The Source for Antiterrorism Information

Fall 2010 | Volume 12 | Issue 3

The GUARDIAN

Antiterrorism Journal

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

The Pentagon, Room MB917 | Washington, DC 20318

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

Historical Antiterrorism Quotes

June 1985

"Over the past few years, many demands have accumulated requiring more resources, both financial and human, in the area of security. Security has not traditionally been given a high priority by diplomatic establishments."

—The Inman Report, conducted in response to the 1983 attacks against the Marine barracks and the US Embassy in Beirut, Lebanon.

30 August 1996

"Force protection is a mission for every member of the Armed Forces from the newest recruit to our most senior commanders. Terrorists have the luxury of searching for a single vulnerability. Only a coordinated, dedicated effort will deter them."

—General Wayne A. Downing, US Army (Ret.), in his Report of the Assessment of the Khobar Towers Bombing (1996). He also notes that "much remains to be accomplished to ensure that our units stationed overseas make this heightened awareness part of their daily routine."

8 January 1999

"[We] were most disturbed at two interconnected issues: first, the inadequacy of resources to provide security against terrorist attacks and, second, the relative low priority accorded security concerns throughout the US government… Saving lives and adequately addressing our security vulnerabilities on a sustained basis must be given a higher priority by all those involved if we are to prevent such tragedies in the future."

—Admiral William J. Crowe, US Navy (Ret.) as Chairman of the Accountability Review Boards on the bombings of the US Embassies in Nairobi, Kenya and Dar es Salaam Tanzania in 1998. He also noted that the Boards were "struck by how similar the lessons were to those drawn by the Inman Commission over 14 years ago."

Corrections In our Summer 2010 issue, we attributed "RAVA: The Risk Analysis Vulnerability Assessment Process" to the wrong author. The actual author's name was Mr. Doug Haines, who works in the NAVFAC ESC Antiterrorism Services Branch.

The Guardian

Fall 2010 | Vol 12, Issue 3

Guardian readers,

It is with great pleasure that I present you the Fall 2010 issue of *The Guardian Antiterrorism Journal*, my first since assuming the position of J-34 Deputy Director for Antiterrorism and Homeland Defense. This issue is one of several recent efforts to provide the latest antiterrorism information to the Department of Defense community. Other Joint Staff publications include the *Chairman's Self-Help Guide to Antiterrorism* (released September 2010) and *Joint Publication 3-07.2 Antiterrorism* (released December 2010).

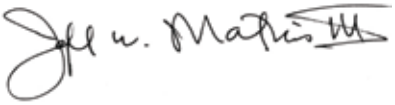
In this issue, *The Guardian Antiterrorism Journal* explores efforts to improve antiterrorism training and surveillance detection, as well as lessons learned from real-world events and exercises. These articles will enrich your tradecraft and are especially useful for Antiterrorism Officers seeking fresh material to incorporate into their curricula. Here is a summary of the articles:

- **Joint Task Force – National Scout Jamboree** recounts lessons learned from a large Boy Scout event on one of our installations.
- **A Force Multiplier for Force Protection** presents a convincing case for expanded use of surveillance detection throughout the DOD.
- **Antiterrorism Is Everybody's Job** draws on field experience to explain ways to improve antiterrorism awareness at all levels of command and throughout the local community.
- **Countering a Subterranean Threat to the Homeland** introduces the threat and use of illegal cross-border tunnels into our homeland.
- **Under Siege: Responding to a Mumbai-Style Attack on the Homeland** details lessons learned from the November 2008 terrorist attack in Mumbai, India, and discusses how we might respond to a similar attack.
- **Slashing the Enemy's Achilles' Heel** discusses the effective use of surveillance detection to prevent terrorist attacks.

I encourage you to share your experiences and lessons learned by submitting essays and book reviews to future issues of *The Guardian*. All works should be sent to guardian@js.pentagon.mil or submitted via the Antiterrorism Enterprise Portal on Army Knowledge Online/Defense Knowledge Online.

Terrorism—as a tactic of illegal violence and a movement that perverts otherwise peaceful philosophies—is not going away. In fact, we should assume that it will only get worse until we defeat all the networks that promote violent extremism at home and abroad. Thus, as antiterrorism professionals, we need to constantly evolve how we share information, manage risk, and train our people. My staff and I are here to assist you in these efforts.

For those who submitted articles to this issue, I would like to personally commend you for taking the time to put pen to paper to expand the professional knowledge of the DOD community. And for our readers, I would like to thank you for making this journal your source for AT/FP theory and practice. My predecessors were wise to note the relevance of Thomas Jefferson's words: "The price of freedom is eternal vigilance." Indeed, your continued vigilance is what keeps this nation free.



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

Photo by Mark Duncan

JOINT TASK FORCE NATIONAL SCOUT JAMBOREE

JTF–NSJ provides security at anniversary celebration

By LTC Jason Strickland, Military Executive, Army GEOINT Office at the National Geospatial-Intelligence Agency

The Boy Scouts of America celebrates its 100-year anniversary during a 10-day jamboree event held at Fort AP Hill.

Fusion in Motion

"Be Prepared," the motto of all Boy Scouts, served as an appropriate reminder to the assembly of more than 1,700 Service members and civilians supporting the 2010 National Scout Jamboree (NSJ). The 100-year anniversary of the Boy Scouts of America (BSA) took the form of celebrations all across the world and reached its apex during the 10-day jamboree event held at Fort AP Hill (FAPH). This installation of only 400 garrison employees and staff became the 13th largest "city" in Virginia in the span of 24 hours, with the arrival of 35,000 Boy Scouts and 10,000 volunteers.

Joint Task Force (JTF)–NSJ, a dual-status command (with active and reserve components), was charged with helping make the event safe and secure.[1] A key task for the JTF was to detect, deter, and respond to hostile threats to the jamboree and the installation. One of the many ways the JTF fulfilled this mandate was through the creation of a fusion cell. The JTF-NSJ fusion cell brought

A key task for the JTF was to detect, deter, and respond to hostile threats to the jamboree and the installation.

together intelligence, law enforcement, FP, and critical infrastructure protection analysts to correlate, fuse, and analyze foreign and domestic threat intelligence to provide JTF-NSJ with timely operational awareness. The fusion cell linked closely with established interagency law enforcement relationships involving the Caroline County Sheriff's Office, the Virginia Fusion Center, the Virginia State Police, and the Federal Bureau of Investigation (FBI).

In executing fusion cell operations at the tactical level, JTF-NSJ took a deliberate step in addressing one of the focus areas recently announced by the commander of the North American Aerospace Defense Command (NORAD) and the US Northern Command (USNORTHCOM). With regard to the discipline of counterterrorism and FP, ADM Winnefeld states: "We will work to improve information sharing in order to better position ourselves to preemptively detect and protect against these threats, particularly in regard to our military bases and other infrastructure. This will include streamlining reporting systems and seeking new ways of developing and integrating information sources."

This brief article will discuss how JTF-NSJ executed two of the aforementioned charges at the tactical level of domestic operations, that is, the assimilation of a variety of information sources and the sharing of information.

Information Sources

At the tactical level, JTF-NSJ had access to numerous threat information sources.

Shortly after being assigned the mission as JTF-NSJ, the fusion cell requested access to Virginia-specific information on the Homeland Security Information Network (HSIN; http://www.dhs.gov/files/programs/gc_1156888108137.shtm). Most states have communities of interest where they share key information across critical sectors for the state. The HSIN community of interest for Virginia consists of three pages: Virginia, Virginia Law Enforcement, and Virginia Emergency Management. Access to this information provided an extremely valuable perspective on activities in the region. The daily tactical brief generated by the Virginia Fusion Center provided JTF-NSJ with relevant law enforcement–sensitive reporting from the seven Virginia State Police divisions throughout the state.

A New Jersey National Guard Blackhawk helicopter carrying hometown news reporters flies over the 2010 NSJ at FAPH, Sunday, August 1, 2010.
(Photo by M.P. King)

Having a nongovernment organization as the primary supported agency (BSA) created unique challenges for sharing information.

JTF's higher-echelon and adjacent headquarters provided action officer augmentation to the JTF-NSJ fusion cell. These subject matter experts, with access to the collaborative tools of their parent commands, brought an enormous wealth of resources, reach-back, and capability to the fusion cell. This augmentation included an FP specialist from Joint Force Headquarters–National Capital Region and a criminal intelligence specialist from US Army North/Joint Force Land Component Commander. Essentially, our access to their capabilities magnified the resources available, creating a comprehensive look at the potential threats.

A key component to JTF-NSJ's situational awareness and information sources came from the integration of an incident awareness and assessment (IAA) structure within jamboree operations. This IAA structure provided outstanding capabilities to the fusion cell as well as operators, planners, and first responders. This fixed, mobile, and aerial layered configuration consisted of 20 fixed "on-the-ground" electro-optical/infrared (EO/IR) imagery systems, two vehicle-mounted EO/IR imagery systems, one rotary-wing aircraft with EO/IR and full motion video (FMV), and two aircraft with EO/FMV (one had IR and wide-area surveillance capabilities). This array of observation platforms provided a crucial information source to quickly detect and assess potential threat activity.

JTF-NSJ took steps to liaison directly with the highest echelons in the federal government. Both the Department of Homeland Security (DHS) and the FBI provided representatives to JTF-NSJ. This marked the first time during a high-profile event (that was not a National Special Security Event [NSSE]) that both of these organizations sent envoys to a military headquarters. Usually, DOD sends representatives to the Multiagency Coordination Center during NSSEs held outside of Washington, DC, but that is not always reciprocated

because DOD is rarely the lead federal agency.

All of these resources provided the necessary tools to develop a comprehensive perspective on potential threats. The fusion cell considered many avenues of approach, domains, and information sources in preparing for and executing the NSJ. Using a traditional intelligence cycle (task, collect, process, exploit, disseminate), the fusion cell had the tools in place to fulfill the first four steps, but information dissemination was the next challenge.

Sharing Information

The methodologies used to disseminate and share threat information ranged from traditional to innovative. Landlines, chat rooms, organizational mail boxes, and document portals were integral for information flow during the jamboree.

Figure 1 depicts a traditional information sharing network. Bringing the core of the JTF down from the Geographic Combatant Command level, past the Service Component Command level to form a tactical-level command presented challenges in adjusting the paradigm for those employees working FP and intelligence issues at the strategic and operational levels. USNORTHCOM's Standing Joint Force Headquarters formed the core of JTF-NSJ and adjusted its information flow to break away from traditional partnerships and align itself with a new command and control structure. Instead of communicating directly with DHS, for example, fusion cell members interacted with a lieutenant

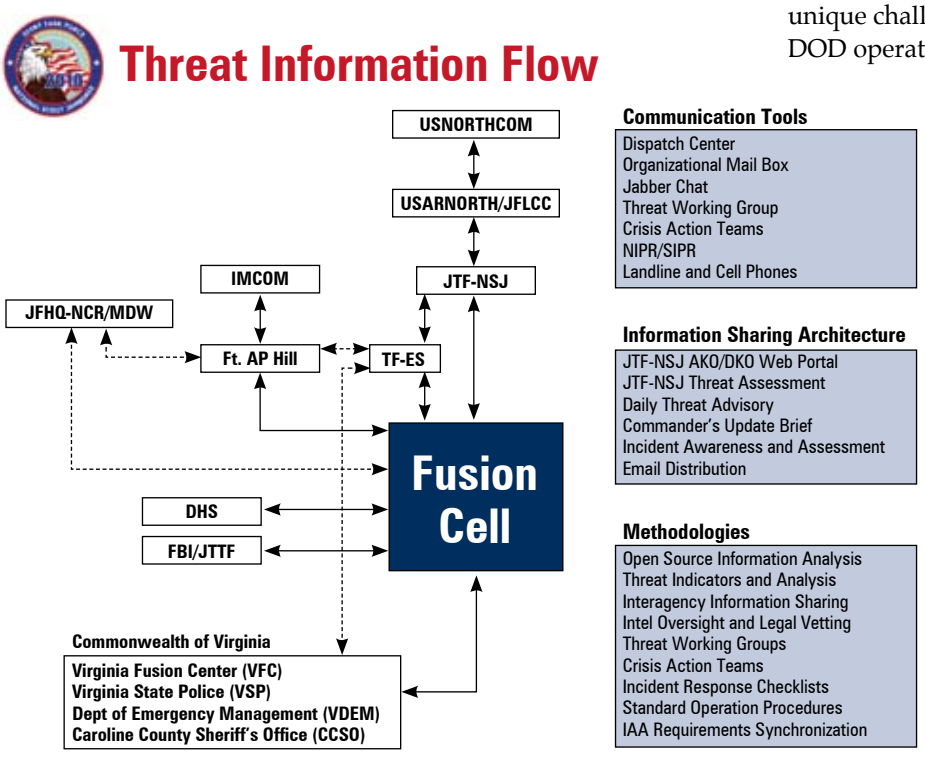


Fig. 1 Information Sharing Network

representing the county sheriff's office. This relatively easy modification allowed the fusion cell to share the wealth of information from a four-star headquarters and fuse it with the report from a cop on the beat in nearby Bowling Green, Virginia.

Common among DOD entities, extensible messaging and presence protocol Jabber Chat is the primary collaboration tool for sharing immediate, raw, and unvetted information within and beyond the JTF. Uncommon were the participants in the many chat rooms available to JTF-NSJ. Establishing another first, organizations external to DOD were provided with access to this chat client. By including non-DOD agencies (Caroline County Sheriff's Office, Virginia State Police, FBI, DHS) and even nongovernment entities (BSA), JTF-NSJ achieved an unprecedented level of collaboration.

Through agreements with relevant organizations, JTF-NSJ was able to appropriately share information with the BSA to protect the force, in this case, the tens of thousands of Scouts roaming the Army installation.

The daily JTF-NSJ fusion cell threat advisory served as another means of sharing information with task force partners. Having a nongovernment organization as the primary supported agency (BSA) created unique challenges for sharing information. Normally, DOD operates within strict information classification guidelines when sharing information; however, the supported agency (and the only reason for the existence of JTF-NSJ) could not be provided with relevant information due to classification or restriction policies. Through agreements with relevant organizations, JTF-NSJ was able to appropriately share information with the BSA to protect the force, in this case, the tens of thousands of Scouts roaming the Army installation. The threat advisory combined recent intelligence information with law enforcement reporting, resulting in a collaborative and analyzed unclassified product with an assessment written directly for the jamboree, JTF-NSJ, and FAPH.

Additionally, with information-sharing agreements in place, the BSA leadership team was incorporated

Subcamp 15 and 16 at the 2010 NSJ at FAPH, Monday, July 26, 2010.
(Photo by David Burke)

into threat working groups, bringing relevant organizations together to collaborate on risk mitigation strategies. In the event JTF-NSJ received classified threat reporting, representatives from subordinate task forces were prepared to take appropriate measures to protect the BSA staff, volunteers, and Scouts.

Conclusion

The 2010 NSJ was quite eventful for the Boy Scouts who arrived here from around the world. More than 70,000 people gathered to witness the Centennial Celebration Arena Show; the jamboree set the world record for the most people receiving certification in CPR; and thousands of Scouts took those vital steps necessary to achieve the coveted status of Eagle Scout.

In contrast, from the perspective of the fusion cell, this event was quite uneventful. No envelopes with white powder arrived on the installation, criminal activity was sporadic, and there was no need to raise the FP condition levels, aside from introducing various random antiterrorism measures. As planned, JTF-NSJ provided the BSA with a safe and secure environment for its jamboree, and the fusion cell used standard architecture to achieve a creative information-sharing construct. Innovative methodologies used in this unique domestic situation attempted to fulfill the charge from the commander of NORAD-USNORTHCOM. JTF-NSJ postured itself to receive information from myriad sources, to detect and deter potential threats, and to propagate reports rapidly.

Scouts mobilize toward the evening arena show at the 2010 NSJ at FAPH, Saturday, July 31, 2010. (Photo by M.P. King)

1 "Public Law 92-249, enacted on 10 March 1972, and codified as section 2554 of Title 10, United States Code, recognizes that Boy Scout Jamborees may be held on military installations and authorizes the Department of Defense, in support of Boy Scout Jamborees, to lend certain equipment and to provide transportation from the United States or military commands overseas, and return, at no expense to the United States Government, and to provide other personnel services and logistical support to the Boy Scouts of America to support national and world gatherings of Boy Scouts at events known as Boy Scout Jamborees: Now, therefore, be it Resolved by the Senate (the House of Representatives concurring), That it is the sense of the Congress that the Department of Defense should continue to exercise its long-standing statutory authority to support the activities of the Boy Scouts of America, in particular the periodic national and world Boy Scout Jamborees."

10 USC § 2554(i): "(1) The Secretary of Defense shall provide at least the same level of support under this section for a national or world Boy Scout Jamboree as was provided under this section for the preceding national or world Boy Scout Jamboree. (2) The Secretary of Defense may waive paragraph (1), if the Secretary— (A) determines that providing the support subject to paragraph (1) would be detrimental to the national security of the United States; and (B) submits to Congress a report containing such determination in a timely manner, and before the waiver takes effect."

Innovative methodologies used in this unique domestic situation allowed JTF-NSJ to receive information from myriad sources, to detect and deter potential threats, and to propagate reports rapidly. As planned, JTF-NSJ provided the BSA with a safe and secure environment for its jamboree.

DOD photo by Cherie Cullen

A FORCE MULTIPLIER FOR FORCE PROTECTION

The Benefits of Integrating Surveillance Detection

By Laura Clark, Owner of Surveillance Detection Consultants, LLC

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

Most successful terrorist attacks against US interests included preattack surveillance on the target. In recent years, hostile surveillance efforts were conducted against military communities in Singapore; Quantico, Virginia; and Fort Dix, New Jersey. Terrorists do not wake up in the morning and attack because the sun has risen. They attack after having studied their target to determine what is required to plan and execute a successful attack, even one that involves suicide. This preattack surveillance is an integral part of the terrorist attack cycle and a common denominator in all types of attacks including bombings, armed assaults, abductions, and assassinations. Paradoxically, surveillance detection (SD) still has not become a fully integrated part of the security efforts for many organizations.

Preattack surveillance is an integral part of the terrorist attack cycle.

Integrated SD =

Vulnerability Assessments
+ Detecting and Reporting Indicators of Surveillance
+ Analysis of the Reported Data
+ Follow-up Actions/Response

Stretching Time

The timing of tactical warning is at the heart of SD. We can harden targets all day long, but at some point, we must realize that our enemies gain tactical advantage if they are able to go undetected while conducting surveillance on the target and collecting information to plan and execute successful attacks. Even when detection occurs, if the data are not properly analyzed and acted on, that detection has little value.

In his report on the 1998 embassy bombings in East Africa, ADM William Crowe noted, "The Inman report and previous experience indicates that terrorist attacks are often not preceded by warning intelligence."[1] Author Paul R. Pillar echoes: "Post mortem studies of major terrorist incidents, such as the Downing report on Khobar Towers and the Crowe report on the East Africa bombings, have cited a lack of specific tactical warning even where strategic intelligence (that is, more general information on the level and sources of threat to US installations in a given country) was good."[2] Attacks occur in real time, in the here and now, thus any tactical warning that is limited to that same here and now only provides us with seconds to respond. Prevention happens prior to that here-and-now moment of attack.

When we take charge of the information that is observed and reported, we gain time for analysis of the data, investigation, and a potential countersurveillance operation.

To understand why SD is so effective, we must consider how our normal time paradigm must shift to work to our advantage. Tactical warning is defined as "a warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources."[3] If we consider hostile surveillance as the "initiation of a threatening or hostile act," we shift the time reference. SD inches us about as close as we can get to tactical warning of terrorist attacks but only if we are willing to accept the surveillance phase as the beginning of the attack. Instead of having only seconds to respond to the present moment in an attack, we now have hours, days, weeks, perhaps even months to prevent the attack altogether.

This does not mean we should panic and have a knee-jerk reaction to every reported incident of surveillance. It means we should take full advantage of the opportunity to follow up on the information. The stark reality is that, in most cases, if we detect someone exhibiting surveillance behavior toward a potential target, we cannot be certain which phase of surveillance they are in, according to the attack cycle. Are they early in the cycle, still trying to select the target that meets their needs? Or are they now using the information they are collecting to plan the actual attack against their already-selected target? For all we know, they are there the day before the attack, just as terrorists were conducting surveillance 24 hours before Khobar Towers were attacked in 1996.

In his report on Khobar Towers, GEN Wayne Downing advised: "Future intelligence collection and analysis must provide improved indications and warnings of attack and increased specificity at the tactical level. Because the terrorist has the ability to choose 'where, when, and how' he will attack, his actions will always be difficult to predict. He has the advantage of time—time to select his target and the choice of the exact time of attack."[4]

When we take charge of the information that is observed and reported, we gain time for analysis of the data, investigation, and a potential countersurveillance operation. Those efforts are fortified by our ability to take specific actions to mitigate the vulnerability in question. Whether that means we reconsider new ways to vary our routes and departure times as we travel to work because someone is watching our residence or we implement additional measures to harden security around a facility because someone across the street has been detected drawing a diagram of it, we can at least be proactive and prevention oriented.

Improving Vulnerability Assessments

The relationship between tactical warning and vulnerability assessments is worth exploring. By conducting an analysis of facilities and personnel for the purpose of identifying where, when, and how they are vulnerable to being attacked, we can use that information

DOD should empower all force members, at home and overseas, to participate in security of the whole. A standardized and streamlined SD approach ensures that everyone within DOD would receive similar knowledge and skills in the areas of surveillance awareness and SD as well as a standardized method of reporting their observations.

to take steps to mitigate the threats. To furnish tactical warning, some real-time information about hostile surveillance efforts must also exist as part of our vulnerability analysis.

After the embassy bombings in Africa, ADM Bobby Inman concluded that our "focus should be on vulnerabilities, not threats."[5] We have to know where to look when we are attempting to detect surveillance. Unfortunately, we tend to focus on locations where the targeted personnel or facility are vulnerable to being attacked rather than identifying where the hostiles would set up to watch these potential attack locations, especially attack locations where we cannot deny them access to information by cloaking our vulnerabilities. If we leave out this step, we run the risk of losing the opportunity to detect and report the preattack surveillance and to prevent the attack from occurring.

As one expert noted: "Tactical warning ... is an alert; it should denote that the activity of concern (such as a surprise attack) is immediately imminent or unfortunately underway. It should be specific with respect to where and when, even [if] it cannot answer who and how."[6] The "activity of concern" is the surveillance efforts detected. Hostile surveillance of the target's vulnerabilities informs the attackers (and us) about the where and the when. The Murrah Federal Building and the Khobar Towers, for example, were attacked at times when the facilities were most occupied, even though the former attack happened in the morning and the latter at night.

In summary, to be successful, those practicing SD must have a clear understanding of hostile surveillance efforts—one that is informed by vulnerability assessments. This is why so often those with only basic SD training are ill-equipped to be most effective.

Shared Security: The Power in Numbers

In discussing the Africa embassy bombings and the Department of State SD program initiative, ADM Crowe said, "Every person in our diplomatic missions abroad has to take greater personal responsibility for his or her security, including assisting in detecting efforts to surveil our facilities."[7]

ADM Inman added a critical realization about the guard force at our embassies abroad: "Those feet on the street were the only likely way of [receiving] any tactical warning that the embassy was under surveillance and ultimately might well become the target of an attack."[8]

These realizations led to the development of the Department of State's SD program, a more concerted effort to increase the "feet on the street" by adding trained SD teams out on the streets in plain clothes. Their role is to blend into the environment and to position themselves where they can detect and report surveillance activities against US personnel and facilities. Even in its infancy, the SD program proved its value not only for terrorism prevention but also for detecting criminal activity. As one expert noted, "properly integrated with the other elements of a security program, SD results in an immediate and significant increase in the security of both U.S. Government personnel and facilities."[9]

DOD should expand this vision by empowering all force members, at home and overseas, to participate in the security of the whole. A standardized and streamlined SD approach ensures that everyone within DOD would receive similar knowledge and skills in the areas of surveillance awareness and SD as well as a standardized method of reporting their observations. When people are trained to systematically observe, detect, and report repeated sightings, correlative behaviors, and suspicious

information, their minds will be prompted to notice what does not fit. Over time, it becomes almost effortless for a trained individual to immediately recognize anything out of the norm. To the average citizen living in Israel, for example, SD has become as much a part of life as looking both ways before crossing a street. It is a skill set that requires instruction and attention at first but that very quickly becomes second nature, a habit practiced effortlessly.

When people are trained to systematically observe, detect, and report repeated sightings, correlative behaviors, and suspicious information, their minds will be prompted to notice what does not fit.

Regardless of whether DOD opts to stand up extensive operational SD teams, the sheer numbers of the DOD population alone will exponentially boost the level of FP. Every housewife, teenager, soldier, and officer alike can use standardized templates to analyze their own on- and off-base patterns, routines, and vulnerabilities and to conduct SD on a daily basis.

Real-Time Intelligence Equals Real-Time Prevention

In any strategy to deter terrorism, removing the ability for the enemy to undermine us is always crucial. The irony of a force that is fighting terrorism and that cannot protect its own would be a public relations problem that would entice terrorists to scout military targets. Hostile surveillance efforts against the force pose an insidious threat, and successful attacks against any part of the US military population only embolden the enemy.

Last year at a Joint Staff event, AT officers and other FP specialists ranked what they would most like to see in the new AT Level 1 training. Wisely, they ranked SD very high on the list. Integrating a more detailed SD program across the DOD for both active and reserve components around the world will mitigate risk and enhance security of all facilities and personnel inside and outside the continental United States, including families, service members, civilians, contractors, and security forces.

By empowering everyone to take a participatory role in FP, security is no longer the sole responsibility of a small group. Real-time information collection feeds and affects the overall strategic efforts and increases the odds of preventing real-time attacks. The force itself, using SD, will boost the overall security efforts and thus will act as a force multiplier for the information line of defense.

Additional Benefits of SD as a Force Multiplier

- Sensitizes the DOD population to the threat of elicitation of information by both terrorist and foreign intelligence entities
- Enhances the relationship between the FP and counterintelligence elements and the base populations
- Fosters in-depth, DOD-wide trend analysis of community predictability and vulnerability
- Facilitates the necessary discreet, nonconfrontational demeanor required when reporting any people who appear to be conducting surveillance
- Discourages racial profiling by teaching the observer to focus on indicators and behaviors versus stereotypes and appearances
- Enhances discreet detection and reporting of insider threats
- Helps prevent crime against the population and facilities
- Improves the effectiveness of surveillance cameras (by empowering those who man the cameras in real time to detect indicators of surveillance)

1 Crowe, William J. "Report of the Accountability Review Board on the Embassy Bombings in Nairobi and Dar es Salaam on August 7, 1998." January 8, 1999. See Executive Overview Number 5. Available at http://www.fas.org/irp/threat/arb/board_overview.html

2 Pillar, Paul R. *Terrorism and U.S. Foreign Policy*. Washington, DC: Brookings Institution Press, 2001. p 110.

3 Joint Publication 1-02.

4 Downing, Wayne A. "Report to the President and Congress on the Protection of U.S. Forces Deployed Abroad" (see "Part I: Background, Terrorism—An Undeclared War Against the United States"). August 30, 1996. Available at http://www.dod.gov/pubs/downing_rpt/unclf913.html

5 Inman, Bobby R. "Admiral Inman Speaks on the Bureau of Diplomatic Security's Surveillance Detection Program." Garmisch Conference for Diplomatic Security. Germany, circa 1999 [video from the author's personal library].

6 Cooper, Jeffrey R. "Commentaries: Warning Analysis for the Information Age: Rethinking the Intelligence Process" (see Overall Comments, p. ix). Joint Military Intelligence College: Washington, DC: Joint Military Intelligence College, 2003. Available at http://www.dia.mil/college/pubs/pdf/3245.pdf

7 Crowe, William J. "Admiral Crowe Speaks on the Nairobi and Dar es Salaam Accountability Review Boards." Garmisch Conference for Diplomatic Security, Germany, circa 1999 [video from the author's personal library].

8 Inman, Bobby R. "Admiral Inman Speaks on the Bureau of Diplomatic Security's Surveillance Detection Program." Garmisch Conference for Diplomatic Security. Germany, circa 1999 [video from the author's personal library].

9 Venekamp, Clint. "Surveillance Detection Program." US Department of State Bureau of Diplomatic Security UPDATE [newsletter]. April–September 2000. p. 7.

ANTITERRORISM IS EVERYBODY'S JOB

US Marine Corps photo by Lance Cpl. Carlos Sanchez/Released

AT measures must utilize all personnel

By Evelyn Byrd, Antiterrorism Specialist (Busan), US Army Garrison Daegu, ROK

The military has become more attuned to the need for an alert and aware populace in deterring, detecting, and preventing terrorist attacks.

Each person in the military community has a role in deterring, detecting, and preventing acts of terrorism. In the military community, we have become familiar with the standard AT roles and responsibilities for commanders, AT officers, contract security guards, and law enforcement officers. We may not be as familiar with how other military-related personnel—family members, taxi drivers, maintenance workers, and others within our local communities—can contribute to the AT awareness picture. AT is everybody's job, from the President of the United States to the maintenance crew chief conducting routine inspections.

All of the military Services have been affected by terrorist and criminal attacks using a variety of tactics. The Marines Corps suffered losses in 1983 in the bombing of the barracks in Beirut, Lebanon. Air Force personnel were killed and wounded at the Khobar Towers dormitory bombing in 1996. The Navy ship USS COLE was attacked in Yemen in 2000. Most recently, the Army's Fort Hood installation was the target of an active shooter. As a result of these and other attacks, the military has become more attuned to the need for an alert and aware populace in deterring, detecting, and preventing terrorist attacks against so-called hard and soft locations. Using a sports analogy, this means the entire team must be active, including the coach, first-string players, those on the bench, trainers, the front office, and the fans. Fitting examples of civic diligence include the heightened awareness in New York City following the World Trade Center bombing in 1993 and the attacks of September 11, 2001. Notably, the recent vehicle bombing attempt in Times Square was diffused based on the awareness and sense of civic duty of a street vendor on the scene.

Commanders

Commanders are responsible for the protection of personnel from terrorism and other hazards, and they have the authority to take appropriate measures to reduce risk and increase protection. Certainly, any awareness program or suspicious activity reporting program is only as good as the command emphasis behind it. One could also argue that all of the elements addressed in this article will have increased effectiveness only with the participation of the entire chain of command.

US Forces Korea recently held its first-ever "Antiterrorism, Force Protection and Consequence Management" symposium in Seoul. The presence of multiple installation and area commanders added intangible and tangible results. Their visible presence alone raised the level of significance of the event. In addition, their comments and questions appropriately enriched the discussions while leading to realistic actions during the table-top exercise. This type of command-level participation can have a significant impact on an AT program.

Commanders also have a role as individual Service members to report suspicious activities they may encounter in the course of performing their duties. It is quite possible that a commander could become aware of an insider threat, for example, in the course of performance counseling, evaluation, or even routine staff meetings. After being reported, that kind of information will become a part of threat analysis, investigation, or disposition. Insider threat tips for commanders are available for review on the Army's Antiterrorism Enterprise Portal on Army Knowledge Online.[1]

AT Officers

The AT Officer (ATO) is probably the most recognized member of the AT team because the ATO's responsibilities are focused on advising commanders and guiding the awareness aspects of an AT program. Army Installation Management Command's (IMCOM) Higher Headquarters Assessment Team recently stressed the nature of the ATO job as "coordinator" of the AT program. In this coordinator role, the ATO can take advantage of a number of useful tools that are available from the Office of the Provost Marshal General to help increase AT awareness. These tools can facilitate spreading the message to military communities Servicewide. Additionally, ATOs, either directly or through AT working groups, can make full use of established communications channels and resources provided by Public Affairs and Morale, Welfare, and Recreation directorates.

ATOs should also be aware of best practices in the area of AT awareness. Best practices are consolidated and available from major commands and Service assessments teams, not to mention various newsletters and publications available from a number of AT organizations. The Joint Staff's *The Guardian Antiterrorism Journal*; Headquarters, Department of the Army's *The Sentry*; and IMCOM's *Warrior* are all excellent sources of best practices discovered across commands. The ATO Refresher Course also offers opportunities to stay up on the latest, most effective tools being used by ATOs.

Contract Security Guards

As Col Shannon Jurrens notes in his article "Slashing the Enemy's Achilles' Heel," (see page 39) the four fundamental principles of surveillance detection are to (1) stay informed, (2) stay low key, (3) stay unpredictable, and (4) stay alert. Therefore, contract security guards are uniquely fitted to be at the forefront of the surveillance detection mission.[2]

IMCOM Korea currently maintains a contract for security guards on Army installations. These guards provide an around-the-clock source of information on possible surveillance within their purview. At some locations, they are armed not only with weapons but with surveillance detection techniques, including sketches and overlays of possible terrorist surveillance locations and the tools necessary to capture images. Recently, our subject matter experts provided these guards with additional training to give them an edge in the urban environment, which is rich in high-rises and full glass windows with direct line of site to access control points.

IMCOM Korea currently maintains a contract for security guards on Army installations. At some locations, they are armed not only with weapons but with surveillance detection techniques, including sketches and overlays of possible terrorist surveillance locations and the tools necessary to capture images.

Military Police

The US Army Military Police School (USAMPS), Force Protection Training Division, provides essential skills and advance training to DOD personnel in the diverse fields of FP and AT by increasing security awareness and effectiveness. The 45-day Police Academy training specifically includes "police skills and first responder tactics" that are critical to AT programs.[3]

The US Army Military Police School (USAMPS), Force Protection Training Division, provides essential skills and advanced training to DOD personnel in the diverse fields of FP and AT by increasing security awareness and effectiveness. (US Army photo by Sgt. Jeffrey Alexander/Released)

In the framework of police and first responder training, two elements require further emphasis. The first is the use of secondary devices by terrorists. In recent years, secondary devices have been used in attacks in Bali and Beirut with the objective of targeting first responders as they approach the scene of an attack. USAMPS' access control handbook also addresses secondary devices as a threat to security personnel.[4] The second situation is a cross between maintaining AT awareness and general situational awareness. This need was demonstrated after the Oklahoma City bombing attack. After the attack,

Discipline, rigorous training, and situational awareness are needed so that terrorists are not able to exploit gaps in coverage.

Timothy McVeigh was pulled over by an Oklahoma patrol trooper for a traffic violation. At the time, most available law enforcement officers were being called into Oklahoma City to respond to the attack. Trooper Charlie Hanger was instructed to remain in his sector of operations, which he did, and he promptly arrested McVeigh on suspicion of illegally concealing a handgun, not knowing that he was involved in the attack. In any case, discipline, rigorous training, and situational awareness are needed so that terrorists are not able to exploit gaps in coverage.

Family Members

DoD Directive 2000.16, AT Standards, contains a very specific definition of family members derived from Title 10 of the US Code. This definition includes spouses, children, adopted children, and stepchildren of Service members as well as DOD civilians. According to AT Standards, family members 14 years or older (or younger at the discretion of the DOD sponsor) require Level 1 AT awareness training. Particular attention is placed on those assigned overseas.[7] For broader antiterrorism awareness purposes, "family members" should also include those visiting such as parents, grandparents, aunts, uncles, and family friends. This aspect is often overlooked. Even an internal family briefing session should include terrorism indicators and community-specific suspicious activity reporting procedures.

Resources for these family briefings can include the latest AT Level 1 Web-based training, which contains new information on insider threat and active-shooter response. One incident highlighted in the Web-based training is the kidnapping of BG James L. Dozier in Verona, Italy, in 1981. In this case, Red Army Brigade terrorists exhibited extensive suspicious behavior during their 30-day operational surveillance, which included watching the site with binoculars, picnicking across the street as a couple without children (which was unusual there), loitering near bus stops or taking a bus and returning quickly, and posing as a pair of utility meter readers (the norm was to have only one). This sort of behavior, some of which was later recalled by family members, should have been preemptively reported as suspicious by the general's family members.

In the past, US analysts and military forces have protected against one tactic while terrorists invented another. The asymmetric threat environment requires us to abandon conservative expectations in favor of creative AT measures.

Host-Nation Employees

For commands outside the continental United States, host-nation employees must be included in any discussion of AT awareness. These partners have close ties in and likely spend more time around the local community. They will have a better understanding of cultural norms and, therefore, a keener sense of what activities would be considered unusual behavior. One of the best ways to take advantage of these partnerships is to have AT Level 1 awareness training translated and presented by appropriate personnel. This training should also include specific and accurate suspicious activity reporting procedures. For US Forces in South Korea and Japan, this method has become an effective part of the local AT awareness programs.

Local Community

In the fight against terrorism, community involvement opportunities in and around installations are virtually endless. The key to success for involving the local community is to ensure an understanding of suspicious activity indicators and to create a willingness to report suspicious activity. In the interest of brevity, we will focus on one pool of candidates: professional drivers.

In the course of their typical duties, taxi drivers are required to be alert and aware of all hazards including safety, fire, or even destructive weather. Tailored awareness training for taxi drivers provides a valuable layer of high-exposure AT protection. The other group of professional drivers involved is school bus drivers, including dispatchers. During a recent exercise, we realized the need to consider appropriate measures to protect school buses, also noting the inherent power bus drivers had over access control. Tailored awareness training for drivers will only expand the local AT awareness paradigm.

Maintenance and Service Workers

An installation's footprint often extends far beyond the fence line. Pipelines, switching stations, communications sites, and piers may be included in a command's list of facilities. Although ATOs or physical security personnel may visit those sites intermittently, maintenance and service workers are inevitably more familiar with what is and is not normal in terms of appearance and operation. During routine visits to off-post sites, ATOs and physical security personnel should brief maintenance and service workers on how to look for tampering or breaches and perhaps deliver a full set of tools for surveillance detection.

In the past, US analysts and military forces have protected against one tactic while terrorists invented another. The asymmetric threat environment requires us to abandon conservative expectations in favor of creative AT measures. With this in mind, we must utilize personnel at all levels. The maintenance crew conducting routine service or the crew chief doing monthly inspections may prevent the next deadly attack on Americans and our allies.

---

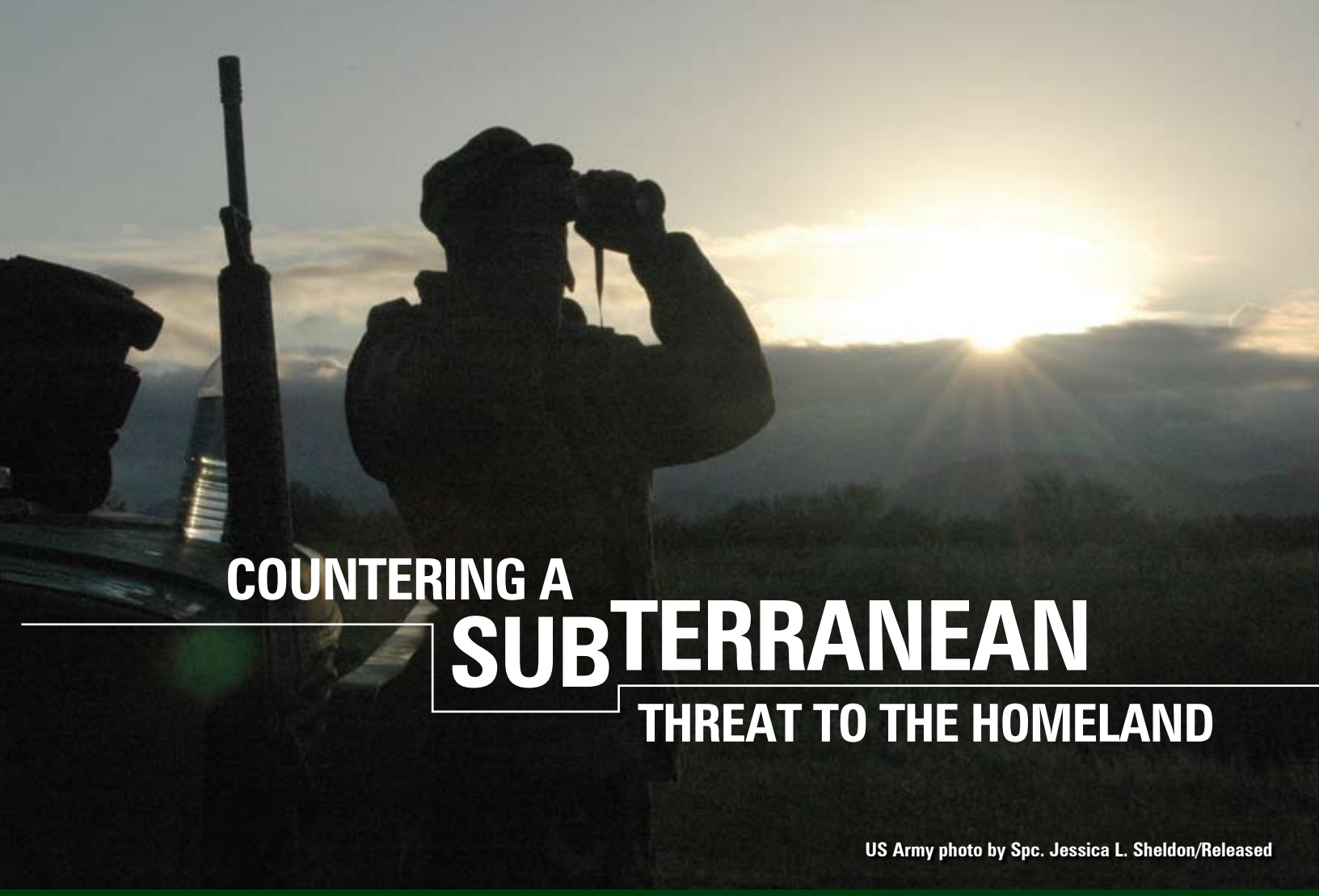
1 "Tips for Commanders: Suspicious Activity Reporting." Available at: https://www.us.army.mil/suite/doc/22539698 [restricted site].

2 Jurrens, Shannon D. "Slashing the Enemy's Achilles' Heel." *The Guardian Antiterrorism Journal*. Fall 2010, p 35.

3 "USAMPS Knowledge Network on AKO, Force Protection Training Division (FPTD)." Available at: https://www.us.army.mil/suite/portal/index.jsp [restricted site].

4 "TC 19-210 Access Control Handbook, Self-Protection Measures," paragraphs 5–12. Headquarters, Department of the Army.

5 DOD Directive 2000.16, AT Standards, Standard 25.



COUNTERING A SUBTERRANEAN THREAT TO THE HOMELAND

US Army photo by Spc. Jessica L. Sheldon/Released

A new threat emerges beneath US borders

by LtCol Chris Downs, Dr. Jason R. McKenna, and Amy L. Clymer

Cross-border tunnels have become an effective means for illegal passage into the United States.

Over the course of the last two decades, an evolving threat has emerged to challenge the territorial integrity and national security interests of the United States. This threat does not come in the form of a commercial airliner transformed into a fuel-laden cruise missile, a weapon of mass destruction smuggled into a container-laden port facility, or an extremist willing to trade his life for an explosive suicide attack. Instead, this new threat is quietly yet persistently emerging beneath our nation's borders.

Illegal cross-border tunnels have become an effective means for criminals, illegal aliens, and potential terrorists to clandestinely gain access to and distribute contraband throughout the homeland. It is necessary to organize, train, and equip our nation's military and law enforcement professionals to effectively detect and locate purpose-built tunnels and deny their use to adversaries.

Equally important, our national leadership must also develop strategic guidance, multidepartment policy, and effective interagency processes that will enable not only timely and reliable tunnel detection and interdiction but also the identification, engagement, and defeat of the illicit networks that are constructing and using these cross-border tunnels to threaten the security and interests of the American people.

The ongoing use and construction of cross-border tunnels represent growing threats to the homeland. Since 1990, 118 cross-border tunnels have been discovered by law enforcement agencies. All but one have originated in Mexico and terminated in California or Arizona. Forty-one tunnels were discovered in 2008 and 2009 alone. Some of these tunnels are very simply built, just a few feet in diameter and only deep enough to bypass border fences and other obstacles. Other tunnels are built to make parasitic use of storm drains, culverts, and other

legitimate underground infrastructure that links many US and Mexican cities. Still other tunnels represent relatively complex engineering undertakings. Some extend thousands of feet north of the international border with nearly 100-foot-deep vertical shafts, elevators, electric lighting, ventilation, and other amenities that increase the ability of those using them to efficiently move illicit contraband into the United States.

As detailed in the President's Southwest Border Counternarcotics Strategy released in June 2009: "The marked increase in the number and sophistication of tunnels along the Southwest border could likely be a result of increased CBP [US Customs and Border Protection] pressure against narcotraffickers and their traditional surface mobility corridors into the homeland. More aggressive enforcement on established overland routes since the 9/11 attacks probably has resulted in Mexican drug trafficking organizations turning more and more to tunnel construction."[1]

Our national leadership must develop strategic guidance, multidepartment policy, and effective interagency processes that will enable not only timely and reliable tunnel detection and interdiction but also the identification, engagement, and defeat of the illicit networks that are constructing and using these cross-border tunnels to threaten the security and interests of the American people.

DOD, the Department of Homeland Security (DHS), and the Department of Justice (DOJ) have correctly identified these tunnels as significant homeland vulnerabilities that constitute an unchecked method of entry for smugglers, illegal aliens, and other transnationals who may desire to carry out nefarious activities. Moreover, these clandestine tunnels offer a potential means for the introduction of weapons of mass destruction into the homeland. The recurring discoveries of tunnels originating in Mexico and crossing into the borderland of the southwestern states illustrate how ineffective existing efforts have been in preventing the use of purpose-built tunnels for narcotics and human smuggling. Despite the documented increase in tunnel activity, the intellectual and materiel investment necessary to counter this emerging threat has not yet been realized.

The countertunnel problem transcends securing and defending the homeland and the territorial integrity of our border. It is widely understood that tunnel detection and interdiction on the battlefield has been a persistent military problem for decades. Dedicated research and development funding to counter this problem started with the realization that the Cu Chi tunnels in Vietnam during the 1960s presented a clear and persistent threat to US troop mobility. The coevolution of a cross-border tunnel threat on the Korean peninsula during the 1970s sharply escalated investment in tunnel defeat with few tangible results.

More recently, a 2006 operational needs statement identified that detainees were attempting to build tunnels as a means to escape from theater internment facilities in Iraq. Although these operational issues are intimately related to the US campaign in Iraq, contemporary tunnel problems are not limited to that country. The flow of weapons, ammunition, and other contraband under the Egyptian border has contributed significantly to the ongoing Israeli-Palestinian conflict. Open-source estimates place the number of tunnels along the Israel-Gaza border between 300 and 1,000. Clearly, clandestine cross-border tunnels are a vulnerability of sufficient scope and magnitude to warrant the development of a coordinated interagency countertunnel capability.

Regrettably, the US government does not yet possess a fielded capability to address the tunnel detection problem in the homeland or in support of our deployed military forces. Given these circumstances, it is clear that the development and use of effective tunnel detection, localization, and characterization capabilities are necessary to protect our national interests.

In response to this dilemma, experts from DOD, DHS, commercial industry, and academia have been working tirelessly to counter this asymmetric threat. Over the past two years, the US Northern Command (USNORTHCOM), through its subordinate formation Joint Task Force–North, has conducted ten tactical missions along the southwest border to locate the presence of illegal cross-border tunnels. Through the use of maturing technologies, several of these missions have been successful in providing actionable intelligence for law enforcement.

Encouraged by these tactical successes, USNORTHCOM and DHS have cosponsored a three-year initiative to field a suite of complementary tools to detect and characterize cross-border tunnels. Their objective is to effect enduring tactical capabilities to detect, precisely locate, exploit, and remediate clandestine, purpose-built tunnels illegally entering the United States and on foreign battlefields. At the completion of this program, materiel solutions, concept of operations, and tactics, techniques, and procedures developed will be transitioned to DOD and DHS for doctrine, organization, training, material, leadership and education, personnel, and facilities (DOTMLPF) integration and subsequent organizational fielding.

This interagency initiative is the culmination of a four-year effort to satiate the demand for a reliable counter-tunnel program. USNORTHCOM began the project in 2005 as the "Tunnel Detection Initiative." The command's first steps in this effort involved the identification and

Since 1990, 118 cross-border tunnels have been discovered by law enforcement agencies. All but one have originated in Mexico and terminated in California or Arizona. Some of these tunnels are very simply built, just a few feet in diameter and only deep enough to bypass border fences and other obstacles. (US Air Force photo by Staff Sgt. John Wiggins/Released)

engagement of US government agencies, nongovernment agencies, academia, and private industry with existing countertunnel programs or potentially promising countertunnel technologies. To test and evaluate the utility of these of programs, USNORTHCOM hand-selected a group of nationally renowned subject matter experts in the field of geophysics. These experts vetted proposed materiel solutions against actual tunnel targets that had been discovered by law enforcement at a number of locations along the southwest border of the United States. The expert assessments revealed that although some sensors were promising, all of the proposed solutions lacked the technical maturity to produce reliable and consistent tactical results because these prototype technologies produced massive amounts of data and unacceptably high false-alarm rates. Hence potential users had very little confidence in either their accuracy or tactical utility.

The US government does not yet possess a fielded capability to address the tunnel detection problem in the homeland or in support of our deployed military forces.

Although USNORTHCOM was evaluating potential countertunnel solutions in the homeland, tactical events within Operation IRAQI FREEDOM also highlighted the need for tunnel detection technology in support of the military's expeditionary operations outside the continental United States. Subject matter experts from the US Army Corps of Engineers Engineer Research and Development Center built a government off-the-shelf system to address rapidly evolving tunnel detection requirements in Iraq. They named their solution the Tunnel Activity Detection System (TADS). This system was rapidly developed and tactically used in response to an operational needs statement to detect and confirm tunnel activity within theater interment facilities in the combat zone. The system worked. In fact, it successfully detected a tunnel that was built by the commander of an internment facility who initially doubted the reliability of the system.[2]

Since the first successful operational deployment of the TADS in 2007, the system has matured and markedly improved. Redesignated as the Border Tunnel Activity Detection System (BTADS), it has become the core technology for USNORTHCOM and the DHS countertunnel initiative. Moreover, the system has been fielded in support of our foreign allies and has demonstrated notable tactical effectiveness and operational utility in support of this international countertunnel effort.

In August 2008, USNORTHCOM began the process of presenting its tunnel detection initiative to the Office of the Secretary of Defense (OSD) for consideration as a FY2010–2012 Joint Capability Technology Demonstration (JCTD). A JCTD is an OSD-sponsored program to rapidly address combatant commanders' capability

gaps using innovative concepts and proven technology. As a result of the obvious homeland security benefit of this program, DHS readily embraced the proposal and aligned resources to support it. US NORTHCOM's tunnel detection initiative was redesignated the Rapid Reaction Tunnel Detection (R2TD) program and was presented to countertunnel stakeholders across the executive branch of the US government as one of the first-ever DOD-DHS JCTDs.

Over the past two years, the R2TD effort has matured and has successfully laid the technical foundation for the integration of complementary tunnel detection capabilities. Other technical systems, such as active seismic imaging, fiberoptic passive surveillance systems, electromagnetic induction, and ruggedized miniaturized robotics platforms used as a holistic, layered complementary systems have been aligned to further advance the countertunnel effort. This "systems" approach is intended to mature, integrate, and ultimately field a "tool box" of materiel solutions with layered components that provide applicability within a number of differing geologic, physical, and battlefield environments. This toolbox will increase the reliability and tactical utility of the layered technologies in support of military and law enforcement commanders' countertunnel requirements. If approved and funded by the US Congress, the R2TD JCTD will integrate these systems into a viable countertunnel capability set that can be readily used and maintained by trained military and law enforcement personnel.

It is important to note that cross-border tunnel detection is not solely a technological capability gap.

If approved and funded by the US Congress, the R2TD JCTD will integrate these systems into a viable countertunnel capability set that can be readily used and maintained by trained military and law enforcement personnel.

Organizational and policy hurdles must be navigated prior to fielding a countertunnel capability. Presently, there are layered and occasionally competing authorities, jurisdictions, and organizational priorities among various law enforcement agencies that often come together once the location of a suspected tunnel has been identified. Effective courses of action are debated and often delayed for months at a time when one law enforcement agency is focused on immediately closing the tunnel as soon as it is identified, whereas others advocate observing the target to build greater understanding and stronger case evidence regarding the network using it to move human and material contraband into the homeland.

To realize a true solution to this emerging national security issue, it is necessary to identify strategic goals and enterprise-wide policy to achieve unity of effort among all stakeholders for tunnel detection, exploitation, and remediation activities. Once attained, this guidance will frame the development of operational and programmatic objectives from which to generate and organize the resources necessary to realize an enduring and layered countertunnel capabilities set with which to execute preemptive and reactive tactical countertunnel tasks.

The collective efforts to effect an enduring capability to detect and precisely locate illegal cross-border tunnels will soon provide our nation's military and law enforcement professionals with needed technical capabilities and capacities to counter the gathering threat these illicit mobility corridors pose to our homeland.

It is equally important that our national leadership direct the promulgation of interagency processes that will enable effective tunnel prevention as well as resource and direct the research and development of improved technology to improve ground-based detection systems to airborne and, ultimately, spaced-based tunnel detection platforms. This capability will enable the interagency planning and process mapping necessary to develop an enduring multiagency methodology to best use the complementary tunnel detection technologies under development within the practical restraints and constraints of military and law enforcement realities. These collective activities are urgently needed to defeat the illicit networks building and using tunnels to threaten the security of the homeland.

Acknowledgments

The authors wish to express their thanks to the numerous federal law enforcement agents and agencies in DHS and the DOJ without whom this article would not have been possible. The director of the US Army Engineer Research and Development Geotechnical and Structures Laboratory as well as the commander, US North American Aerospace Defense Command (USNORAD)–USNORTHCOM, granted permission to publish.

The contents of this article reflect the personal views of the authors. The commanders, USNORAD-USNORTHCOM, US Army Engineer Research and Development Center, and Joint Task Force-North have approved this article for public release. It has also been approved for release by the chief, Office of Security Review, DOD.

1 "National Southwest Border Counternarcotics Strategy," Office of National Drug Control Policy (June 2009): 45. http://www.whitehousedrugpolicy.gov/publications/swb_counternarcotics_strategy09/swb_counternarcotics_strategy09.pdf

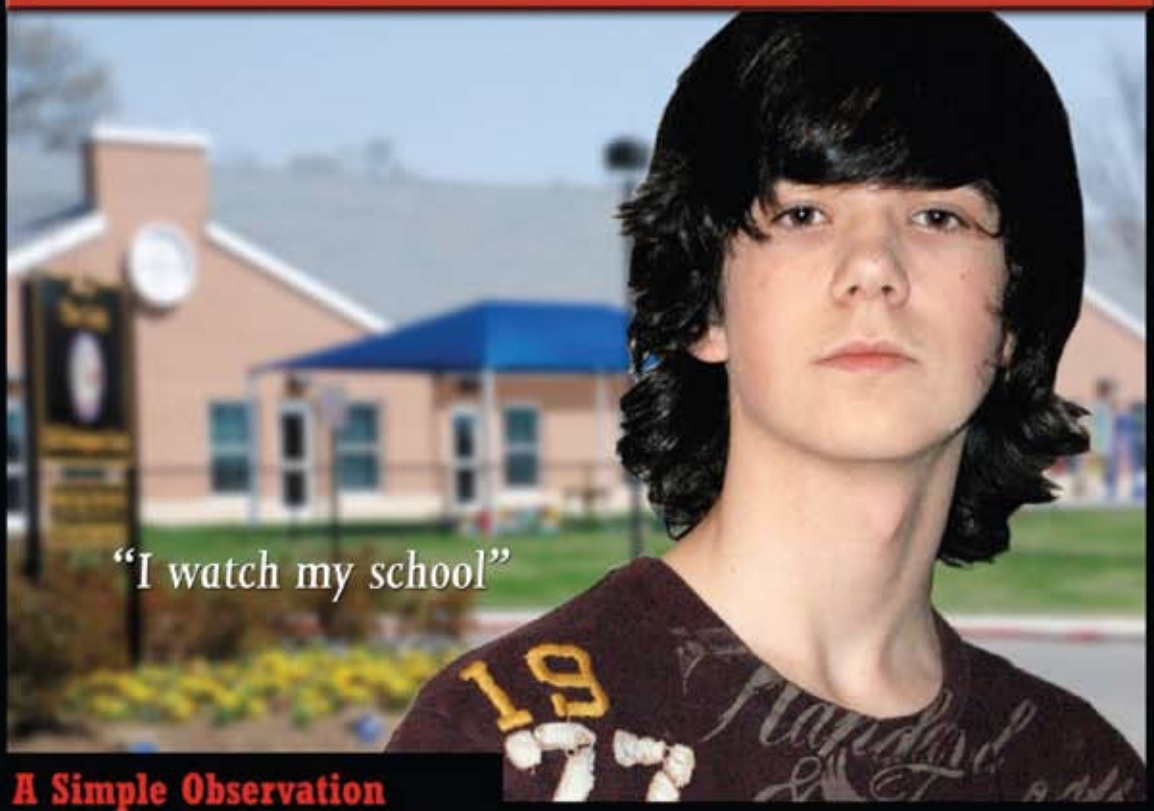
2 Clymer, Amy L. Interview with Colonel James Brown. Colorado Springs, CO: Headquarters, US Northern Command, January 10, 2009.


Watch This
"Standalone" may not be as alone as you think
Army Strong
U.S. ARMED FORCES
RECRUITING STATION
ARMY • NAVY • AIR FORCE • MARINES
Don't Be a Soft Target
We've learned many things from prior attacks. Terrorists target Army Installations and facilities; and they reconnoiter a target before they attack. Standalone facilities—inherently vulnerable—rank among the likeliest targets. But they don't have to be soft targets.
Be alert at all times for suspicious activity such as a person lingering curiously near an entrance or one asking unusual questions about a facility. Do that and your ordinary daily routine becomes part of a crucial Army-wide mission: protecting our Army community at home like we do abroad.
Always Ready, Always Alert
Because someone is depending on you

iWATCH ARMY

iREPORT

i KEEP US SAFE



A Simple Observation

A Single Report can lead to actions that may STOP a terrorist attack

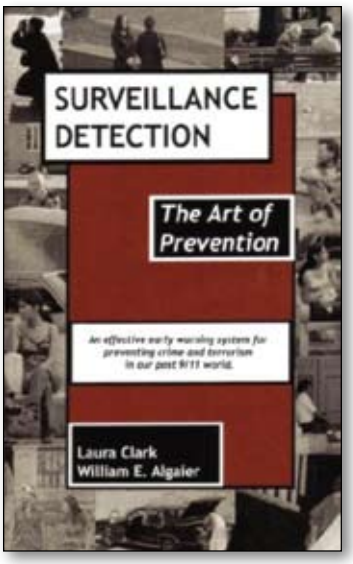
THINK ABOUT THE POWER OF THAT. THE POWER OF iWATCH.

See Something Say Something

Always Ready, Always Alert

Because someone is depending on you

Book Review



Surveillance Detection: The Art of Prevention

by Laura Clark and William E. Algaier

Review by LCDR Christopher F. Hill, USN

After the attacks against the US embassies in Kenya and Tanzania in 1998, the Department of State concluded that the vast majority of its facilities maintained poor security standards and were vulnerable to terrorist attacks. In conjunction with numerous physical security improvements, Diplomatic Security created "surveillance detection teams" to find preattack, terrorist surveillance directed at its facilities and officials. These teams have likely thwarted a number of attacks and saved American lives.

Diplomatic Security's surveillance detection program has increasingly informed the creation of other surveillance detection efforts across the US government, including DOD. As many of the articles in this issue point out, surveillance detection needs to be a part of everyone's routine rather than the domain of specialized experts. In their book *Surveillance Detection: The Art of Prevention*, Clark and Algaier provide an essential primer and resource for building a surveillance detection culture in any organization, whether military, civilian, or corporate. *Surveillance Detection* is a valuable resource for any unit Antiterrorism Officer, security professional, or law enforcement officer looking to beat the enemy well before an attack starts.

Surveillance Detection fills a vacuum where very little informative, open-source literature is available, especially for nonsecurity personnel. It details how terrorists and criminals operate to collect on individuals and resources, conveying real-world lessons learned where such surveillance was observed but little action was taken. It walks the reader through the implementation of travel route reviews, building reviews, use of cover, and technology— all with cogent examples including several advanced techniques of value to professional surveillance detection teams. Clark and Algaier address what they call the "James Bond Myth" by carefully outlining the sober, routine procedures necessary to disrupt terrorist or criminal preattack surveillance.

Clark and Algaier have decades of experience protecting key government resources and people in hostile environments. Their goal is to make "SD" a household term by making these concepts accessible to all in practical, entertaining language. As the authors note, "The more people out there practicing SD, the better chance we all have of preventing crimes and acts of terrorism."

Recommended Reading

J-34 Antiterrorism Reading List

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDER SIEGE:

RESPONDING TO A MUMBAI-STYLE ATTACK ON THE HOMELAND

DOD photo by Cpl. Albert F. Hunt, US Marine Corps/Released

Preparing for future large-scale attacks

By Lt Col Brad C. Felling, Air Force Reserve Officer, U.S. African Command Operations and Logistics Directorate

US agencies and departments work to examine preparedness for Mumbai-style attacks

American homeland defenders are quick to criticize the Government of India's (GoI) counterterrorism techniques, or lack thereof, in response to the November 2008 attacks in Mumbai. But several gaps would be apparent if the whole of the US government were required to counter a "Mumbai-style" assault in the United States. This article outlines the Mumbai attacks, examines a homeland defense simulation mandated by the National Security Council (NSC) to amplify gaps, and recounts recent success stories demonstrating what departments and agencies are doing to remedy deficiencies.

On November 26, 2008, 10 well-trained Lashkar-e-Taiba (LeT or "Army of the Pure") militants attacked seven targets and successfully detonated two improvised explosive devices (IEDs) in Mumbai, India. More than 60 hours later, when the GoI neutralized the last terrorist, 166 people, including 6 Americans, had been killed and 308 had been injured.[1] In 2008 alone, there were reports of three Mumbai-style attacks: the February assault on the Kabul, Afghanistan government buildings; the March attack on the Sri Lankan Cricket Team in Lahore, Pakistan; and the attack on the Manawan Police Academy, also in Lahore.[2]

How could such a devastating attack occur in a world-renowned city like Mumbai, the "Entertainment Epicenter" of India? Excerpts from a popular tour guide describe Mumbai, formerly known as Bombay, like this: "Measure out: one part Hollywood; six parts traffic; a bunch of rich power-moguls; stir in half a dozen colonial relics … add a smattering of swish bars and restaurants … equal parts of mayhem and order; as many bazaars as you have lying around … throw it all in a blender on high … and presto: Mumbai."[3] Mumbai is also a port city with a major financial center. These characteristics can be applied to many burgeoning metropolises in the United States.

Mumbai Attack Overview

Preoperational Reconnaissance

Up to two years prior to the Mumbai attacks, LeT operatives were making sketches of potential targets and stockpiling weapons.

Commando Assault by Well-trained Operatives

The sole LeT survivor, Ajmal Amir Kasab, told Indian authorities he had been preparing for the Mumbai attack for one year. His training focused on small arms tactics, marine assault, and close-quarters battle. He was also issued ten false identifications.[4]

Like the LA and San Francisco law enforcement officers involved in the US shootouts, the local Mumbai police were not equipped to confront heavily armed attackers. Rather than shoot back at the attackers, most first responders ran away, hid behind civilians, were wounded, or were killed.

Soft, Iconic Targets

The ten terrorists split into four teams, placed up to five IEDs around the city, and synchronized their conventional-style assaults on preidentified targets. They also knew that hitting their targets simultaneously would inhibit a properly coordinated response by Indian authorities. The targets were picked due to their landmark status, ensuring international media would be on the scene immediately.

Maritime Approach

The attackers used four different types of watercraft to travel from Karachi, Pakistan, to the Sassoon Docks in Mumbai harbor. They hijacked an Indian-flagged fishing vessel and killed the entire crew. After entering Mumbai harbor undetected, they boarded two rigid hull inflatable boats for their amphibious approach to the Sassoon Docks.

Communications

The attackers used voice-over-IP (VOIP) technology, BlackBerry smart phones, and fraudulently acquired Subscriber Identity Module (SIM) cards to coordinate their attacks with each other and with their leadership in Pakistan. As the LeT leaders watched the Indian security response on television news broadcasts, they relayed this real-time intelligence to the attackers in Mumbai.[5]

Simultaneous Attacks to Confuse Responders

LeT used armed assaults, car jackings, drive-by shootings, prefabricated IEDs, targeted killings (policemen and selected foreigners), building takeovers, and barricade and hostage situations.[6] The GoI thought they were under siege by a significantly larger force. The attackers opened fire in the emergency room of the hospital where ambulatory patients from the train station attack were being treated.

Military-grade Equipment

Each attacker was equipped with AK-56 (Chinese version of the AK-47) automatic weapons, semiautomatic 9 mm pistols, at least 300 spare rounds of ammunition, hand grenades, and IED-making equipment.[7]

IEDs

Each of the devices contained the high explosive RDX, ball bearings to create shrapnel, a digital timer, and a 9-V battery.[8] Three IEDs failed to detonate; two detonated via timing devices in cabs that were used to transport attackers to the train station and to the Taj Mahal Palace Hotel.

Social Media Exploitation

An estimated 80 messages, or "tweets," were sent to Twitter.com via SMS every five seconds, providing eyewitness accounts and updates. Some messages were coming from hostages inside the hotels. The GoI sent a message asking tweeters to stop sending messages from Mumbai; the GoI was worried that the terrorists were using the medium to gain information about what Indian security forces were doing.[9]

Counteroptions: United States Versus India

Although there has not been a parallel attack of this size and scope within the United States to compare response mechanisms and draw lessons learned, there have been events in which heavily armed gunmen seriously challenged law enforcement agencies in urban environments similar to Mumbai. Two specific 1990s shootouts that occurred in the two largest cities in California demonstrate that even well-trained and well-equipped law enforcement officers can be overmatched when engaged in paramilitary urban-combat situations.

On November 14, 1994, Victor Boutwell kept dozens of San Francisco Police officers at bay in the peaceful Pacific Heights section of the city for approximately 30 minutes before he was shot by a SWAT officer. Officer James Guelff, first at the scene and armed with a department-issued six-shot revolver, was killed in action. Boutwell, dressed in camouflage, two layers of body armor, and a bullet-resistant helmet, was armed with Belgian FB and Steyr automatic machine guns (both of which use M-16–compatible ammunition), an automatic pistol, two other handguns, and 2,500 rounds of ammunition.[10]

On 28 February 1997, two heavily armed gunmen, protected by body armor impenetrable by most caliber handguns, engaged numerous Los Angeles Police Department officers in a gunfight that lasted for 45 minutes outside a North Hollywood bank. The shootout occurred not far from the Disney, Universal, and Warner Brothers studios, and the busy Hollywood Freeway was closed in both directions, tying up midday traffic.[11] Stunned officers were out-gunned to such a degree that they burst into a local gun store and walked out with more powerful guns and ammunition. LAPD Police Commander Timothy McBride said, "We have many suspects who have multiple guns, and they continue to out-gun us and fire at us at will."[12]

A former CIA officer recently warned that Mumbai is the "worst-case active shooter problem" because it involved "multiple shooters, multiple locations, mobile threats, willingness to fight the first responders and follow-on SWAT/commando units, well-equipped, and well-trained operatives, and a willingness to die."[13] Like the LA and San Francisco law enforcement officers involved in the US shootouts, the local Mumbai police were not equipped to confront heavily armed attackers. Rather than shoot back at the attackers, most first responders ran away, hid behind civilians, were wounded, or were killed.

Surprisingly, in early 2008, the GoI had recognized these inadequacies and spent $187 million "modernizing" local, state, and national law enforcement. But instead of properly equipping their police officers, they built new police stations and administrative offices and purchased luxury sedans for senior officers.[14] To its credit, the GoI drafted a proposal to purchase AK-47 automatic assault weapons but never followed up. The Indian National Security Guard (NSG), loosely equivalent to the FBI Hostage Rescue Team, was the only group that had bulletproof vests at the time of the attacks.

Mumbai police also lacked the sophisticated technical equipment used by the attackers, including night-vision goggles, rifle scopes, and global positioning systems. State and local communication devices were old and incompatible. BlackBerry smart phones, a staple among Mumbai civilians, could have been used to exchange tactical data and monitor new coverage but were not issued to law enforcement officers.[15] The military on-scene commander, for example, did not comprehend the long-term ramifications when he ordered power turned off at the scenes of attack. One sharpshooter spent 60 hours stationed outside the Taj Majal Palace Hotel without firing a shot because he could not distinguish gunmen from civilian victims.[16]

Mumbai police had no equivalent to a SWAT team. After four hours of prolonged deliberations, the GoI made the decision that these attacks were more than random acts of crime. They also decided to send the NSG to Mumbai, but the NSG is headquartered in the Indian capital of New Dehli, 875 miles from Mumbai. Further complicating the problem, NSG is not colocated with its Russian-contracted aircraft. Due to the transportation problems and protocols requiring a written request for assistance prior to the release of NSG assets and manpower, another five hours passed before the specially trained NSG commandos arrived in Mumbai.[17]

Once the GoI intervened in Mumbai and took control, it was clear that there was inadequate on-scene command at attack sites. Authorities cleared sections of buildings but failed to secure them, allowing the terrorists to reestablish positions.[18] A victim claimed security personnel let him pass unchecked as he escaped from one of the hotels. NSG forces failed to identify themselves during the counterattack. Victims did not know if the NSG troops were terrorists or a rescue force.[19]

As mentioned previously, the terrorists exploited the media to their advantage; however, the media also may have directly interfered with response forces. Militants gained information about police actions while watching news broadcasts. The media also played a telephone conversation with terrorists occupying the Nariman House and the Oberoi Hotel. Media spokesmen later defended their actions, claiming they helped law enforcement officials find the terrorists.[20]

Preexisting command and control procedures, better training and equipment, and increased interagency intelligence sharing should lessen the consequences of a Mumbai-style attack in the United States.

US Preparedness Plans and Exercises

Preexisting command and control procedures, better training and equipment, and increased interagency intelligence sharing should lessen the consequences of a Mumbai-style attack in the United States. But has the law enforcement community significantly updated its procedures since Mumbai? According to a 2009 report released by the National Tactical Officers Association (NTOA): "Law enforcement is unprepared to respond to even a single terrorist attack on a soft U.S. domestic target, such as a school. If attacks such as the Moscow Theatre Incident (2002) or the Beslan school [North

The Protect and Defend the Homeland Group coordinated a table-top exercise simulating federal department and agency responses to an attack on a US city, mirroring the events in Mumbai. The participants chose Chicago due to its relatively similar geographic characteristics (e.g., port city, distance from national capital, tourist destination, financial hub).

Ossetia, Russian Federation 2004] should occur here [in the United States] in the near future, the loss of the lives of hostages, other civilians who might become involved, and first responders could be calamitous."[21] Soft targets like these within the United States are just as vulnerable as those attacked in Mumbai.

In December 2008, the NSC tasked the National Counterterrorism Center (NCTC) to evaluate how the United States would respond to a Mumbai-style attack. The Protect and Defend the Homeland Group within the NCTC Directorate of Strategic Operational Planning convened an interagency working group and coordinated a table-top exercise simulating federal department and agency responses to an attack on a US city, mirroring the events in Mumbai. The participants chose Chicago due to its relatively similar geographic characteristics (e.g., port city, distance from national capital, tourist destination, financial hub).

The exercise participants represented 14 federal departments and agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), DOD, and other intelligence agencies. Five state and local police departments representing Chicago, New York, Los Angeles, Washington, DC, and Illinois also participated.

The interagency participants received a notional intelligence bulletin warning that there was an imminent threat to the United States, possibly in the Chicago area, from a group of Canadian-Pakistani militants with dual passports working with al Qaeda; shortly thereafter, ten operatives in two teams infiltrated Chicago and attacked eight targets. One of the assumptions in the exercise was that federal assistance would be required because the attacks overwhelmed state and local law enforcement agencies.

Potential Gaps in US Preparedness

During the exercise, the participants identified some of the same lessons learned from the GoI Mumbai investigations. These included problems with sustainability and availability of specialized national response assets, impediments to intelligence and information sharing (e.g., releasing "tearline" messages), and the security risks associated with social media. These lessons also bring to light a number of federal, state, and local authority gaps that affect US preparedness.

Federal Authority Gap

Indian paramilitary forces, including the NSG, were severely outmatched in Mumbai, particularly in the area of equipment. This was the case despite the fact that Indian military and law enforcement agencies are legally authorized to conduct joint operations and training as well as use the same equipment. The rapid growth of internal GoI intelligence bureaus and the increased use of paramilitary forces against communal unrest have given the Indian Home and Defense Ministries increased control over paramilitary operations. Indian Army units, for example, are also deployed for internal security duty.[22]

In contrast, the US Posse Comitatus Act of 1878 does not allow DOD entities to conduct law enforcement operations without the concurrence of the president and the secretary of defense and upon the recommendation of the attorney general. One US legal statute, 10 US Code §380,23 is in place to facilitate equipping, training, and information sharing between DOD and state and local law enforcement agencies; however, it is irrelevant in

today's security environment, when so much emphasis is placed on homeland defense, specifically domestic counterterrorism operations. Besides being outdated, the program itself is underutilized.

Section 1033 of 10 USC §380 is tucked in an obscure section within Title X called "General Provisions." The main focus of General Provisions is counterdrug operations, not counterterrorism. Furthermore, it does not adequately address post-9/11 state and local law enforcement requirements by federal authorities, including preparations required for a response to a Mumbai-style attack in the United States.

The provisions for state and local law enforcement agencies to obtain information, equipment, training, expert advice, and other personnel support from DOD are inadequate and need to be modernized and signed into law.

10 US Code §380 (1033)[23]

The author's own investigation of federal agency awareness of the requirements outlined in 10 USC §380 revealed that several agencies were not aware of the provisions or were only partially compliant. Representatives of the Law Enforcement Support Office (LESO) at the Defense Logistics Agency (DLA), which operates the DOD Surplus Property Program, had never heard of the 10 USC §380 requirements.[24] DLA representatives stated they were in partial compliance through the activities of their Reutilization and Management Office, which sponsors an annual national conference of state LESO coordinators. This conference is mandated under 10 USC §380, and the state LESO coordinators are responsible for identifying excess military equipment that may be used by their state's law enforcement agencies. Notably, not all states and territories choose to participate in the LESO program, some due to lack of proximity to military installations and others due to lack of funds for training of reutilized equipment; still others are simply noncompliant with DOD regulations.[25] Furthermore, LESO does not provide any training, expert advice, or other personnel support to state and local law enforcement agencies when distributing reutilized DOD equipment, as stipulated in 10 USC §380.

New York is one example of a state that does not participate in the LESO program, despite being home to the worst terrorist attack in history. As LESO Deputy Director Craig Barrett noted, "New York is no longer in compliance with DOD regulations due to corruption charges and equipment misappropriation."[26] Barrett stated that New York officials had allegedly reutilized DOD property and then sold it for profit.

Other Authority Gaps

In the ensuing investigations following the Mumbai attacks, the GoI Administrative Reforms Commission recommended the legalized tapping of cellular phones and internet connections.[27] Although the GoI considered restricting media coverage of live emergency incidents, broadcasting networks agreed to "self-regulate" by implementing delays in live coverage and expunging information about operational details.[28] The Indian Constitution, although not mentioning the word "press," provides for "the right to freedom of speech and expression" (Article 19[1]a).

This right is subject to restrictions under Subclause 2, whereby this freedom can be restricted for reasons of "sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, preserving decency, preserving morality, in relation to contempt, court, defamation, or incitement to an offense." GoI laws such as the Official Secrets Act and Prevention of Terrorist Activities Act have been used to limit press freedom.[29]

Internal surveillance of US persons and forced self-regulation of media outlets is not in accordance with the First and Fourth Amendments of the US Constitution; however, following Mumbai, major US cities, like New York, are examining ways to shut down cell phones when dealing with hostage-taking scenarios. According to New York Police Department (NYPD) Commissioner Kelly in an open session of the Homeland Security and Governmental Affairs Committee: "Cell phones were simple tools used to deadly effect in the Mumbai terror attacks. According to phone transcripts, the attackers received instructions and real-time updates about the officers amassing against them. Some of the phones they used for the calls apparently were taken from hostages."[30]

Another gap, as noted earlier, is the sharing of information and intelligence from federal sources with the state, local, tribal, and private sectors. Despite the creation of regional intelligence centers (RIC), DHS, and the Office of the Director of National Intelligence, there are still challenges to overcome when sanitizing or producing tearlined classified intelligence reports for transfer to state and local agencies before and during attacks.

Information Sharing Success Stories

The US government and state and local agencies are collaborating with NCTC to remedy the gaps with regard to federal, state, and local authorities. Recent success stories suggest information sharing and technology transfer is improving.

Two days before the attacks on the World Trade Center and the Pentagon in 2001, for example, a Maryland State Trooper stopped 9/11 hijacker Ziad Jarrah for speeding near the Delaware state line. The trooper checked Jarrah's license and registration against a database of "wants and warrants," and it came back clean.[31] The trooper called the stop routine. He had no way of knowing that Jarrah was on a CIA watch list and that he was a key player in a major plot to attack the United States.

If Jarrah were stopped for speeding today, his information would be automatically queried in the FBI's National Crime Information Center (NCIC). His data would be checked against a master list of known or suspected terrorists. The presence of Jarrah's name on this list would raise a flag, and the trooper would be prompted to call the US Terrorist Screening Center (TSC). TSC analysts would run more extensive checks to see if the Jarrah at the traffic stop is the same one of interest to the intelligence community. The screening center would then guide the trooper through some questions for Jarrah or contact an operational unit to coordinate a response, such as an FBI-led Joint Terrorism Task Force.[32]

An example of how this screening process works occurred in Maryland in August 2005. Muhammad Asif Haider was a passenger in a vehicle stopped by Baltimore County Police because the vehicle's lights were not on. The driver could not produce a driver's license, so the officer ran a criminal history check on the driver and the passengers. The NCIC database matched Haider to the terrorist watch list. The arresting officer contacted his operations desk, which alerted the local FBI.[33] Haider was later indicted.

Conclusion

The international intelligence community warned the GoI twice that Pakistani-trained militants would attack Mumbai up to a year in advance of the attacks.[34] Even with these advanced warnings, the GoI was unable to deter or counter the Mumbai attacks effectively. How would the US government respond if foreign intelligence services shared information pertaining to a pending attack against the homeland?

The provisions for state and local law enforcement agencies to obtain information, equipment, training, expert advice, and other personnel support from DOD are inadequate and need to be modernized and signed into law. This will remove ambiguity and strengthen the "whole of government" approach to homeland security.

The deadly attacks in India may have provided a low-frills but bloody blueprint for other violent groups to follow, NYPD Commissioner Kelly and other US AT officials told Congress during a hearing in 2008. "I think we can expect that groups will look to that [Mumbai] as a model for themselves," Chief FBI Investigations Officer Donald Van Duyn said at the hearing.[35]

One should look to interagency lessons learned and success stories to set proper benchmarks for increased cooperation in the future.

In 2008, GEN (Ret.) Barry R. McCaffrey, former commander, US Southern Command, and former director, National Drug Control Policy, stated, "Terrorists will strike at America during the Obama Administration's first term."[36] It is difficult to counter the argument that there are gaps within the US government and state and local law enforcement agencies that require immediate attention if the whole of government is going to properly respond to a terrorist attack in the United States. Rather than criticize, one should look to interagency lessons learned and success stories to set proper benchmarks for increased cooperation in the future.

Lt Col Felling is an Air Force Reserve Officer assigned to the US African Command Operations and Logistics Directorate working as an operations officer in the Global Force Management Branch. In his civilian capacity, he is a supervisor with the Federal Air Marshal Service. His last position was assistant to the special agent in charge and squad leader in the Washington, DC, Field Office.

---

1 "Statements made by Indian Prime Minister Shri P. Chidambaram." Government of India Press Information Bulletin, 11 December 2008.

2 "The Lessons of Mumbai." RAND Corp, 1 February 2009, p. 2.

3 "Mumbai." Lonely Planet Tour Online Destination Guide, August 25, 2009.

4 "Mumbai Combined Arms Operation." Department of State Overseas Security Advisory Council, 1 December 2008.

5 "Statements made by India's Interior Ministry." Reuters News International, 12 February 2009.

6 "The Lessons of Mumbai." RAND Corp, 1 February 2009, p. 5.

7 DHS/TSA Field Intelligence Report, "US Files Case Against

Mumbai 26 November 2008 Attackers." FBI sources, August 21, 2009.

8 "The Lessons of Mumbai." RAND Corp, 1 February 2009, p. 4.

9 "Many More Questions About the Terror Attacks." Rediff India Abroad, 28 November 2008. Available at: http://www.rediff.com/news/2008/nov/28-some-questions-about-the-terror-attacks.htm

10 Margolick, David. "25 Minutes of Terror in San Francisco." *New York Times*, 15 November 1994. Available at: http://articles.cnn.com/1997-02-28/us/9702_28_shootout.update_1_armored-police-chief-willie-williams-car-wreck?_s=PM:US

11 Moore, Solomon. "Felons Banned from Sale, Possession of Body Armor." *Los Angeles Times*, 19 August 1998. Available at: http://articles.latimes.com/1998/aug/19/local/me-14629

12 "Botched L.A. Bank Heist Turns Into Bloody Shootout." CNN Online, 28 February 1997.

13 Ignatius, David. "The Next Mumbai." *Washington Post*, 3 December 2008. Available at: http://www.washingtonpost.com/wp-dyn/content/story/2008/12/02/ST2008120203579.html

14 "Mumbai Police Bought Luxury Cars Not New Weapons." The Times of India Online, 1 December 2008.

15 Magnier, Mark. "Systemic Failure Seen in India's Response to Attacks." *Los Angeles Times*, 1 December 2008.

16 Sengupta, Somini, and Keith Bradsher. "India Faces Reckoning as Terror Toll Eclipses 170." *New York Times*, 29 November 2008. Available at: http://www.nytimes.com/2008/11/30/world/asia/30mumbai.html

17 Magnier, Mark. "Systemic Failure Seen in India's Response to Attacks." *Los Angeles Times*, 1 December 2008.

18 Ibid.

19 Anana, Geeta, Peter Wonacott, and Matthew Rosenber. "India Security Faulted as Survivors Tell of Terror." *Wall Street Journal*, 1 December 2008.

20 "India TV Defends Broadcast of Conversations with Mumbai Attackers." PTI News Agency, 29 November 2008. Available at Open Source Center, SAP2008112950040.

21 "A Reality Check on the Preparedness of Law Enforcement to Respond to Attacks on Highly Vulnerable U.S. Domestic Targets." NTOA Project Red Report, 30 May 2009.

22 "India Military Guide." GlobalSecurity.org, 23 April 2009.

23 10 U.S. Code § 380 Section 1033: Enhancement of cooperation with civilian law enforcement officials.

(a) The Secretary of Defense, in cooperation with the Attorney General, shall conduct an annual briefing of law enforcement personnel of each State (including law enforcement personnel of the political subdivisions of each State) regarding information, training, technical support, and equipment and facilities available to civilian law enforcement personnel from the Department of Defense.

(b) Each briefing conducted under subsection (a) shall include the following:

(1) An explanation of the procedures for civilian law enforcement officials—

(A) to obtain information, equipment, training, expert advice, and other personnel support under this chapter; and (B) to obtain surplus military equipment.

(2) A description of the types of information, equipment and facilities, and training and advice available to civilian law enforcement officials from the Department of Defense.

(3) A current, comprehensive list of military equipment which is suitable for law enforcement officials from the Department of Defense or available as surplus property from the Administrator of General Services.

(c) The Attorney General and the Administrator of General Services shall—

(1) establish or designate an appropriate office or offices to maintain the list described in subsection (b) (3) and to furnish information to civilian law enforcement officials on the availability of surplus military equipment; and (2) make available to civilian law enforcement personnel nationwide, toll free telephone communication with such office or offices.

24 E-mailed statements to the Office of the Secretary of Defense (OSD) for Homeland Defense from Donald Lapham, OSD Policy, 13 March 2009.

25 Telephone interview with Craig Barrett, deputy director of the LESO, Battle Creek, Michigan, 13 October 2009.

26 Ibid.

27 "Government Decides to Legalize Internet Connections Tapping." Hindustan Times Online, 8 December 2008.

28 "Indian State Considers Restricting Live Broadcasting During Emergencies—Private Broadcasters to 'Self Regulate' Live Coverage Following Mumbai." PTI News Agency, 3 December 2008.

29 India Prevention of Terrorism Act, 2002 (repealed 2006); GoI Official Secrets Act, 1923.

30 "Cops Look to Jam Cell Phones if Terror Strikes." Associated Press, 9 January 2009.

31 "Look Inside the Terrorist Screening Center," NewsBlaze.com, 2 September 2007.

32 Ibid.

33 "Man Arrested in Maryland May Have Terror Ties—On National Watch List." *Washington Post*, 10 August 2005.

34 "Mumbai Attack Warnings Ignored: A Report." ABC News Australia, 2 December 2008.

35 Statements by FBI Chief Investigating Officer Donald Van Duyn and NYPD Commissioner Raymond Kelly while addressing the Senate Committee on Homeland Security and Government Affairs, 8 January 2009.

36 McCaffrey, Barry R. "Strategic Challenges Facing the Obama Administration." Presentation, August 2009. Available at: http://www.airforce.forces.gc.ca/CFAWC/Contemporary_Studies/2009/2009-Aug/2009-08-31-Strategic_Challenges_Facing_the_Obama_Administration_e.asp

Don't Be a Soft Target

We've learned many things from prior attacks. Terrorists target Army Installations and facilities; and they reconnoiter a target before they attack. Standalone facilities—inherently vulnerable—rank among the likeliest targets. But they don't have to be soft targets.

Be alert at all times for suspicious activity such as a person lingering curiously near an entrance or one asking unusual questions about a facility. Do that and your ordinary daily routine becomes part of a crucial Army-wide mission: protecting our Army community at home like we do abroad.

Always Ready, Always Alert
Because someone is depending on you

SLASHING THE ENEMY'S ACHILLES' HEEL

Using Surveillance Detection to Prevent Terrorist Attacks

By Col Shannon D. Jurrens, USAF, Chief, Antiterrorism/Force Protection Division, Directorate of Operations and Logistics, US Africa Command

The key to stopping terrorist attacks is to drop traditional reactive policies and to begin to detect and prevent attacks before they ever happen.

On 30 November 1989, Deutsche Bank Chairman Alfred Herrhausen left his home in Bad Homburg, a suburb of Frankfurt, Germany, at the usual time about 8:30 a.m.[1] His security detail included three fully armored Mercedes-Benz sedans and a 30-man protective detail, reportedly made up of former operators from GSG-9 (the German counterterrorism team).[2] At least 6 weeks prior to the attack, several Red Army Faction (RAF) members posing as construction workers laid the wiring needed to connect an improvised explosive device (IED) trigger mechanism to its remote arming point.[3] This device was hidden in plain sight along the route Herrhausen routinely took to work.[4]

On the day of the attack the RAF triggering mechanism, made up of a simple light beam and a reflector placed across the road from one another, armed after the lead car in the convoy passed by.[5] The IED, which consisted of 22 kgs of TNT behind a metal plate, was placed on the back of a bicycle and positioned to line up next to the right rear seat of Herrhausen's vehicle.[6] At approximately 8:34 a.m., Herrhausen's vehicle broke the light beam and triggered the device, which heaved his 2.8-ton armored Mercedes 82.5 ft across the road.[7] Herrhausen was critically injured and subsequently died.[8] Despite the considerable physical security measures used,

Herrhausen's habitual daily routine established the time and place of his own death. Clearly, "roadside bombs" are nothing new, demonstrating that good "shooters" and armored cars alone do not guarantee protection.

This trip down terrorism's "memory lane" was not just to gain the reader's attention, but to highlight a mode of attack that has been used repeatedly for more than 30 years. Because of the dominance of US forces, terrorist attacks continue to be the most probable form of "enemy contact" and the most persistent threat US forces face. Unprecedented amounts of time, money, and energy have been applied to protecting military members around the world, yet one critical aspect of force protection still needs improvement: antiterrorism (AT) education and training. Specifically, DOD can do more to teach fairly simple yet effective techniques to detect terrorist pre-operational surveillance. These techniques may be a Service member's only means of defense in areas outside the current combat zones where armored vehicles and fortified defenses are few.

Service members must understand and implement surveillance detection as part of their defense. Although this information is not new, it is unfortunately only taught in a few specialized courses. The impact of this training gap is that although training programs tell people to look for surveillance, most people have no idea what to look for or where to look. Simply providing examples or describing what surveillance may look like and then telling someone to look for it is of little help.[9] Teaching military members to look for "suspicious" individuals is no better and can even be misleading because surveillants can, and often do, look just like everyone else. Because terrorist surveillance always precedes an attack, detecting that surveillance is perhaps the best, and often the only, indication and warning of an impending attack. Fortunately, this situation can be fixed fairly cheaply and quite easily, although training the force will take time.

Perhaps the most significant aspect of terrorism is to understand that the violent action is part of a larger process. Focusing on the process preceding a terrorist attack (aka left of boom) can disrupt a terrorist attack, regardless of the attack method used.

The tools described and the ideas behind them can be applied anywhere, although they have less utility in lawless regions like Iraq, Afghanistan, or Somalia. Indeed, while the current DOD focus on those areas is essential, most countries in the world do not have active insurgencies underway, and so terrorists have to operate in a more covert manner, with their own weaknesses to be exploited.

Surveillance detection failure. German Police investigate the wreckage of Alfred Herrhausen's car destroyed by the leftist terror group known as the Red Army Faction (RAF) on 30 November1989. *[Source: US Department of State, Terrorist Tactics and Security Practices, 1994]*

Understanding the Threat: The Terrorist Attack Process

Terrorism is a term that carries a lot of baggage. Rather than get into all the varied definitions and perspectives, this article will focus on terrorism as a tactic that threat groups of many categories (terrorist, guerilla, insurgent) use to accomplish their objectives.

Perhaps the most significant aspect of terrorism is to understand that the violent action is part of a larger process. Focusing on the process preceding a terrorist attack (aka left of boom) can disrupt a terrorist attack, regardless of the attack method used. With respect to the target, a terrorist attack is actually a seven-step process:[10]

► TERROR ATTACK SEVEN-STEP PROCESS:

1. **Preliminary target list prepared.**
2. **Initial surveillance conducted.**
3. **Victim/target selected from list.**
4. **Attack planned (more surveillance).**
5. **Attack team deploys.**
6. **Victim arrives.**
7. **Attack takes place.**

The second and fourth steps are the weakest in this chain of events. In the second step, the terrorists have to collect information and conduct physical surveillance. This step usually lasts for weeks or months and is frequently conducted by individuals with little training. In the fourth step, the terrorists plan the details of the attack. This step includes additional surveillance to identify the best method, time, and specific location of the attack and can last from several days to several weeks. In contrast, the last three steps, in which the attack team deploys, the target arrives, and the attack initiates, may take only minutes or seconds. On the day of the attack, the terrorists have the advantage of knowing (1) the time of the attack, (2) the location of the attack, and (3) the method of the attack. In addition, the terrorists only have to be successful once, whereas US forces have to remain vigilant and on guard every day.[11] In true asymmetric form, the day of the attack is the point at which the defenders are weakest and the terrorists are strongest.

Defeating the Threat

How do we prevent terrorist attacks? Traditional approaches involving guards, weapons, and barriers serve only to mitigate the effects of and response to attacks. This conclusion has been reached by multiple government commissions. For example, more than 25 years ago, following the bombing of the US Marine Battalion Landing Team Headquarters in Beirut, Lebanon, the Long Commission concluded that "too much faith is put in physical defenses."[12] The commission also stated in its report: "Combating terrorism requires an active policy. A reactive policy only forfeits the initiative to the terrorists."[13] The commission members believed that "all military personnel assigned overseas can expect to encounter terrorism in some form. Consequently, they need some understanding of the terrorist threat and how to counter it."[14] Rather than trying to mitigate and respond, more can be done to prevent terrorist attacks.

By focusing on Step 7 of the terrorist attack process—the attack and its aftermath—commanders and security personnel allow the terrorists to maximize their strengths and the element of surprise. Terrorism is an asymmetric form of warfare, so simply doing more of what DOD does best does little to address DOD's own weaknesses nor reduces terrorists' asymmetric advantages. Instead, DOD must focus some of its considerable resources on building a capability at the individual level to exploit the terrorists' weaknesses.

The terrorists' weaknesses are inherent in the terrorist attack process. Thinking asymmetrically where the defenders have the greatest advantage and the terrorists are at the greatest disadvantage, that seven-step chain of events has to be broken at the weakest link. Early in the attack process, defenders can limit the terrorists' advantages related to time, method, and location. One weakness inherent in the physical surveillance method is that the terrorists must be close enough to the target to collect information.[15] News media accounts, Web searches, and commercial satellite photos can provide information about a potential target, but none of these methods can offer the tactically relevant information terrorists need. At best, these methods provide a snapshot in time and cannot be used alone to develop the target's "pattern of life."

Another weakness that offers multiple opportunities for surveillance detection, as previously described in Steps 2 and 4, are the extended periods of time needed to conduct target surveillance in order to plan an attack. Time and the known methods of target surveillance can become advantages for the good guys. The final and most significant advantage, surveillance location, can be determined or at least narrowed to a manageable pool of possibilities by using an effective surveillance detection program.

Four Fundamental Principles of Surveillance Detection

A simple but effective AT education and training program includes four fundamental principles of surveillance detection rooted in good common sense. Service members must understand both the underlying principles (the why) and the specific techniques (the how). The fundamental principles are:[16]

1. **Stay informed.**
2. **Stay low key.**
3. **Stay unpredictable.**
4. **Stay alert.**

These four principles are fairly familiar to anyone who has been involved in AT education or training. However, both the reasons for utilization and the methods of implementation have changed since they first came into vogue in the 1980s.

Stay Informed

The logical first step in this program is that its subjects must first stay informed. This first step is a common part of most security programs, so it will be covered relatively quickly. Staying informed means knowing your enemy and your operating environment. As the term implies, staying informed is a continuous process. Knowledge of the operating environment and the enemy should be covered in a surveillance detection instruction course prior to deployment. Learning about the customs and culture of an area is essential, both in building helpful alliances and in recognizing when dangerous events are about to occur.

Stay Low Key

Staying low key may mean staying off the terrorists' "radar" (the initial target list in Step 1) and to make surveillance more difficult (Steps 2 and 4). Terrorists may find it harder to surveil someone whose general appearance is similar to the local population, particularly if trying to observe from a safe distance. To keep the subject in sight, the surveillance team will probably have to stay closer, either on foot or in traffic, making surveillants easier to detect. As a general rule, the smaller the "bubble" in which a surveillance team has to operate, the better the chance a subject will have of detecting the surveillance. The first two fundamental principles set the stage for the last two.

Stay Unpredictable

Staying unpredictable and staying alert are the most important, most misunderstood, and most poorly covered steps in many AT education and training programs. Staying unpredictable, in and of itself, will not prevent the terrorists from planning an attack because no one can be completely unpredictable. And staying alert for possible surveillance or developing attacks is of little utility if an individual does not know what to look for or where to look for it. Both of these fundamental concepts are useful only if they are used in the right way.

Staying unpredictable is a broad concept that defines how to narrow the playing field and simplify surveillance detection. Four simple steps define the specific technique:

1. Reduce the Number of Routine Stops and Visited Locations. The first step in reducing the size of the security dilemma is to teach individuals how to reduce the number of places they visit as a matter of routine.[17] The average person probably has many places that they visit routinely, including home, the office, favorite restaurants and bars, place of worship, and sporting locations. With this many routine stops and routine routes in between, the terrorist has many options for potential attack sites. Trying new restaurants and altering the locations of social events can effectively eliminate places as potential attack sites without affecting a person's quality of life. Terrorists simply cannot afford to wait at a location for days or weeks hoping that the target will show; instead, they will be forced to go where they know they can find their target. This is particularly true for the initial phase of surveillance. Ultimately, the goal should be to limit the number of routine stops (known locations) to just a few, like the home or office.

STAYING UNPREDICTABLE

1. Reduce the number of routine stops and visited locations.
2. Vary the routes and/or the vehicles used between those routine locations.
3. Analyze routes of travel.
4. Vary times of travel.

2. Vary Routes of Travel. The next step is to vary the routes between these routine stops. This step is a common part of most AT training programs, but the purpose is rarely explained.[18] This step is extremely important because even after the number of routine stops has been reduced, the routes to and from each location still offer the terrorists a number of potential attack sites. To reduce vulnerability further, each individual should develop three to five routes between routine stops. If possible, these routes should not have overlapping segments or cross at any point. The actual number of routes will vary in each situation. Randomly varying routes decreases the number of places that the potential target can be routinely found, forcing the terrorists to go where they know they can find their target. The size of the terrorists' playing field has been reduced from a great number of sites to just a few.

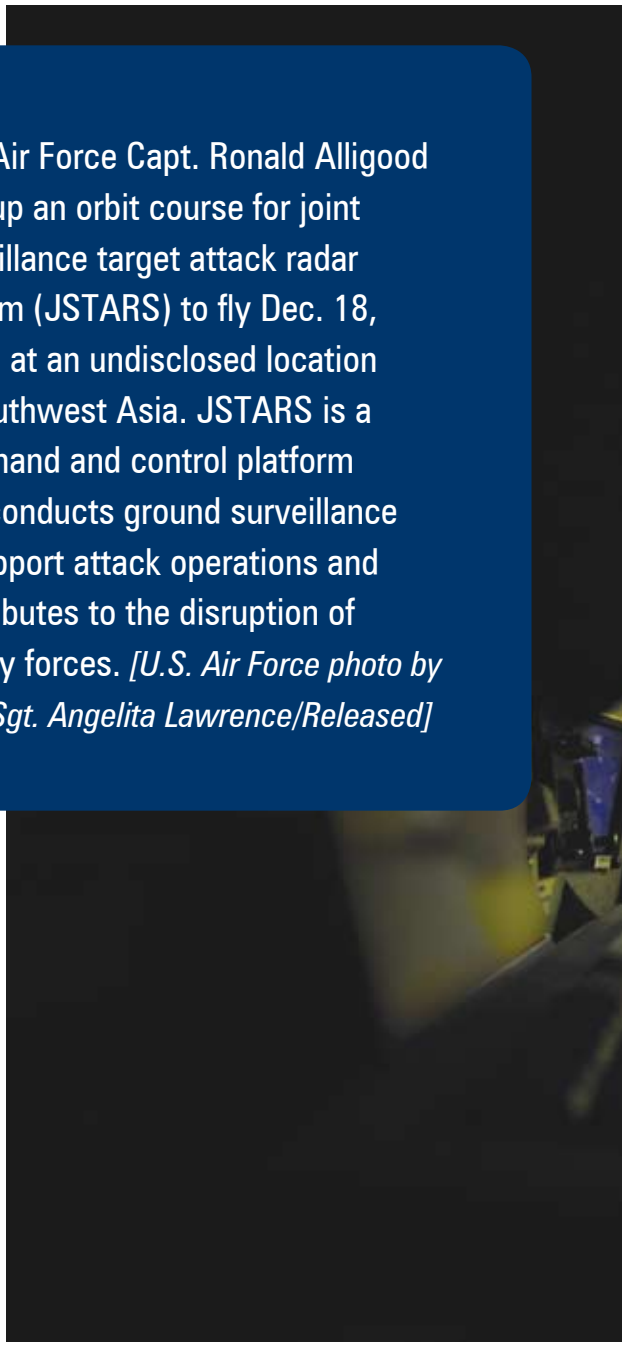
3. Analyze Routes of Travel. Route analysis can narrow the playing field even further. To identify those specific locations where terrorists will most likely conduct surveillance or attacks, military members must be taught how to conduct an analysis of their planned routes. Terrorists' attack or surveillance sites typically possess the following characteristics.

- Site is routinely visited by target at predictable times.
- Site has no or limited security or police presence.
- Site offers cover or camouflage for surveillance or attack teams.
- Site offers a means to effectively control or limit the target's movement.
- Site offers a variety of good escape routes.

Varying one's routes has already limited the number of places where a potential target can predictably be found, but every route has at least two places where the subject must be: at the beginning and at the end of the route. Any location along the route where the potential target must be, either by habit or by necessity, is known as a chokepoint, meaning that every route has at least two chokepoints. If routes overlap or cross at the same point, either by habit or because of the terrain, the route will have an additional midroute chokepoint.

Route analysis first identifies chokepoints and then looks for the characteristics described above.[19] If surveillance detection is virtually impossible at any of the potential attack sites, the route must be avoided. Routes should also be analyzed to determine whether road or traffic conditions create additional sites that offer an opportunity to control movement. When traveling through any area that contains the characteristics listed, the individual should be at the highest state of alert (actively looking for surveillance or attack teams).

4. Vary Times of Travel. AT training often teaches students to vary times of travel, but, again, many programs do not explain the reasons for using the technique. Routine travel times allow the surveillance team to deploy for a minimum amount of time. This short time period makes detection difficult because the surveillance team can "cover" their activities with "normal" actions for a short period. Varying times of departure by 30 minutes or more forces the surveillance team to deploy for an extended period. To be effective, the surveillance team has to arrive before the earliest possible departure time and may have to stay until the latest departure time. Normal activities such as sitting on a park bench, waiting for a bus, or reading a newspaper in a car can only go on for so long before they become "stale" or awkward. Time variation is often misused and can even lead to a false sense of security.[20] Locations that have too much activity, such as market areas or universities, do not lend themselves to short variations in departure times. Surveillance or attack teams can effectively hide in these busy locations and evade detection. Large variations in time; a large, active security presence; or a good-sized, well-trained countersurveillance team are required in such locations. When used correctly, time variation can make terrorist surveillance noticeable.



U.S. Air Force Capt. Ronald Alligood sets up an orbit course for joint surveillance target attack radar system (JSTARS) to fly Dec. 18, 2009, at an undisclosed location in Southwest Asia. JSTARS is a command and control platform that conducts ground surveillance to support attack operations and contributes to the disruption of enemy forces. *[U.S. Air Force photo by Staff Sgt. Angelita Lawrence/Released]*

Stay Alert

The final fundamental principle of surveillance detection is to stay alert. Now that the problem of where to look for surveillance has been reduced, military members must be taught what to look for. Generally speaking, they should look for people who seem to be doing nothing. Surveillants may look like they are trying to accomplish a task, but they will be paying more attention to where the target will be than to their cover activity.

Service members also must understand how to determine whether those people in a vulnerable location are correlating with them. In this context, correlation refers to individuals who are in the right place at the right time to conduct surveillance. In fixed surveillance, surveillants arrive before the target arrives and leave after the target leaves. In moving surveillance situations, individuals should remember a simple phrase: "Same faces, different places." If a military member notices a person in two or more places that are somewhat geographically separated, he or she should take note of the details of that person's appearance. The same technique can be used for vehicles. Correlation is the defining aspect of surveillance detection; it must never be taken lightly.

Service members should also look for "mistakes." Terrorists are not perfect and occasionally make mistakes like paying close or unwarranted attention, writing down notes, or checking their watches as a military member drives past. Because of insufficient training, these occasional mistake make up much of current surveillance reporting.

Conclusion

Effective AT education and training programs play a central role in defending against terrorist attacks. Unfortunately, useful surveillance detection training is often missing from these programs. The simple but effective techniques explained in this article are also an efficient use of resources because, once taught, they can be used anywhere without additional investment. Pre-operational surveillance detection is too important to leave to luck or terrorist mistakes. The US military must be given the tools to make surveillance detection an achievable goal. These techniques are already taught to some. The time has come to bring them to the rest of the force.

About the Author

COL Shannon D. Jurrens is the Chief, Antiterrorism/Force Protection Division, Operations and Logistics Directorate, US Africa Command, Stuttgart, Germany. He has extensive operational experience in nuclear and conventional weapon system security, law enforcement, antiterrorism, and wartime air base defense and has been both a squadron and expeditionary group commander. He is also a former director of the Dynamics of International Terrorism course at Hurlburt Field, Florida.

Bibliography

Alexander, Yonah, and Dennis A. Pluchinsky. *European Terrorism, Today and Tomorrow.* Washington DC: Brassey's, 1992.

Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD SO/LIC). Message to Chairman, Joint Chiefs of Staff and others. Subject: "Terrorist Surveillance Detection Guidance for Commanders and Antiterrorism Planners." December 2002.

Bell, J. Bowyer. *Assassin.* New York: St. Martin's Press, 1979. Bell derives attack information from Julen Agirre's book *Operation Ogro: The Execution of Carrero Blanco* (New York: Quadrangle, 1975) based on his interviews with four members of Basque terrorist group ETA who were involved in the attack.

Boesen, Jacob. "Incidents of Interest: An Analysis of Force Protection Measures and Terrorist Incident Modus Operandi." Unpublished research paper funded by the Defense Intelligence Agency [contract no. OR-98-3]. August 10, 1999.

Boughatsou, Aristea. "17N Instructions for Secure Action". I Kathimerini, 28 May 2002, 7. Foreign Broadcast Information Service Report (No. GMP20020529000048). 29 May 2002.

Clutterbuck, Richard. *Living with Terrorism.* New York: Arlington House Publishers, 1975.

Defense Intelligence College. Counterterrorism Analysis Course (Publication Control No. 1770). Washington, DC: Defense Intelligence Agency, n.d.

Department of Defense. "Antiterrorism Level 1 Training System."

Department of Defense. DOD Commission on the Beirut International Airport (BIA) Terrorist Act of 23 October 1983.

Department of Defense. Report to the President and Congress on the Protection of US Forces Deployed Abroad.

Department of Defense, Office of Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. DOD Instruction 2000.16, DOD Antiterrorism Standards. June 2001.

Department of Defense, Office of Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. DOD O-2000.12H, Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence. February 1993.

Department of State, Bureau of Diplomatic Security. Manual: New Arrival Briefing, Diplomatic Security Service, Athens, Greece. (Provided 15 October 2002, by a Diplomatic Security Service special agent.)

Department of State, Bureau of Diplomatic Security. Significant Incidents of Political Violence Against Americans: 1988. Publication 9644, 1989.

Department of State, Bureau of Diplomatic Security, Mobile Security Division. "Counter-Terrorism Seminar: Attack Recognition" [Lesson Plan 1187N]. Prepared by Gunars Berzins. 21 November 1988.

Department of State, Bureau of Diplomatic Security, Mobile Security Division. "Counter-Terrorism Seminar: The Terrorist Target Selection Process and Victim Reactions" [Lesson Plan 1184N]. Prepared by Gunars Berzins. November 11, 1988.

Department of State, Bureau of Diplomatic Security, Office of Intelligence and Threat Analysis. Terrorist Tactics and Security Practices, 1994. Publication 10099. 1994.

Department of State, Bureau of Diplomatic Security. Hostage Taking: Preparation, Avoidance, and Survival. Publication 9400, Department and Foreign Series 390, 1988.

Drake, C. J. M. *Terrorists' Target Selection.* Hampshire, England: Palgrave; 1998.

Exner, Eric D. "Intelligence Support to Force Protection: A Case Study." Unpublished master's thesis. Quantico, Virginia: US Marine Corps Command and Staff College, 1998.

Frantz, Douglas. "Terror in Bali: TerrorismWatch; Al Qaeda Evolves Into Looser Network, Experts Say." *New York Times*, October 15, 2002.

General Accounting Office. Report to the Chairman, Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives. *Combatting Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations* [Report No. GAO-03-14]. November 2002.

Hoffman, Bruce. "Change and Continuity in Terrorism." Studies in Conflict and Terrorism 24 (2001): 417–428.

Hoffman, Bruce. *Inside Terrorism.* New York: Columbia University Press, 1998.

International Training Inc. "Route Analysis" (handout

provided during the Air Force Office of Special Investigations sponsored course, "Counterreconnaissance in Support of Force Protection," 16–27 June 1997.

International Training Inc. "Surveillance Detection" (handout provided during the Air Force Office of Special Investigations sponsored course, "Counterreconnaissance in Support of Force Protection," June 16–27, 1997).

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. *Countering the New Terrorism.* Santa Monica, California: Rand, 1999.

Meyer, Josh, and Bob Drogin. "Bali Blast Signals Terrorist Shift: U.S. officials say Islamic militants, no longer content to attack Western 'symbols of freedom,' are aiming at softer targets." *Los Angeles Times,* October 15, 2002. (Distributed via HQ Air Force Security Forces Center, Terrorism Periodical 101502).

Mickolus, Edward F. *Terrorism 1998-1991: A Chronology of Events and Selectively Annotated Bibliography.* Westport, Connecticut: Greenwood Press, 1993.

National Strategy for Combating Terrorism. Washington, DC: White House, February 2003.

Nesfiye, Lia, and Panayis Galiatsatos. "How 17 November Collected Information." In Athens Ta Nea (August 10, 2002), 10. Foreign Broadcast Information Service Report [No. GMP20020813000217], 13 August 2002.

Omnibus Diplomatic Security and Antiterrorism Act of 1986. 22 US Code § 4801 (1986).

O'Neill, Bard E. *Insurgency and Terrorism: Inside Modern Revolutionary Warfare.* Washington, DC: Maxwell Macmillan Pergamon, 1990.

Papakhelas, Alexis. To Vima tis Kiriakis (14 July 2002), A4–A6. Foreign Broadcast Information Service Report (No. GMP20020715000113), July 14, 2002.

Security and Criminal Justice Titles [brochure]. Butterworth-Heinemann, Winter 1998–1999.

Shlapak, David A., and Alan Vick. Check Six Begins on the Ground: Responding to the Evolving Ground Threat to US Air Force Bases. Santa Monica, California: Rand, 1995.

Smith, Gerald O. "Attack Recognition and Surveillance Detection." Lecture series presented at the Dynamics of International Terrorism Course, US Air Force Special Operations School, Hurlburt Field, Florida, 1995–1997.

Terrorist Training Manual. Washington DC: National Security Division's Operational Training Unit, FBI Headquarters, November 2001.

Tompkins, Thomas C. *Military Countermeasures to Terrorism in the 1980s.* N-2178-RC. Santa Monica: Rand, 1984.

TWSG 2002 Review: Combating Terrorism. Technical Support Working Group, n.d.

US Air Force Pamphlet 208-3. *International Terrorism: The Other World War.* GPO 1987-180-976 (62044). Washington DC: Air Force Office of Antiterrorism, SAF/IGST, 26 February 1987.

Wade, Nicholas. "On the Scent of Terrorists." *New York Times*, 5 January 2003. http://www.nytimes.com/2003/01/05/weekinreview/05WADE.html?8hpib

When It Turns Serious (WITS): Counter Stalking and Threat Management in High Risk Situations. (Video developed by Tom Smith of Mark One, S.A., 35 minutes. Butterworth-Heinemann, 1995).

1 Department of State, Bureau of Diplomatic Security, Office of Intelligence and Threat Analysis, Terrorist Tactics and Security Practices, 1994. Publication 10099 (Washington DC: Department of State, 1994), p. 4.

2 Smith, Gerald O. "Attack Recognition and Surveillance Detection." Lecture series presented at the Dynamics of International Terrorism Course, US Air Force Special Operations School, Hurlburt Field, Florida, 1995–1997.

3 Supra 1, pp. 4–9.

4 Ibid, p. 4.

5 Ibid, p. 8.

6 Ibid.

7 Ibid.

8 Ibid.

9 This same critique was explained 15 years ago in the Department of State publication *Hostage Taking: Preparation, Avoidance, and Survival* (Publication 9400, Department and Foreign Series 390, 1988), p. 12.

10 International Training Inc. "Surveillance Detection" (handout provided during the Air Force Office of Special Investigations sponsored course, "Counterreconnaissance in Support of Force Protection," 16–27 June 1997), p. 1.; the Department of State briefer's manual uses an eight-step process that is essentially the same.

11 Following the unsuccessful 12 October 1984, attack on British Prime Minister Margaret Thatcher at the Grand Hotel in Brighton, England, the PIRA released a statement saying, "Today we were unlucky, but remember, we only have to be lucky once; you will have to be lucky always." Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), p. 182.

12 DOD Commission on the Beirut International Airport (BIA) Terrorist Act of 23 October 1983, p. 133.

13 Ibid, p. 128.

14 Ibid, p. 132.

15 Terrorists primarily rely on physical surveillance, as opposed to technical surveillance, to collect information. This process is sure to evolve as technical solutions become more accessible.

16 Although the number of principles varies anywhere from as few as three to as many as six in the current Internet training, the result is basically the same.

17 This first step comes from the When It Turns Serious (WITS) video cited in the bibliography.

18 The reasons for why this is important come from the Gerold O. Smith lecture series, the International Training Inc. courses, and the video When It Turns Serious (WITS): Counter Stalking and Threat Management in High-Risk Situations.

19 For more detail and useful examples, see Drake (*Terrorists' Target Selection*, Hampshire, England: Palgrave; 1998), pp. 63–72.

20 This point is emphasized in the When It Turns Serious (WITS) video.

Strategic Event Assessment

by LCDR Christopher F. Hill, USN

EVENT: *Inspire* released by Al Qaeda in the Arabian Peninsula

July 2010: Al Qaeda in the Arabian Peninsula (AQAP) releases the first issue of *Inspire*, a recruiting and training tool for Islamic extremists.

October 2010: Second issue is released.

STRATEGIC SIGNIFICANCE:

After overcoming a series of technical glitches in its online release, AQAP published its first issue of *Inspire* magazine this summer in an attempt to expand al Qaeda's extremist message in the English-speaking world. Using readily available publishing software, this periodical includes sleek graphics and a professional magazine-style layout.

Although the magazine tries to dazzle the reader with witty prose and cool, colloquial English, it is still just another medium for the persistent radical Islamic message available on numerous extremist blogs. It tries to be a "one-stop shop" for extremist motivation and terrorist skill building. It includes motivational articles from the top al Qaeda leadership such as Osama bin Laden, Anwar al Awlaki, and others, who recommend the use of smaller and more numerous attacks on less significant targets, similar to what occurred at Fort Hood and the failed aircraft bombing on 25 December 2009. It also includes do-it-yourself pieces on making pipe bombs and encrypting e-mail messages, all designed to enable aspiring lone terrorists. There is nothing new in the two issues published to date, and they do not contain information that cannot be found elsewhere in greater detail.

What concerns many officials is the potential that *Inspire* could energize the English-speaking Muslim world. As *The Guardian Antiterrorism Journal* noted in the summer 2010 issue, there is evidence that homegrown terrorism has increased over the past decade. Already there have been attempts to reach out to the English-speaking extremist world through publications in English. Nevertheless, some experts suggest that the deluge of radical propaganda will only contribute to information overload for potential recruits.

It is too soon to judge the strategic impact of this magazine, but *Inspire* will continue to draw scrutiny from the DOD antiterrorism community.

QUOTES:

"In the West; in East, West and South Africa; in South and Southeast Asia and elsewhere are millions of Muslims whose first or second language is English. It is our intent for this magazine to be a platform to present the important issues facing the ummah today to the wide and dispersed English speaking Muslim readership. We also call upon and encourage our readers to contribute by sending their articles, comments or suggestions to us."

— Letter from the Editor
Inspire, July 2010

"This magazine is clearly intended for the aspiring jihadist in the US or UK who may be the next Fort Hood murderer or Times Square bomber."

— Bruce Riedel
Brookings Institution, guardian.co.uk, July 2010

"The idea is that AQAP can reach, influence and inspire other like-minded individuals in the west. No longer do these individuals need to travel to Yemen or read Arabic in order to take instructions from AQAP. Now they can just download and read the magazine in English."

— Gregory Johnsen, Yemen expert
guardian.co.uk, July 2010

"There is really nothing new about an English-language magazine like this. We've seen them since the early '90s really, and in recent years there have been several online. There is nothing new in the idea of the magazine or its content."

— Thomas Hegghammer, Senior Fellow, Norwegian Defense Research Establishment,
www.npr.org, July 2010

by LCDR Christopher F. Hill, USN

EVENT: Al Shabaab's July 2010 Twin Bombings in Uganda

- Seventy-six people were killed and scores of others were wounded while watching World Cup soccer at two separate venues in Kampala, Uganda.
- This attack is considered al Shabaab's first terrorist attack outside of Somalia.

STRATEGIC SIGNIFICANCE:

Al Shabaab, or "the youth," is a 2006 outgrowth of a militant faction in the former Islamic Courts Union in Somalia. Based on its ties to al Qaeda, the group was added to the US list of foreign terrorist organizations in February 2008. The July 2010 twin bombings in Uganda represented al Shabaab's first venture into the realm of transnational terrorism. In the past, al Shabaab had been known to conduct border raids into neighboring Kenya but had not done anything on the scale of the attack in Uganda. In its efforts to wage an insurgency against the Transitional Federal Government and the African Union Mission in Somalia (AMISOM), al Shabaab and its approximately 6,000 fighters (including some Americans) now control much of southern Somalia outside the capital of Mogadishu. They have also conducted several high-profile attacks inside the capital, the Mumbai-style attack in August 2010 notwithstanding.

A gruesome reminder of al Qaeda's 1998 bombing of US embassies in Kenya and Tanzania, the twin bombings in Kampala, Uganda, occurred at a rugby club and at an Ethiopian restaurant where hundreds gathered to enjoy the World Cup. Two of the three explosions occurred at the rugby club, the second one probably intended to kill those who were helping the victims of the first bombing. After responding to attacks at both locations, Ugandan authorities discovered an unexploded suicide vest in a trash can next to a nightclub.

In recent years, al Shabaab has made repeated promises to target countries like Uganda, Kenya, and Ethiopia, which have contributed thousands of troops to AMISOM as peacekeepers. This attack raises the specter of similar attacks occurring in neighboring countries, many of which already deal with local insurgencies, porous borders, and a host of other problems. There is also the fear that al Shabaab will export violence abroad, including to the United States, which has large pockets of Somalis in places such as Minnesota, Washington, DC, and Columbus, Ohio.

Many experts are now asking the question: Is Somalia the next Afghanistan?

QUOTES:

"Uganda is a major infidel country supporting the so-called government of Somalia. We know Uganda is against Islam and so we are very happy at what has happened in Kampala. That is the best news we ever heard."

— Sheikh Yusuf Isse, an al Shabaab commander in Mogadishu
Reuters, 12 July 2010

"Shabaab has confirmed they are working with al Qaeda and they are giving bases to many foreign criminals. If we fail to eradicate them here they will strengthen their bases in Somalia. … If the international community ignores taking quick action against Shabaab, this escalating violence will endanger neighboring countries."

— Abdirahman Omar Osman, Somali Minister of Information,
Los Angeles Times, July 2010

"On the one hand, you have a vision of an Africa on the move, an Africa that is unified, an Africa that is modernizing and creating opportunities. And on the other hand, you have got a vision of al-Qaida and al-Shabaab that is about destruction and death. … If al-Shabaab takes more and more control within Somalia, it is going to be exporting violence the way it just did in Uganda."

— President Barak Obama
14 July 2010

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

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