The Source for Antiterrorism Information

FALL 2011 | Volume 13 | 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

Antiterrorism Quotes

8 September 2011

"[Lone-wolf] threats will not come to our attention because of an intelligence community intercept. They will come to our attention because of an alert police officer, an alert deputy sheriff, an alert store owner, an alert member of the public sees something that is suspicious and reports it."

—John Cohen, Department of Homeland Security, Reuters.com.

31 August 2011

"A decade after 9/11, the nation is not yet prepared for a truly catastrophic disaster."

—Tenth Anniversary Report Card: The Status of 9/11 Commission Recommendations, www.bipartisanpolicy.org.

31 August 2011

"Our terrorist adversaries and the tactics and techniques they employ are evolving rapidly. We will see new attempts, and likely successful attacks. One of our major deficiencies before the 9/11 attacks was a failure by national security agencies to adapt quickly to new and different kinds of enemies. We must not make that mistake again."

—The Honorable Lee Hamilton and the Honorable Thomas Kean, www.bipartisanpolicy.org.

30 August 2011

"A lot of the work that remains requires a decision by Congress and ultimately the American people. Do they want this increased security and are they willing to pay for it and give up some civil liberties?"

—Rick Nelson, Center for Strategic and International Studies, latimes.com.

14 September 2011

"We need to recognize the need to be in this for the long haul ... Much work remains to be done."

—CIA's new director David Petraeus, GEN (Ret.), wsj.com.

The Guardian

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

Guardian readers,

We in the combating terrorism community have come a long way since the attacks of 9/11. We brought the fight directly to the enemy overseas, routing terrorists from their safe havens almost everywhere, while reducing the vulnerability of millions of Service men and women and their families to terrorist attacks. Terrorism, as a philosophy and tactic, has become an increasingly unwise life choice for extremists, and we would like to keep it that way.

At home, DOD provides critical support to our interagency partners, especially the Department of Homeland Security and the intelligence community. Together we have made our country safer, but there is more work to be done. We still have several key security challenges to address such as border controls, transportation security, and emergency preparedness and response, not to mention making tough risk management decisions in an age of dwindling budgets. In DOD in particular, we need to continue to counter the danger of insider threats and to embrace the idea that FP requires much more than increased guards, guns, and bullets at the perimeter.

As always, *The Guardian Antiterrorism Journal* offers a diverse look at some of the challenges confronting the AT/FP community:

- In **Force Protection Detachment Indonesia: Setting the Standard for Security in the Ring of Fire**, the author, a U.S. Naval Criminal Investigative Service (NCIS) agent, details lessons learned while spearheading FP efforts in a volatile region of the world.

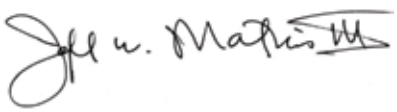
- In **Intelligence Preparation of the Garrison Environment**, the writer demonstrates how to apply Intelligence Preparation of the Battlefield (IPB) methodology to AT planning.

- **Active Shooter Lessons Learned from the 2011 Norway Attack** makes a sober analysis of the worst lone-wolf active shooter assault in history and questions whether any real lessons can be gleaned from it.

- This issue also examines **Terrorist Use of Body Packing** as a means to defeat aviation security and **Terrorist Use of Symbolic Dates** to exploit certain key dates in attack. The author of **What Is Geotagging?** examines a new vulnerability stemming from posting digital photos online.

Thanks to your service, the scourge of terrorism in the United States today may be less severe than it was in 2001, but the threat will not go away anytime soon. As the CIA's new director, David Petraeus correctly notes, "We need … to be in this for the long haul." As AT/FP professionals, we do our part, not only by deterring and mitigating future threats through robust, intelligent AT programs but also by sharing our lessons learned through journals and newsletters such as this one.

We look forward to hearing from you.



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

FORCE PROTECTION DETACHMENT INDONESIA

Kevin Aurell from Indonesian Wikipedia

Setting the Standard for Security in the "Ring of Fire"

By Scott M. Bernat

FPD Indonesia has met and exceeded the challenge and sets the standard for security programs in the Asia Pacific region.

Force Protection Detachment (FPD) Indonesia, led by the U.S. Naval Criminal Investigative Service (NCIS), is the front line of defense for all DOD forces visiting and training in Indonesia. Situated within the Pacific "Ring of Fire," so designated due to the area's significant number of active volcanoes and earthquakes, Indonesia is composed of more than 17,500 islands and a population of nearly 240 million, making it the fourth most populous nation in the world[1]. Islam is the dominant religion. The country's motto, "Unity in Diversity," reflects its diverse ethnic, linguistic, and cultural character. The nation's dynamic landscape, which includes an active terrorist threat, a spate of natural disasters, public integrity issues, and public unrest, represents a significant challenge to the safety and security of in-transit DOD personnel. FPD Indonesia has met and exceeded the challenge and sets the standard for security programs in the Asia Pacific region.

The Beginning

The terrorist attack on the USS COLE (DDG-67) in the Port of Aden, Yemen, on 12 October 2000 identified the need for increased security support for in-transit DOD personnel and assets in overseas locations with no permanent DOD security presence. The USS COLE Commission, charged with investigating the circumstances leading to the attack, highlighted this need, and the overall FPD program was initiated. The primary mission of the FPD is to detect and warn of threats to in-transit DOD personnel and resources as well as to act as an FP force multiplier for the American Embassy Country Team in each designated overseas location. This

role includes working closely with host nation security forces for threat warning and security. Other missions include providing routine DOD counterintelligence and FP services to the country team, criminal and counterterrorism investigative response, and surge capabilities in the event of crises and/or contingencies.[2] There are currently 38 FPD offices worldwide, with additional offices planned.

FPD Indonesia

Situated within the American Embassy Jakarta, FPD Indonesia began full operations in 2009. A component of the NCIS Singapore Field Office, it is staffed by an NCIS Resident Agent in Charge, a U.S. Army (USA) Special Agent, and an Office Management Assistant. In close coordination with the American Embassy Regional Security Office (RSO), the Defense Attaché Office (DAO), and the Office of Defense Cooperation (ODC), the FPD is the embassy's authority for developing, coordinating, and overseeing FP information and security for more than 140 events per year, including U.S. military exercises, aircraft and ship visits, flag and general officer visits, and other engagements. These efforts not only support U.S. interests but also significantly increase the overall security of both the Indonesian and international communities. Through close cooperation with and assistance from the Indonesian military (Tentara Nasional Indonesia [TNI]) and the Indonesian National Police (INP), FPD Indonesia activities focus on threat awareness and mitigation, physical security, risk assessments and vulnerability studies, emergency preparedness, crisis action planning and response, executive protection, and investigations. The FPD is augmented by NCIS, the U.S. Air Force Office of Special Investigations (AFOSI), and USA and U.S. Marine Corps (USMC) FP-focused personnel and teams as individual service component requirements arise.

The primary mission of the FPD is to detect and warn of threats to in-transit DOD personnel and resources as well as to act as an FP force multiplier for the American Embassy Country Team in each designated overseas location.

The Key to Success: Information

The key to keeping people and assets safe and secure is to ensure that threat information is current and is disseminated on a timely basis. Coordination, cooperation, mutual support, and information sharing are paramount to threat identification and mitigation. The FPD accomplishes this through the fusion and utilization of all available resources, including those associated with American and foreign embassies, the TNI and INP, expatriate community contacts, and business and other professional contacts as well as commercial and private sector security companies located within Indonesia and regionally. Building contacts and relationships through liaison and networking is critical to the development of a sound and comprehensive security program.

FOURTH MOST POPULOUS NATION. Situated within the Pacific "Ring of Fire," so designated due to the area's significant number of active volcanoes and earthquakes, Indonesia is composed of more than 17,500 islands and a population of nearly 240 million people.

Working in close cooperation and in conjunction with the American Embassy RSO, FPD personnel are active participants in the U.S. Department of State Overseas Security Advisory Council (OSAC)[3] as well as routine contributors of safety and security articles to the American Chamber of Commerce Indonesia magazine, *The Executive Exchange*.[4] In addition, FPD personnel are members of both the Asia Crisis and Security Group[5] and ASIS International[6], organizations dedicated to advancing security assistance and cooperation. This interaction and involvement in the overall security community not only establishes the FPD as a security partner but also exponentially expands the office's ability to gain critical information through an extensive and wide-reaching contact base.

The U.S. Pacific Command (PACOM), the NCIS Multiple Threat Alert Center, and other individual service component information centers play critical roles in this process by collating, analyzing, and disseminating the information received from the FPD, resulting in the promulgation of area threat assessments and timely indications and warnings of potential threats to the in-

BANDUNG, INDONESIA (25 March 2009) SGM William Smith, United States Army, Pacific Operations Sergeant Major, addresses Tentara Nasional Indonesia—Angkatan Darat (TNI-AD) Warrior Leader Course students after the Commandant's Inspection. Instructors from the Non-Commissioned Officer Academy and USARPAC trained Indonesian NCOs on U.S. Army techniques, tactics and procedures. (Photo Credit: SSG Joann Moravac, USARPAC PAO)

transit forces. Relevant security information derived from FPD activities is utilized by in-transit forces to develop appropriate FP and crisis action plans tailored to the operating environment.

Assessing Vulnerabilities

FPD team members, as well as any AFOSI, NCIS, USA, and USMC security personnel assigned temporary duties in direct support of specific events and missions in conjunction and coordination with the TNI, INP, and private-sector establishments, routinely conduct security assessments of ports, airfields, travel routes, training areas, hotels and lodging sites, and various other facilities to identify and subsequently mitigate vulnerabilities. NCIS Security Training, Assistance, and Assessment Team (STAAT) members play a vital role in this process. The assessments they conduct in coordination with and with assistance from the FPD on the various ports and airfields become essential to the development of FP plans for visiting ships and aircraft. The identified vulnerabilities and proposed mitigation measures, when associated with the joint establishment of security for an actual event, are often shared with Indonesian government and/or private-sector security personnel, further enhancing teamwork and effectively increasing the safety and security of all.

Capacity Building

The PACOM Theater Security Cooperation program is a key component of the FPD mission in Indonesia. Through the conduct of various security training programs and seminars, the FPD assists in building security capacity for the TNI and INP. Significant training events involving the FPD have included executive protection training for the Indonesian Presidential and Dignitary Protection Force (PASPAMPRES), law enforcement tactics, techniques and safety training for the Bali Regional Police, postblast investigation and crime scene management training for the INP Detachment 88 counterterrorism unit and forensics division, and security

training for the INP assigned to protect Indonesia's international ports. Course organizers and participating instructors include subject matter experts from the FBI, the American Embassy RSO, NCIS STAAT, the U.S. Coast Guard (USCG), the Joint Inter-Agency Task Force West, and the Los Angeles County (CA) Sheriff's Department.

These events significantly contribute to the overall understanding of the capabilities and limitations of Indonesia's security forces—information that is essential to the development of comprehensive and mutually supportive FP plans. Through the combined efforts of the FPD, NCIS, RSO, and USCG, security and law enforcement equipment has been donated to the Indonesian government, effectively increasing the capabilities and expertise of security forces. The equipment included crime scene investigation materials, entry control point search apparatus, seaport interdiction kits, bomb suppression blankets, and police officer protective training gear. The donation of this equipment as well as demonstrations of its use are part of an ongoing FPD Indonesia port and critical infrastructure security enhancement initiative for locations visited and/or utilized by in-transit DOD forces.

Through effective liaison, comprehensive engagement, and mutually supportive programs, FPD Indonesia has set the standard for security programs in the Asia Pacific region.

Operationally Engaged

The FPD routinely provides direct support to the various U.S. military ships, aircraft, and personnel visiting Indonesia, serving as PACOM's front line in the detection and warning of threats. With more than 140 military events and visits per year, the FPD is actively engaged with the TNI and INP to develop comprehensive FP, security, and crisis action plans. Major PACOM events supported by the FPD include Cooperation Afloat Readiness and Training, Garuda Shield, and Pacific Partnership, activities designed to enhance interoperability, readiness, and cooperation between the Indonesian and U.S. militaries. In addition, the July 2009 terrorist bombings of two prominent Jakarta hotels and the September 2009 Padang earthquake and associated humanitarian assistance/disaster relief (HA/DR) operation demonstrated the FPD's surge capabilities to provide immediate and comprehensive investigative and security support.

Following the nearly simultaneous terrorist suicide bombings of the JW Marriott and Ritz Carlton hotels in the Kuningan district of Jakarta on 17 July 2009, the FPD in coordination with the American Embassy DAO, ODC, and RSO assisted in accounting for all DOD personnel and associated assets. The FPD also interviewed military members and other U.S. government employees who were present in the hotels during the bombing to gain immediate and actionable information to assist in identifying the terrorists and attack methods involved.

In response to the Padang earthquake, the FPD, in direct coordination with the American Embassy DAO and RSO, led a team of security professionals composed of AFOSI, NCIS, and USA personnel within the quake zone in direct support of U.S. government and military HA/DR efforts. Support included coordination with and assistance to the TNI, INP, and nongovernmental organizations as well as the conduct of site vulnerability surveys, which were utilized to build and adjust safety and security plans. Suspicious incidents were quickly investigated and addressed by the team. The FPD's overall efforts guaranteed the timely and accurate receipt of information by American Embassy and U.S. military supervisors responsible for ensuring the safety and security of deployed HA/DR personnel.

Another example of FPD direct support occurred during the PACOM Pacific Partnership disaster relief exercise that was held throughout the North Maluku province in Summer 2010. The centerpiece of this exercise was the USNS MERCY (T-AH 19) hospital ship, requiring close coordination with and assistance from the TNI and INP for security support. The FPD in conjunction with NCIS conducted numerous security assessments of the various ports and helicopter landing zones as well as the many medical, dental, veterinary, engineering assistance, and community service project sites located across the North Maluku island chain. These assessments were utilized to build and establish solid security and crisis action plans as well as to keep key decision makers apprised of the security environment so that an appropriate security posture could be maintained.

Protecting Dignitaries

In coordination with the American Embassy DAO and RSO, the FPD coordinates and provides FP assistance and support to Protective Service Operations involving authorized U.S. military flag and general officers visiting Indonesia. In support of this mission, the FPD routinely conducts route vulnerability surveys and security assessments for associated hotels, hospitals, and meeting locations to aid the protective detail in formulating a comprehensive security plan. Occasionally, FPD personnel will augment the protective detail as the in-country security expert.

In preparation for President Obama's November 2010 visit to Indonesia, the FPD utilized NCIS STAAT personnel to conduct executive protection training for PASPAMPRES, significantly enhancing interoperability and strengthening a strategic security relationship with the American Embassy. The FPD also provided support to both the White House Military Office and the Commander U.S. Seventh Fleet forward command

element. This support included the conduct of numerous lodging, route, and site vulnerability surveys; the synchronization and facilitation of private sector security contacts; and the provision of daily ground-level situational reports and briefings, all of which significantly contributed to a safe and successful presidential visit.

Leading the Way

Through effective liaison, comprehensive engagement, and mutually supportive programs, FPD Indonesia has set the standard for security programs in the Asia Pacific region. The FPD's effectiveness as an FP force multiplier in Indonesia is well documented. This is a direct result of the close cooperation and coordination achieved with the American Embassy RSO, the Senior Defense Official/Defense Attaché, ODC, and Indonesian military and police. The safety and security of our in-transit forces depends on it.

Note: This article is an update to "FPD Thailand Shows the Way," U.S. Naval Institute Proceedings, February 2008.

Scott M. Bernat is the Resident Agent in Charge and Chief of U.S. Military Security of the American Embassy Jakarta, Indonesia Force Protection Detachment (FPD). Since its establishment, FPD Indonesia has received several U.S. Department of State Meritorious Honor Awards for the establishment and integration of an effective FP program and security support to HA/DR operations as well as a White House Military Office commendation for outstanding security support to U.S. presidential travel.

1 Indonesia. Wikipedia. Available at http://en.wikipedia.org/wiki/Indonesia

2 Department of Defense. *Force Protection Detachment Joint Standard Operating Procedures*. September 2008.

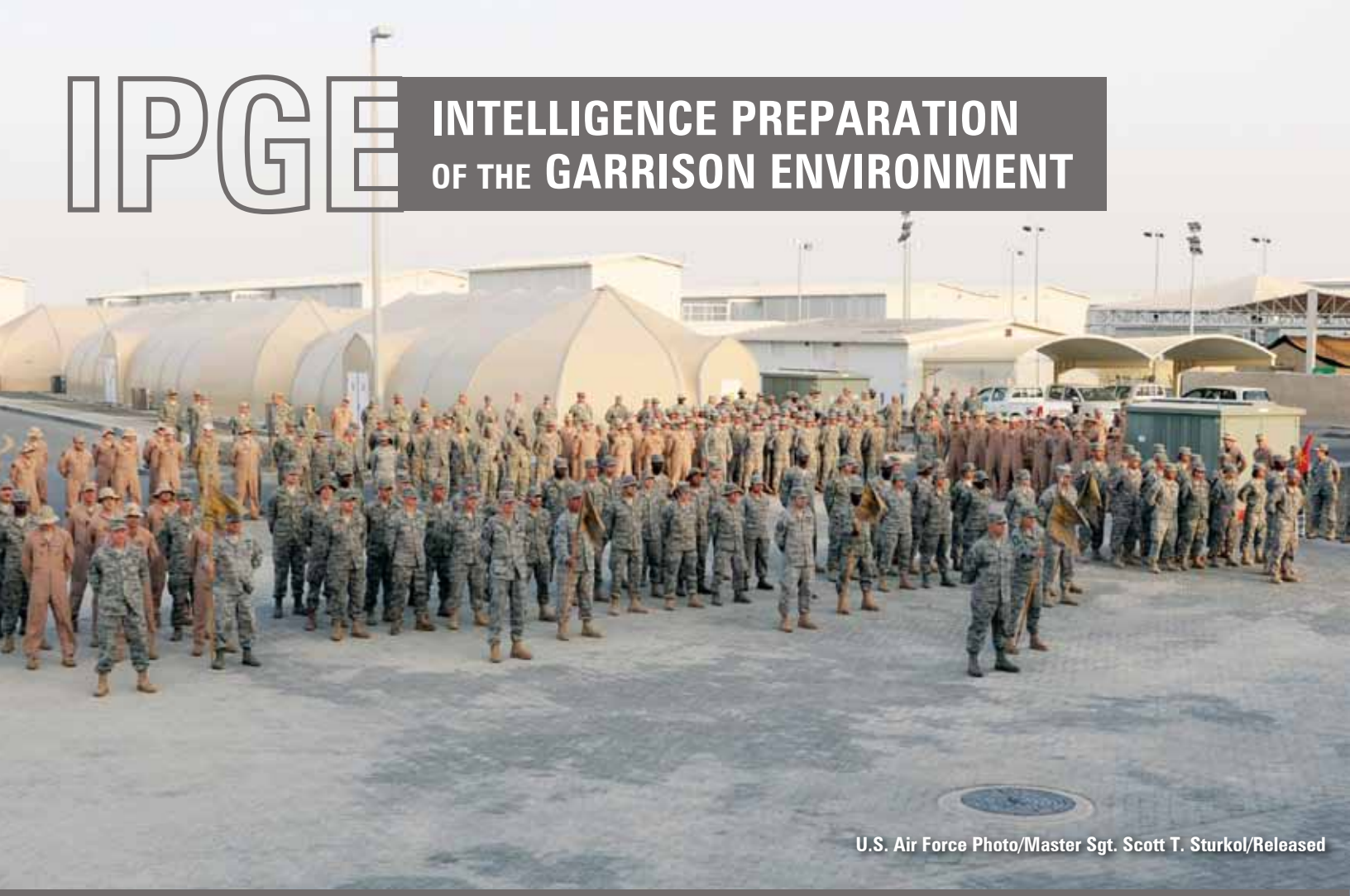
3 U.S. Department of State Bureau of Diplomatic Security. OSAC [Overseas Security Advisory Council]. Available at http://www.osac.gov

4 American Chamber of Commerce in Indonesia. Available at http://www.amcham.or.id

5 Asia Crisis and Security Group. Available at http://www.acsgroup.org

6 ASIS International. Available at http://www.asisonline.org

IPGE INTELLIGENCE PREPARATION OF THE GARRISON ENVIRONMENT



U.S. Air Force Photo/Master Sgt. Scott T. Sturkol/Released

Applying Tactical Intelligence Doctrine To Antiterrorism

By Peter Huller

We can adapt traditional IPB techniques to ensure the life, health, and safety of our garrison communities.

Many quote Sun Tzu's brilliant precepts regarding knowledge of one's enemy, but the following quote crystallizes the concept of Intelligence Preparation of the Battlefield:

> When I took a decision or adopted an alternative, it was after studying every relevant—and many an irrelevant—factor. Geography, tribal structure, religion, social customs, language, appetites, standards—all were at my finger-ends. The enemy I knew almost like my own side.
>
> —T.E. Lawrence (Lawrence of Arabia), 1933

The traditional application of Intelligence Preparation of the Battlefield/Battlespace (IPB) focuses on the tactical, operational, and strategic aspects of warfighting and often is constrained by time. In the FP arena, we can implement a very similar planning technique called Intelligence Preparation of the Garrison Environment (IPGE) to ensure the life, health, and safety of our garrison communities.

Because the garrison's mission is of an enduring nature, we are less constrained by time than in the tactical sense of traditional IPB. We can apply many of the doctrinal tenets of IPB to traditional AT concepts and use IPB products to provide the commander with a unique method of identifying threats, vulnerabilities, and risk using a six-step process. This process can be applied to the overarching umbrella of FP, which, depending on the service, encompasses multiple disciplines such as force health protection, safety, security, and law enforcement. This article will address the application of IPB to AT specifically.

The garrison AT mission dictates a more protracted planning process than the tactical battlefield

environment. By using doctrinal IPB methods and processes with certain modifications, we can develop a means for systematically mitigating potential enemy courses of action (COAs; i.e., the terrorist threat) and improving FP at the installation level. Although IPB exists to provide a framework for an S2 (intelligence officer) to advise the commander in a conflict situation, the same requirement exists for an AT officer (ATO) to advise the garrison commander in our battle against the enduring and persistent threat of international terrorism.

Because the garrison's mission is of an enduring nature, we are less constrained by time than in the tactical sense of traditional IPB. We can apply many of the doctrinal tenets of IPB to traditional AT concepts and use IPB products to provide the commander with a unique method of identifying threats, vulnerabilities, and risk using a six-step process.

Field Manual 2-01.3 defines IPB as "a systematic process of analyzing and visualizing the portions of the mission variables of threat/adversary, terrain, weather, and civil considerations in a specific area of interest and for a specific mission." The application of this definition of IPB for Army garrisons is obvious and critical to FP at the home station. The garrison commander must always be aware of threats to the installation and ready to leverage resources to mitigate them. The DOD concept of FP calls for the synchronization of an extensive base of disciplines in a broad program to protect Service members, civilian employees, family members, facilities, and equipment. As one of those disciplines, AT provides the commander with specific tools to accomplish a critical part of the FP mission.

The garrison ATO uses a variety of methods to enable the commander to accept a certain level of risk in the garrison environment, and many of these methods correlate to tactical IPB quite closely. The first step in the IPB process, for example, is to define the operational environment. To do this, the S2 must identify specific features of the operational environment and their concomitant physical locations. Similarly, the ATO must define the installation as an area of operations (AO) to identify the characteristics that will influence friendly and threat operations. In both cases, there also has to be a defined area of interest (AI). Although IPB typically defines the battlespace geographically, the ATO must consider factors beyond geography in identifying the garrison's AI, such as political concerns; local, state, and federal intelligence and law enforcement assets; and population centers. These factors all become part of the AO and the AI as they relate to mitigating the terrorist threat.

In addition to the tools mentioned, ATOs can use additional planning resources to develop a comprehensive program that will deter, detect, and deny terrorists from accomplishing their missions. The ATO conducts three assessments (criticality, vulnerability, and risk) as the core building blocks of the AT program. This approach is supported by the indispensable foundation of the threat assessment provided by the intelligence community. Additionally, the *Joint Antiterrorism Guide (JAG)* offers tools to address risk such as the Risk Management Application, which delves deeply into the capabilities and vulnerabilities associated with installation assets. The Unified Facilities Criteria provide a unique formula to develop a product known as Design Basis Threat, which assists FP professionals (e.g., ATOs, physical security officers, civil engineers) in identifying how best to design and build facilities to withstand the variety of threats against them. This exercise provides a solid baseline for construction, but it still falls short of the holistic approach of an IPB process and therefore should be incorporated into it.

In U.S. Army Europe, some ATOs use a methodology known as the Risk Assessment Tool (RAT). The RAT is based on an article written by MAJ Gino Amoroso in the April 2004 edition of *The Guardian* entitled, "Using Analytical Risk Management to Determine Antiterrorism Risks." Mr. Mick Lacy, Installation Management Command-Europe ATO, further refined MAJ Amoroso's concept into the RAT, which provides a quantifiable means of valuing criticality against threat and vulnerability to reach a risk assessment metric. A great feature of the RAT is that the ultimate risk factor for each asset is developed for a series of five different types of threats: transnational terrorists, indigenous/domestic terrorists, criminals, foreign intelligence services, and weapons of mass destruction.

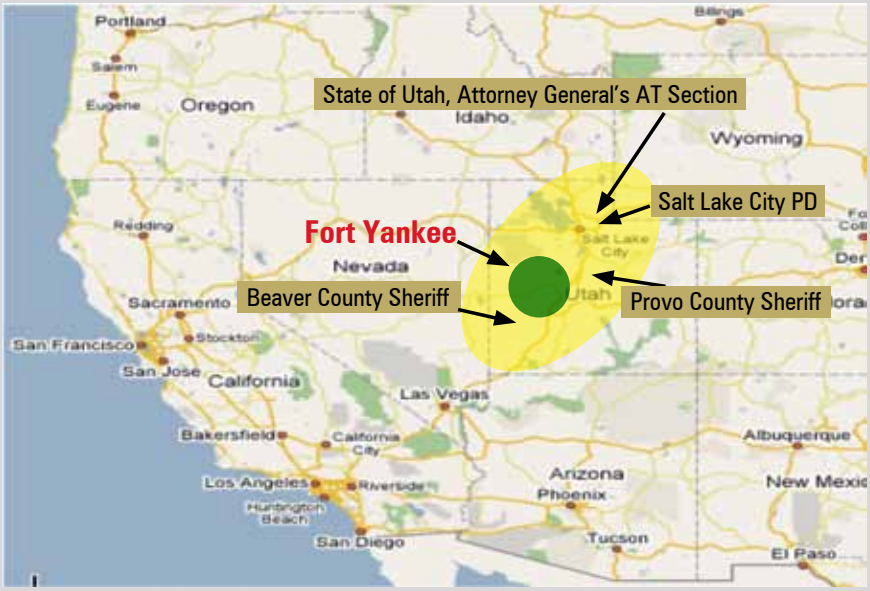
Just as traditional IPB products provide the commander and staff with the ability to leverage elements of combat power to find, fix, and defeat the enemy, the AT style of IPB similarly serves to focus the commander's resources to deter, detect, and deny enemy COAs.

Just as traditional IPB products provide the commander and staff with the ability to leverage elements of combat power to find, fix, and defeat the enemy, the AT style of IPB similarly serves to focus the commander's resources to deter, detect, and deny enemy COAs. Surveillance systems, random AT measures (RAMs), and awareness programs combine to deter, detect, and prevent terrorist activity. Passive and active barriers, FP condition (FPCON) action sets, realistic training and exercises, and mass notification systems can deny an enemy's ability to successfully engage a target. The first step in protecting the garrison has to be defining the operational environment, that is, the installation.

Figure 1. Fort Yankee - HRT and MEVA Overlay

Water Communications MEVA HRT

Figure 2. Area of Operations (AO)/Area of Interest (AI)



Step 1: Define the Installation AO and AI

In defining the installation and its characteristics, the ATO develops graphic representations of the garrison. A map of the installation annotated with high-risk targets (HRTs) and mission-essential vulnerable areas (MEVAs) provides a tangible depiction of the garrison's AO with the critical facilities that may be targeted and may require protection. Figure 1 shows the AO of Fort Yankee (a fictitious installation) with an HRT and MEVA overlay (including critical infrastructure such as water and communications assets). By graphically depicting this information, the ATO can more easily visualize potential threats and their likelihood and can develop better mitigating measures. In defining the AI, the ATO must consider factors such as available support and nearby military installations. Figure 2 illustrates the significant characteristics of the AI in relation to the installation.

Step 2: Determine Effects of the Local Environment

An analysis of the environment always includes an examination of terrain and weather, but the ATO may also study geographic and infrastructural characteristics along with their effects on friendly and threat operations. Geographic characteristics can include terrain and weather aspects as well as politics, civilian press, local population, and demographics. An area's infrastructure consists of the facilities, equipment, and framework needed for the functioning of systems, cities, or regions.

In a garrison environment, the ATO must draw on a variety of local and federal agencies for assistance in identifying the threat, especially in the United States.

Analyzing terrain represents a similarity between IPB and IPGE. Whereas in IPB the S2 prepares the combined obstacles overlay (COO), the ATO develops a very similar product aimed at identifying terrain features that may help or hinder an enemy. The ATO identifies avenues of approach into the installation, both from a high-speed (i.e., vehicular) view and an unobstructed perspective (see Figure 3), and, like the S2, depicts terrain features that can delay threat forces from entering the installation unobstructed. The ATO can further refine this analysis by applying the results of the criticality assessment (MEVAs and HRTs from Figure 1 remain in Figure 3) of the garrison's facilities meshed with terrain features to

produce a result similar to a modified COO, as used in tactical IPB. The ATO now has a good picture of the AO, enabling identification of potential vulnerabilities, and can share this information with the physical security officer in developing the installation's barrier plan.

The AO is important, but the ATO must also know the AI and its features. In a garrison environment, the ATO must draw on a variety of local and federal agencies for assistance in identifying the threat, especially in the United States. Other features of the AI that might be critical to the ATO include transportation resources, an understanding of the area's demographics, and knowledge of friendly forces in the AI. Figure 4 depicts some of the features that would be valuable to an ATO in understanding the local threat. Radical groups use venues such as universities, religious centers, and the Internet to recruit and to plan operations. Activist groups in the area may be opposed to military construction on the installation for some reason. These elements are in the ATO's backyard, and ignorance of them can be dangerous. The value of coordinating with other regional ATOs cannot be understated and must be leveraged as force multipliers in developing the threat picture for the garrison commander.

Step 3: Develop Installation Awareness into a Force Multiplier

To provide the commander with the clearest threat picture possible, the ATO must leverage multiple and varied sensors available to support the threat assessment effort, much like an S2 uses all elements to report essential elements of information. By developing a detailed Threat Information Collection Plan (see Figure 5) and sharing it within the community, the ATO can leverage these assets to improve awareness of the local threat. But before that happens, the ATO must ensure that community members understand their role in the process.

Key players in the ATO's daily sphere of operations know exactly what information is valuable and will bolster understanding of the threat. For community members, a robust AT awareness program will clarify the importance of identifying and reporting suspicious activity. The annual required AT Level I briefing is the foundation of this program because it provides a general picture of AT and individual protective measures. The

Figure 3. Fort Yankee—Avenues of Approach Overlay

Figure 4. Factors Affecting the AI

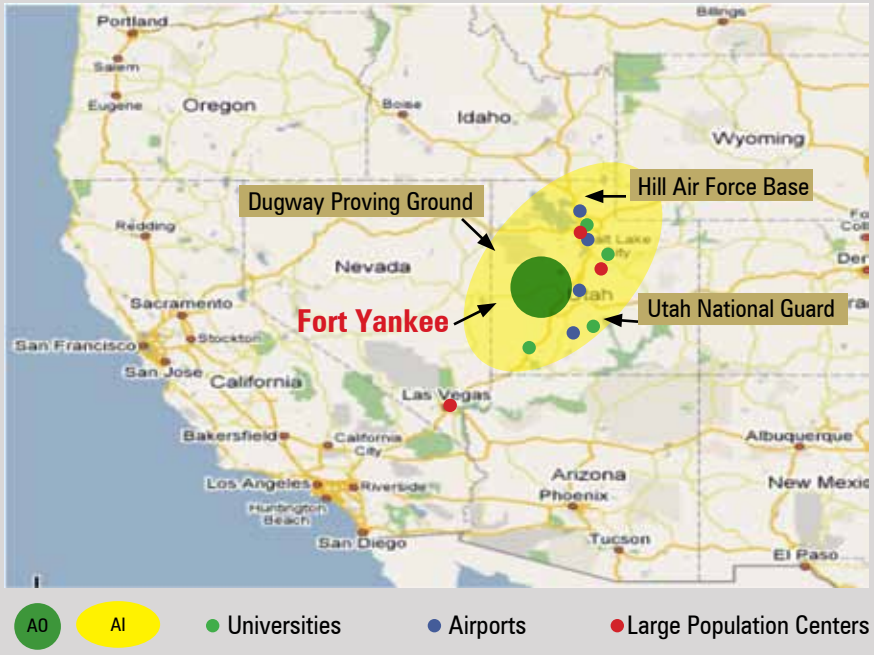


Figure 5. USAG-Yankee Threat Information Collection Plan

PIR	IR/CCIR	EEFI	Specific Information Requirements	Indicators	Specific Orders and Requests	Collection Agencies: DES /CID	MI Det	Div G2	Tenants	Directorates	Adjacent bases	Nat'l Agencies
PIR #1												
1. Will terrorists attempt to attack USAG-Yankee installations with explosives, cyber, by air, CBRNE, or infiltration?	1.1. Has surveillance been conducted for the purpose of targeting our HRTs, MEVAs, or High-Risk Persons (HRPs)? What is the installation's current center of gravity?	What are the USAG-Yankee installations MEVAs/HRTs?	What is the most effective current attack tactic against USAG-Yankee installations? What are the threats to designated HRPs on USAG-Yankee installations? What installation facility or person would be a target of a terrorist attack and why? What terrorist tactic(s) would cause the greatest disruption to installation missions? How can terrorists gain information about the installation, its activity and personnel?	Personnel observed standing, parking, or loitering with no apparent reason. Personnel using/ carrying video cameras, (Night Vision Goggles (NVGs), or observation equipment with high magnification lenses. Personnel observed drawing or possessing maps or diagrams of installation infrastructure or personnel. A noted pattern or series of false alarms requiring law enforcement or emergency services response. Unattended packages, briefcases, or boxes.	Report any surveillance of HVTs, MEVAs, or HRPs, and/or suspicious-looking packages, briefcases, boxes, bags, etc., in vicinity of HVTs, MEVAs, or HRPs. Report violations to safeguarding sensitive or classified information. Report disruptions and denials of service of telecommunications or computer equipment.	X	X	X	X	X		

ATO should make every effort to provide tailored information in the briefing to convey the concept that "it takes a community to protect a community."

Building on this foundation, initiatives like the U.S. Army Garrison Vicenza's Residential Security Program attach a layer of awareness to community personnel who want to protect their homes and property. Periodic messages to the community such as monthly newsletters, FP advisories, and articles in the community newspaper serve as additional building blocks in constructing a bastion of community consciousness of the terrorist threat. Some garrisons develop information pamphlets, whereas others use outside-the-box concepts like informational posters sized to fit on dining-facility and fast food trays to spread the message (see Figure 6). Although it is necessary to aggressively address ignorance of the threat, the ATO must be careful to avoid information overload, which can result in complacency. In the end, the goal is to synthesize a collective understanding that will result in all of these "sensors" contributing to the overall threat picture.

Step 4: Evaluate the Threat

The ATO receives threat information through a variety of resources including national-level agencies, military intelligence resources, and open source media. These sources provide information on all of the same informational aspects about an enemy that an S2 requires—composition, disposition, tactics, training, logistics, operational effectiveness, recruitment, and support—albeit in a less comprehensive fashion. The Defense Intelligence Agency, for example, provides a macro-level assessment of the terrorist threat that will address many of the noted data points. Theater-level intelligence assets prepare more detailed threat assessments that provide the garrison ATO with a general picture of the regional threat environment. Local intelligence elements also can help identify possible threats via SPOT reports. SPOT reports can include suspicious activity reporting provided by the full range of garrison sensors: military police, contract security guards, military personnel, family members, and even contractors

on the installation. The ATO must take all this information and use the threat fusion cell (or similar threat working group) to apply it to the garrison AO and AI to ensure that the garrison AT program is addressing the threat properly. Similarly, an S2 will work with fellow staff members in evaluating the threat on the battlefield using products developed by key intelligence sources in theater.

Figure 6. Awareness Posters/Placemats

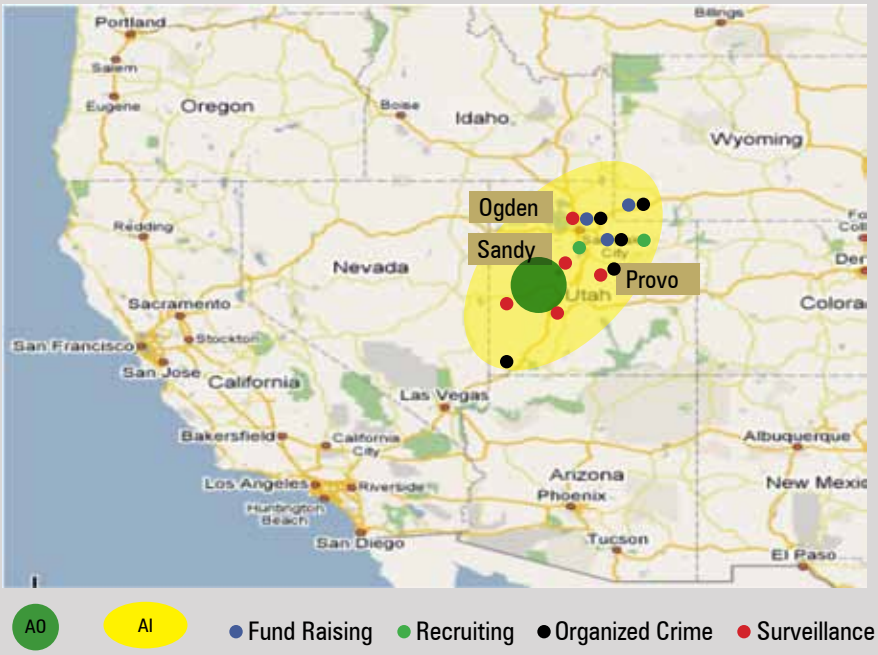
The synergy of asset products, whether national-level assessments or a high school student's report of possible surveillance, can result in developing a clearer local threat picture for the commander (see Figure 7). The ATO must use this information and other indicators of potential threats to develop mitigation strategies that reduce risk and justify funding requests to procure resources needed for implementing these mitigation strategies. Knowing, for example, that radical extremist groups are recruiting in your AI may explain a report of a Soldier suddenly exhibiting unusual behavior consistent with insider threat behavior. This is also why Step 3 (Develop Installation Awareness into a Force Multiplier) is so crucial. Likewise, if a critical asset is located near an unobstructed avenue of approach, the ATO may recommend to the commander that this concern be mitigated by installing surveillance devices like a closed-circuit television (CCTV) system or improved lighting. The ATO must address the criticality of assets through both friendly and threat lenses. Only through in-depth knowledge of the AO and the AI can the ATO effectively support the garrison commander. In the final analysis, using available information to recommend ways to counter the threat is a key function of the ATO.

Step 5: Determine Threat COAs

In the wartime environment, a unit already engaged with an enemy has an idea of what possible COAs are available. The S2 may already know the likely objectives of the threat and thus can effectively analyze specific COAs based on multiple factors such as terrain, weather, and enemy capabilities to prioritize and select the most likely and most dangerous COAs. In the garrison environment, the ATO can address threat COAs in much the same way. The ATO must consider the history, intentions, and capabilities of the enemy along with a wide variety of threat tactics to determine the likelihood of a particular COA. The main difference between these two environments is time. In battle, the enemy is likely to take action sooner rather than later. In garrison, the threat may appear tomorrow or never. Regardless, the ATO must ensure that the garrison is prepared. By understanding potential COAs, from the most likely to the most dangerous, the ATO can advise the commander accordingly.

Given what the adversary normally prefers to do and the effects of the specific environment in which the adversary is now operating, what are the likely objectives and what tactics are available? What are the potential targets? How can those targets be attacked successfully? What are the adversary's capabilities? An adversary would analyze all of these questions, and the ATO must do likewise. In Cold War S2 terms, the ATO must "think Red." What does the enemy want to do, and how and when will he do it? These are the questions the ATO must raise within the threat fusion cell and the AT working group. By using the results of the four basic assessments—threat, criticality, vulnerability, and risk—the ATO, along with garrison stakeholders, can properly address enemy COAs. The U.S. Army Corps of Engineers has developed a tool that allows the ATO to template critical assets overlaid against a wide variety

Figure 7. Threat Activities (Notional)



of threat tactics to quantifiably assess the likelihood of a threat COA. By using this tool, the ATO can not only establish an effective baseline for protective design of future facilities but also focus on mitigation measures for managing risk and protecting critical facilities and personnel.

Step 6: Mitigate Enemy COAs

The critical difference between the garrison setting and the battlefield is in the ability to predict when a potential COA will occur. Consequently, it is increasingly important for the AT program to execute its function of deterring, delaying, and preventing terrorist attacks. Applying the tactical IPB to the garrison environment is an extension of portions of Step 4 of IPB, developing each COA. The S2 looks at the who, what, when, where, why, and how of a COA. The ATO does the same but has to do so over a more prolonged period of time.

An ATO can develop situational templates like an S2 but also must develop the means to counter COAs, again, in concert with the AT working group. In effect, this is the ATO's version of wargaming, albeit with a more strategic level of urgency. Once COAs have been identified and prioritized, the AT working group can address each one systematically using a myriad of preventive measures. These measures include RAMs, structural hardening, FPCON action sets, exercises and training, electronic security systems (i.e., CCTV and intrusion detection systems), AT awareness, and surveillance detection.

RAMs in particular form the backbone of an effective AT program because they accomplish multiple objectives simultaneously. The main goal of a RAM is to be visible and to ensure a robust security posture from which terrorists cannot easily discern patterns or routines that are vulnerable to attack. An observer might notice, for example, that guards typically perform a cursory check on vehicles entering a certain access control point (ACP); however, on certain days of the week and at certain times (never on a routine schedule), the same observer will see the guards using military working dogs to assist in vehicle searches. In this way, security appears unpredictable and imposing.

Military police and contract security guards perform the bulk of security functions and implement the majority of RAMs (because of their inherently visible presence at ACPs and on the installation perimeter). By developing a dynamic and aggressive RAM program, the ATO creates conditions for security forces that counteract the potential for complacency by those forces. The RAM program should be integrated throughout the installation.

AT working group members are essentially the ATOs for their organizations and units. They are the face of AT to their commanders or directors, and they coordinate the conduct of RAMs at their locations. Their diligence in executing RAMs elevates the level of awareness in the community and serves to alter what appear to be daily security measures. The RAM program pays an additional dividend in that it validates the installation's ability to implement measures from higher FPCON levels and any additional resources that may be required to do so. All of these functions occur over time and require planning and resourcing to accomplish the goal of mitigating potential threat COAs.

The tactical S2 has a complicated job in spearheading the IPB process and is further challenged by time, resource, and information constraints. Similarly, the garrison ATO must act as the linchpin of a difficult process. Limited resources, information gaps, and uncertainty about the enemy confront the ATO on a daily basis. By using a modified six-step form of the IPB process, the ATO can leverage an additional tool to more quantifiably identify risk and portray it in terms of the garrison AO and AI and present the commander with a risk assessment and recommendations to mitigate risk to an acceptable level. ATOs have a variety of methods of performing risk management, and IPGE should be considered one of them.

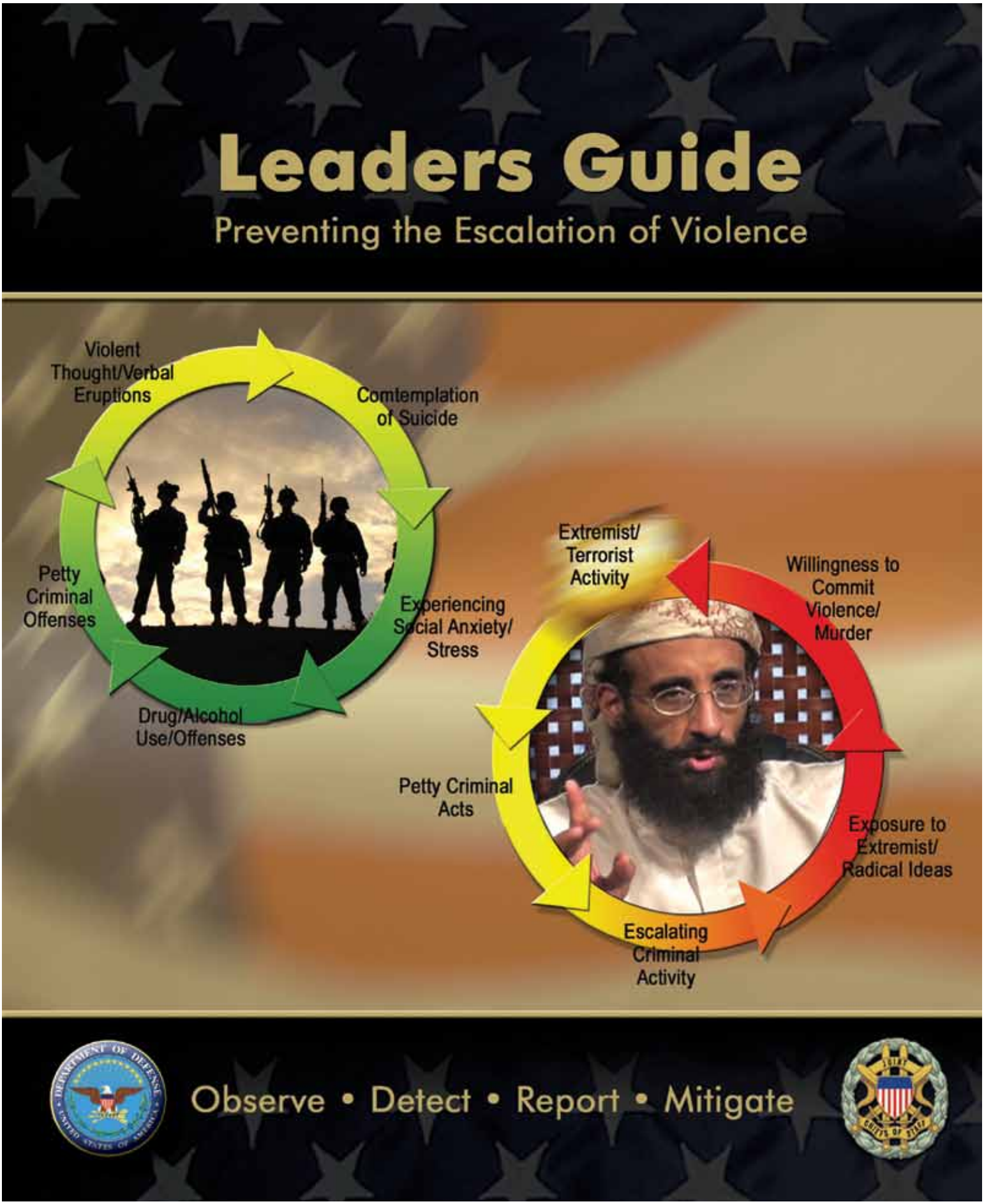
Indicators of Potential Terrorist Associated Insider Threat

- Advocating support for terrorist organizations or objectives.
- Expressing hatred of American society, culture or government, or principles of the U.S. Constitution.
- Advocating the use of violence to achieve political, religious, or ideological goals.
- Sending large amounts of money to persons or financial institutions in foreign countries.
- Expressing a duty to engage in violence against DoD or the United States.
- Purchasing bomb-making materials.
- Inquiry or obtaining information about the construction and use of explosive devices.
- Expressing support for persons or organizations that promote or threaten the unlawful use of violence.
- Advocating loyalty to a foreign interest over loyalty to the United States.
- Financial contribution to a foreign charity or cause linked to an international terrorist organization.
- Evidence of terrorist training or attendance at terrorist training facilities.
- Repeated viewing of Internet Web sites, without official sanction, that promote or support international terrorist themes.
- Posting comments or exchanging information, without official sanction, at Internet chat rooms, message boards, or blogs that promote the use of force directed against the United States.
- Joking or bragging about working for a foreign intelligence service or associating with international terrorist activities.

Report Suspicious Activity:

- Contact your local Counterintelligence (CI) office
- CONUS Hotline: 1 – 800 – CALL SPY (1–800–225–5779)
- iSALUTE – The CI reporting portal via AKO at: https://www.us.army.mil/suite/page/633775
- iWATCH ARMY – https://www.us.army.mil/suite/page/605757

U.S. ARMY ARMY STRONG®



See poster insert on page 19 for details.

LEADERS GUIDE

Preventing the Escalation of Violence

OBSERVE • DETECT • REPORT • MITIGATE

Recognizing Signs of High-Risk Behavior

Indicators of high-risk behavior may include the following:

- Lack of positive identification within community
- Involvement across the violence spectrum
- Participation in lower-impact criminal activity or rule-breaking
- Increased use of alcohol or drugs
- Diagnosis of a mental health disorder, including depression
- Increased severe mood swings and noticeably unstable or emotional responses
- Increase in unsolicited comments about violence, firearms, and other dangerous weapons or violent crimes
- Defense of extremist or radicalized views
- Unusual accumulation of weapons, training manuals or other dangerous supplies

When indicators of potential violent behavior overlap with indicators of suicidal tendency, a synergistic effort between these elements should lead to information sharing, cross-talk, and standardized processes to aid in identifying personnel who may present an insider threat or have a potential for terrorist-related activity.

Personnel who are identified within this realm warrant further investigation by leadership and possibly law enforcement.

Monitoring Behavior

Commanders are empowered with numerous tools and authorities to take steps to promote the general welfare of Soldiers under their command. Examples:

- Organizational Inspection Programs
- Health and Welfare Inspections
- Urinalysis
- Privately Owned Weapon Registration
- Individuals participating in medical treatment programs and services, such as drug abuse prevention, family advocacy, and behavioral health programs, should also be screened for violent and extremist behavior, including a propensity toward violent and extremist activity

Preventing the Worst

Preventing insider threats or terrorist attacks involves much more than physical security measures. Recognizing indicators of high-risk behavior (such as criminal activity or associating with violent groups) that may lead to an escalation of violence, and addressing those issues, may reduce the potential for violent acts committed against the community.

Unit leaders, medical service providers, and the protection community must communicate effectively to develop a complete and accurate picture of an individual's propensity for future violence.

- Antiterrorism & Protection Professionals

- Unusual, unexplained selling or giving away of personal possessions

Unity of Effort

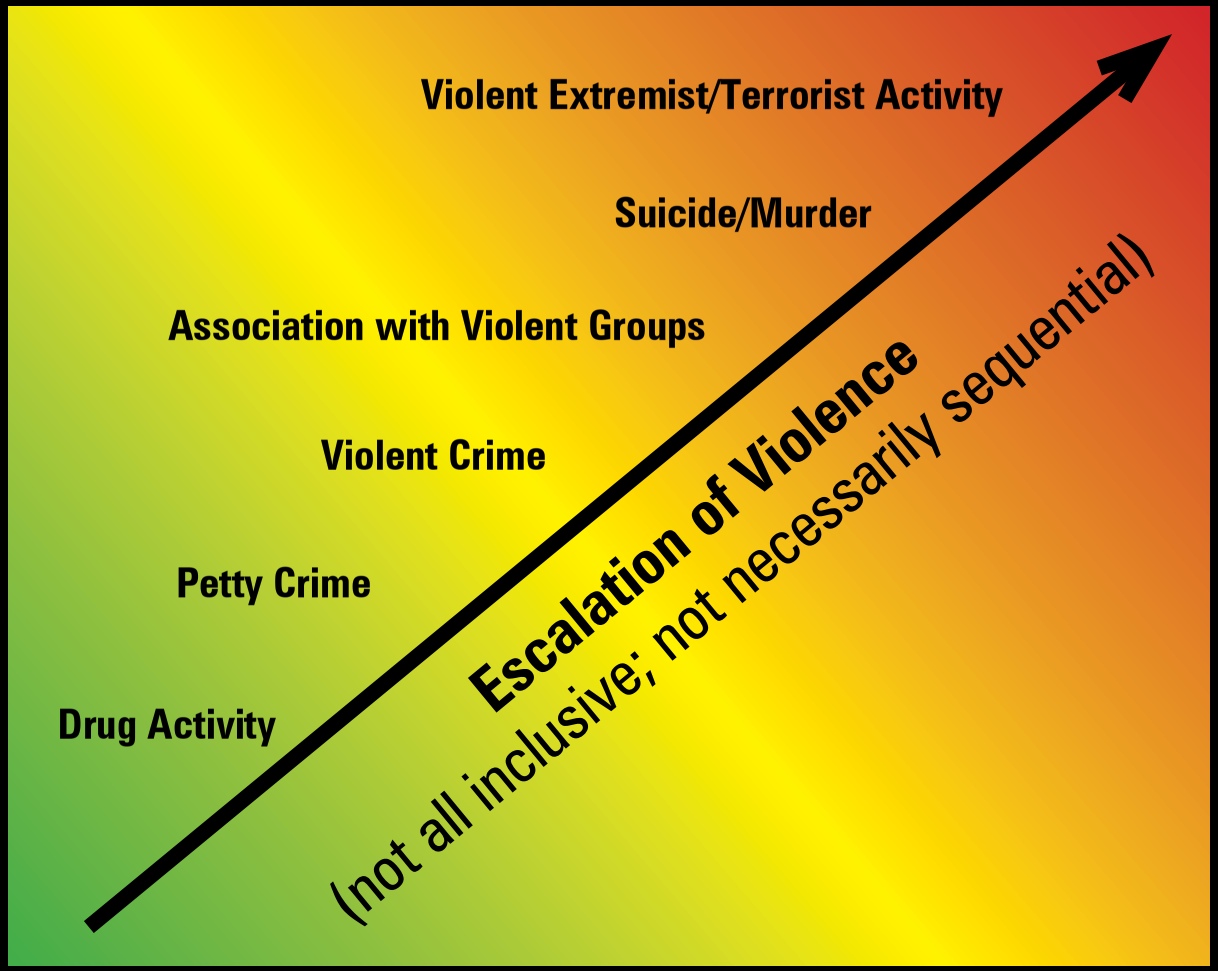
By approaching violence prevention comprehensively, medical service providers, supervisors/leaders, and protection personnel can work together to detect indicators of possible future violent or extreme behavior.

- Commander's Disciplinary Action
- Commander's Risk Indicator Dashboard
- Family Readiness and Feedback

Detection of high-risk behavior requires a multidisciplinary approach. Administrative tools that commanders use to improve unit readiness may have a secondary and positive risk reduction benefit to help counter insider threat or terrorist activity.

- Law Enforcement
- Medical Providers
- Commanders and Leaders (particularly first line supervisors)
- Soldiers and Civilians.

The Violence Spectrum



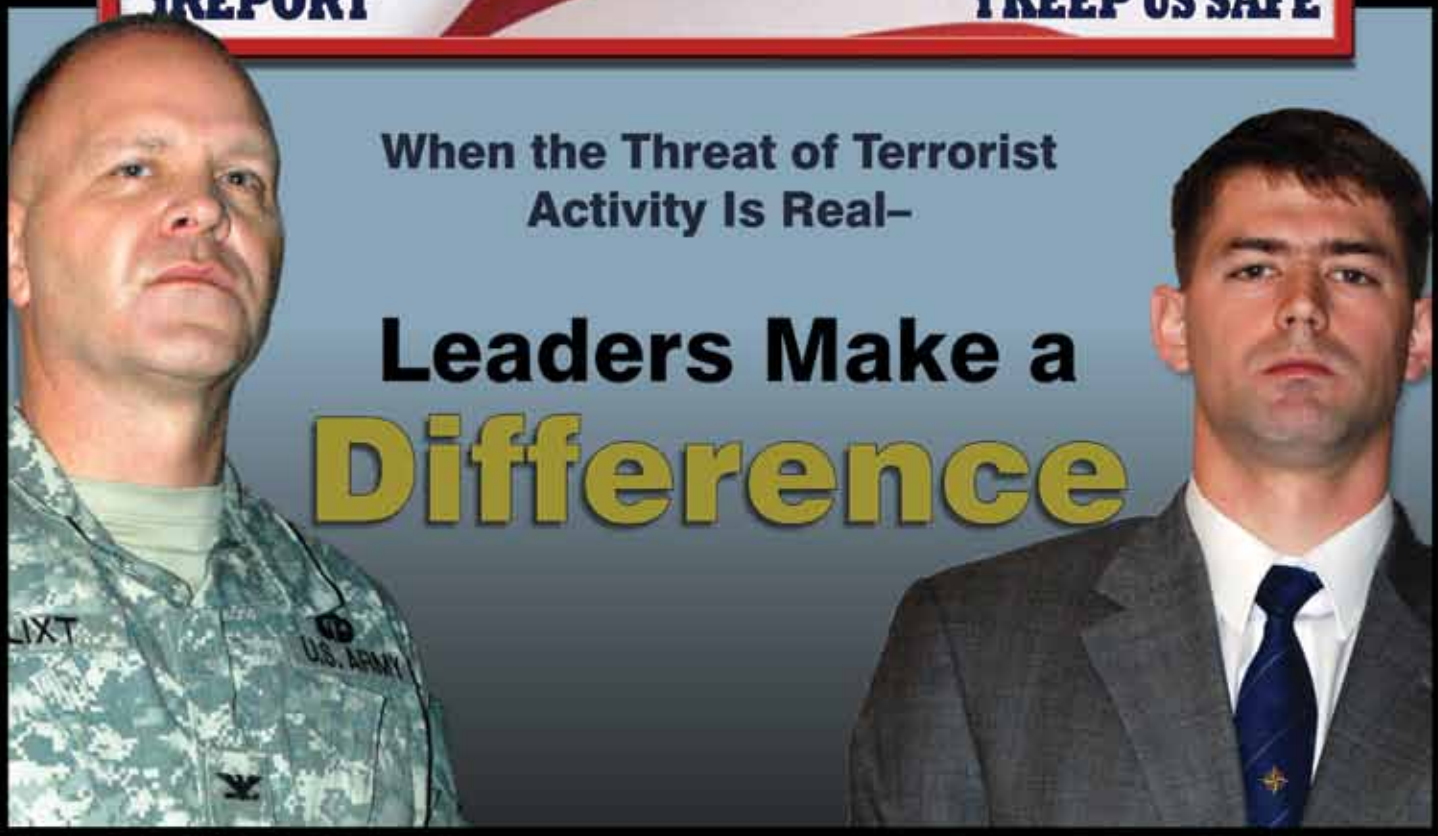
By mitigating lower-impact, higher-frequency violence (particularly high-impact criminal acts) leaders may be able to prevent an escalation of violence.

- Small-scale violence or antisocial behavior (such as simple assault, harming animals) may indicate a propensity for violence.
- Individuals who defend violent extremism, regardless of political or religious affiliation, should be monitored closely.
- High-risk indicators overlap, and the potential effects of those behaviors should not be treated in isolation (e.g., suicidal tendencies could lead to an active shooter situation, individuals exhibiting high-risk behavior may be vulnerable to extremist/terrorist group radicalization).
- Health promotion/risk reduction monitoring and treatment programs may help detect indicators and reduce possibilities of violence.

iWATCH

iREPORT

i KEEP US SAFE



When the Threat of Terrorist Activity Is Real–

Leaders Make a Difference

Leaders, do you know:

- Your role and responsibility?
- Your unit's responsibility?
- What to tell your soldiers, DoD civilians and families?
- What individuals can do to prevent terrorist acts?
- How to report suspicious activity or behavior?
- The indicators of high-risk behavior?
- Where you can find antiterrorism information?

Always Ready, Always Alert

Because someone is depending on you

COPING WITH AN ACTIVE SHOOTER

Evacuate—Hide—Take Action

By Peter Huller

Adapting traditional IFB techniques to ensure the life, health, and safety of our garrison communities

Profile of an Active Shooter

An Active Shooter scenario refers to one or more subjects participating in a shooting spree, random or systematic, with intent to continuously harm others. (Source: U.S. Army Military Police School, Active Shooter POI)

An Active Shooter may be a current or former employee associated with the U.S. Army (Soldier, Department of Army civilian, government contractor, or family member). An Active Shooter could also be an individual not directly associated with the Army who gains access to an Army installation, stand-alone facility, or unit.

Characteristics of an Active Shooter Incident

- The event is unpredictable and evolves rapidly.
- Victims are generally targets of opportunity.
- Ending an active shooter incident usually requires direct military police or law enforcement intervention.

Recognizing Signs of High-Risk Behavior

Indicators of potential violent behavior may include one or more of the following:

- Increased use of alcohol or drugs
- Unexplained increase in absenteeism or vague physical complaints
- Depression or withdrawal
- Increased severe mood swings and noticeably unstable or emotional responses
- Increasingly talks about personal problems or problems at home

- Increase in unsolicited comments about violence, firearms, and other weapons or violent crimes

HOW TO RESPOND

When Shooting Begins:

1. Evacuate

- Have an exit route and plan in mind.
- Leave your belongings behind.
- Keep your hands visible.

2. Hide

- Hide in an area out of the Active Shooter's view.
- Lock doors and block entry to your hiding place.

3. Take Action

- Only as a last resort
- Only when your life is in imminent danger
- Attempt to incapacitate the Active Shooter

When Police Arrive

- Remain calm.
- Obey all police instructions.
- Put down any items in your hands (such as backpacks, phones, jackets).
- Raise your hands, spread your fingers, and keep hands visible to police at all times.
- Avoid quick or sudden movements.
- Avoid pointing, screaming, or yelling.
- Do not stop to ask officers for help or directions while evacuating.

Information

Call 911 (or other local emergency number) when it is safe to do so.

You should provide the following information to the police or to the 911 operator:

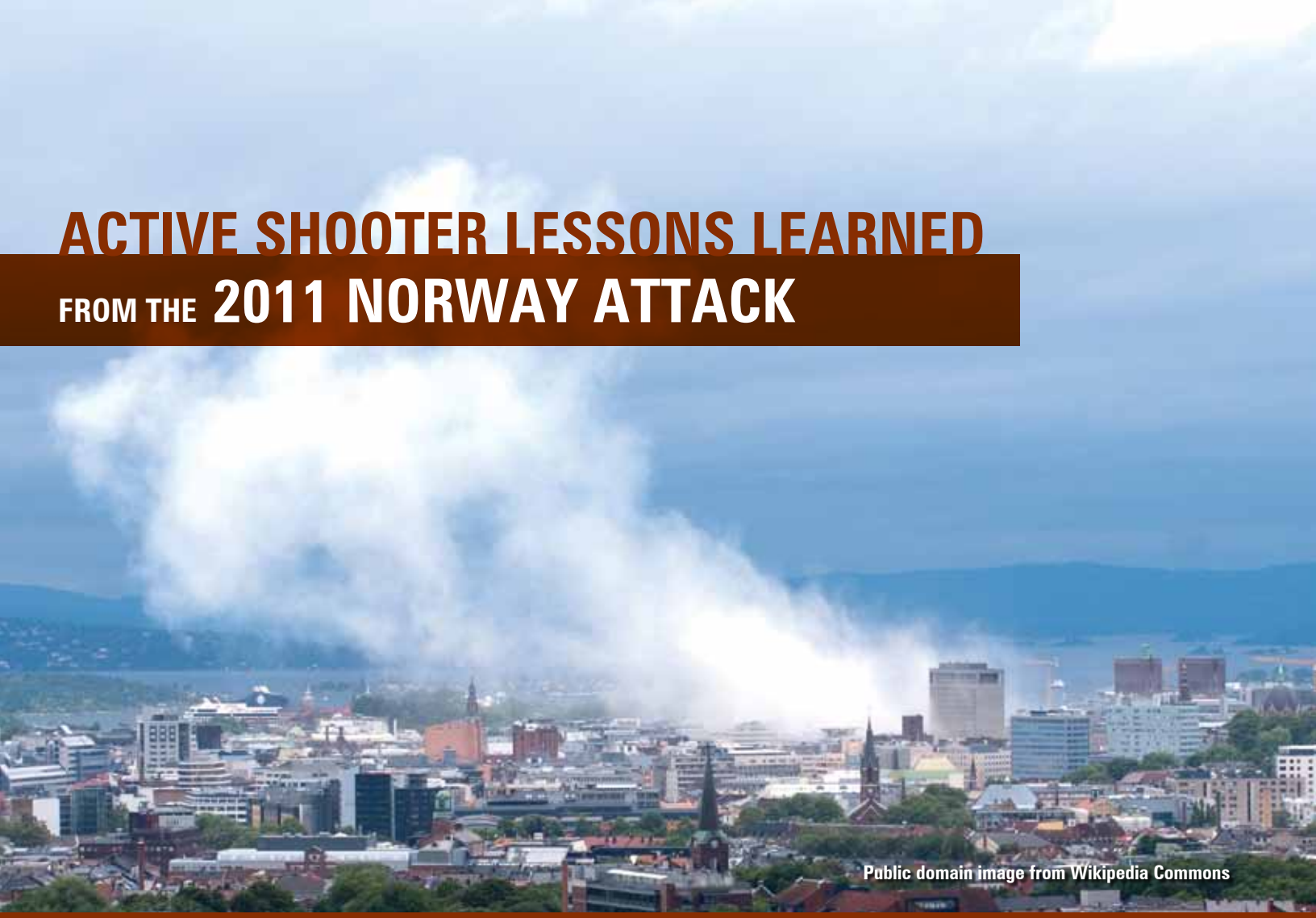
- Location of the shooter
- Number of shooters
- Physical description of shooters
- Number and type of weapons the shooters have
- Number of possible victims.

Coping with an Active Shooter

- Be aware of your surroundings and any possible dangers.
- Take note of the nearest exists in any facility you visit.
- If you are in an office at the time of an attack, stay there and secure the door.

Only as a last resort should you attempt to take action against the shooter.

ACTIVE SHOOTER LESSONS LEARNED FROM THE 2011 NORWAY ATTACK



Public domain image from Wikipedia Commons

The "lone-wolf" terrorist is particularly hard to detect

By CDR Chris Hill

Intelligence and law enforcement officers need to become experts on differentiating real threats from run-of-the-mill "nut jobs," especially when monitoring Internet activity.

The 22 July attack in Oslo, Norway, was one of the worst active shooter assaults committed by a single individual in history, a fact that calls for rigorous examination by AT experts. Sixty-nine people were killed at gunpoint. This toll is more than double that from the United States' worst active shooter incident, which occurred at Virginia Polytechnic Institute and State University (Virginia Tech) on 16 April 2007 and resulted in 32 people killed and 25 wounded.

Two big questions arise in the wake of any terrorist attack: (1) Could the attack have been prevented? (2) Could authorities have responded better? Although investigations into the Norway attack will likely continue over the next several months, enough data suggest that the answer to both questions is no (Figure 1). Given the attacker's fastidious preparation and Norway's law enforcement culture, which is accustomed to low crime, it is not likely that this attack could have been avoided. Some fixes could be enacted to deter future attacks, such as increasing guns, guards, and surveillance, but even these measures would not likely have stopped this well-prepared lone wolf. As one columnist noted, perhaps

Could the attack have been prevented? Could authorities have responded better? Although investigations into the Norway attack will likely continue over the next several months, enough data suggest that the answer to both questions is no.

"the lesson to be learned from the Norwegian tragedy is probably that there's no lesson to be learned from it."[1]

Figure 1: Summary of 22 July 2011 Norway Attack

- 22 July 2011, 1530: Vehicle-borne improvised explosive device detonates in Oslo next to a government building, resulting in eight killed. According to the suspect, the van contained 950 kilograms (about 2,100 pounds) of homemade ammonium nitrate-based explosives.
- Suspect departs scene and travels to the island of Utoya, located west of Oslo, where 700 children are at a Labor Party camp.
- Meanwhile, suspect dons body armor, tactical police gear, and insignia and arms himself with a handgun, a shotgun, and a rifle.
- Shortly after 1700: Suspect begins shooting and kills 69 more people on the island over a period of at least 60 minutes.
- After capture, the suspect, Anders Breivik, a Norwegian citizen, confesses to both attacks.

Did Anders Breivik Exhibit Threat Behavior?

As the lessons of Fort Hood highlighted, a number of telltale signs can expose a scheming terrorist. If we apply the U.S. Army's 10 Indicators of Terrorist-Associated Insider Threat (Fig. 2), a list of the more obvious terrorist behavioral indicators, we can conclude that Breivik exhibited at least half of the key indicators. If he were a member of Norway's armed forces, he may have been red-flagged by his leadership.

Breivik had been unemployed since 2002. He spent most of his spare time planning the attacks while secretly developing a 1,518-page manifesto cataloging his progress and justifying his warped political rationale for terror. The manifesto includes hundreds of pages on how he acquired bomb-making materials and weapons, what operations and security measures he preferred, and how he obtained thousands of like-minded anti-Islamic and xenophobic Facebook "friends." In addition to his steroid-induced physical conditioning, he prepared himself by playing first-person-shooter computer games such as Call of Duty. All of these details are included in the manifesto.

The fact that his manifesto was released the same day as the attack did not help detection efforts. As he noted in the manifesto, he avoided ending up on watch lists through vigilant surveillance-detection techniques. He even created an elaborate cover story that involved renting a farm so he could purchase ammonium nitrate fertilizer. The farm also provided a remote location in which to build his improvised explosive device.[3] After purchasing additional weapons components on eBay, he

Figure 2: U.S. Army's 10 Indicators of Terrorist-Associated Insider Threat[2]

The following behavior may be indicators of potential terrorist activity and should be reported immediately to the local counterintelligence office, Military Police, local aw enforcement , or military chain of command:

1. Advocating violence, the threat of violence, or use of force to achieve goals that are political, religious or ideological in nature
2. Advocating support for international terrorist organizations or objectives
3. Providing financial or other material support to a terrorist organization or to someone suspected of being a terrorist
4. Association with or connections to known or suspected terrorist
5. Repeated expression of hatred and intolerance of American society, culture, government, or principles of the U.S. Constitution
6. Repeated browsing or visiting internet websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes without official sanction in the performance of duties
7. Expressing an obligation to engage in violence in support of international terrorism or inciting others to do the same
8. Purchasing bomb making materials or obtaining information about the construction of explosives
9. Active attempts to encourage others to violate laws, disobey lawful orders or regulations, or disrupt military activities
10. Family ties to known or suspected international terrorist or terrorist supporters

Figure 3: Excerpt from Breivik's manifesto

There are thousands of video cameras all over European major cities and you will always risk leaving behind DNA, finger prints, witnesses or other evidence that will eventually lead to your arrest. They are overwhelmingly superior in almost every aspect. But every 7 headed monster has an Achilles heel. This Achilles heel is their vulnerability against single/duo martyr cells.

— Anders Breivik, page 934 of his manifesto

used FedEx shipping because he felt that public postal services had stricter customs routines.[4]

Perhaps Breivik's family or friends could have alerted authorities in advance, much like Umar Farouk Abdulmutallab's father did prior to the 2009 Christmas Day underwear bomb attack.[5] But even if Breivik were considered clinically psychotic, it is still possible, according to one Norwegian psychiatry expert who studied the case, "to live in a society for years with psychosis without being detected for treatment." Furthermore, Breivik was "socially isolated for a long time and seems to have [had] little contact with family and a few close friends."[6] The same can be said of other lone-wolf militants such as Theodore Kaczynski and Eric Rudolph, who schemed for years without detection or capture. By all preliminary indicators, Breivik's terrorist intent was practically invisible.

Was There Enough Security on Utoya Island?

Dressed in full police gear, Breivik executed an hour-long active shooter assault against 700 children on the remote island of Utoya. Altogether, he killed or wounded as many as 130 individuals, which averages just over 2 persons shot per minute. This number is slightly lower than the November 2009 Fort Hood shooting, which averaged 4.3 people killed or wounded every minute.[7] Notably, the historical average for active shooter scenarios is around 3 persons killed and 3.6 wounded in total.[8] One explanation for the lower hit rate in Norway compared to Fort Hood could be the environment. The Fort Hood attack occurred inside a building with fewer exits, whereas the Utoya Island incident occurred in an open wooded area with more hiding places.

In the Fort Hood case, armed base police officers with active shooter training were able to engage the shooter within 10 minutes of the start of the attack. The response time in Norway was 60 minutes—an eternity to the victims in Norway, many of whom pretended to be dead or tried to swim away from the island because there was no one to shoot back at the killer.

Preliminary reports suggest that the single police officer on duty, Trond Berntsen, was among the first to be killed. He did not carry a weapon. In Norway, very few police officers carry sidearms in their day-to-day duties. By law, police officers must have specific authorization from their chain of command to gain access to a sidearm, and such requests are rare in a country with such a low violent crime rate. It is also uncommon, for example, for high-ranking Norwegian officials to have a security detail.[9]

To be fair, even in the United States, it is also rare to assign armed security details to youth gatherings at schools, summer camps, and youth rallies, and it is especially rare in remote rural areas. Over the past two decades, however, U.S. schools and summer camps have developed security programs to mitigate active shooter and terrorist threats. The Columbine attacks, for example, forced many school districts to develop protocols for locking doors, installing security cameras and mass-notification systems, and implementing strict visitor controls, bully-prevention programs, and active shooter response drills.[10] From a security perspective, today's schools are different from those before Columbine. The American Camp Association provides similar recommendations to the more than 8,000 summer camps across the United States. Although most camps do not employ armed security, many have close relationships with local law enforcement to include, at a minimum, drive-by patrols at regular intervals (with weapons).[11] Still, our vulnerabilities are not that different from Norway's, and we should not expect that the lone police officer on duty would have survived Breivik's surprise assault, even if he had his own personal arsenal.

Was the Norwegian Police Response Too Slow?

In the United States, we expect armed police responses to active shooters to be swift and decisive. Police response times in most major cities in the United States, from the "911" call to police-on-scene, vary between 6 and 11 minutes.[12] On our military bases, we expect the response time to be better based on the smaller amount of populated real estate to protect. The time from the Fort Hood shooting 911 call to police-on-scene, for example, was only 2 minutes and 40 seconds.[13]

Local police from the nearest mainland town of Honefoss received the first report of the shooting at Utoya Island at 1727.[14] As can be expected when multiple, near-simultaneous terrorist attacks occur (e.g., 9/11;

Mumbai, India, in 2008), emergency operators in Norway were in a state of incredulity over the notion that there could be another attack just 2 hours after the explosion in Oslo.[15] This response may have led to a period of inaction and confusion as phone lines were tied up.[16] The police eventually arrived at the pier across the water from Utoya about 25 minutes later, a significant length of time partly due to needing to travel approximately 14 miles on rural country roads to get there.

As for Oslo's special antiterrorism "Delta" unit, it was 28 miles from Oslo. The Delta unit determined that it was faster to travel by car than to get on the unit's helicopter, which was located 35 miles south of Oslo in the opposite direction of Utoya.[17] The unit arrived approximately 42 minutes after the first emergency call, without any known delays. If one considers, for example, the Los Angeles Police Department SWAT response time in the famous 1997 North Hollywood shootout—a little more than 20 minutes from notification to on-scene—the Norwegian Delta unit's response time seems adequate, given the long distance traveled.[18]

Meanwhile, the police officers abandoned efforts to use a defunct police boat at the pier and commandeered two slower civilian recreational vessels. By the time they obtained the civilian vessels, the Delta unit had arrived, and all were on their way to the island. The shooter surrendered to police approximately 18 minutes later.[19] The fact that he surrendered to police is not common: According to a New York City Police Department study, only 14 percent of active shooter incidents end without the application of force.[20]

As a result of this attack, some critics have suggested that Norway should beef up its airborne antiterrorism response capability. Others have expressed concerns about how long it took forces to get there and how long local police waited for the Delta unit. To be sure, if police had arrived at the island just 10 minutes earlier, they could have prevented the shooting of approximately 20 people, based on Breivik's assault tempo. Nevertheless, as the on-scene commander commented, "I don't think we had any chance to be there faster than we made it."[21] This statement appears to be honest, given the distance, the difficult terrain (water travel), and the typical time lag involved in notifying and preparing forces.

FATAL TIME LAG. Distance and difficult terrain prevented a timely response by law enforcement to the simultaneous attacks.

Same Old Strategic Lessons

If there are no real tactical lessons to be learned from this incident, what about the strategic lessons? Even these are lacking. First, it goes without saying that not all terrorist attacks are perpetrated by Muslims. We all know that indigenous nationalist and antigovernment extremists (left and right wing) are also part of the American threat landscape. Some pundits have suggested that Breivik represented a new Christian extremism, but a careful read of his manifesto suggests that his underlying rationale for terror is based on a hatred of multiculturalism in general and of Muslim immigration in particular. Again, this points to a political rather than an extremist-religious goal. As is often the case in so-called religious violence, religious scripture is abused and warped to the extent that the religion itself becomes a victim.

The bottom line is that lone terrorists are hard to detect. We are all well aware of this fact. You cannot infiltrate their organization because they do not have one. They are not likely to turn themselves in. They do not use cell phones to discuss attack plans because they do not discuss their plans with anyone.

Second, we learned that one man can pull off a mini-Mumbai-style attack with varied tactics and weapons in multiple locations. Is this really a surprise? The only new development is that we will be using the term "Norway-style attack" the next time a lone-wolf terrorist strikes using multiple tactics.[22]

The final strategic lesson is the fact that more people died from firearms than by explosives, and this seems to reflect a larger trend in terrorism. In Mumbai, for example, 10 gunman killed more than 160 people in the 26 November 2008 attack.[23] Did we really think that terrorists would use only bombs after the Oklahoma City bombing or just planes after 9/11?

The bottom line is that lone terrorists are hard to detect. We are all well aware of this fact. You cannot infiltrate their organization because they do not have one. They are not likely to turn themselves in. They do not use cell phones to discuss attack plans because they do not discuss their plans with anyone.[24] Even if a lone-wolf terrorist were to express extreme political views online, it may not raise any concerns—indeed, the web is saturated with people who express nonsense.

Still, no matter how daunting the challenge, intelligence and law enforcement officers need to become experts on differentiating real threats from run-of-the-mill "nut jobs," especially when monitoring Internet activity. Breivik spent a decade expressing his views in blogs and chat rooms and cultivating a like-minded network on the Internet. He even spent 200 days on the Google search engine researching ways to make a bomb.[25] Are men like this truly undetectable? Not likely.

---

1 Marmur, Dow. "Marmur: A Mute Tragedy Without Lessons." *Toronto Star,* 21 August 2011. Available at http://www.thestar.com/opinion/editorialopinion/article/1042438--marmur-a-mute-tragedy-without-lessons

2 U.S. Army. "Antiterrorism: Suspicious Activity Reporting." Available at http://www.25idl.army.mil/Anti%20Terrorism%20Month/FY%2011/AT%20Awareness%20for%20Civilians/Info_paper_Suspicious_Activity_Reporting.pdf

3 Stewart, Scott. "Tactical Intelligence. Oslo, Norway: Lessons Learned from a Successful 'Lone-Wolf' Attack." PoliceOne.com, 1 August 2011. Available at http://www.policeone.com/terrorism/articles/4146174-Oslo-Norway-Lessons-learned-from-a-successful-lone-wolf-attack/

4 Mann, Camille. "Norway Suspect Anders Behring Breivik Released Manifesto, 'A European Declaration of Independence.'" CBS News, 25 July 2011. Available at http://www.cbsnews.com/8301-504083_162-20082953-504083.html

5 Associated Press. "Abdulmutallab Shocks Family, Friends." CBS News, 29 December 2009. Available at http://www.cbsnews.com/stories/2009/12/28/world/main6029782.shtml

6 Preel, Marc. "Norway Gunman Not Crazy Enough To Stay Out of Jail—Experts." *Agence France-Presse*, 1 August 2011. Available at http://newsinfo.inquirer.net/34365/norway-gunman-not-crazy-enough-to-stay-out-of-jail%E2%80%94experts

7 McMillin, Eric F. "An Out-of-the-Box Proposal: Countering Active Shooter Attacks on DOD Installations." *The Guardian Antiterrorism Journal*, Spring 2011.

8 New York City Police Department, Counterterrorism Bureau. "Active Shooter: Recommendations and Analysis for Risk Mitigation." Available at http://www.nypdshield.org/public/SiteFiles/documents/ActiveShooter.pdf

9 Schwirtz, Michael. "Unsettling Wariness in Norway, Where Police Are Rarely Armed." *New York Times*, 25 July 2011. Available at http://www.nytimes.com/2011/07/26/world/europe/26police.html

10 Toppo, Greg, & Marilyn Elias. "Lessons from Columbine: More Security, Outreach in Schools." *USA Today*, 13 April 2009. Available at http://www.usatoday.com/news/education/2009-04-13-columbine-lessons_N.htm

11 American Camp Association. Available at www.acacamps.org

12 "Police Response to 911s Slowing." *Washington Times*, 10 May 2004. Available at http://www.washingtontimes.com/news/2004/may/10/20040510-122711-8996r/; "Response Times—City to City." *American Police Beat*. Available at http://www.apbweb.com/featured-articles/1188-response-times-city-to-city.html

13 U.S. Department of Defense. *Protecting the Force: Lessons from Fort Hood*. Report of the DOD independent review. January 2010.

14 Reuters. "Oslo Terror Attacks: Leaky Police Boat Slowed Access To Utoya Island." Huffington Post, 24 July 2011. Available at http://www.huffingtonpost.com/2011/07/24/oslo-terror-attacks-leaky-police-boat_n_907986.html

15 Agence France-Presse. "Norway Announces Probe into Police Response." *The StarPhoenix*, 28 July 2011. Available at http://www.thestarphoenix.com/news/Norway+announces+probe+into+police+response/5170858/story.html#ixzz1Tt3CLyIU

16 "Norway Police Face Questions over Attacks Response." CNN, 28 July 2011. Available at http://articles.cnn.com/2011-07-28/world/norway.attacks.response_1_police-boat-elite-police-unit-elite-officers?_s=PM:WORLD

17 Reuters, supra 14.

18 History Channel. "1997 North Hollywood Shootout." Documentary. Available at Youtube.com.

19 Reuters, supra 14.

20 New York City Police Department, supra 8.

21 CNN, supra 16.

22 The term "Norway-Style Attack" is already being used by some news outlets. See "Feds Warn of 'Norway-style' Attack." CNN, 17 August 2011. Available at http://situationroom.blogs.cnn.com/2011/08/17/feds-warn-of-norway-style-attack/

23 Fishman, Brian. "Norway Attack Teaches Lessons on Terrorism." CNN, 22 July 2011. Available at http://articles.cnn.com/2011-07-22/opinion/fishman.norway_1_terrorist-attack-norway-terrorists-use-bombs?_s=PM:OPINION

24 For information on "lone terrorists," see *Joint Pub 3-07.2, Antiterrorism*.

25 Moses, Asher. "Could Google Have Caught the Norway Killer?" *Newcastle (Australia) Herald*, 28 July 2011. Available at http://www.theherald.com.au/news/national/national/general/could-google-have-caught-the-norway-killer/2241268.aspx

>WHAT IS GEOTAGGING?

U.S. Navy photo by Mass Communication Specialist 3rd Class Kristopher Regan/Released

Recommendations from Joint Staff Integrated Vulnerability Assessment (JSIVA) Teams

Article reprinted courtesy of *USAG Vicenza Antiterrorism Newsletter*, 31 July 2011

Tactics, techniques, and procedures compiled by the JSIVA can be applied at most DOD installations.

A new function of many portable computing devices such as smart phones, digital cameras, and even some portable game systems is the ability to track the user's location to near-GPS precision. While these location service features can be fun and useful, they also present a risk.

Many devices imbed location data into photos by default. Known as geotagging, the data becomes part of the image file and goes wherever the image goes. By uploading or sending such images through the Internet, the user may inadvertently provide an adversary with critical information.

Consider:

- Public sharing sites such as Flickr® and Google™ Maps can make a user's information openly available online. Adversaries can search for photos tagged in specific locations and use this information to research the users who uploaded the photos.
- Even users who make their profiles private could compromise their security if the privacy controls are not set properly. The hosting service itself could sell or lose your data as well.

- Pictures taken at sensitive locations can lead adversaries directly to supply depots, command centers, or to our troops. Pictures taken from home, which are often found in the same user's profile, can also paint a target on friends and family.
- If one user has many photos available or a group of related users (several individuals in the same military unit, for example) make their photos available, an adversary may be able to use the photographs' imbedded location data to determine behavior patterns for such individuals or groups.

What to Do:

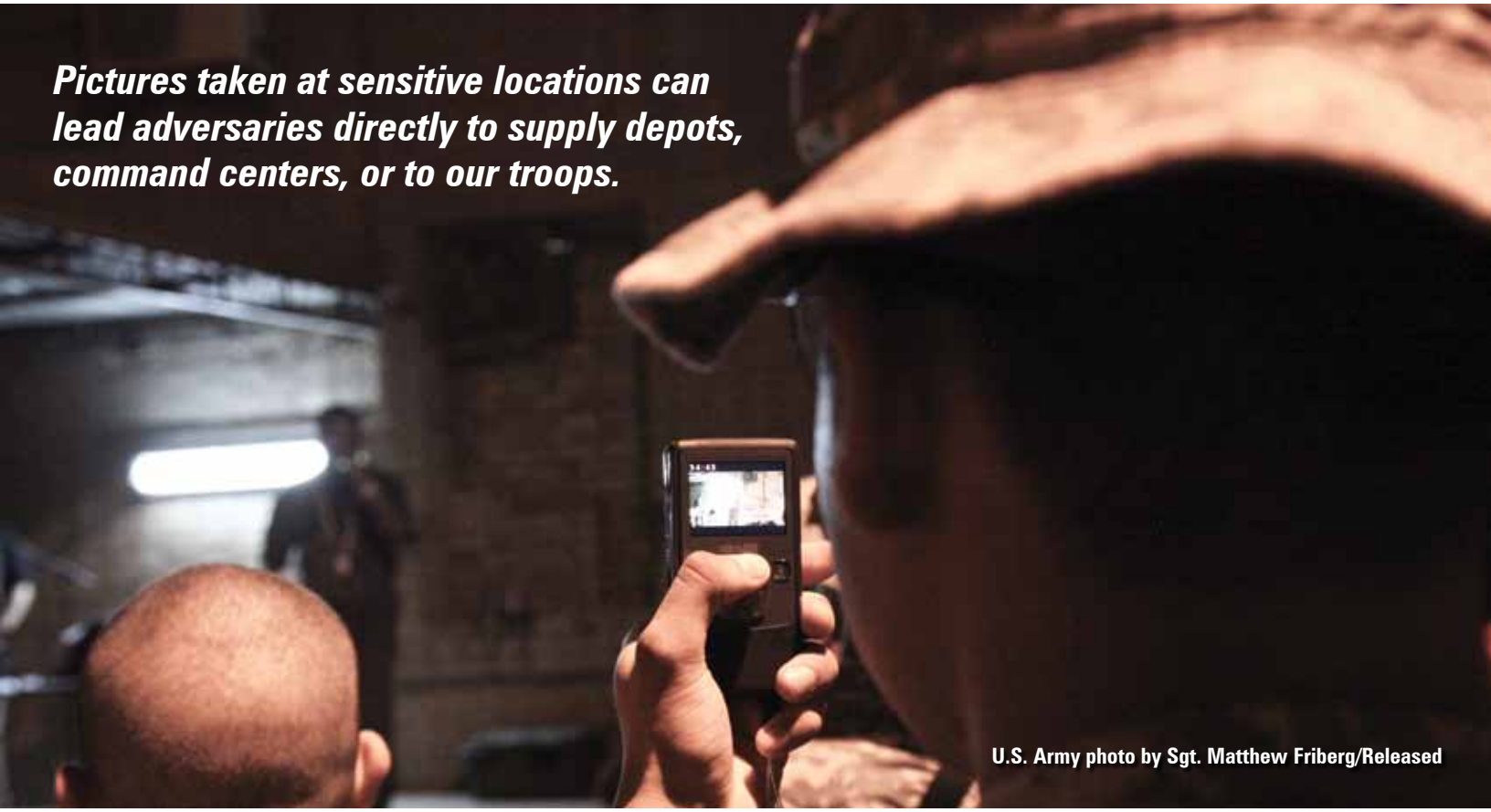
Be Aware. Knowing these risks, think twice before taking and sending photos. You can test a device's geotagging capability by taking a photo and checking its properties in Windows® Vista or higher. Some photo editors and several custom applications allow the user to view and manipulate location data as well.

Evaluate the Need. Ask yourself whether you have a specific point or purpose to tagging photos. If you do not, it is much simpler to disable the feature than to try remove the location data later. If you are unsure of how to disable the feature, search for the model of your phone with keywords "disable" and/or "geotag."

IT POLICY. A U.S. Marine assigned to Marine Corps Recruiting Command holds a government-issued smart phone in Quantico, Va. According to a policy change, recruiters and officer selection officers may now use smart phones to photograph applicants and forward the photographs to approved e-mail addresses. (U.S. Marine Corps photo by Lance Cpl. David Flynn/ Released)

Bottom Line:

Even if photos only appear online briefly, they can enable the adversary to capture vital information and record exact grid coordinates. Consider disabling the feature and avoiding the risk entirely.



U.S. Army photo by Sgt. Matthew Friberg/Released

TERROR TRENDS

U.S. Marine Corps photo by Lance Cpl. Carlos Sanchez/RELEASED

Key facts and statistics about terrorist activity over the past 40 years

The following is the Executive Summary from a paper written by David B. Muhlhausen, Ph.D., and Jena Baker McNeill, "Terror Trends: 40 Years' Data on International and Domestic Terrorism," Heritage Foundation, 20 May 2011. Available at http://report.heritage.org/sr0093

In an ever-changing threat environment, the sources, targets, and effectiveness of terrorist attacks are fluid and dynamic factors.

Between 1969 and 2009, there were 38,345 terrorist incidents around the world. Of these attacks, 7.8 percent (2,981) were directed against the United States, while 92.2 percent (35,364) were directed at other nations:

- Nearly 5,600 people lost their lives and more than 16,300 people suffered injuries due to international terrorism directed at the United States;
- While terrorist attacks against the United States tend to be slightly deadlier (2.01 fatalities per incident) than attacks against other nations (1.74 fatalities per incident), this is primarily due to the large number of deaths resulting from the 9/11 attacks;
- Terrorism directed at the United States accounts for only 7.8 percent of all terrorism worldwide, but almost 43 percent of all attacks against military institutions are leveled against U.S. institutions; and
- 28.4 percent and 24.2 percent of all worldwide terrorist attacks against diplomatic offices and businesses, respectively, are aimed at U.S. institutions.

Between 2001 and 2009:

- There were 91 homegrown terrorist attacks against the United States, while there were 380 international terrorist attacks against the United States;
- The two most prevalent U.S. targets of international terrorism were businesses (26.6 percent) and diplomatic offices (16.6 percent)

- The two most prevalent U.S. targets of domestic terrorism were businesses (42.9 percent) and private citizens and property (24.2 percent); and

- The preferred method of attack against the United States for international terrorists was bombings (68.3 percent), while the preferred method for domestic terrorists was arson (46.2 percent).

Additional Terrorism Statistics

The following statistics are summarized from a study done at the National Consortium for the Study of Terrorism and Response to Terrorism, University of Maryland, 6 September 2011. Available at http://www.start.umd.edu/start/announcements/announcement.asp?id=253

- More people died in the 9/11 attacks than in all other U.S. terrorist attacks from 1970 to 2010.

- The 9/11 attacks involved the first terrorist hijackings in the United States since 1984. There has not been a successful terrorist hijacking in the United States since 9/11.

- Prior to 9/11, al-Qaeda launched only three other successful terrorist attacks globally: the U.S. embassies in Kenya and Tanzania in 1998, and the USS COLE in Yemen's Port of Aden in 2000.

- Since 9/11, groups allied with al Qaeda are responsible for over 12,000 deaths worldwide. In total, more than 65,000 people have perished in terrorist attacks since 2001, with an average of 7,258 deaths per year.

- From 1991 to 2000, the United States was subject to an average of 41.3 terrorist attacks per year. After 2001, the average number of attacks against the United States decreased to 16 per year from 2002-2010.

- From 2003 to 2007, there were no fatalities from terrorist activity in the United States.

Strategic Event Assessment

By CDR Christopher F. Hill

EVENT: Terrorist Body Packing

This summer, the U.S. Government issued a warning that terrorists may be considering surgically implanting explosives into humans in response to increased aviation security measures.[1] Notably, the original chairs of the National Commission on Terrorist Attacks, former Gov. Thomas H. Kean (R-NJ) and former Rep. Lee H. Hamilton (D-IN), also assessed that the current U.S. airport screening system "still falls short in significant ways." They noted that the new body scanners with advanced imaging technology that were deployed following Umar Farouk Abdulmutallab's so-called Christmas Day 2009 underwear-bomb attack "are not effective at detecting explosives hidden within the body."[2] The Government Accountability Office has supported this assertion.[3]

STRATEGIC SIGNIFICANCE:

The idea of using the body to courier explosives is not new, but according to U.S. security officials who spoke to media outlets this summer, there is "fresh interest" in using these tactics.[4] Body packing has its genesis in international drug smuggling, where "mules" ingest carefully packaged drugs and later excrete the packages or insert the packages in other bodily orifices. The first known example occurred in 1973 when a man traveling from Lebanon to Canada checked himself into the hospital after the hashish-filled condom he swallowed lodged itself in his intestines and nearly killed him.[5]

The use of surgical implantation for hiding drugs or explosives appears to be a more recent phenomenon. Some security experts claim that female suicide bombers recruited by al Qaeda have had explosives inserted in their breasts with the same techniques used for breast enhancement surgery.[6] The Drug Enforcement Agency has also reported examples in which puppies were surgically "impregnated" with heroin packets.[7] Possible indicators of either surgically implanted or ingested contraband include a distended stomach or other unusual bulging accompanied by visible discomfort during pat-downs.[8]

Compared with ingestion, surgical implantation has tactical drawbacks. There are only a few places to hide bulky explosives under the skin, not to mention the detonators. Furthermore, the surgery would require some recovery time before getting on the plane, and the probability of complications due to infection are high.[9] Still, terrorists consider it a viable tactic.

Every AT officer knows that our enemies never cease to find new tactics, be they airplane bombs, shoe bombs, underwear bombs, bombs in printer cartridges, or bombs in soda cans. The next logical step for terrorists is to eat the bomb or to pack it under the skin—this is predictable based on drug-smuggling lessons learned. What will they think of next? Our job is to determine that.

---

1 Associated Press. "US Warns Airlines: Terrorist Interested in Surgically Implanting Bombs in Humans for Attacks." *Washington Post,* 6 July 2011.

2 Bennett, Brian. "Post-9/11 Assessment Sees Major Security Gaps." *Los Angeles Times*, 20 August 2011. Available at http://articles.latimes.com/2011/aug/30/nation/la-na-911-report-card-20110831

3 "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11." Government Accountability Office Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, 7 September 2011.

4 Associated Press, supra 1.

5 Deitel, Mervyn. "Intestinal Obstruction by an Unusual Foreign Body." *CMA Journal*, 4 August 1973.

6 "Terrorists Could Use Explosives in Breast Implants to Crash Planes, Experts Warn." Fox News, 24 March 2010. Available at http://www.foxnews.com/world/2010/03/24/terrorists-use-explosives-breast-implants-crash-planes-experts-warn/#ixzz1XCc5Y99f

7 "Heroin Packets Surgically Implanted In Puppies." Orlando (FL) News, 1 February 2006. Available at http://www.clickorlando.com/news/6666966/detail.html

8 Associated Press, supra 1.

9 Ibid.

By CDR Christopher F. Hill

EVENT: Terrorist Use of Symbolic Dates

"As of February 2010, al Qaeda was contemplating large attacks in the homeland on symbolic dates and specifically identified U.S. Independence Day as a key date."

—Department of Homeland Security Bulletin, June 2011[1]

STRATEGIC SIGNIFICANCE:

Symbolic dates play a small but significant role in the terrorist attack planning calculus. AT officers need to keep an eye on vulnerable dates because deliberate attack timing could demonstrate a terrorist's ability to strike any target at any time with impunity. A strike on a symbolic date would create additional media buzz, calling to mind previous events that occurred on that date.

When determining a vulnerable date, the difference between coincidence and calculated intent is challenging. The 11 March 2004 Madrid bombing, for example, occurred exactly 911 days after 9/11; however, most experts agree that the date was chosen not because of any numerological significance with 9/11 but because it would influence Spanish elections a few days later—and it did.

The date of 19 April has become symbolic for antigovernment extremists in the United States. According to his taped confession, Timothy McVeigh chose the 19 April 1995 attack date in Oklahoma City for two symbolic reasons: It was the 2-year anniversary of the siege in Waco, Texas, and the 220th anniversary of the beginning of the American Revolution.[1]

In another twist, one of the Columbine High School attackers allegedly wanted to conduct his attack on 19 April 1999 in honor of McVeigh's Oklahoma City bombing but delayed for 1 day due to an ammunition shortage.[2] From a neo-Nazi perspective, 20 April is an important date because it is Adolph Hitler's birthday. On 20 April 2011, a bomb similar to those used in the Columbine attack was discovered in a mall just 1 mile from Columbine High School.[3]

American national holidays and religious celebrations are magnets for increased FP—bin Laden's documents indicate that 4 July was a key date[4]—but with only 365 days in a year, attack-date coincidences are inevitable. The so-called underwear bomber, Umar Farouk Abdulmutallab, chose to strike on Christmas over the skies of Detroit not because Christmas was symbolic or because Detroit was his intended target but because that particular flight was the cheapest one he could afford.

Despite the low probability of increased terrorist attacks on most symbolic dates, enough evidence of terrorist intent recommends increased vigilance, at a minimum, on certain days. To be sure, the best attack will always be the unexpected one that creates yet another symbolic date.

---

1 "15 Years Later, Hear McVeigh's Confession." MSNBC. Available at http://www.msnbc.msn.com/id/36633900/ns/msnbc_tv-documentaries/t/years-later-hear-mcveighs-confession/

2 Burke, Jeffrey. "Columbine Myths Shattered in Vivid Book; Media, Cops Blundered." Bloomberg, 7 April 2009. Available at http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aix.zkBRIh2M

3 Coffman, Keith. "Suspect Arrested in Columbine-Area Bombing Attempt." Reuters, 26 April 2011. Available at http://www.reuters.com/article/2011/04/26/us-security-colorado-idUSTRE73P4R220110426

4 Esposito, Richard, Pierre Thomas, & Jason Ryan. "FBI and DHS Urge Vigilance on July 4." ABC News, 27 June 2011. Available at http://abcnews.go.com/Blotter/fbi-dhs-urge-vigilance-july/story?id=13944689

5 Caulfield, Philip. "Christmas 2009 'Underwear Bomber' Targeted Detroit Because It Was the Cheapest Flight: Report." *New York Daily News,* 24 March 2011. Available at http://articles.nydailynews.com/2011-03-24/news/29358640_1_umar-farouk-abdulmutallab-underwear-bomber-al-quso

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.