their cause.

Terrorist actions around the world indicate that it is necessary for DOD to prepare for non-DBT attacks such as IDF, rudimentary chemical attacks, and squad-sized assaults. IDF assaults are currently used by terrorists in such places as the Palestinian territories, Lebanon, Iraq, Afghanistan, Chechnya, Yemen, and Saudi Arabia. Chemical attacks are currently being carried out in Iraq, and the world witnessed the terrifying ramifications of the sarin attack in Tokyo, Japan, in 1995. Squad-sized assaults are being carried out in countries such as Mali, Algeria, Saudi Arabia, Yemen, Iraq, Afghanistan, Chechnya, Turkey, and Thailand (and almost in the United States at Fort Dix).

As main gates (and all entry control points) become hardened, attackers will likely be forced to pursue different courses of action. Although forcing the attackers to "Plan B" may be considered a success, it may also steer the attackers to less protected targets outside the facility or to access the facility through routes other than the ECP.

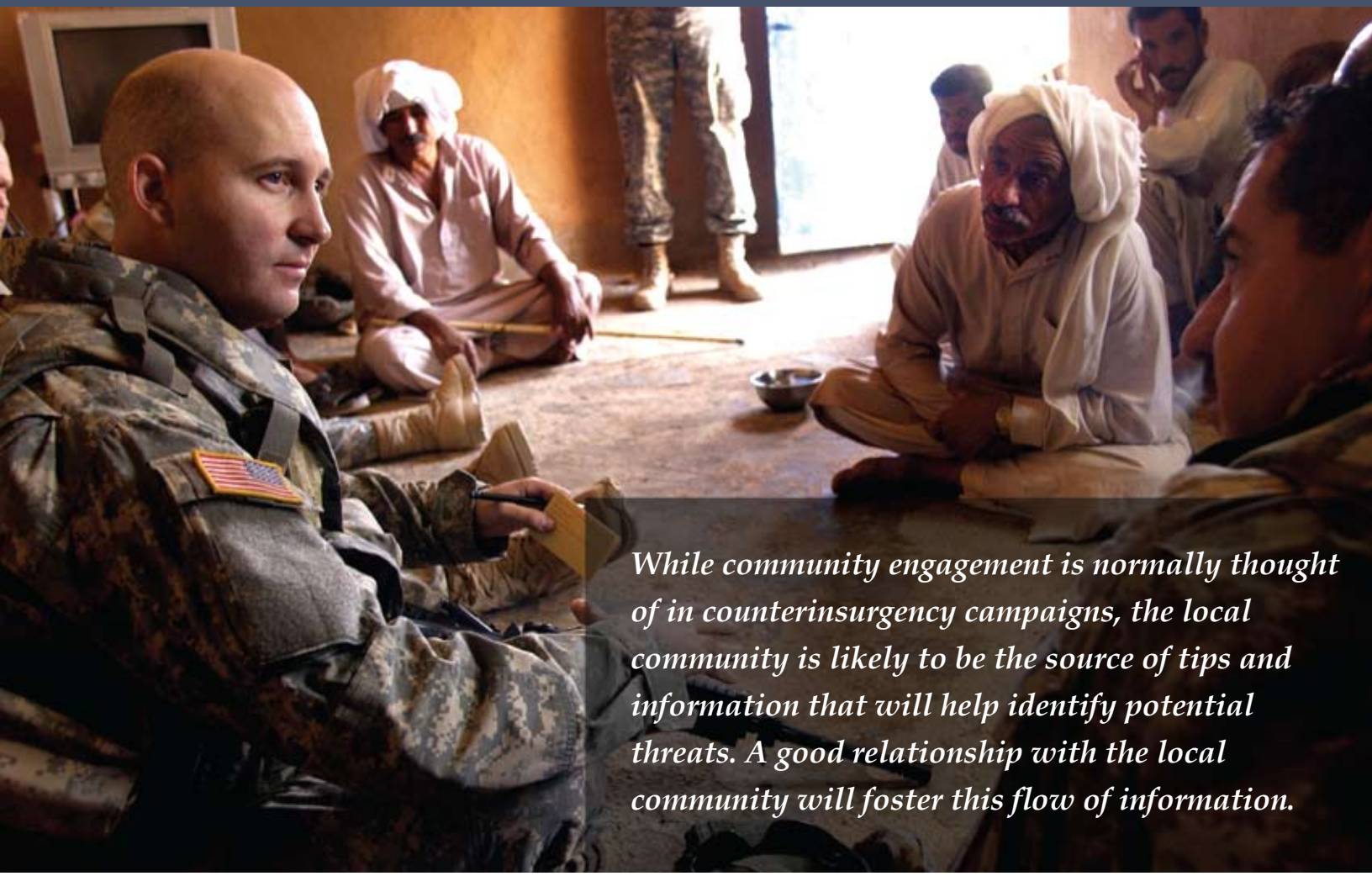
While two out of three of these threats have not surfaced in the United States, it is important to begin to discuss how an installation would deal with these threats if presented. Home-grown extremists and "sleeper cells" that are already in the United States can easily learn from the myriad examples throughout the world. IDF attacks are primarily from mortars and rocket attacks. Googling "home made mortars" yielded more than 2 million hits (not all were for IDF weapons). Both Hamas and Hezbollah can easily provide the know-how to make home-made rockets and warheads. Chlorine precursors (and the chemical itself) are readily available (try Googling "how to make chlorine gas"). The arrest of the Fort Dix Six and countless criminals can attest to the availability of assault weapons and the ease with which they are made fully automatic.

The Main Gate Paradox

There is a certain irony that as main gates (and all entry control points [ECP]) become hardened, attackers will likely be forced to pursue different courses of action. This change in attack methodology may actually lead to more catastrophic attacks. Although forcing the attackers to "Plan B" may be considered a success, it may also steer the attackers to less protected targets outside the facility or to access the facility through routes other than the ECP. Multimillion-dollar nonintrusive inspection systems are being considered for many installations. It is doubtful that a terrorist in a large VBIED is going to purposefully drive into the inspection lane only to be found carrying thousands of pounds of military or home-made explosives. The attacker will be forced to find an alternate method of gaining access that may involve a complex attack against the main gate to allow the vehicle to enter, to choose an easier target set, or to target the main gate.

It is also important to consider whether the major investments in the main ECP make the main gate the target. If one considers rate of return, symbolic value, and seams in jurisdiction and protection, the main gate can be a lucrative target. A large crater and casualties at the entrance to an installation may be powerful enough for the intended audience and may be considered a success despite DOD public affairs efforts to label it a success in force protection.

VBIED attacks in CONUS are not without precedent. In CONUS, the 1995 attack on the Murrah federal office building conjures up horrific images of extremist destruction; however, this attack was not the first VBIED attack in the United States. In 1970, Karl Armstrong used more than 2,000 pounds of fuel-oil soaked ammonium nitrate fertilizer in an attempt to destroy a federally funded laboratory at the University of Wisconsin; the attempt killed one and damaged 26 buildings.[7] In 1990, Dean Hicks planted a bomb inside a vehicle in Los Angeles, California, that "could have leveled two city blocks" if it had detonated; luckily, it did not.[8] In contrast, the Murrah bombing used 4,000 pounds of explosive.[9] For those who think attacks of



While community engagement is normally thought of in counterinsurgency campaigns, the local community is likely to be the source of tips and information that will help identify potential threats. A good relationship with the local community will foster this flow of information.

this magnitude cannot recur, consider that the federal government and most states have yet to restrict or control the purchase of ammonium nitrate. Indeed, in a 2006 press release, Senator Charles Schumer (D-NY) highlighted New York Police Department officers who posed as ordinary citizens and were able to purchase 1,400 pounds of ammonium nitrate.[10]

Off-Post Threats

While hardening the installation presents many challenges, it is important to remember that the need to protect DOD personnel extends well beyond the base perimeter. A good case in point is the 1986 attack against Servicemen at a restaurant in Germany, an event which finally drove US air strikes against Libya. Millions of dollars are being spent to protect the base and its contents, but little outside of Level 1 AT training is done for threats outside the perimeter. Understandably, the security of citizens outside "the wire" rests with civilian authorities, and their resources have been increased to counter the threat; however, commanders are still responsible for adequately protecting their personnel.

This can be accomplished through an effective community engagement plan. While community engagement is normally thought of in counterinsurgency campaigns, the local community is likely to be the source of tips and information that will help identify potential threats. A good relationship with the local community will foster this flow of information. In addition, local and state law enforcement should be kept fully in the loop, not only invited to installation threat working groups but also readily informed of intelligence and analysis of the threat.

If the primary threat exists off post (and, historically, it does), should the local establishments that routinely cater to DOD personnel be assessed for vulnerabilities? Although some might answer that such action is beyond the scope of DOD, the true solution needs to be shared between DOD and law enforcement. In periods of increased threat, should some of the more vulnerable off-post bars, restaurants, and facilities be avoided, even those inside the United States? If so, how would this information be disseminated? FPCON measure CHARLIE 10 specifies that part of this effort is to "coordinate any other precautionary measures taken outside the installation perimeter."[11] The impetus behind implementing FPCON CHARLIE is that "an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel

or facilities is likely."[12] This intelligence can be very difficult to obtain. The likelihood that such threats will be reported increases with good community relations. This measure may be considered in certain circumstances when the threat may not be so palpable as to drive FPCON CHARLIE, but enough suggestion exists for concern.

It is also important to educate DOD personnel and their dependents about off-post vulnerabilities. Although the vast majority of threats are improbable, education is the only method for raising awareness and possibly thwarting the efforts of the terrorists.

Conclusion

There is a multitude of possible threats that face DOD personnel, equipment, and installations. Fortunately, few have found their way to the United States. The historical and current examples of terrorism and insurgency provide many illustrative examples on how to successfully conduct an attack, and DOD forces must be prepared to neutralize and respond to them.

Countering the threat must begin with a realistic educational curriculum. The current Level 1 AT awareness training contains many examples of past attacks against DOD personnel. This good foundation can be expanded outside of Level 1 to include recent kidnappings, VBIED attacks, and sniper awareness. People must be educated without being alarmed: The curriculum must present reasonable actions to take in particular events and provide awareness to inform law enforcement if surveillance or attack planning is being undertaken by a terrorist group.

Threat working group members must also be made aware of the likelihood and consequences of IDF attacks, rudimentary chemical attacks, MANPAD attacks at air fields, and squad-size assaults. At minimum, table-top exercises ("wargaming") should also be conducted to discuss responses to those threats. Although resource constraints will not provide complete protection, identifying ways to mitigate threats (and to assist in recovery) via training may prove useful. DOD should not accept another "failure of imagination" in preparing for, responding to, and recovering from attacks. Local law enforcement and first responders must also be made aware of the threat and how to recover from these incidents. A few questions come to mind: If a military facility is attacked via Qassam rockets, will the response force go to the identified launch area or to the attack site or both? Are procedures in place to prevent fratricide between military quick response forces and local law enforcement? Have the issues of legal authority and ROE inside CONUS been sufficiently addressed?

Services, defense agencies, combatant commands, and others are working on detecting many of these threats and mitigating their effects. Many of the current solutions utilize technology to make more efficient use of personnel or to downsize personnel ranks. Before any reduction in manpower (or manned capability like incident response or threat nullification) is pursued, the question must be asked whether the system to be procured reduces overall capability in pursuit of an increase in capability against a particular threat. The solutions against most of the threats mentioned in this article are manpower intensive.

DOD has greatly increased its protection mindset since the four major terror attacks. The efforts taken have made DOD forces and installations safer. These four attacks, however, should not dominate the protection mindset. Recent examples of non-IED attacks should help DOD adjust its approaches and responses to the omnipresent threat of terror attacks and begin to develop solutions and recovery plans for such attacks.

---

1 US Army. "Timeline of Terrorism." Available at www.army.mil/terrorism

2 Joint Publication 1–02. *Department of Defense Dictionary of Military and Associated Terms*. April 12, 2001 (as amended through May 30, 2008).

3 MacFarquhar, Neil. "Saudi Arabia Arrests 13 Men Tied to Attack on a U.S. Base." *New York Times*, June 19, 2002. Available at http://query.nytimes.com/gst/fullpage.html?res=9B05E0D9163FF93AA25755C0A9649C8B63

4 Space Daily. "DHL Aircraft Hit by Missile over Baghdad Had Lost All Hydraulics." December 8, 2003. Available at http://www.spacedaily.com/news/iraq-03a.html

5 CNN. "Israeli Report Links Kenya Terrorist to al Qaeda." November 29, 2002. Available at http://archives.cnn.com/2002/WORLD/africa/11/28/kenya.israel/

6 Plushnick-Masti, Ramit. "Holes Plentiful in Israel's Expensive Tunnel-Finding Defense Technology." *USA Today,* December 13, 2004. Available at http://www.usatoday.com/tech/world/2004-12-13-tunnel-tech-fails_x.htm

7 Capital Newspapers. "Sterling Hall Bombing." Available at http://www.madison.com/library/LEE/sterlinghall.html

8 Associated Press. "Man Angry at the I.R.S. Admits Bombings." *New York Times,* August 17, 1991. Available at http://query.nytimes.com/gst/fullpage.html?res=9D0CEFDD1338F934A2575BC0A967958260

9 Kenworthy, Tom. "Prosecution Rests in McVeigh Trial." *Washington Post,* May 22, 1997. Available at http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/prosecution.htm

10 Schumer, Senator Charles E. "Schumer: Fed Paralysis Undermines Ability to Stop Large Bombs from Being Built – Demonstrated Ability of NYPD to Build 2400 lb Ammonium Nitrate Bomb with Ease Shows Need for Action" [press release,] September 18, 2006. Available at http://www.senate.gov/~schumer/SchumerWebsite/pressroom/record.cfm?id=263230

11 DOD Instruction (DODI) 2000.16. DOD Antiterrorism Standards. December 8, 2006. p. 44.

12 DODI 2000.16. DOD Antiterrorism Standards. December 8, 2006. p. 39.

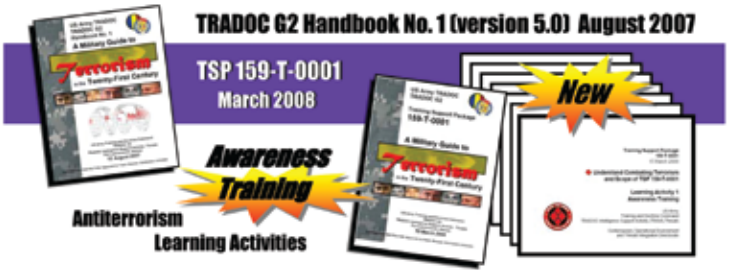
Terrorism Awareness in Today's Operational Environment

By Jon H. Moilanen

Introducing a Terrorism Awareness Training Support Package

As US joint forces fight a War on Terror (WOT), understanding the enemy and acts of terrorism is critical to the antiterrorism and counterterrorism mission success of friendly forces, allies, and coalition partners. *Training Support Package* (TSP) 159-T-0001, published by the US Army Training and Doctrine Command (TRADOC) in March 2008, presents situational awareness of the terrorism threat in a broad perspective related to the contemporary operational environment (COE). The COE is a realistic combination of current and near-term operational-environment variables with a capabilities-based composite of potential adversaries.[1] This assessment projects the circumstances and influences that confront US military forces in managing risk, training for unit readiness, educating leaders, and protecting the force. Offensive, defensive, and stability operations challenged by terrorism will continue to be a norm for the foreseeable future in complex and uncertain settings.

To provide clear awareness and understanding of foreign and domestic terrorism threats to the United States, TRADOC publishes a series of unclassified handbooks that support individual and organizational training, institutional joint professional military education, and operational missions. The TRADOC G2 focuses these handbooks with a "threats" perspective on terrorism. TSP 159-T-0001, A Military Guide to Terrorism in the Twenty-First Century, is a concise, unclassified TSP on terrorist capabilities and limitations that indicate possible and probable enemy actions against the United States in the homeland and abroad. This TSP complements TRADOC G2 Handbook No. 1, *A Military Guide to Terrorism in the Twenty-First Century* (version 5.0), dated August 15, 2007. This TRADOC capstone terrorism handbook is a user-friendly support tool to train, educate, and conduct antiterrorism and force protection to Army standards.[2]



TRADOC G2 Handbook No. 1 and TSP 159-T-0001

The TRADOC Intelligence Support Activity (TRISA), an organizational agent of the TRADOC G2, operates with an Army charter to produce doctrinal material that describes an opposing force (OPFOR) as the common opponent for all Army training.

OPFOR doctrine and related instructional material present conditions to stress selected US Army training objectives and decision-making process with applied lessons learned and insights from an uncompromising and adaptive adversary.[3] Contemporary observation of enemy patterns and trends are incorporated into OPFOR doctrine to develop and maintain US Army operational and institutional readiness with realistic conditions of the operational environment.

Commanders, organizational leaders, and other military or civilian members can use the TSP and other TRADOC G2 handbooks to understand the perspective and operational opportunities of a threat. More important, Army training and readiness can focus on critical tasks to deter, dissuade, or counter acts of terrorism.

Commanders, organizational leaders, and other military or civilian members can use the TSP and other TRADOC G2 handbooks to understand the perspective and operational opportunities of a threat.

Applying TSP 159-T-0001 for Threat Awareness

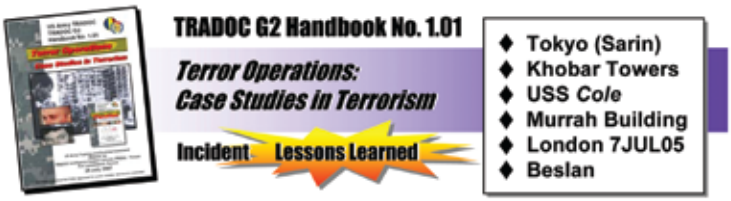
The TSP is very versatile for a training audience, an educational setting, or an operational mission. The TSP focuses on one terminal learning objective (TLO) supported by seven learning activities. Each learning activity displays concise notes and a graphic training-aid packet. The TLO is to recognize foreign and domestic terrorism threats to US Army forces in the COE.

Conditions for TSP use are flexible and can range from small- or large-group instruction to self-paced individual study on current and predicted terrorism threats in the US homeland and other combatant command areas of responsibility. Vignettes include possible US Army vulnerability to terrorism effects during Army operational and institutional missions. The standard of individual performance is to determine terrorism capabilities and limitations in terms of terrorist motivations and behavior, organizational models, and targeting challenges against US military forces. Awareness training is not formally tested; however, the TSP can present topics in a sequential manner or be organized for selective reading, study, and review of specific learning activities. Knowledge can be applied during the insights of a professional mentoring session, the details of a robust training scenario, or the lessons learned from historical terrorist incidents in an ongoing area of combat or stability operations.

Each TSP learning activity has one "learning feedback" slide and one "learning summary" slide for immediate self-assessment of learning activity themes. The TSP and its learning activities are provided in two formats. A Portable Document Format (PDF; i.e., file suffix .pdf) condenses byte space for efficient transfer or storage, while the PowerPoint (i.e., file suffix .ppt) format allows easy tailoring of text or graphics. When a learning activity displays as a slideshow in PowerPoint, an animation feature progresses sequentially through each feedback question and answers appear as a "fade in and remain" text image based on self-paced clicks on the computer mouse.

The TRISA website at https://dcsint-threats.leavenworth.army.mil provides a TSP orientation on a terrorist planning cycle for a generic seven-phase threat and an introduction to using terrorism case studies for lessons learned and insight of enemy tactics, techniques, and procedures. A composite TSP file on the TRISA website of all seven learning activities provides a PDF file and a PowerPoint version as an easily retrievable resource for images and supporting narratives. Access to the TRISA website requires an Army Knowledge Online (AKO) password.

An example of other TSP support aids at the TRISA website is TRADOC G2 Handbook No. 1.01, *Terror Operations: Case Studies in Terrorism*, dated July 25, 2007, which presents six case studies in detail. Terror incidents include the sarin attack in the Tokyo subway (1995); the US domestic terrorist bombing of the Murrah Federal Building (1995); the Khobar Towers bombing (1996) in Saudi Arabia; the maritime bombing of the USS COLE (2000) in Yemen; the London subway and bus bombings (July 7, 2005); and the Beslan, North Ossetia–Russia mass hostage and mass murder incident (2004).



TRADOC G2 Handbook No. 1.01 and Terrorism Case Studies

Terrorism Handbook Initiatives in 2008

In addition to the recently published TSP 159-T-0001, TRADOC G2 will publish TRADOC G2 Handbook No. 1.06, *Kidnapping and Terror in the COE,* in late summer 2008. Historical perspective provides an entry point to appreciating the contemporary risks of kidnapping and terrorism. Assessing trends and patterns over modern decades since the 1960s can illustrate the conditions that can occur in military missions and the civilian community. Vignettes such as the kidnapping–hostage crisis of three US Army soldiers near Kumanovo in the former Yugoslav Republic of Macedonia in 1999 or the kidnapping raid and murder of US Army members near Karbala, Iraq, in 2007 indicate the threat that exists in contemporary operational missions.

TRADOC G2 Handbook No. 1.06 Kidnapping and Terror

Leaders must understand and appreciate the threat and can use this handbook to understand terrorist goals and objectives as well as patterns, trends, and emerging techniques of kidnapping and terrorism operations. Threats also concern institutional locations such as training and education sites, installations, and support facilities and encompass military members, family members, Department of the Army Civilians (DAC), and contractors in support of Army missions. The threat of kidnapping as part of force protection vulnerability analysis applies to deployed forces on operational missions and Army members operating as installation, activity, or institutional support.

Knowing the Threat Environment

The threat of terrorism pervades the US military's entire spectrum of conflict. The TRADOC G2 handbooks focus on the principal terrorist threats to the United States. The seven learning activities of TSP 159-T-0001 display the primary themes for improving terrorism situational awareness and guarding against complacency during the WOT. This awareness spans individual acts of wanton damage or deliberate destruction of property and people by groups or individuals. A rationale for using terrorism can emerge from extremist ideological, social, environmental, cult, economic, or political agendas. Terrorist organizations with demonstrated global-reach capabilities and those terrorist organizations that seek to acquire and use weapons of mass destruction (WMD) are the most significant concerns of the United States.

Terrorist violence has changed dramatically in recent years from a sporadic agenda-forcing or attention-getting tool to a significant asymmetric form of conflict. Although terrorist acts were extraordinary several decades ago, the scope of today's terrorism eclipses these former acts and can have a profound impact on populations in local, regional, national, and international communities. Adversaries do not plan to defeat the United States through terrorism alone; rather, adversaries approach terrorism from a much broader strategic context. Whether through an explicit tactical operation or an operational campaign, terrorist acts aim to create anxiety and fear to fracture and break the target population's resolve and cause strategic effects that favor the terrorist.

T3 Network of Subject Matter Experts

TRISA at Fort Leavenworth hosts an informal consortium, the Threats Terrorism Team (T3), to connect an extensive and growing network of subject matter experts and users in training, education, and operational disciplines. Representatives include members of the US Joint Staff; US Northern Command (USNORTHCOM) and its Army component of Army North (ARNORTH); other combatant commands; and US departmental, interdepartmental, and intergovernmental offices. Information sharing among the Army, Navy, Marine Corps, Air Force, and Coast Guard is fundamental to improving the military capabilities involved in homeland security and defense.

Army TRADOC schools and centers provide an excellent means of linking training readiness with operational readiness in organizational units and institutional garrisons and activities. Focused expertise and stakeholders exist at locations such as the Sergeants Major Academy, Command and General

Blah blah blah

Staff College, Infantry School, Armor School, Chemical School, Engineer School, Military Intelligence School, and Military Police School.

As the Army proponent for antiterrorism training, the Military Police School uses the TRADOC G2 terrorism handbooks, as does the US Navy's Center for Antiterrorism and Navy Security Forces. The Air Force Security Forces Center has been involved in reviewing handbook use for antiterrorism activities with base and deployed forces. The Marine Corps Training and Education Command has distributed handbooks to several installations and to Marine forces abroad.

In applying a threat capabilities–based assessment, US military forces must understand and prevent or counter threat options to exploit friendly force vulnerabilities, assumptions, plans, programs, and processes.

The Homeland Security and Defense Education Consortium (HSDEC), established by the North American Aerospace Defense Command and USNORTHCOM in collaboration with the University of Colorado, the University of Denver, and the US Naval Postgraduate School, is an expanding network of teaching and research institutions focused on promoting education, research, and cooperation related to and supporting the US homeland security and defense mission. See some of the TRADOC G2 terrorism handbooks at http://www.hsdec.org.

The Joint Staff J-34 Deputy Directorate for Antiterrorism/Homeland Defense (DD AT/HD) provides TRADOC G2 handbook terrorism awareness to senior military officers and DOD civilians attending the Level IV Antiterrorism Executive Seminar. TRADOC G2 terrorism handbooks are available on the JCS J-34 Antiterrorism Enterprise Portal (ATEP), available at https://atep.dtic.mil. The Army's Reimer Digital Library (RDL) provides public access to some TRADOC G2 terrorism handbooks at http://www.adtdl.army.mil.

Operating for the Future

We are in the midst of the WOT. The aim of the TRADOC G2 handbook series is to create situational awareness and understanding of current terrorism capabilities and limitations and to complement military risk management, force protection, mission-orders conduct, and leader decision making. In applying a threat capabilities–based assessment, US military forces must understand and prevent or counter threat options to exploit friendly force vulnerabilities, assumptions, plans, programs, and processes.

The TRADOC G2 terrorism handbook series provides a straightforward description of an increasingly dangerous element of conflict: terrorism. These terrorism handbooks, updated regularly, are living documents for daily assessment and action in installation and operational mission areas in the US homeland and abroad. They are a critical soldier and leader antiterrorism tool for institutional organizations, in-transit forces and activities, and deployed operational units.

---

1 US Army TRADOC G2 definition of "Contemporary Operational Environment," December 20, 2007. At the time of publication, a TRADOC G2 definition describing COE is being considered for inclusion in the pending revision of US Army Field Manual (FM) 7–0, Training the Force.

2 US Army Regulation (AR) 350-1, Army Training and Education, April 9, 2003. See also, current AR 525–13, Antiterrorism, and Joint Publication 3–26 Counterterrorism (first draft), April 30, 2008.

3 US AR 350–2, Opposing Force (OPFOR) Program, April 9, 2004.

4 This generic terrorist planning cycle sequences through broad target selection, intelligence and surveillance, specific target selection, preattack surveillance and planning, attack rehearsal, actions on the objectives, and escape and exploitations decisions. See Appendix A of *TRADOC G2 Handbook No. 1* (version 5.0) (2007) and Appendix B of TSP 159–T–0001 (2008).

How Is Your Antiterrorism Program Doing, and Where Is It Headed?

By LTC Mike King, US Army, Joint Staff, J-3

Antiterrorism (AT) assessments from the past 10 years indicate that the AT program has come a long way. It manages to identify and correct many vulnerabilities, but it has not reached the finish line yet.

The AT community must determine how to evaluate the effectiveness of an AT program. No requirement in existing doctrine establishes quantitative metrics to evaluate performance of the programs in place. Therefore, this article will discuss AT programs in the context of an Assess, Manage, and Respond methodology, as found in Department of Defense Directive (DODD) 3020.40.[1]

The AT community must determine how to evaluate the effectiveness of an AT program. No requirement in existing doctrine establishes quantitative metrics to evaluate performance of the programs in place.

Assess

Available data shows that the AT community conducts good AT vulnerability assessments (VAs). Ample relevant and current policies and instructions direct what to accomplish in the execution of an AT VA throughout the DOD, down to the installation level. At a higher headquarters level, a minimum of 853 AT VAs were conducted in calendar year 2007. The Services, combatant commanders, unit commanders, and installation commanders have all done well in establishing methods of conducting and recording AT VAs. These commands execute assessments, either on a periodic schedule or on an as-needed basis using existing DOD-wide, standardized benchmarks[2] that highlight vulnerabilities.

During the past five years, the Core Vulnerability Assessment Management Program (CVAMP) has been established as a repository for all vulnerabilities, and in late 2006, its use was directed for the AT community.[3] CVAMP is a centralized database for cataloging vulnerabilities and, if used correctly, assists commanders in establishing risk visibility throughout the chain of command.

Unfortunately, not all vulnerabilities are being entered into CVAMP. There seems to be a desire to not air "dirty laundry" when it comes to vulnerabilities. The attitude that "we don't know what we don't know" undermines the ability to adequately address vulnerabilities and determine the overarching risks to missions. If local AT officers (ATOs) or their commanders choose not to enter a known vulnerability into CVAMP, the risks posed by the vulnerability cannot be properly mitigated or remediated.

Because the AT community does not have visibility into all vulnerabilities, this area is perhaps its greatest weakness.

Blah blah blah

Manage

Awareness of program vulnerabilities and associated risks facilitates their management and enables senior leaders to make informed decisions about allocating funding and meeting the future needs of the AT community.

Ample AT training is available throughout DOD. The Joint Staff works with the Defense Threat Reduction Agency (DTRA) , the Services, and agencies to offer a variety of subjects, from a basic understanding of terrorism levels and mobile training teams to graduate-level seminars on executing and owning an AT program.

Since the mid-1990s, the Unified Facilities Construction (UFC) Standards have been incorporated into new military construction and into renovation projects of existing facilities. The use of UFC standards helps eliminate the inheritance of vulnerabilities and provides a method for addressing issues during the design and construction phase of a building project.

AT VAs show that the AT community is not doing as well as it could in taking corrective actions on known vulnerabilities. This is visible when, for example, similar vulnerabilities are observed in multiple assessments and those vulnerabilities tend to remain constant throughout the AT community.

Without a risk-acknowledgement process in place, the AT community may find that it has very limited ideas about exactly how much risk is being accepted in protection against terrorist acts. Do you know how much risk you are accepting currently at your installation?

The Joint Staff, through the Combating Terrorism Readiness Initiative Fund (CbTRIF), works diligently each year to provide funding to mitigate or remediate the combatant commanders' highest priority emergent or emergency requirements. Unfortunately, the funding available through CbTRIF is not enough to address all of the known vulnerabilities and was not designed to accomplish that task. The Services and combatant commanders have the inherent responsibility of resourcing strategies to mitigate or remediate vulnerabilities that are not eligible for CbTRIF funding, and these requirements should be programmed into funding requests.

For the Services and combatant commanders to obtain resources to mitigate or remediate vulnerabilities, they must first have visibility into the vulnerability and understand the measures that local commanders recommend to offset the associated risk. If the AT community fails to "paint the picture" of vulnerabilities and risks, senior leaders at all levels will be unable to shape the AT program to ensure protection of our assets (mission, facilities, and people).

Respond

As the AT program currently exist, the Services and combatant commanders may not have adequate visibility on the amount of risk accepted throughout the chain of command. Unfortunately, one of the ways commanders determine whether they have an adequate level of visibility is after an event has been intercepted or completed and the defined threat becomes known.

Several events within the last two years have enabled commands to retrospectively determine that similar vulnerabilities had already been identified.

Such a discovery usually leads to a more thorough review, with or without a higher commander's involvement, of the amount of risk being accepted at installations and units. Sometimes there may be a "knee jerk" reaction to immediately address the risks DOD-wide without regard to other, possibly higher risk vulnerabilities. An example of such a reaction might be restricting installation entrance to only decal-bearing vehicles driven by Service members after

another installation has been penetrated by a civilian with only a state driver's license ostensibly making a commercial delivery.

The acceptance of risk varies among Services and commands and is not currently codified into a DOD instruction or directive. The community must define what the correct level of risk acceptance is and who further up in the hierarchy needs to be aware of individual risks. The amount of risk that accrues may become the primary concern rather than the vulnerability itself. Without a risk-acknowledgement process in place, the AT community may find that it has very limited ideas about exactly how much risk is being accepted in protection against terrorist acts. Do you know how much risk you are accepting currently at your installation? Does the commander or his designee actually receive assessment reports and ensure they are entered into CVAMP? Is the commander fully engaged in the AT program?

Fortunately, CVAMP is more than just a resource tool that provides data for CbTRIF funding. CVAMP assists commanders in managing risk by communicating vulnerabilities, risks, and risk acceptance to the next higher level when it cannot be fixed at the lower level of command. CVAMP is used by the Joint Staff to conduct trend analysis and to determine where weaknesses may exist in the community.

If commanders are actively involved with CVAMP, they are able to consider alternative options for reducing risk. An example of such use involves a particular installation with an access control point requirement that warrants new construction but funding is not readily available to correct the vulnerability. A risk-management process can be used to develop techniques or procedures for handling the problem, such as providing additional security over watch or the placement of temporary barriers. If the vulnerability was entered into CVAMP along with the risk-mitigation technique, then higher level commanders would have visibility into the local commander's acceptance of risk and requirements for resources to fix it.

Conclusions

In the process of conducting a self-assessment of the AT program, you may find results strikingly similar to these observations or you may already have identified the areas you want to improve. To face the future of AT, the community must acknowledge what it does well and what it needs to improve. There will never be enough funding to solve all vulnerabilities, but with the judicious application of available funds combined with good risk-management processes, we will continue to protect the force and deter, detect, or defeat another terrorist attack.

If commanders are actively involved with CVAMP, they are able to consider alternative options for reducing risk. For example, a particular installation may have an access control point requirement, but no funding for new construction. A risk-management process can be used to develop techniques or procedures for handling the problem, such as the placement of temporary barriers.

1 Department of Defense Directive 3020.40. "Defense Critical Infrastructure Program (DCIP,)" August 19, 2005.

2 Department of Defense Instruction 2000.16. "DOD Antiterrorism Standards," October 2, 2006.

3 Chairman of the Joint Chiefs of Staff Instruction. "Combating Terrorism Readiness Initiatives Fund," April 27, 2007.

Terminology to Define the Terrorists: Recommendations from American Muslims

Department of Homeland Security, Office for Civil Rights and Civil Liberties

Words matter. The terminology that senior government officials use must accurately identify the nature of the challenges that face our generation. It is critical that all Americans properly understand the gravity of the threats we face and prepare themselves to take the steps necessary to build a secure future. We are facing an enemy that holds a totalitarian ideology and seeks to impose that ideology through force across the globe. We must resist complacency. The language that senior government officials use can help to rally Americans to vigilance.

At the same time, the terminology should also be strategic—it should avoid helping the terrorists by inflating the religious bases and glamorous appeal of their ideology. One of the most common concerns expressed by Muslims in America, and indeed the West, is that senior government officials and commentators in the mass media regularly indict all Muslims for the acts of a few. They argue that terminology can create either a negative climate, in which acts of harassment or discrimination occur, or, by contrast, a positive climate, such as President Bush's remarks while visiting a mosque in the days after 9/11.

If senior government officials carefully select strategic terminology, the government's public statements will encourage vigilance without unintentionally undermining security objectives. That is, the terminology we use must be accurate with respect to the very real threat we face. At the same time, our terminology must be properly calibrated to diminish the recruitment efforts of extremists who argue that the West is at war with Islam.

This paper outlines recommendations from a wide variety of American Muslim leaders regarding the difficult terrain of terminology. **This paper does not state official Department of Homeland Security (DHS) policy nor does it address legal definitions.** Rather, it outlines recommendations compiled by the DHS Office for Civil Rights and Civil Liberties (CRCL) from its discussions with a broad range of experts from the Muslim American community, including civic leaders, academics, and writers.

Assumptions

Starting from the premise that words do indeed matter, three foundational assumptions inform this paper:

(1) We should not demonize all Muslims or Islam;

(2) Because the terrorists themselves use theology and religious terms to justify both their means and ends, the terms we use must be accurate and descriptive; and

(3) Our words should be strategic; we must be conscious of history, culture, and context.

In an era where a statement can cross continents in a manner of seconds, it is essential that officials consider how terms translate, and how they will resonate with a variety of audiences.

Terminology to Avoid

Recommendation 1:

Respond to ideologies that exploit Islam without labeling all terrorist groups as a single enemy.

The public statements of the US Government (USG) must convey the ideological dimensions of the terrorist threat, in addition to conveying its tactical dimensions. Specifically, it is important for the public to understand that many extremist groups seek to impose their totalitarian worldview by seizing political power through force. In labeling specific organizations and movements, however, the experts recommend that the USG should not feed the notion that America is engaged in a broad struggle against the so-called "Muslim World." Currently, the US and its allies are facing threats from a variety of terrorist organizations operating across the globe, but the threats presented by transnational movements like al Qaeda are perhaps the most serious.[1] According to these experts, al Qaeda wants all Muslims to line up under its banner. Collapsing all terrorist organizations into a single enemy feeds the narrative that al Qaeda represents Muslims worldwide. Al Qaeda may be spreading its influence, but the USG should not abet its franchising by making links where none exist. For example, the cult members arrested in Miami should not be called members of al Qaeda; and, while they are both terrorist organizations who threaten global security and stability, Hezbollah and Hamas are distinct in methods, motivations, and goals from al Qaeda. When possible, the experts recommend that USG terminology should make this clear.

Recommendation 2:

Do not give the terrorists the legitimacy that they seek.

What terrorists fear most is irrelevance; what they need most is for large numbers of people to rally to their cause. There was a consensus that the USG should avoid unintentionally portraying terrorists, who lack moral and religious legitimacy, as brave fighters, legitimate soldiers, or spokesmen for ordinary Muslims. Therefore, the experts counseled caution in using terms such as "jihadist," "Islamic terrorist," "Islamist," and "holy warrior" as grandiose descriptions.

Using the word "Islamic" in a phrase will sometimes be necessary in order to distinguish terrorists who claim the banner of Islam from other extremist groups who do not invoke religion or who invoke other faiths. Nevertheless, CRCL understands the experts' caution in this regard to be rooted in the concern that we should not concede the terrorists' claim that they are legitimate adherents of Islam. Therefore, when using the word, it may be strategic to emphasize that many so-called "Islamic" terrorist groups twist and exploit the tenets of Islam to justify violence and to serve their own selfish political aims.

The same is true of the moniker "Islamist" (or the related "Islamism"), which many have used to refer to individuals who view Islam as a political system in addition to a religion. The experts we consulted did not criticize this usage based on accuracy; indeed, they acknowledged that academics and commentators, including some in the Arab and Muslim Worlds, regularly use "Islamist" to describe people and movements. Nevertheless, they caution that it may not be *strategic* for USG officials to use the term because the general public, and specifically overseas audiences, may not appreciate the academic distinction between Islamism and Islam. In the experts' estimation, this may still be true, albeit to a lesser extent, even if government officials add qualifiers, such as "violent Islamists" or "radical Islamism."

Regarding "jihad," even if it is accurate to reference the term (putting aside polemics on its true nature), it may not be strategic because it glamorizes terrorism, imbues terrorists with religious authority they do not have, and damages relations with Muslims around the globe.

Some say that this is a war against "Salafis." However, Salafism is a belief system that many people follow. This includes al Qaeda leadership, as well as many individuals who are not violent at all. Again, if we assign this term to al Qaeda, we will be handing them legitimacy that they do not have but are desperately seeking.

The consensus is that we must carefully avoid giving bin Laden and other al Qaeda leaders the legitimacy they crave, but do not possess, by characterizing them as religious figures or in terms that may make them seem to be noble in the eyes of some.

Recommendation 3:

Proceed carefully before using Arabic and religious terminology.

USG officials may want to avoid using theological terms, particularly those in Arabic, even if such usage is benign or overtly positive. Islamic law and terms come with a particular context, which may not always

It may be strategic to emphasize that many so-called "Islamic" terrorist groups twist and exploit the tenets of Islam to justify violence and to serve their own selfish political aims.

be apparent. It is one thing for a Muslim leader to use a particular term; an American official may simply not have the religious authority to be taken seriously, even when using terms appropriately.

Terminology to Use

Recommendation 4:

Reference the cult-like aspects of terrorists, while still conveying the magnitude of the threat we face.

In describing al Qaeda, its supporters, and other violent extremists, some commentators have used the term "death cult."[2] While the term may not fully encompass or describe the threat posed by groups like al Qaeda, it may be both accurate and useful when used as a point of comparison. Cults, while often linked to mainstream religions, have a negative connotation. As a practical matter, terrorist groups use recruitment tactics that are similar to cults: separation from family, indoctrination, and breaking down previously held beliefs.[3]

This negative connotation also exists in the Muslim world. Indeed, the experts highlighted previous instances in Islamic history where heretic sectarian groups formed, followed a cultish strategy of recruitment, and were eventually marginalized. This began with the Kharijites, the first radical dissidents in Islam, who assassinated the fourth Caliph Ali in 661 CE. There is even a genre of literature, the *Kitab al-Firaq* or *Book of Sects,* which discusses these movements.

Based on this history and context, senior officials might use terms such as "death cult," "cult-like," "sectarian cult," and "violent cultists" to describe the ideology and methodology of al Qaeda and other terrorist groups. "Cult" is both normative and accurate in that it suggests a pseudo-religious ideology that is outside the mainstream. Moreover, as there is no overt reference to Islam, these terms are not as likely to cause offense. Referring to bin Laden's movement as "fringe" or "outside the mainstream" may also be helpful.

Of course, the threat posed by terrorist organizations such as al Qaeda is far greater than that posed by most cult groups. Nevertheless, "cult" comparisons may advance strategic USG objectives by marginalizing those who falsely claim to represent ordinary Muslims.

Recommendation 5:

Use "mainstream," "ordinary," and "traditional" in favor of "moderate" when describing broader Muslim populations.

In characterizing the broader Muslim American community, the Muslim World, and Islam generally, "mainstream," "ordinary," and "traditional" are preferable to "moderate." One can be deeply religious, strictly adhere to fundamental doctrines, and nevertheless abhor violence. In addition, "mainstream" is a useful foil to the "cult" terminology referenced above. By contrast, the term "moderate" has become offensive to many Muslims, who believe that it refers to individuals with whom the USG prefers to deal and who are only marginally religious. Notably, "mainstream" is a term that is emerging among Muslim American commentators.[4]

Recommendation 6:

Pay attention to the discourse on takfirism.

As discussed, USG officials should use caution before employing religious terminology, but they should not be ignorant of useful phraseology. According to the experts we consulted, one such term is "takfirism," which refers to the practice of declaring a Muslim a "kafir," or nonbeliever, and then proclaiming that their lives can be forfeited. Al Qaeda and other terrorist groups employ "takfir" to name as apostates all Muslims who reject their ideology, arguing that this makes their blood violable.

This is not a new phenomenon; indeed, takfiri practices arise sporadically in Islamic history. For

example, the Kharijites' practice of takfir became the justification for their indiscriminate attacks on civilian Muslims. Modern examples are the Iraqi insurgent groups who justify their actions against Shi'as by labeling them kafirs (e.g., the bombers of the Golden Mosque in Samarra).[5]

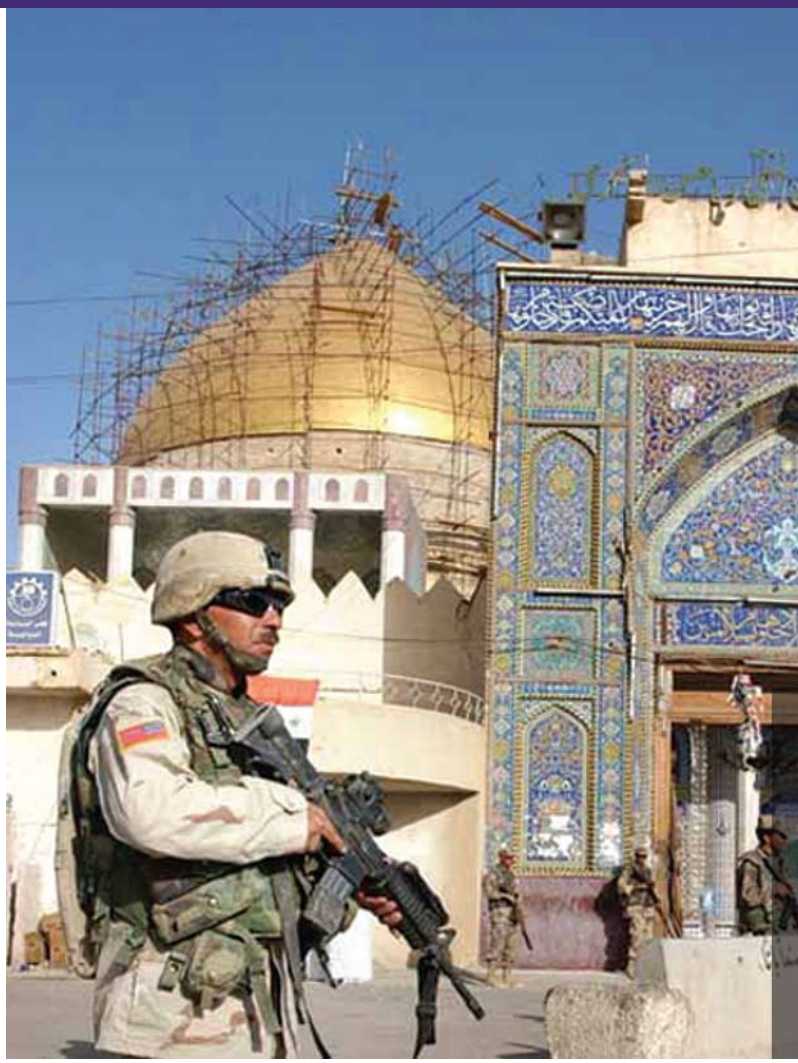
Strictly speaking, takfirism most accurately describes terrorism by Muslims against other Muslims. But it may be strategic to employ the term in a wider context given that (1) many of the leaders of al Qaeda are known to have adopted a takfiri ideology,[6] and (2) part of the USG's antiterrorism strategy should be to emphasize that the majority of the victims of modern terrorism are Muslim.[7] There may also be a useful nexus to cult terminology; regarding takfiri indoctrination, French terrorism expert Roland Jacquard states: "Takfir is like a sect: once you're in, you never get out. The Takfir rely on brainwashing and an extreme regime of discipline to weed out the weak links and ensure loyalty and obedience from those taken as members."[8] Thus, the phrase "takfiri death cult" may have some relevance.

The experts we consulted acknowledged that USG officials may feel uncomfortable using religious and Arabic terminology. And as discussed above, it may not be strategic for them to do so. Nevertheless, given its relevance to Islamic history and present-day conflicts, the experts believe government officials should pay attention to the discourse on takfirism for three reasons.

First, unlike jihad, which arguably has a variety of interpretations, takfir has historically had an overwhelmingly negative connotation. Second, and as the articles referenced here demonstrate, commentators do use the term to describe terrorists and their ideology. As such, no one can argue that the USG invented the concept. Last, and perhaps most important, some of the most influential Muslim religious leaders have strongly come out against the takfiri doctrine.

In July 2005, King Abdullah II of Jordan convened a conference in Amman of 200 of the world's leading Islamic scholars from 50 countries.[9] The group, which included Sunnis and Shi'as, unanimously issued a ruling, known as *The Amman Message,* specifically forbidding the practice of takfir.[10] Since then, more than 500 Islamic scholars worldwide have adopted the ruling.[11]

While it is undoubtedly a welcome development, the experts agreed that *The Amman Message* is just one step and that its effect on the ideology and operations of al Qaeda will be negligible. They pointed out, however, that the audience the USG is attempting to reach includes mainstream Muslims, the majority of whom denounce violence, yet still believe the US is waging a war against their religion.[12] It is this group,



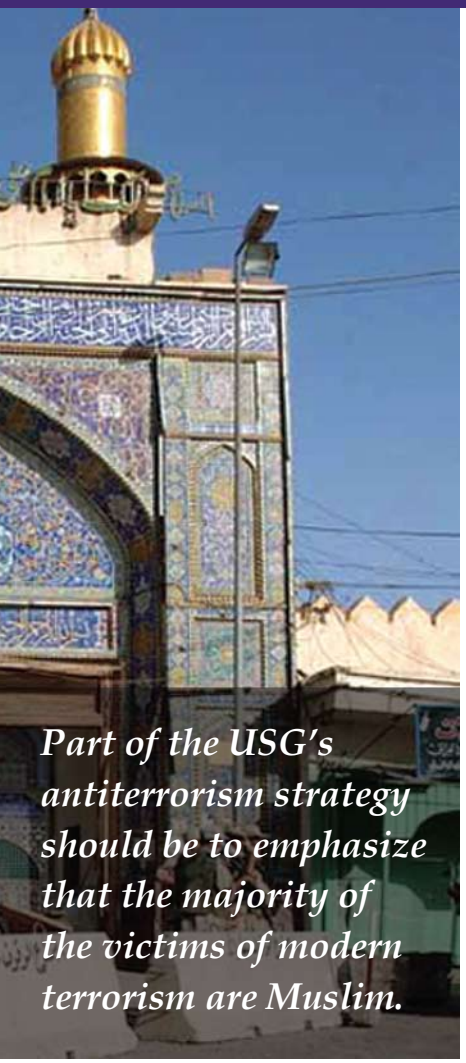
the experts reasoned, that may pay attention to *The Amman Message* and its anti-takfiri stance.

The experts did not recommend a wholesale adoption of takfirism or related terms into the USG lexicon. Rather, they advised us to pay attention to how this term is used and consider future opportunities for utilization. The experts themselves believe in its efficacy and accuracy and have pledged to reference the term in their writings.

Nevertheless, they recognized that takfirism is a religious term and that, at least initially, it may be awkward for USG officials to use it. But this was also true of "jihadi," which is now used regularly. Moreover, unlike other terms, using takfirism does not create a division between Islam and the West. To the contrary, its usage, the experts maintained, will allow the USG to linguistically sever the violent actors from broader Muslim communities without sacrificing accuracy, succumbing to political correctness, or alienating mainstream Muslims.

Recommendation 7:

Emphasize the positive.



Part of the USG's antiterrorism strategy should be to emphasize that the majority of the victims of modern terrorism are Muslim.

USG officials should emphasize the positive—what we are seeking together. In addition to recognizing the dark vision of our terrorist enemies and the need to counter their actions with all elements of national power, the USG should also attempt to convince people that this generation needs to unite to promote a common vision for the future. The experts we consulted suggested defining the challenge of our times as "A Global Struggle for Security and Progress." It is unlikely that this phrase will replace existing monikers such as "the war on terror" or "the long war," which are more widely used both within and outside the government. Moreover, as a comprehensive descriptor, the phrase may not sufficiently reflect the need to promote public vigilance and rally support for the USG's antiterrorism mission. Nevertheless, we understand the experts' recommendation to be grounded in the realization that we must define what we stand *for*, in addition to defining what we stand *against*. More specifically, it may be strategic to emphasize the following:

1. **The civilized world is facing a "global" challenge, which transcends geography, culture, and religion.**

2. **This struggle is for "security," a global aspiration that all people seek.** In particular, Islam emphasizes order and structure. The takfiri ideology is the antithesis of this and in many respects resembles anarchism: killing wantonly, destroying great buildings and mosques without reason, and bringing chaos and disorder. Moreover, the concept of "security" is one that resonates with mainstream American audiences, as well as with Muslims around the world.

3. **This struggle is for "progress," over which no nation has a monopoly.** The experts we consulted debated the word "liberty," but rejected its usage in the international context, despite its obvious importance and relevance to American interests and history: They believed that overseas audiences around the world would discount the term as a buzzword for American hegemony. But all people want to support "progress," which emphasizes that there is a path for building strong families and prosperity among the current dislocations of globalization and change. And progress is precisely what the terrorists oppose through their violent tactics and through their efforts to impose a totalitarian worldview.

Recommendation 8:

Emphasize the success of integration.

Bin Laden and his followers will succeed if they convince large numbers of people that America and the West are at war with Islam and that a "clash of civilizations" is inevitable. Therefore, USG officials should continually emphasize a simple and straightforward truth: Muslims have been and will continue to be part of the fabric of our country. Senior officials must make clear that there is no "clash of civilizations;" there is no "us versus them." We must emphasize that Muslims are not "outsiders" looking in but are an integral part of America and the West. Officials should look to incorporate concepts such as these, and the following, into their remarks:

- Muslims have successfully integrated into American communities for generations. From decades of experience, Muslims know that the environments created by democracies such as ours give them the freedom to choose the best way to raise their families, get an education, relate to their governments, become part of the government, start a business, and become prosperous in their professions.
- Muslim Americans are successful doctors, lawyers, teachers, first responders, Boy Scout leaders, and political leaders.
- We honor and value the contributions that Muslim Americans make to our communities.
- The motto on the seal of the United States is, "E pluribus unum"—out of many, one. We all need to work together to make this great motto our reality.
- In America, there are no guests and no hosts; all citizens are politically and culturally equal.
- The fact is that Islam and secular democracy are fully compatible; in fact, they can make each other stronger. Senior officials should emphasize this positive fact.

Recommendation 9:

Emphasize the US Government's openness to religious and ethnic communities.

Bin Laden's narrative presumes a war against Islam and rampant mistreatment of Muslims by the American and other Western governments. Extremist recruiters argue that Muslims should segregate from the larger society; moreover, their recruitment pitch depends on isolation. These appeals are undercut by the fact, true for decades, that the USG works openly with religious and ethnic communities and takes aggressive steps to protect their rights. Senior USG officials should emphasize themes such as the following:

- The USG is engaged with the American people, including Muslim Americans, looking for ways to make our communities prosperous and just.
- We are listening; we have an open door. There is no reason for Muslim Americans to feel isolated from their governments; we are working together regularly.
- Muslims Americans are playing a constructive and proactive role in improving the public policy of our country.
- There is no war against Muslims or Islam in America. In fact, the American government is committed to ensuring justice in our country. For example, we have aggressively prosecuted allegations of hate crimes against Muslims; the Department of Justice Civil Rights Division has sued a school district that refused to allow a teenage girl to wear a hijab; and we actively pursued justice for Muslims victimized during the conflict in the Balkans.
- There is a good level of engagement between the federal government and Muslim American communities, and it will continue to increase over the upcoming months and years. Indeed, we have the hope of seeing levels of engagement between the USG and Arab and Muslim Americans that have never been reached in the history of this country. For example, leading Arab, Muslim, and South Asian American groups have met multiple times with the Secretary of Homeland Security, the Attorney General, the Director of the FBI, the Secretary of the Treasury, and senior officials at the State Department.
- If senior officials will emphasize these themes, it will undercut those who attempt to develop a "grievance" or "victim" mentality in the American Muslim community.

Conclusion

Words matter. The terminology the USG uses should convey the magnitude of the threat we face but also avoid inflating the religious bases and glamorous appeal of the extremists' ideology. Instead, USG terminology should depict the terrorists as the dangerous cult leaders they are. They have no honor, they have no dignity, and they offer no answers. While acknowledging that they have the capacity to destroy, we should constantly emphasize that they cannot build societies and do not provide solutions to the problems people across the globe face.

Where our reach is limited, we should strongly encourage Muslim writers, commentators, and scholars to use terminology that will drive the debate in a positive direction. While the USG may not be able to effectively use terms like "takfirism," others certainly can.

Finally, we should view our words as bricks used to build a foundation. The USG should draw the conflict lines not between Islam and the West but between a dangerous, cult-like network of terrorists and everyone who is in support of global security and progress.

1 "National Intelligence Estimate: The Terrorist Threat to the US Homeland," p. 6., July 2007. http://www.dni.gov/press_releases/20070717_release.pdf (accessed July 28, 2007).

2 Thomas L. Friedman, "If It's a Muslim Problem, It Needs a Muslim Solution." *New York Times*, July 8, 2005. http://www.nytimes.com/2005/07/08/opinion/08friedman.html?ex=1278475200&en=a1cbffb46f2ac7d0&ei=5088 (July 28, 2007) ("[I]t is essential that the Muslim world wake up to the fact that it has a jihadist death cult in its midst"); see also, Reza Aslan, "Why Do They Hate Us? Strange Answers Lie in Al-Qaida's Writings."

Strategic Terminology: Nine Recommendations

1. Respond to ideologies that exploit Islam without labeling all terrorist groups as a single enemy.
2. Do not give the terrorists the legitimacy that they seek.
3. Proceed carefully before using Arabic and religious terminology.
4. Reference the cult-like aspects of terrorists, while still conveying the magnitude of the threat we face.
5. Use "mainstream," "ordinary," and "traditional" in favor of "moderate" when describing broader Muslim populations.
6. Pay attention to the discourse on takfirism.
7. Emphasize the positive.
8. Emphasize the success of integration.
9. Emphasize the US Government's openness to religious and ethnic communities.

Slate, August 6, 2007. http://www.slate.com/id/2171752 (September 6, 2007) (referring to Osama bin Laden as a "cult leader literally dwelling in a cave").

3 For a discussion of terrorist indoctrination, see, Robert Baer, "A Talk With a Suicide Bomber." *Time Magazine,* July 20, 2007. http://www.time.com/time/world/article/0,8599,1645461,00.html (July 28, 2007).

4 Shahed Amanullah, "Western Muslims need a 'fourth estate.'" *Altmuslim.com*, April 9, 2007. http://www.altmuslim.com/a/a/a/western_muslims_need_a_fourth_estate/ (September 6, 2007) ("Dynamic, independent, and professional Muslim voices, free of restrictions based on organizational affiliation yet **intimately connected to the mainstream Muslim community,** can make a difference even if their numbers are small" [emphasis added]).

5 James S. Robbins, "Al Qaeda Blows It." *National Review Online,* February 23, 2006. http://www.nationalreview.com/robbins/robbins200602230743.asp (July 28, 2007).

6 A *Time Magazine* article published shortly after 9/11 is instructive: Bin Laden and al-Qaeda may have learned, by violent experience, to pre-empt and harness the new fanaticism. In late 1995, bin Laden's compound in Khartoum was attacked by gunmen believed to be Takfiri. A Sudanese friend of bin Laden's who questioned the surviving attacker said, "He was like a maniac, more or less like the students in the USA. who shoot other students. They don't have very clear objectives." By the time al-Qaeda had resettled in Afghanistan, ideological training was an integral part of the curriculum, according to a former recruit who went on to bomb the US embassy in Nairobi. Students were asked to learn all about demolition, artillery and light-weapon use, but they were also expected to be familiar with the fatwas of al-Qaeda, including those that called for violence against Muslim rulers who contradicted Islam—a basic Takfiri tenet.

Michael Elliot, "Hate Club: Al-Qaeda's Web of Terror." *Time Magazine,* November 4, 2001. http://www.time.com/time/nation/article/0,8599,182746,00.html (July 28, 2007).

7 David McKeeby, "Terrorism Report Highlights Global Challenge." *USINFO*, April 30, 2007. http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2007&m=April&x=20070425112825idybeekcm0.2628443 (July 28, 2007).

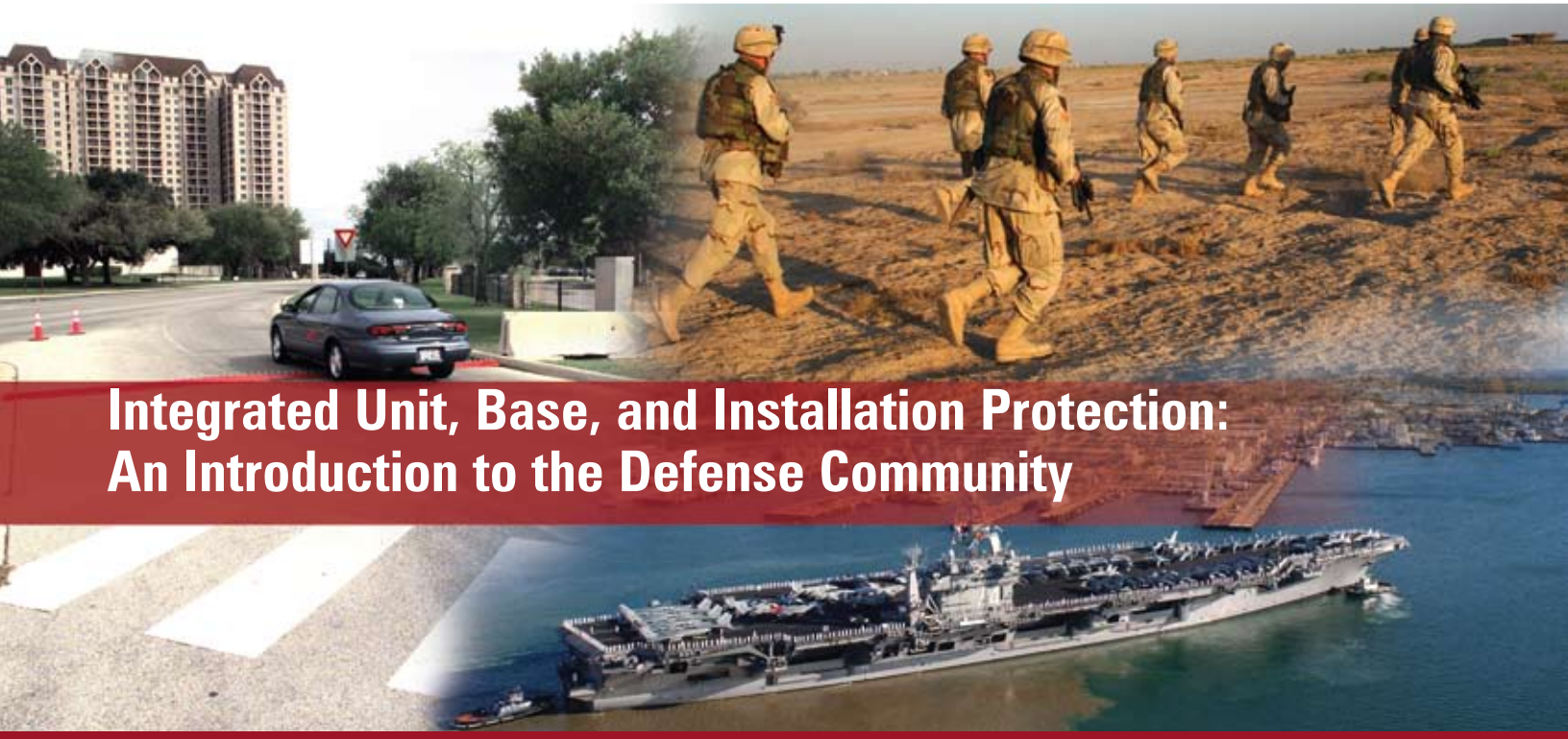
8 See, supra note 6.

9 In *The Amman Message*, the participating scholars issued a unanimous ruling, known as the "Three Points of the Amman Message." In it, they took the following actions:
1. They specifically recognized the validity of all eight Mathhabs (legal schools) of Sunni, Shi'a, and Ibadhi Islam; of traditional Islamic Theology (Ash'arism); of Islamic Mysticism (Sufism), and of true Salafi thought, and came to a precise definition of who is a Muslim.
2. Based upon this definition, they forbade takfir (declarations of apostasy) between Muslims.
3. Based upon the Mathahib (Islamic legal procedures), they set forth the subjective and objective preconditions for the issuing of fatwas, thereby exposing ignorant and illegitimate edicts in the name of Islam.
Prince Ghazi Bin Muhammad, "Muslims Speak Out." *On Faith,* July 22, 2007. http://newsweek.washingtonpost.com/onfaith/muslims_speak_out/2007/07/ghazi.html (August 2, 2007).

10 Ibid.

11 Ibid.

12 "Muslims Believe US Seeks to Undermine Islam." *World Public Opinion,* April 24, 2007. http://www.worldpublicopinion.org/pipa/articles/home_page/346.php?nid=&id=&pnt=346&lb=hmpg1 (July 29, 2007).



Integrated Unit, Base, and Installation Protection: An Introduction to the Defense Community

By Colonel Art Clark, Lieutenant Colonel Dave Koonce, Mr. Mike Martori

Colonel Clark is assigned to the Joint Chiefs of Staff J-34, Deputy Directorate for Antiterrorism and Homeland Defense, with his primary duty being J-3 Coordinator for the IUBIP initiative. His combat deployments include Operation Desert Shield and Operation Desert Storm, 1990–1991; Operation Enduring Freedom, 2002–2003; and Operation Iraqi Freedom (Qatar and Kuwait), 2005.

At the time this article was written, LTC David Koonce was assigned to the Maneuver Support Center, Concept Development Directorate, Fort Leonard Wood, MO, with his primary duty being the Joint Team Lead for the IUBIP initiative. His combat deployments include Operation Enduring Freedom, 2005–2006. He is currently assigned to CSTC-A, Detainee Operations, Camp Eggers, Kabul, Afghanistan.

Mr. Michael Martori is the Program Manager for L3/Global Security & Engineering Solution at Fort Leonard Wood, MO. He supports the Maneuver Support Center, Concept Development Directorate and was the lead action officer for the IUBIP initiative. Mr. Martori retired from service in January 2006 after more than 21 years as a Military Policeman.

In the 1966 film production of the classic Broadway comedy "A Funny Thing Happened on the Way to the Forum," a cast of diverse characters with contrary agendas and invested hostilities eventually achieves harmony and satisfaction of their competing needs. They find out that they have a great deal more in common than the differences they first saw between each other. To our great benefit, the Department of Defense (DOD) has witnessed in the first decade of this millennium a similar sequence of events in the joint capability area (JCA) of protection.

One might say that in August 2006, a funny thing happened on the way to the Chairman of the Joint Chiefs of Staff (CJCS) Force Structure, Resources, and Assessment Directorate (J-8) Protection Functional Capabilities Board (PFCB). In short, the Army—informed by success in the Comprehensive Force Protection Initiative (CFPI)—began aggressively exploring and developing joint dependencies with the sister Services for protecting our forces through the continuum of movement from garrison to the forward edge of battle and back to garrison. Not surprisingly, we (the Services and Joint Staff) came to realize that the future of protection is fundamentally a joint mission of Service and combatant command equals, who have many more similarities than differences, with the common purpose of enabling the success of the joint warfighter. As a result of the decision of the Joint Requirements Oversight Council (JROC) in November 2006, the Integrated Unit, Base, and Installation Protection (IUBIP) capabilities-based assessment was initiated for the years 2012 to 2024, and IUBIP has been on a fast track with unanimous Service and combatant command approval ever since. The Service sponsor for joint protection is the Army. The combatant command sponsor is the United States Transportation Command (USTRANSCOM).

We recognize that terrorist, militant, and low-intensity threats remain among our nation's most pervasive challenges. At risk and considered high-value targets are DOD personnel, facilities, and information. Unfortunately, no change to these hazards is predicted in the future. Furthermore, asymmetric threats may not be deterred by our military tactical superiority and may not lend themselves to traditional protection solutions, suggesting a more active application of protection

capabilities that a focus on asymmetric and irregular warfare must not obscure the danger from traditional tactical military threats. Integrated protection capabilities against historical kinetic and explosive threats are essential for the future joint force. Joint operations demand integrated capabilities to meet the entire threat spectrum, which can only be realized by dedicated support from the Services, the Title 10 foundation of national defense for equipping, manning, and training the force.

In response to these challenges and with focus on the future, IUBIP—a joint endeavor—integrates protection capabilities across the force, eliminating unnecessary redundancies. With interoperability as the touchstone, IUBIP seeks to immediately improve protection with nonmateriel solutions in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF), while specifically constraining the materiel of DOTMLPF to investment in current programs and avoiding new acquisition. Separate from DOTMLPF, IUBIP proposes new acquisitions on a case-by-case basis, only when necessary, and in coordination with the CJCS J-8 and the Office of the Secretary of Defense (OSD).

IUBIP seeks to break the mold of performing acquisition and delivery of systems independent from the essential DOTMLPF support structure. In the past, we have received our materiel systems only to discover that doctrine, organization, training, personnel, and facilities are insufficient and must be quickly backward-engineered to accommodate large financial acquisition investments. The resulting stovepipes, vertical cylinders of excellence, make attractive slide presentations, but deny joint interoperability and fall short of delivering the best possible protection capabilities that our Sailors, Soldiers, Airmen, and Marines deserve. Under the joint force construct of detect, assess, warn, defend, and recover (see the protection joint functional concept issued by the Director of the Joint Staff, CJCS, *www.dtic.mil/jointvision/jroc_protection_jfc.doc),* IUBIP delivers 360-degree hemispherical surface and subsurface protection against threats, to include kinetic; electronic; informational; and chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE). IUBIP provides the Services and combatant commands with a unique opportunity to solve gaps and seams in command and control and net-centric operations, while offering a case study to other JCA proponents for integration and portfolio management.

IUBIP—a joint endeavor—integrates protection capabilities across the force, eliminating unnecessary redundancies. With interoperability as the touchstone, IUBIP seeks to immediately improve protection with nonmateriel solutions in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).

IUBIP's principal objectives are to—

- Integrate protection capabilities for units, bases, and installations across the full range of military operations from the operational to tactical levels in the 2012 to 2024 timeframe.
- Leverage existing protection efforts and increase interoperability.
- Support homeland defense and critical infrastructure protection.

IUBIP's Operational View (OV-1) (see Figure 1) presents the end state goal. Using the joint construct of detect, assess, warn, defend and recover, IUBIP provides integration and synchronization of protection capabilities across three operational modes:

- Fixed sites
- Semifixed or expeditionary sites
- Mobile operations

The OV-1 shows the enabling function of worldwide connectivity through the Global Information Grid (GIG) with scaleable and tailorable capabilities that can be delivered through economies of scale and standardization. The connecting lines between the three operational modes depict the deliberate and purposeful integration and interoperability of protection capabilities. The protection functions, when applied synergistically, yield a mosaic of integrated military tasks providing interoperable protection capabilities for the joint force.

To date, the Services and CJCS J-8 have given unanimous approval to IUBIP at all milestones in the Joint Capabilities Integration and Development System (JCIDS). The Army-led joint team at the United States Army Maneuver Support Center (MANSCEN), Fort Leonard Wood, Missouri, began work immediately following the JROC approval of the concept in November 2006. With all Services participating, the joint team accomplished a record performance by delivering a concept of operations, functional area analysis, joint capabilities document, and interoperability functional solution analysis by September 2007—less than 12 months from the start. The Navy-led joint team at Commander Naval Installations Command (CNIC), Norfolk, Virginia, stood up in September 2007 and joined the Fort Leonard Wood team in delivering the interoperability initial capabilities document and the detect-assess-defend functional solution analysis by May 2008—less than 9 months from the start. The teams anticipate

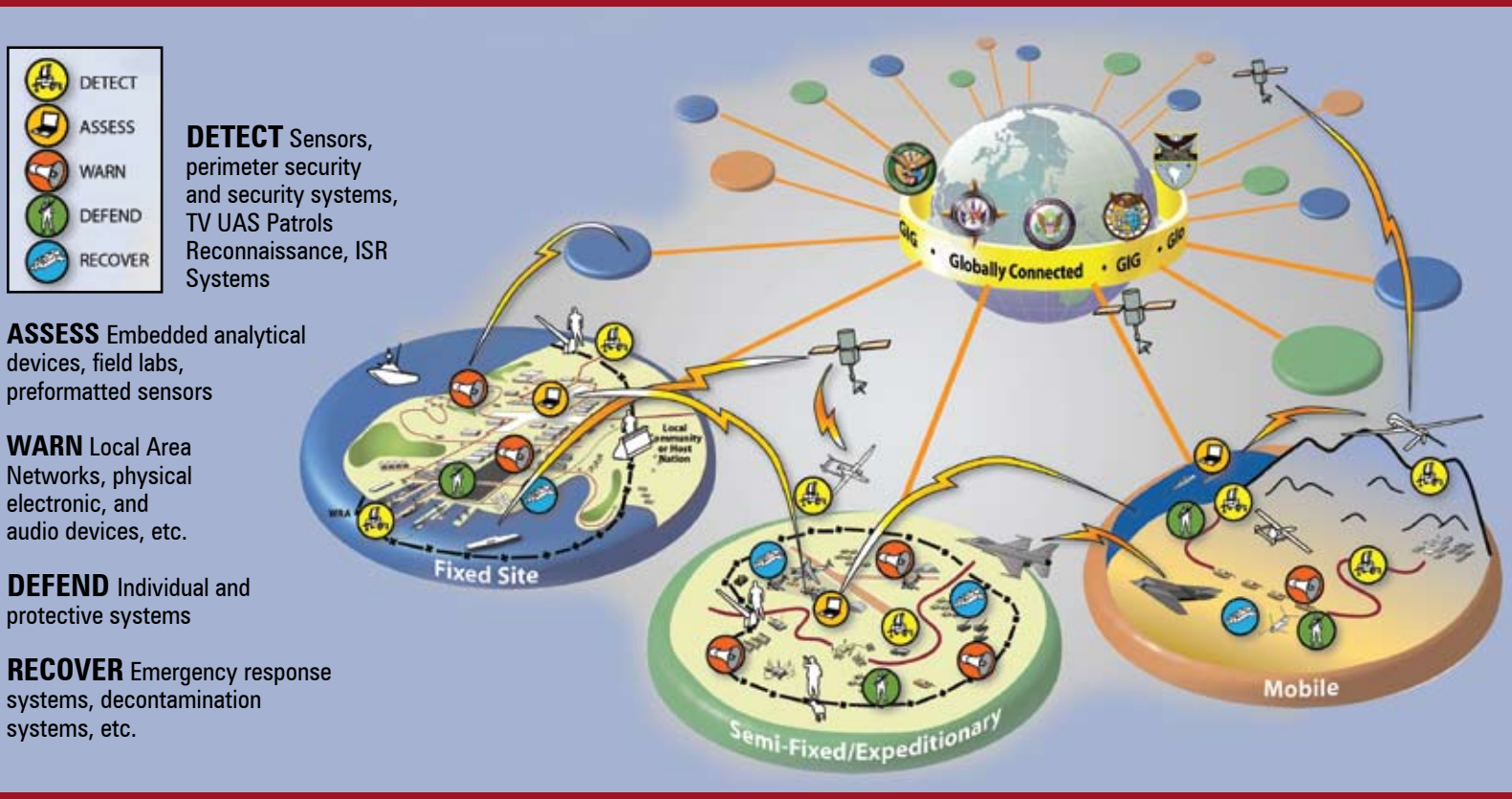


Figure 1. IUBIP's Operational View: OV-1

completion and approval of the final capabilities-based analysis product, the detect-assess-defend initial capabilities document, in September 2008.

Fiscal year 2009 is payday for the hard work that the IUBIP team has invested, a team spanning DOD from the United States Navy, United States Army, United States Air Force, and United States Marine Corps representatives at Fort Leonard Wood and Norfolk to the Service staffs, joint staffs, and OSD secretariats. Without question, the team's performance has been admirable, selfless, and beyond reproach. Thanks to the support of the Assistant Secretary of Defense for Homeland Defense (ASD-HD); the Director of Operations for the Joint Staff (J-3); the Army Deputy Chief of Staff for Programs (G-8); and the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD), fiscal year 2009 work is funded. Preparations are on track.

In fiscal year 2009, the Fort Leonard Wood joint team will produce the interoperability and detect-assess-defend DOTMLPF change recommendations with nonmateriel solutions to be approved by the JROC for rapid implementation across DOD. The Norfolk joint team will perform the IUBIP interoperability analysis of alternatives to define the future acquisition trade space (the degree of flexibility in trading performance objectives with costs against one another to achieve the best results) for protection and provide specific investment recommendations to the JROC and the Deputy Secretary of Defense's advisory working group.

Note: A future article will provide an overview of the DOTMLPF change recommendations and analysis of alternatives processes.

Special thanks are given to the following commands and offices for particularly significant contribution and support: CJCS Operations Directorate (J-3); CJCS Force Structure, Resources, and Assessment Directorate (J-8); CJCS Command, Control, Communications, and Computer Systems Directorate (J-6); USA Maneuver Support Center (MANSCEN), USA Capabilities Integration Center (ARCIC), USN Commander Naval Installations Command (CNIC), USAF Office of Aerospace Studies (OAS), USAF Air Armament Center (AAC), USAF Directorate of Security Forces (A7S), USAF Directorate of Operational Capability Requirements (A5R), USMC Force Protection, USMC Capabilities Development Center (MCCDC), USMC Plans, Policies & Operations (PPO), USN Deputy Chief of Naval Operations Director, Assessments Division (N81), USN Naval Surface Warfare Center (NSWC), USN Naval Expeditionary Combat Command (NECC), USA Deputy Chief of Staff for Programs (G-8), USA Deputy Chief of Staff for Operations (G-3), USA Air Defense School and Center (ADSC), Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD), US Transportation Command (USTRANSCOM) J3, USTRANSCOM J5J4, USTRANSCOM J2, US Central Command (USCENTCOM) J3, Defense Intelligence Agency (DIA), Assistant Secretary of the Navy for Installations and Environment (ASN I&E), ASN Identity Management (IM), Assistant Secretary of Defense for Homeland Defense (ASD-HD), Under Secretary of Defense for Acquisition, Technology and Logistics (USD-ATL), USD for Intelligence (I), OSD Networks and Information Integration (NII), Defense Acquisition University (DAU), DOD Physical Security Equipment Action Group (PSEAG), Defense Threat Reduction Agency (DTRA), Unified Cross Domain Management Office (UCDMO), Department of Homeland Security Science and Technology (DHS S&T) and DHS Office of Infrastructure Protection (OIP). Editorial Review: Mr. Nash Howell, Mr. Joe Heck, Mr. Dwight Grose, Mr. Don Murray, and Mr. Mark Ferguson, USA MANSCEN, Fort Leonard Wood, MO.

Understanding the Threat:
American Embassy team, Thai security officials work together to protect visiting US military forces

By Scott M. Bernat

Scott M. Bernat is an NCIS special agent assigned to FPD Thailand as chief of US naval security. He also is a member of the US Navy League's Thailand Eastern Seaboard Council. During his 21-year career, Bernat has deployed throughout Asia, Australia/Oceania, Central America, Europe, the Middle East and the United States in direct support to the US Navy. He recently was selected to establish an FPD at the US Embassy in Jakarta, Indonesia. Beginning in July, he will be the resident agent in charge and chief of US military security there.

Thailand's southern insurgency, political instability and military coups all remain critical factors in determining the correct force protection posture for US Navy deployments to the "Land of Smiles."

The security of visiting ships, aircraft, personnel and associated equipment is dependent on an excellent understanding of the threat environment, as well as the capabilities, limitations and intentions of Thailand's security forces. Thailand's southernmost provinces routinely experience unrest, with frequent deadly attacks on not only public officials and religious figures, but also civilians. Attacks include the use of improvised explosive devices (IEDs), armed ambushes and assassinations.

The US government halted US Navy ship visits after the Thai military-led coup of September 2006, which ousted then-Prime Minister Thaksin Shinawatra. A series of unsolved IED bombings in the capitol city of Bangkok followed several months later. Speculation as to the perpetrators ranged from pro-Thaksin supporters to southern insurgents. Graft and corruption allegations and court proceedings involving public officials remain commonplace.

Full US military engagement with Thailand, to include US Navy ship visits, was restored following the democratic elections in December.

The complexity of Thailand's security environment requires that US deployed military forces remain vigilant and set appropriate force-protection measures.

An effective force-protection program accounts for all seen and unseen challenges and mitigates the threat through an aggressive host nation engagement strategy.

Force protection is a continuous campaign that does not begin and end with the arrival and departure of visiting forces. It is dependent

Environment Observations

Force Protection Detachment (FPD) Thailand is directly involved in operationally preparing and monitoring the environment for this month's Cobra Gold exercise.

- The FPD presents and participates in US–Thai security seminars.
- It deploys various security-related equipment to Thai security forces.
- Members conduct port, airfield, route, exercise, and liberty venue vulnerability surveys and monitor and report on the overall threat to deployed forces.

on a thorough understanding of the threat and operating environment, as well as the interoperability of American and host nation security forces.

The US Navy relies on multiple sources to ensure the safety and security of forces transiting through or visiting Thailand. External sources of force protection support include the American Embassy Country Team—comprising the Defense Attaché Office and Force Protection Detachment (FPD) and the US Naval Criminal Investigative Service (NCIS)—as well as the local Royal Thai Police and military, who provide critical land-based and waterborne security.

The cooperation and teamwork established among these key partners, through routine liaison and engagement, ensures a comprehensive understanding of the threat and security force-mitigation capabilities, allowing for the development of an effective security plan.

Thailand hosts more than 40 US military exercises, seminars and exchanges each year, with some events involving more than 5,000 US military participants. US Navy ship visits average two or more per month, with deployed personnel numbering from 50 to 7,000. The average length of each ship visit ranges from one to seven days. US military aircraft visits average two to three per week.

The period between the coup and the recent elections, however, was marked by a significant decline in US military traffic in Thailand.

As a permanent American military presence is not maintained in Thailand, US Pacific Command (PACOM) is dependent on the FPD to operationally prepare the environment through the continuous interaction with, and support to, Thailand's security forces.

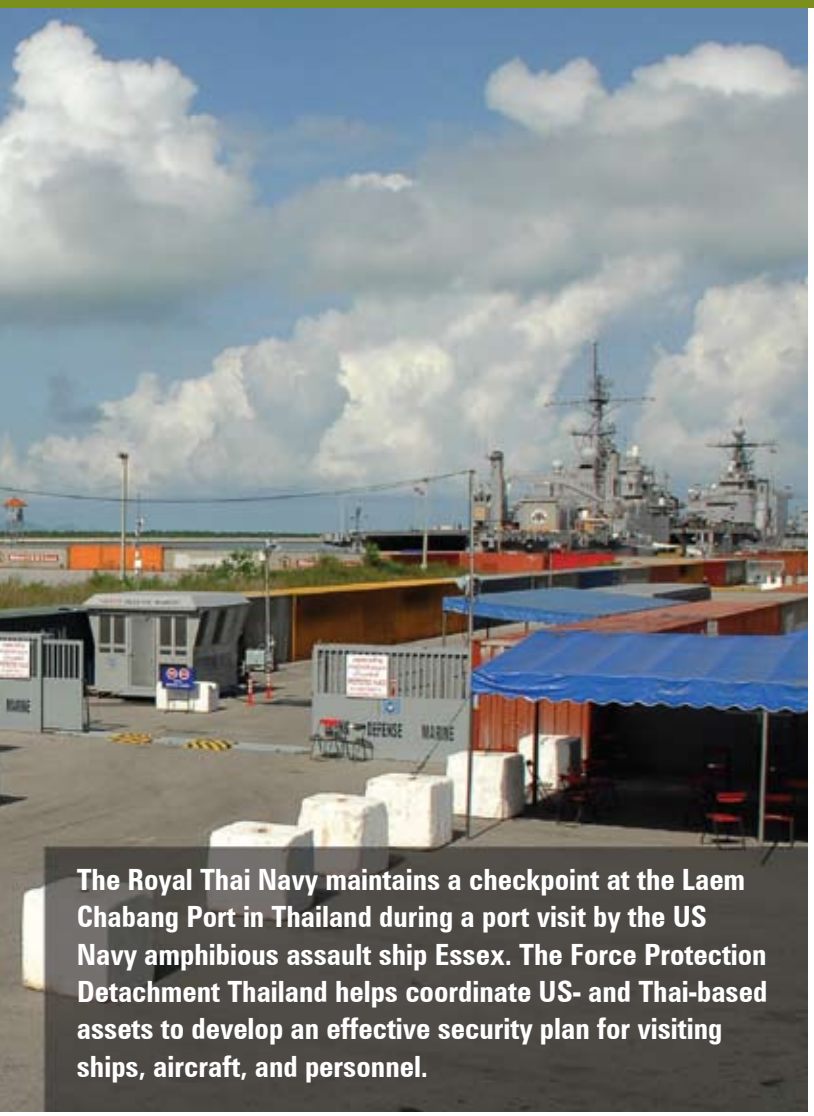
FPD Thailand is led by a US Army Military Intelligence agent, David L. Turner, with additional staffing by NCIS and US Air Force Office of Special Investigations special agents. Through the development of overt information sources and associated threat reporting, port, airfield, route, lodging, training area, and liberty venue vulnerability assessments, the conduct of security seminars and subject matter expert exchanges, as well as the deployment of various force protection-related equipment (e.g., bomb-suppression blankets, search mirrors, and hand-held and walk-through metal scanners),the FPD is able to identify potential threats. It also promotes mutual understanding and interoperability between American and Thai security forces.

The security of visiting ships, aircraft, personnel and associated equipment is dependent on an excellent understanding of the threat environment, as well as the capabilities, limitations and intentions of Thailand's security forces.

While FPD Thailand provides continuous in-country security engagement and expertise, the overall effectiveness of its port, route and liberty area security initiatives is enhanced by NCIS asset integration and support.

The NCIS Multiple Threat Alert Center, based in Washington, provides visiting ships, aircraft and personnel with threat analyses, assessments and alerts. Major military exercises, such as Cobra Gold and Cooperation Afloat Readiness and Training (CARAT), as well as routine ship visits, are often supported through the collective effort of FPD Thailand and NCIS personnel deployed from Singapore or assigned to visiting aircraft carrier and expeditionary strike groups.

Cobra Gold, which this year takes place May 8–21, is an annual PACOM-sponsored exercise designed to improve US joint and multinational interoperability and capability to effectively respond to and execute



The Royal Thai Navy maintains a checkpoint at the Laem Chabang Port in Thailand during a port visit by the US Navy amphibious assault ship Essex. The Force Protection Detachment Thailand helps coordinate US- and Thai-based assets to develop an effective security plan for visiting ships, aircraft, and personnel.

complex multinational operations. The total number of participants this year could exceed 10,000 personnel, numerous ships, military aircraft, vehicles and equipment.

Planned direct participants include US forces from various commands, the Royal Thai Armed Forces, Singapore Armed Forces, Japan Self Defense Forces, and Indonesian National Defense Forces.

Planned observer nations include China, South Korea, Sri Lanka, Pakistan, Nepal, Vietnam, Cambodia and Laos. Other possible participants include Australia, Brunei, France, Italy, the United Kingdom, Bangladesh, India, Malaysia, Mongolia, and the Philippines.

Security Assistance, Assessment

In addition to augmenting FPD Thailand activities, deployed NCIS personnel provide proactive and reactive criminal investigative support to visiting American forces. NCIS Security Training, Assistance and Assessment Teams are used, in direct coordination with the FPD, to not only conduct port and airfield vulnerability assessments, but develop, present and participate in law enforcement, safety and security seminars with the Thai Police and military. These seminars, primarily focusing on port, transportation route and liberty area security concerns, promote theater security cooperation and provide the foundation for security force mutual understanding and interoperability.

The US Navy uses Royal Thai Navy and commercial berthing facilities, both pier-side and at-sea anchorages. Ship security postures vary with location, mindful of Thai government restrictions against foreign security personnel disembarking weapons or other equipment, such as bulletproof vests, handcuffs, and batons.

Naval facilities rely heavily on Thai military security, while the use of commercial facilities requires the combined force of private security guards, Thai military and civilian police. In addition, the US Navy-contracted husbanding agent, Glenn Defense Marine (Asia) Co. Ltd., with its inventory of force-protection equipment—X-ray machines, walk-through metal detectors, floodlights, barricades, picket boats, secure waterborne perimeters, hand-held metal detectors, bomb sensors and detectors, K9 units, and closed-circuit TV cameras—and a Nepalese Ghurka security contingent provide critical and essential assets to deter, detect and counter potential threats.

The challenge of implementing an impenetrable port/berthing area security plan is to ensure the interoperability and mutual support of all security forces, American and Thai. The omission of interoperability plans and training creates an unknown factor unacceptable to the establishment of a solid security posture.

Interoperability and integration of security plans, policies, procedures, and force protection equipment is essential to a seamless approach to a potential threat.

Due to the short length of port visits, work/repair schedules, and a desire to maximize liberty time following intense deployments, it is not always possible for visiting commands to participate in interoperability planning, seminars, or training. These activities are usually relegated to specific American–Thai military exercises such as Cobra Gold and CARAT, often not including ships that will eventually visit Thailand's ports.

FPD Thailand and NCIS, through continuous coordination and interaction with visiting ships' force-protection personnel and Thai security forces, fill the gap and assist in the development and oversight of effective and mutually supportive security plans.

Threat Awareness

The security of American forces does not end at the port. Transportation routes to and from liberty areas, as well as the actual liberty areas, require as much, if not more, security planning and attention. It is outside the port area that US Sailors and Marines are the most

US EOD team members discuss explosive ordnance logistics with Royal Thai Navy EOD team members during Cobra Gold 2006 in Sattanhip,Thailand. Cobra Gold is an annual joint training exercise aimed at developing interoperability, strengthening relationships between Services, and developing cross-cultural understanding among participating nations. [*Photo credit US Navy]*

vulnerable and exposed to potential criminal and terrorist threats.

Awareness of the threats and the application of common sense are the first lines of defense for all personnel. Local police provide the physical presence to detect and deter the threats, while unarmed and discreetly dressed American shore patrol personnel are deployed to assist service members and achieve and maintain an appropriate individual force protection posture.

Additional security personnel and measures can be implemented, depending on the level of a threat, in and around vehicle pick-up/drop-off points and liberty venues. Local police need to fully understand their role in protecting American service members, as well as be professionally capable of accomplishing the task.

To meet this objective, many Thai law enforcement officers, attend the FPD-sponsored security seminars and training, focusing on direct security support to US service members.

Visiting US Navy ships, aircraft, and personnel require the most accurate threat and security force information in order to plan for and accomplish a safe and secure visit. Although there are no absolutes or guarantees, the effective use of all available force protection resources, both Thailand-centric and shipboard, mitigates the threat and maximizes the potential for success. The comprehensive force-protection program instituted for Thailand provides commands with the necessary information and assistance to effectively manage potential risks.

Reprinted with the permission of Seapower *magazine.*

Notes from the War on Terror

Overcoming the ideology of hate and terror

Information collected by the J-5
Strategic Plans and Policy Directorate

"As you track these numbers month by month, you do see peaks and valleys in levels of violence. It is not surprising to see peaks in the spring and summer. The biggest concern is the sheer levels of violence incrementally increasing since 2002. The biggest concern is that violence levels are higher than they ever have been."

Seth Jones
Rand Corp. expert on Afghanistan
Washington Post
2 July 2008

"It is just plain embarrassing that al Qaeda is better at communicating its message on the Internet than America. As one foreign diplomat asked a couple of years ago, 'How has one man in a cave managed to out-communicate the world's greatest communication society?'"

Defense Secretary Robert M. Gates
Islam Online
Qatar – 24 June 2008

"The word 'jihad' means to 'strive' or 'struggle,' and in the Muslim world it has traditionally been used in tandem with 'fi sabilillah' ('in the path of God'). The term has long been taken to mean either a quest to find one's faith or an external fight for justice. It makes sense, then, for terrorists to associate themselves with a term that has positive connotations. For the United States to support them in that effort, however, is a fundamental strategic mistake. American leaders would do best to call terrorists by their rightful name: 'terrorists.' The label may seem passé, but terrorism is an internationally recognized word for an internationally recognized crime. If we want to win a war of words, we would do well to choose the ones we use with greater care."

P.W. Singer and Elina Noor
New York Times
2 June 2008

"You are not going to hear me say that al Qaeda is defeated, but they've never been closer to defeat than they are now."

US Ambassador Ryan Crocker
Denver Post
25 May 2008

"Any peace agreement that does not move the effective writ of the Pakistani government into the tribal region and push the rule of law there gives these groups the opportunity to continue to train, refit, and move across the Afghan border. It's something we certainly could not look kindly on."

Lt. Gen. Michael Hayden
CIA Director
AP
27 May 2008

"But let me be clear: we will not be satisfied until all the violent extremism emanating from FATA is brought under control. It is unacceptable for extremists to use those areas to plan, train for, or execute attacks against Afghanistan, Pakistan, or the wider world. Their ongoing ability to do so is a barrier to lasting security, both regionally and internationally."

John Negroponte
Deputy Secretary of State
Daily Times
7 May 2008

"He who is able to fix the public utilities holds the keys to the kingdom in terms of winning the support of the Iraqi people and ultimately ending this conflict. People tell me time and time again that they see their basic needs as being more than food, clothing, and shelter; they include electricity, water, and sewage and until the Iraqi government provides them with such basic services, they won't trust them."

Sgt. Alex J. Plitsas
312th Psychological Operations Company, Company B, First Battalion, 14th Infantry Regimente
New York Times
22 April 2008

Notes from the War on Terror

Current events and their effect on the Global Antiterrorist Environment (GATE)

Information collected by the J-5 Strategic Plans and Policy Directorate

	Event	Strategic Significance
Negative effects on the GATE	**US Deaths Rise in Afghanistan.** June was the deadliest month for US troops in Afghanistan since the war there began in late 2001, as resilient and emboldened insurgents have stepped up attacks in an effort to gain control of the embattled country.	June marked the second month in a row in which militants killed more US and NATO troops in Afghanistan than in Iraq. Attacks have increased 40 percent this year from 2007 in areas where US troops operate along the Afghan/ Pakistan border, and a recently published Pentagon report indicates militants will maintain or increase their attacks.
	Hundreds Escape in Taliban Prison Attack. More than 600 prisoners escaped during a brazen Taliban bomb and rocket attack on the main prison in southern Afghanistan that knocked down the front gate and demolished a prison floor, officials said Saturday. At least nine police officers were killed.	The well-planned and coordinated attack had been planned for two months, according to a Taliban spokesman. Many, if not all, of the Taliban militants that escaped from prison linked up with Taliban forces in Arghandab to reinforce their troop strength. If Taliban militants control Arghandab, they would be in perfect position to launch ambushes and attacks on Kandahar city more easily than any other place in the province.
Uncertain effects on the GATE	**US Losing to Media-Savvy Qaeda.** With sophisticated, high-tech tools and a growingly powerful online machine, al Qaeda is winning over the United States in the long-run propaganda war. US officials and experts admit that Washington is losing the media platform to al Qaeda and its affiliates.	The war against terror is being fought not only with bullets and bombs but also with the Internet and television. Al Qaeda's voice has grown more powerful over the past few years by taking advantage of new technology, enabling it to communicate constantly and more securely. Al-Jazeera was al Qaeda's preferred media outlet; however, in 2005, they had stopped airing al Qaeda videos in their entirety. Al Qaeda now uses as-Sahab, an in-house propaganda studio. Videos released by al Qaeda can now appear online within days of being recorded.
	9/11 Accused Asks For "Martyr's" Death. Khaled Sheikh Mohammed, the alleged mastermind of the 9/11 attacks on the World Trade Center and the Pentagon, told a US military tribunal that the death penalty would allow him to achieve his goal of becoming a "martyr."	Khaled Sheikh Mohammed (KSM) is the former senior operations chief for al Qaeda. His arrest marks one of the most important breakthroughs in the fight against al Qaeda. KSM has always maintained that he was the mastermind behind the September 11, 2001 attacks. If he and his four co-defendants are convicted and put to death, they would be elevated to martyr status. Martyrdom is the highest honor that could be bestowed upon an extremist and it may possibly encourage others to take up arms against the US.
Positive effects on the GATE	**Pentagon to Charge Saudi in USS COLE Bombing.** The Pentagon said Monday it is charging a Saudi Arabian with "organizing and directing" the 2000 bombing of the USS COLE—and will seek the death penalty.	Abd al Rahim al-Nashiri claims that he confessed only to stop being tortured. In 2002 and 2003, al-Nashiri was subjected to waterboarding, and any evidence gathered then could be deemed inadmissible. Al-Nashiri has been linked to (1) 1998 East Africa US Embassy bombing that killed 224 people; (2) the 2002 attack on the French supertanker S.S. *Limburg* that killed one crew member and spilled 90,000 barrels of oil; and the (3) 2000 failed attempt to bomb the USS THE SULLIVANS.
	Iraq Begins New Crackdown on Shiite Militias. The crackdown in the southern part of the country began June 19 in the Maysan province and its capital Amarah, a region US commanders say is used as a base to smuggle weapons from neighboring Iran.	As Prime Minister Nouri al-Maliki seeks to assert government control over the country, he launched his fourth US-backed Iraqi military operation against Sunni and Shiite extremists. Gunmen had four days to surrender their weapons or face arrest. Some handed in weapons while others threw them into the streets or canals. As a result of the operation, Iraqi security forces have located large weapons caches and munitions.