The Source for Antiterrorism Information

SUMMER 2011 | Volume 13 | Issue 2

THE GUARDIAN
ANTITERRORISM JOURNAL

A Joint Staff, Deputy Directorate for Antiterrorism/Homeland Defense,
Antiterrorism/Force Protection Division Publication
The Pentagon, Room MB917 | Washington, DC 20318

Historical Antiterrorism Quotes

April 2011

"The terrorist threat facing our country has evolved significantly over the past ten years, and in today's environment—more than ever—we know that the best strategy is one that counts on the American people as a key partner in securing our country."

—Homeland Security Secretary Janet Napolitano, 20 April 2011, in a speech about the Department of Homeland Security's new threat alert system.

2000

"It is the same unbelief [of Allah] that drove Sadat, Hosni Mubarak, Gadhafi, Hafez Assad, Saleh, Fahed—Allah's curse be upon the non-believing leaders—and all the apostate Arab rulers to torture, kill, imprison, and torment Moslems."

—"The Al Qaeda Manual," discovered by police in Manchester, England, in 2000 (http://www.justice.gov/ag/manualpart1_1.pdf), offers a prescient warning regarding several Arab leaders who are now removed from power or under pressure to step down.

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.

The Guardian is not a doctrinal product and is not intended to serve as a program guide for the conduct of operations and training. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Joint Staff, DOD, or any other agency of the Federal Government. Information within is not necessarily approved tactics, techniques, and procedures. Local reproduction of our newsletter is authorized and encouraged.

The Guardian Antiterrorism Journal Summer 2011 | Vol 13, Issue 2

Guardian readers,

We entered this tenth year since 9/11 with a brilliant strike against the heart of al Qaeda, Osama bin Laden. This strike added a new dynamic to DOD force protection efforts, resulting in heightened security and awareness around the globe.

By no means, however, is the long-term fight over. Al Qaeda remains strong in places like Yemen, northern Africa, and Pakistan, while al Qaeda affiliates and sympathizers continue to assemble close to home. Indeed, much evidence shows that more Americans have been participating in terrorist activities at home and abroad, oftentimes assuming leadership roles..

As we all know, it is never enough simply to remain aware of this ever-evolving threat. As leaders, we need to provide specific guidance to our Service men and women, to periodically review our policies and tactics, and to constantly test our day-to-day security efforts. This work should include everything from improved surveillance detection on the streets to how we microblog on social media websites: This is what we mean by "increased vigilance."

This issue of *The Guardian Antiterrorism Journal* discusses several ways in which we can address this ever-evolving threat:

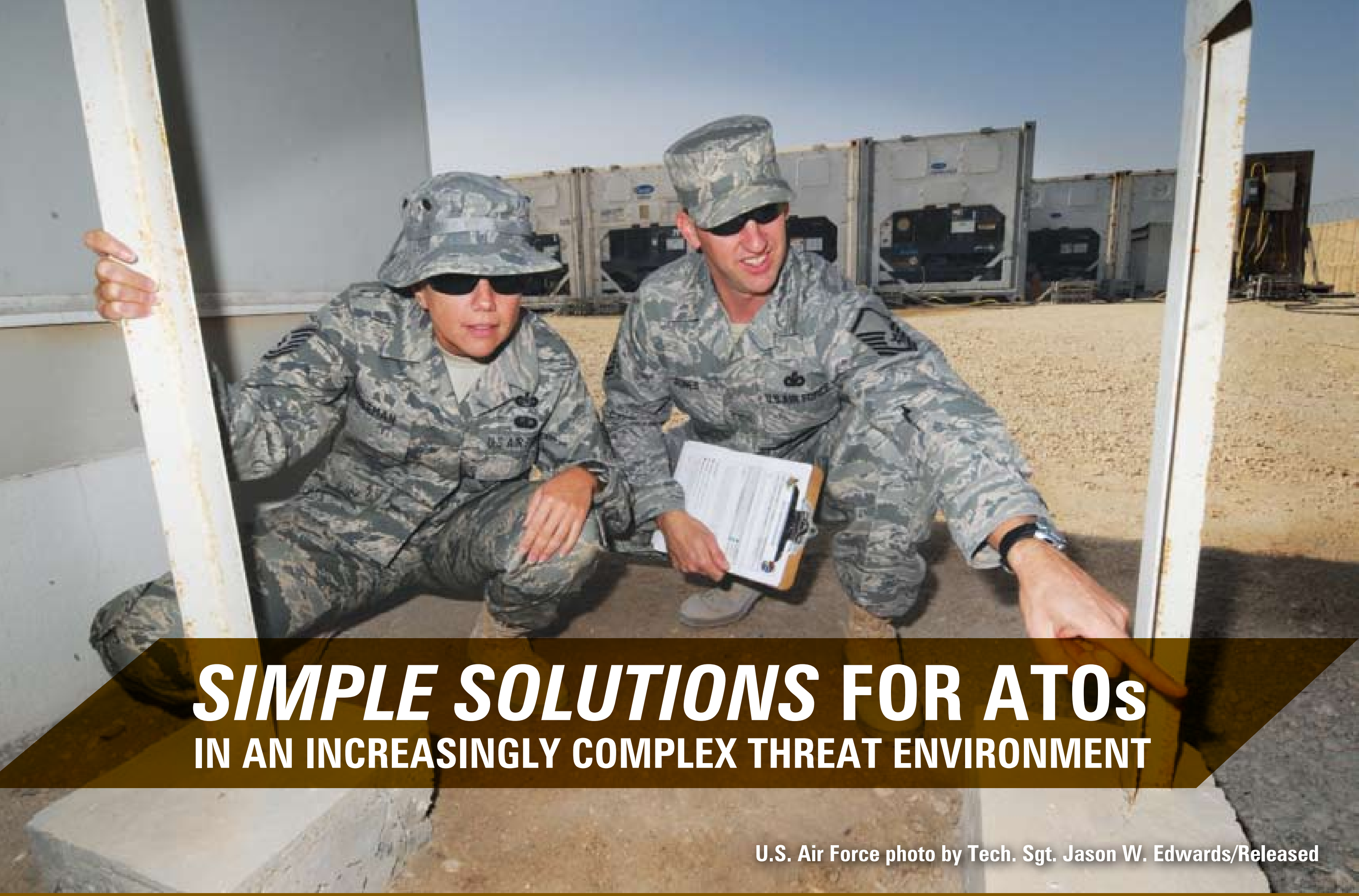
- In **Simple Solutions for ATOs in an Increasingly Complex Threat Environment,** the author, a Naval Criminal Investigative Service agent, offers a number of tips for Antiterrorism Officers (ATOs), including ways to adapt to a variety of new threats.
- In **TSA's Highway Antiterrorism Program Helps Foil Hijacking and Bomb Plots,** the Transportation Security Administration discusses how its "First Observer" highway security program can be incorporated by the DOD to increase security at little cost.
- **Target Type and Mumbai Model Variants** makes the argument that Mumbai-style attacks are possible against hard targets as long as the terrorists adapt their tactics, and the author demonstrates how this happened in Pakistan.
- "**Teach Them Properly"** advocates realistic decisionmaking training for sentries and commanders in use-of-force concepts.
- **Best Practices for the AT Community** describes exactly that: Joint Staff Integrated Vulnerability Assessment teams often discover best practices during their assessments that can be used to benefit the whole DOD AT Community.
- In **The Pros and Cons of Social Media: An Antiterrorism Perspective,** the author recommends that commanders and ATOs become familiar with the benefits and risks associated with social media.
- The article **DHS's National Terrorism Advisory System** introduces the new NTAS Alerts.
- Finally, **Understanding the Threat** describes how the terrorist threat is continually evolving and adapting.

One thing that the ongoing "Arab Spring" has taught us—as autocratic regimes across the Middle East and North Africa are threatened and toppled—is that the future remains dangerously uncertain. Increased vigilance has become our new normal. This explains why, for example, the Department of Homeland Security has introduced the new National Terrorism Advisory System, which will improve how the public is alerted while increasing vigilance on a national scale.

Part of how the DOD increases its vigilance is by sharing and communicating new ideas. There is much to learn, for example, from the nuclear crisis in Japan because the consequence management response resulting from a terrorist chemical, biological, radiological, or nuclear attack would be similar to the one implemented in Japan. I ask you to continue providing your feedback, ideas, and articles to the Joint Staff so that we can collectively adapt to this changing threat landscape.

Jeff W. Mathis III

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



SIMPLE SOLUTIONS FOR ATOs
IN AN INCREASINGLY COMPLEX THREAT ENVIRONMENT

U.S. Air Force photo by Tech. Sgt. Jason W. Edwards/Released

21st century threat environment presents new challenges

By Special Agent David Salazar, Naval Criminal Investigative Service

ATOs need to proactively lead their teams in creating a sense of teamwork among uniformed Service members, civilian organizations, and host-nation partners.

Since December 2010, multiple incidents, both man-made and natural, have occurred in rapid succession: massive antigovernment protests roiling the Middle East and North Africa, with refugees fleeing the resulting violence and unrest; a tragic three-part earthquake, tsunami, and nuclear accident in Japan; a lone-wolf attack against US Air Force personnel in Germany; and, finally, the increased threat resulting from the successful strike against Osama bin Laden. These events serve as vivid reminders that Antiterrorism Officers (ATOs) need to be prepared to mitigate and adapt preexisting plans and procedures against a variety of threats that can morph quickly and often.

ATOs and their networks of military and civilian partners have to maintain nimble and resilient AT programs that are able to handle increasingly complicated incidents and threats. The Naval Criminal Investigative Service's (NCIS) Europe and Africa Field Office (EUFO), located in Naples, Italy, provides this type of support to Department of the Navy (DON) and DOD ATOs working on the two continents. Based on recent experiences, this article provides some basic suggestions about how ATOs can help their own programs work more effectively in this threat environment. It is intended for use by those in the field—that is, the men and women who patrol our fence lines, airfields, and piers—to ensure security for DOD installations worldwide.

Social Networks and Antiterrorism

The meteoric rise of Internet-based social networks has had a profound impact on the way people everywhere communicate. It is now common for individuals, commands, and many government agencies to maintain websites and other popular social media applications, such as Facebook or Twitter. Although these tools are useful for disseminating information or staying in touch with friends, they continue to represent a potential weak link through which unknown actors can perform preoperational surveillance and planning. Reports covering the antigovernment protests in Egypt earlier this year indicated that "Facebook and Twitter were used by protestors not just to communicate with one another, but as a platform to show the demonstrations in real-time."[1] Although the protests were not specifically aimed at DOD installations or personnel, this real-time posting capability, paired with the popularity of social networks, raises a potential concern for ATOs. Those who plan attacks against DOD installations do not live in a vacuum; they have access to the same web-based media and technology as the regular civilian population.

Hypothetically, a person tasked with gaining information for a future attack on a US base or ship in a foreign port could accomplish a great deal of surveillance simply by visiting a command's Facebook page or other website. His job will be made that much easier if the command is not vigilant in ensuring the content of its page does not contain sensitive information. The term "sensitive" is used in this article to describe information that may not be classified but still should not be made available publicly. Even seemingly innocuous open-forum messages, which are popular on applications like Facebook, should be carefully edited by the individual author. Publishing photos and providing ongoing commentary about the latest on-base events can encourage a sense of community, but it can also provide unintended insight into what is occurring within a base community. This ongoing commentary combined with other open-source media reports could provide far too much information to our hypothetical terrorist. With today's easy-to-use online publishing applications, which combine text, still photos, video, and live-chat features, surveillance data that may have taken a long time to package can now be provided to autonomous users worldwide and in real time. Meanwhile, this hypothetical terrorist has risked less time in the vicinity of the target.

Publishing photos and providing ongoing commentary about the latest on-base events can encourage a sense of community, but it can also provide unintended insight into what is occurring within a base community. This ongoing commentary combined with other open-source media reports could provide far too much information to our hypothetical terrorist.

ATOs must work to prevent online surveillance from occurring to the greatest extent possible. In a recent paper, "Cyber Jihad and Web 2.0," authors Dondi West and Christina Latham noted that "the question is not whether extremists will adopt social networking technologies. The question is how so."[2] The question for the installation ATO is how to maintain good situational awareness with regard to the realities of the Web 2.0 environment.

RELIEF EFFORT. The mass exodus of refugees fleeing the political unrest in North Africa have demanded the precise execution of both AT and emergency management disciplines. (US Marine Corps photo by Lance Cpl. Tammy Hineline/Released)

One solution used by NCIS EUFO has been to encourage collaboration among tenant commands' information assurance (IA) representatives. By raising awareness of the risks of placing too much information about one's command or installation online, along with how easily extremists could use that information, we have been able to initiate an all-hands evolution. Reaching out to tenant command IA representatives, we have provided focused threat briefings, responded to suspicious online activity, and helped evaluate online content as a result of increased threat conditions affecting the region. Through these efforts we are able to provide greater Internet situational awareness for naval leaders in Europe and Africa.

The bottom line for ATOs regarding IA is this: Stay current on your installation's web profile, establish first-name relationships with your installation/command's public affairs officers, and know your IA points of contact and counterintelligence team members. Social networks and technology have closely connected everyone more than ever before, but security does not have to be sacrificed needlessly.

Working Locally While Planning Regionally

Recent man-made and natural incidents have required the rapid response of DOD personnel and material. Two

SECURITY BREACH. DOD personnel posting information on social media sites can unwittingly provide surveillance data to terrorists. (US Marine Corps photo by Chief Warrant Officer 2 Clinton W. Runyon/Released)

examples include the mass exodus of refugees fleeing the political unrest in North Africa for southern Europe and the tragic threefold disaster of the Japanese earthquake-tsunami-nuclear material release. These responses have demanded the precise execution of both AT and emergency management disciplines and demonstrated the increasingly complex nature of incidents in the 21st century. Effective responses to each incident require the sophisticated pairing of sound AT practices with those of emergency management. It would do little good to deliver much-needed supplies to survivors or refugees if doing so would allow unknown actors to learn our tactics, techniques, and procedures to use against us during a future response. ATOs have to be certain that security is not compromised in the rush to assist.

Although AT and emergency management are distinct and separate programs, they support one another. This resilient partnership is critical in our rapidly changing security environment. At the federal level, the National Response Framework encourages this teamwork and provides best practices "for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters."[3] Due to the unique position DOD occupies domestically and abroad, DOD Instruction 6055.17, Installation Emergency Management (IEM) Program, 19 November 2010, provides needed clarity.[4] This instruction details how the Services and commanders may best achieve the vital partnership between installation AT and emergency management teams. Equally important, it provides flexibility for installation commanders to achieve the best practices of IEM with respect to specific diplomatic agreements between DOD and a host nation. This flexibility is instrumental in enacting the robust use of random AT measures. Examples include ad hoc security checkpoints, use of K-9 assets to sweep areas for explosives, and increased countersurveillance in concert with host-nation counterparts. All of these measures provide critical protection and can increase situational awareness as different threats emerge. Unfortunately, despite best efforts, incidents are bound to occur eventually. That is when the ATO's preincident planning with the installation's emergency management team is needed locally.

A clear understanding of strategic guidance is necessary; however, installation AT and emergency management team members need to understand what resources are available locally. NCIS EUFO has offices throughout Europe and Africa; if a single all-hazard plan were developed for all of the offices, the result would be an entire bookshelf filled with phonebook-sized binders, most likely sitting unused, dull to read, and not very helpful in a crisis. Instead, EUFO developed a regional Crisis Action Plan, providing key information for supported DOD personnel.[5] Localized procedures and capabilities developed by satellite offices and their installation partners were included as appendices to the plan. The result is an easy-to-read, short document that tells senior- and local-level leaders what they need to know, quickly, regarding NCIS EUFO support of AT and emergency management activities. This commonsense approach to planning ensures that "everything should be made as simple as possible, but not simpler."[6] Incidents are complicated enough and are not likely to become simpler in the future. Senior and junior personnel involved with AT should continue to critically review their planning documents to not only ensure they are complete, but also that they are accessible to outside readers. It does little good to produce a bookshelf full of plans that go unread.

Everything should be made as simple as possible, but not simpler.
—Albert Einstein

Maintaining Security Outside the Wire After the Raid in Abbottabad, Pakistan

Recently, a US Navy Seabee Battalion stationed in Rota, Spain, held its annual Seabee Ball with a formal dinner, dancing, and ceremonies. The event was held at one of the famous Spanish sherry wine bodegas and was attended by more than 100 personnel. To safely transport everyone, multiple shuttle buses and vans ran back and forth between the event and Naval Station Rota. Working together, Naval Station Rota's ATO, NCIS Rota, and the command were proactive in their security planning to mitigate a possible ad hoc attack against the shuttle vehicles by either a small group or a lone-wolf terrorist. This concern is very real in the aftermath of the strike that killed Osama bin Laden in Abbottabad, Pakistan. CNN reports that a joint US Department of Homeland Security and Federal Bureau of Investigation advisory released 9 May 2011 stated, "Lone offenders who share al Qaeda's ideology are the greatest near-term threat because they are 'unburdened by organizational constraints that can slow operational decisions by established terrorist groups.'"[7] Mitigating this specific threat and others at large public events overseas is one of the toughest challenges ATOs are likely to encounter. It is in this scenario that the successful ATOs stand out. Insisting on a group effort involving the hosting command, the ATO's team, and most importantly, host-nation security services can mitigate this threat to the greatest extent possible. Solid relations with the key Defense Criminal Investigative Organizations, like NCIS, which facilitate host-nation support of these events, are paramount in accomplishing this mitigation. A key component of the NCIS job overseas is to provide ATOs with the appropriate amount of support so they can ensure Service member security during off-base events. Pre-event coordination between commands and ATOs will help ensure that the level of support provided matches the local threat level. In the new threat environment resulting from the strike against Osama bin Laden, appropriate levels of security are something that ATOs need to get right.

Using this team approach with ATOs, NCIS EUFO has been able to provide sophisticated support to various command-sponsored social events and a myriad of other official functions and operations throughout Europe and Africa. This support has been achieved through a three-pronged approach that includes the NCIS Referent Program, NCIS Security Training Assistance and Assessment Teams (STAATs), and strong liaisons with the local security services that support the communities outside of DOD installations overseas. The NCIS Referent Program allows special agents to engage with host-nation law enforcement and security forces to support transiting DON personnel across the globe. By providing situational awareness and security liaisons between host-nation security services and visiting US DOD units, these efforts have proven useful in successfully completing secure visits and operations. STAAT personnel are subject matter experts who provide Integrated Vulnerability Assessments for seaports, airfields, and other expeditionary locations in support of DON missions. Current successes in each effort include—

- Effective force protection support to ship visits in Europe and Africa
- Integrated Vulnerability Assessments in support of a recent European Command planning conference and in preparation for the Africa Command's Exercise AFRICAN LION
- Continued liaisons with host-nation law enforcement to maintain awareness of the large increase of illegal immigration affecting southern Europe. The number of illegal immigrants from North Africa is estimated to be between 20,000 and 25,000 individuals over a period of four months. Although the majority of these individuals may simply be fleeing the unrest in the region, many disenfranchised people may resort to criminal activity if pushed to desperation. These activi-

The successful strike against Osama bin Laden caused much celebration, but also presents the United States with heightened threats from al Qaeda. (US Marine Corps photo by Sgt. Randall Clinton/Released)

ties and possible host-nation responses could certainly alter the threat environment of a community where an overseas military installation is located.

Early and sustained cooperation with host-nation security colleagues has been critical to this success. Matching up security requirements with relevant on-the-ground threat information allowed for common-sense security solutions to be enacted throughout the previous winter and spring. Overall in 2010, NCIS "conducted 1,142 missions providing on-the-ground coverage ... to safeguard in-transit naval units around the globe."[8] The success of these efforts is only possible through ongoing collaboration with ATOs, our defense criminal investigative organization (DCIO) counterparts, and host-nation law enforcement partners.

Conclusion

The emerging threats and incidents of winter and spring 2011 have included man-made and natural disasters that highlight the need for ATOs to remain flexible and vigilant in their efforts. Whether it is a tsunami, an arrival of a boat full of refugees, or a lone-wolf threat against an off-base function, our changing security environment is becoming more complicated and crossing multiple disciplines more often. ATOs need to proactively lead their teams in creating a sense of teamwork among uniformed Service members, civilian organizations, and host-nation partners. This sustained effort is the key to maintaining vigilance and is paramount in dealing with rapidly emerging threats.

Special Agent David Salazar is assigned to the NCIS Resident Agency in Rota, Spain, which is a satellite office under the NCIS European Field Office. He has 10 years of experience working on AT, force protection, and counterintelligence issues and threats.

The opinions and conclusions expressed are those of the author and do not necessarily represent the views of the Naval Criminal Investigative Service or any other government agency.

[1] Hamid, Triska. "New Weapons of Protest: The Call for Change." *Middle East Economic Digest* 55 (2011).

[2] West, Dondi, & Christina Latham. "The Extremist Edition of Social Networking: The Inevitable Marriage of Cyber Jihad and Web 2.0." *Proceedings of the International Conference on Information Warfare and Security* (2010): 523-531.

[3] FEMA National Response Framework. Washington, DC: Federal Emergency Management Agency, 2008. p. 1.

[4] DOD, Office of Under Secretary of Defense for Acquisition, Technology and Logistics. DOD Instruction 6055.17, DOD Installation Emergency Management (IEM) Program. November 2010.

[5] Naval Criminal Investigative Service, 2011, European Field Office Crisis Action Plan (CAP). Naples, Italy: Naval Criminal Investigative Service, 2011.

[6] Chapman, John. *Muddy Boots Leadership: Real Life Stories and Personal Examples of Good, Bad, and Unexpected Results.* Mechanicsburg, PA: Stackpole Books, 2006. p. 57.

[7] "Beware 'lone wolves' in aftermath of bin Laden killing, advisory says." CNN, 10 May 2011. Available at: http://www.cnn.com/2011/US/05/10/bin.laden.attacks/index.html

[8] 2010 Year in Review. Washington, DC: Naval Criminal Investigative Service, 2011. p. 2.

TSA'S HIGHWAY ANTITERRORISM PROGRAM HELPS FOIL HIJACKING AND BOMB PLOTS

DOD photo by Cherie Cullen

TSA's eyes are focused on the road as well as the airports

By Mark Messina, TSA Highway and Motor Carrier Security Specialist

The First Observer program is a low-cost, easy-to-implement force multiplier that has widespread applications for counterterrorism.

Many travelers only see the Transportation Security Administration (TSA) working at airports screening passengers at security checkpoints. However, with more than 200,000 trained First Observers™ —several of whom contributed to the recent foiling of a motor coach hijacking and a Texas bomb plot linked to terrorism—the TSA's eyes are also focused on the road. The First Observer™ program was created by the Highway and Motor Carrier Division (HMC) to train highway professionals to accurately observe, assess, and report terrorist behavior. This AT domain awareness program is one safeguard for protecting critical highway and road infrastructure. TSA believes the First Observer program is a low-cost, easy-to-implement force multiplier that has widespread applications for counterterrorism.

Recent success stories of the First Observer program include the foiled hijacking of a Greyhound motor coach traveling between Arlington, Virginia, and Durham, North Carolina; the disruption of a Texas bomb plot targeting former President George W. Bush; and foiled plots against power plants along the West Coast. All of these successes validate HMC's mission.

In February 2011, a Greyhound motor coach was

leaving Arlington, VA, making its way toward Durham, North Carolina, with 35 passengers onboard when an alleged hijacker, 32–year–old Jose Darwin Flores of Arlington approached the driver with a handgun and took control of the bus. While traveling southbound on Interstate I-85, Flores told the driver to pull over near Exit 223, and there, 33 terrified passengers were allowed to leave the bus. Two passengers remained on the bus: One hid in the back of the motor coach, and the other would not leave the driver alone to face the hijacker. On being released at the exit, passengers contacted the police.

FOILED. Alleged Greyhound bus hijacker Jose Darwin Flores sits behind bars after a TSA First Observer–trained driver used her skills to thwart the crime. (Photo: Warren County Sheriff's Office)

Flores allegedly forced the driver, a veteran motor coach operator from Carey, North Carolina, to continue down the road. The driver followed many of the lessons presented in the TSA/First Observer training she received when she joined the company. She remained calm and convinced Flores that she could not continue if she were not allowed to use a restroom, a tactic used to buy time for authorities to catch up with the bus. Agreeing to her request, Flores allowed the driver to pull over at a local gas station where she and both remaining passengers exited to use the restroom, leaving Flores alone on the bus. Shortly afterward, sheriff deputies stunned Flores after he refused to leave the bus, and he was taken into custody.

HMC is receiving an increased number of intelligence reports suggesting motor coaches and school buses are becoming attractive targets and weapons for terrorists, so heightened awareness is critical for reducing risk.

The Greyhound driver, a mother of three with previous school-bus driving experience, credits her TSA training and her years of experience for her success. She commented: "I tried to keep everything calm and convinced him it would be easier to proceed if we had less passengers and commotion. I explained we had too many babies on board for this to succeed and I could concentrate better if we let passengers off the bus."[1]

Training had been optional for domestic motor coach and over-the-road bus (OTRB) operators, but the 9/11 Commission Act of 2007 requires OTRB operators to provide AT domain awareness training such as First Observer to its frontline employees. TSA is currently preparing a rule requiring training of specific passenger carriers. According to HMC General Manager William "Bill" Arrington—

> The possibility of sharing TSA resources with DOD in an effort to protect our troops as they travel on highways across our nation and throughout the world will result in development of united security teams trained to quickly detect signs of terrorism and report it through chains of command and emergency communications networks. If we report quickly and accurately, we may be able to disrupt the attack process and defeat the attack before it's initiated. By continuing to develop and grow no-cost programs such as First Observer, which are embraced by our stakeholders, we'll not only achieve many of our overarching national security goals but terrorists will quickly realize hundreds of thousands of trained observers are out in the field ready to detect and report their activity.[2]

HMC is receiving an increased number of intelligence reports suggesting motor coaches and school buses are becoming attractive targets and weapons for terrorists, so heightened awareness is critical for reducing risk.

This training can be quite valuable in other venues and used effectively by other professionals. Similar TSA training led to the February 2011 FBI bust of Khalid Ali-M

NEW VULNERABILITIES. The 9/11 Commission Act of 2007 requires OTRB operators to provide AT domain awareness training such as First Observer to its frontline employees.

PRESIDENT TARGETED. The Dallas, Texas, home of President George W. Bush was one of many targets of alleged terrorist Khalid Ali-M Aldawsari, a 20-year-old Saudi student living in Texas. (Photo courtesy of Dallas Morning News, A. H. Belo Corporation)

Aldawsari, a 20-year-old Saudi student studying in Texas. Aldawsari was charged with attempting to bomb nuclear power plants and dams along the West Coast as well as the home of former President George W. Bush. An alert employee of Con-way Inc., an Ann Arbor, Michigan-based transportation and logistics service provider with a hub in Lubbock, Texas, quickly initiated the process of alerting local law enforcement personnel and the FBI to a shipment of phenol, a chemical used in homemade bomb manufacturing.

Following First Observer principles rolled out to Con-way associates under the program's previous "Highway Watch" moniker, the Con-way employee realized something "just didn't look right" when the chemicals passed through the Lubbock hub.[3] Based on the nature of the chemicals shipped and inconsistencies regarding the intended use, provisions in Con-way's incident management program triggered a US Department of Homeland Security / TSA notification plan.

Reacting to reports, the FBI gained entry into Aldawsari's apartment on Valentine's Day and found concentrated sulfuric acid; concentrated nitric acid; lab equipment, including beakers and flasks; wiring; Christmas lights; a hazardous materials (HAZMAT) suit; and clocks.[4] These materials, the government alleges, could be used to make an improvised explosive device. The FBI arrested Aldawsari on 23 February 2011 and charged him with attempted use of a weapon of mass destruction.

"[This] arrest demonstrates the need for and the importance of vigilance and the willingness of private individuals and companies to ask questions and contact the authorities when confronted with suspicious activities," said James T. Jacks, US Attorney for the Northern District of Texas.[5] This same vigilance and notification process is at the heart of the First Observer program.

First Observer motor coach security and cargo modules used by the Greyhound driver and the Con-way logistics associate clearly define processes enabling users to nonconfrontationally and accurately observe, assess, and report terrorist and criminal activity.

Eleven training modules within the First Observer program cover all national highway modes such as infrastructure, trucking, cargo, HAZMAT, school bus, motor coach, parking structures, highway workers, port authority operations, vehicle rental and leasing, and law enforcement industries and organizations. First Observer is not a substitute for current emergency services, as explained by First Observer CEO Charles Hall:

> One thing we'd like to stress is we train users to be vigilant reporters but we're not a substitute for dialing 9-1-1 during an emergency nor are we attempting to replace an organization's emergency communications program. Should anyone observe a terrorist or criminal act, dialing 9-1-1 is the first course of action. … What First Observer works toward is ensuring someone is in a position to identify and positively act on suspicious activity when it occurs. First Observer trains security professionals and sometimes the general public how to detect possible terrorist behavior and report it. It's a security empowerment program.

> It affords a safe opportunity for a trained First Observer to become a trusted agent in our fight against terrorists and criminals.[6]

Following the killing of two US Air Force members at the Frankfurt, Germany, international airport, it became clear that recent training for personnel involved in huge sporting events and large metropolitan areas, such as the Detroit Central Business District (e.g., casinos, colleges, universities, hospitals, entertainment venues, and professional sports), could also serve the DOD to protect Service members and civilian employees associated with troop and materiel logistics.

When a user is trained to observe, assess, and report "red flags" or suspicious situations, the reporting and subsequent follow-up process can often disrupt the sequence or "chain" of events leading to an attack.

In the case of the Frankfurt shootings and similar incidents, it is possible that "red flags" indicating the possibility of an attack may have existed and, if detected by a trained observer, could have prevented the attack or mitigated the loss. In Frankfurt, it is likely that the alleged attacker, Arid Uka, a 20-year-old Kosovo citizen living in the city, "flagged" his action as he initiated and completed target selection, surveillance, and security elicitation processes associated with terrorist or active-shooter attacks.

BREAKING THE CHAIN. Alleged bomb plot suspect Khalid Ali-M Aldawsari is taken into custody after the FBI accused him of plotting to target West Coast nuclear power plants, dams, and the home of former President George W. Bush. (Photo: Associated Press)

As detailed in First Observer and in many similar countersurveillance programs, when a user is trained to observe, assess, and report these flags or suspicious situations, the reporting and subsequent follow-up process can often disrupt the sequence or "chain" of events leading to an attack. First Observer also trains participants to identify these links in the terrorist targeting chain and illustrates to trainees how timely, accurate reports break the chain and reduce risk.

Many Armed Forces commanders may find First Observer to be a cost-effective and time-saving approach to reducing troop and materiel movement risk along global highway modes. At a recent meeting with the DOD Force Protection Working Group, HMC security specialists detailed how the program could be used to train military and DOD civilian transportation personnel quickly and easily and to integrate the program into existing training doctrine. At a time when every public- and private-sector organization is attempting to do more with less, First Observer training is provided at no cost to stakeholders.

Most First Observer training is online (www.FirstObserver.com), but TSA knows the most effective training is classroom-based. That is why First Observer offers "train the trainer" sessions as a significant part of the curriculum. Onsite and webinar training opportunities are also available, depending on the needs of the organization.

Commanders, DOD civilian associates, and other security professionals interested in learning more about the First Observer program and how it can be modified to fit diversified training missions can e-mail HMC at highwaysecurity@dhs.gov. Those interested in becoming a certified First Observer at no cost are encouraged to enroll in the program at the First Observer website (www.FirstObserver.com). Additional information about First Observer and the HMC mission is found on the HMC website (www.tsa.gov/highway).

[1] From the author's interview with the motor coach driver.

[2] Interview with the author.

[3] Interview with the author.

[4] Carver, Logan G. "Related Stories and Terror Timeline." *Lubbock Avalanche-Journal*, 25 February 2011. Available at http://lubbockonline.com/local-news/2011-02-25/terror-timeline

[5] Savage, Charlie, & Scott Shane. "US Arrests Saudi Student in Bomb Plot." *New York Times*, 24 February 2011. Available at http://www.nytimes.com/2011/02/25/us/25terror.html

[6] Ibid.

TARGET TYPE AND MUMBAI MODEL VARIANTS

Trident Hotel in Mumbai, site of the 26 November 2008 attacks. Photographer unknown

A case-study analysis

By James Pelkofski, Director, Antiterrorism/Force Protection, Pentagon Force Protection Agency

Evidence suggests that target type determines which variant of the Mumbai Model an extremist group uses.

In 5 coordinated attacks, 10 assailants killed more than 170 people, took a city of 12 million residents hostage for 60 hours, and captured worldwide attention. Less than a year later, in a single attack, 10 assailants killed 14 people, took a national military command hostage for 22 hours, and captured national-level attention. The former is an example of a complex combined arms attack (CAA) against a soft target, and the latter is a simple CAA against a hard target. Both attacks fit within the construct of a similar terrorist model.

Lashkar-i-Taiba's (LT's) 2008 assault on Mumbai, India, and the Tehrik-i-Taliban Pakistan (TTP) assault on Pakistan's military general headquarters (GHQ) are connected by operational style and the shared general goal of challenging the existing political and military order. The two events epitomize an attack model long under development among extremist groups. LT's attack represents a shocking, near-perfect execution of the complex variant of the "Mumbai Model"; TTP's attack represents an audacious application of the model's simple variant.

This article conducts a case-study analysis of the two attacks and proposes that the target type determines which variant of the Mumbai Model an extremist group uses.[1] The complex variant of the Mumbai Model holds a higher probability of success—and greater potential payoff—against a soft target than against a hard target. The simple variant is probably the only option for success against a hard target. A relationship between target type and attack variant carries implications for target defense.

The Mumbai attack and others like it fit within the general category of a CAA. CAAs involve multiple assailants using a variety of weapons and usually some combination of firearms and explosives. A complex CAA assaults several targets, approaching these targets from different directions. A simple CAA assaults a single target, usually from one direction. The University of Maryland's Global Terrorism Database lists 1,119 armed assaults occurring between 1970 and 2008, most of which fit this article's definition of either a simple or complex CAA. The Mumbai and GHQ attacks build on this already considerable body of extremist CAA work.

"Just a taste"[2]

LT, or "Army of the Righteous," assaulted the city of Mumbai on 26 November 2008, executing a complex CAA with deadly precision. After a covert, night maritime landing, 10 assailants split into 5 teams of 2 and assaulted 5 different planned targets along with several targets of opportunity over a span of 60 hours.

According to a US police study of the attack, the scouting and activities in prior months allowed the assailants to proceed at night with alacrity and comfortable familiarity. Taxi rides only hastened arrivals; the assailants knew the paths to their designated targets. With Indian identification cards, training in the local dialect, and Western-style dress, the assailants blended with the target population without sparking suspicion.[3]

CAAs involve multiple assailants using a variety of weapons and usually some combination of firearms and explosives. A complex CAA assaults several targets, approaching these targets from different directions. A simple CAA assaults a single target, usually from one direction.

When shooting, the assailants fired indiscriminately and extensively, maximizing casualties. Explosives supplemented the gunfire. At least six timed bombs were either used in or placed near the main targets, although only three of the bombs actually exploded. The use of firearms resulted in many more deaths than did the bombs, but the bombs that detonated increased public panic and contributed to inaccurate reports on the overall number of terrorists.[4]

The taking of hostages at two of the locations lengthened the duration of the Mumbai siege. Although not necessarily according to plan, the attack included negotiations between the attackers and the authorities over the release of the one terrorist, Ajmal Kasab, who had been taken alive. Likely out of frustration, the attacker's lead handler, Sajid Mir, offered to trade two female hostages at the Nariman/Chabad-Lubavitch Jewish Center for Kasab.[5] In the end, however, the murders of the Jewish women meant more to Mir than his accomplice.

A summary of the Mumbai attack is provided in Table 1.

"When this is over, there will be much more fear in the world"

Mumbai presented its planners with a soft target—one lacking a dedicated, concentrated, and sufficiently armed defense force. The Chhatrapati Shivaji Terminus (CST) had a Railway Protection Force (RPF), but only 50 percent of its officers carried firearms and those weapons were characterized as "antiquated." Not an AT force but rather an anti–petty crime division, the RPF was essentially impotent against the threat. Regarding overall city defense, like any other large police force, the Mumbai police are a multimission force but are mostly anticriminal oriented, dispersed throughout the city, and dedicated only in general terms to protecting the targets hit during the attack.[7]

Mumbai targets were thoughtfully chosen for human concentration, symbolism, and lack of defense. The CST accommodates 3.5 million people per day, promising that an attack at almost any hour will have ample opportunity for double- and possibly triple-digit death counts. The Leopold Café, the Trident-Oberoi Hotel, and the Taj Mahal Palace and Tower Hotel are all upscale establishments catering to and frequented by Western visitors; the tower is an iconic landmark. The Nariman/Chabad-Lubavich Jewish Center represented not only a Jewish target but, founded by Jews from New York, was also a Western target. The Cama and Albless Hospital was not a planned target but one the assailants could not neglect, given the opportunity to kill.[8]

Without armed defense, soft targets facilitate higher body counts. Although the attack fell far short of the purported objective of 5,000 casualties, the assailants tallied more than 170 dead and hundreds more wounded, most occurring in the first hour of the attack.[9] Lacking adequate and timely defense, soft targets are vulnerable to smaller but well-armed teams who are able to inflict immense damage and high casualties at will for an extended period when attacking multiple targets.

Attacking the "Pakistan Pentagon"

The TTP executed a simple but audacious CAA on the Pakistan military's GHQ in Rawalpindi on 10 October 2009—simple because the assault occurred along a single axis against one target, and audacious because the target is characterized as the "Pakistan Pentagon," housed within a fortified, overtly guarded complex considered to be immune to terrorist attack.[10]

Reports differ on the exact number of attackers but most agree on a range of 8–10 attackers and on the general attack sequence of events. Major General Athar Abbas, a Pakistan military spokesman, described the

Table 1. Summary of the Mumbai Attack in Approximate Sequential Order[6]

DATE/TIME	LOCATION	EVENT	WEAPONS	RESULT
11/23/08	Karachi, Pakistan	Attackers depart aboard motor vessel *Al Husseini*		
11/24/08		Attackers hijack trawler Kuber	Knives, firearms	4 crewmen killed
11/26/08 Night, before ~9:00pm	Mumbai	Attackers transfer to small boats; land in a Mumbai slum		Remaining crewman killed
Night ~9:20pm	Mumbai Leopold Café	2 taxis transport attackers into city 2 attackers throw grenades, enter, begin shooting	Grenades, automatic weapons	11 killed, 28 injured
~9:20pm	Nariman/Chabad-Lubavitch Center	2 attackers take 2 hostages, begin extended siege	Automatic weapons, explosives	7 killed, hostages held for 2 days
~9:20pm	Chhatrapati Shivaji Terminus (CST)	2 attackers enter station, begin shooting	Automatic weapons, explosives	52 killed, more than 100 injured
~9:20pm	Trident-Oberoi Hotel	2 attackers enter hotel, begin extended siege	Automatic weapons, explosives	35 killed, 24 injured, more than 140 hostages taken
~10:30pm	Cama & Albless Hospital	2 CST attackers open fire in vicinity of hospital, then on police vehicle the attackers then hijacked	Automatic weapons	6 killed, 1 wounded
~9:20pm	Taj Mahal Palace and Tower Hotel	4 attackers (2 from Leopold Café) enter hotel, begin extended siege	Grenades, automatic weapons, explosives	~58 killed, 76 injured;100–150 hostages taken
~10:30pm	Metrobig Cinemas	2 CST attackers fire from police van on crowd outside theater	Automatic weapons	10 killed
~10:30pm	Wadi Bundar and Vile Parle	Delayed attack on taxis	Timed explosives	5 killed, including both drivers; 22 injured
Night	Barricade-Girguam Chowpatty	Shootout between police and the CST/Cama Hospital attackers		1 attacker killed, 1 wounded and captured
11/27/08 Night	Nariman/Chabad-Lubavitch Center	400 special security forces arrive from Delhi Wassi order hostages killed	Automatic weapons	2 killed
11/28/08 7:30am	Nariman/Chabad-Lubavitch Center	Security forces storm the center		
11am	Trident-Oberoi Hotel	Indian authorities regain control	Automatic weapons	2 attackers killed
Night	Nariman/Chabad-Lubavitch Center	Indian authorities regain control	Automatic weapons	2 attackers killed
11/29/08	Taj Mahal Palace and Tower Hotel	Indian authorities regain control		Hostages held 3 days; 4 attackers killed

attackers as "well-equipped with automatic weapons, IEDs [improvised explosive devices], mines, grenades, and suicide jackets."[11] The assailants wore army uniforms and traveled to their target in a van with military license plates and a GHQ emblem, allowing them easier approach to security checkpoints.[12]

Attack planning involved the use of inside information by the attack leader, Muhammed Aqeel. Aqeel's knowledge of the GHQ compound came from his time with the Army Medical Corps four years earlier.[13] As reported in the *New York Times*, the attack "showed intimate knowledge of the layout of the military headquarters in Rawalpindi and was skillfully planned."[14]

Outfitted in military trappings, the assailants blended enough with the target population to clear the first security post.[15] According to Pakistani officers, the uniforms delayed reaction and confused the Pakistani response.[16] Stopped at the second security post, the assailants engaged in a 45-minute gun battle, leaving 4 of the attackers dead. Once inside the GHQ compound, the attackers continued the assault using grenades and automatic weapons.[17]

The assailants took hostages and held them in separate rooms. During the hostage standoff, Aqeel issued a series of unrealistic demands, including the release of 100 terrorists in Pakistani custody, an end to "American bases" in Pakistan, and the trial of former president General Pervez Musharraf.[18] In the final Pakistani commando response, two commandos were shot and killed in the rescue attempt in one room and several commandos and hostages were injured when an attacker

Table 2. Summary of the GHQ attack in approximate sequential order[20]

DATE/TIME	LOCATION	EVENT	WEAPONS	RESULT
Pre-attack 5/08 (date approximate)	Pakistani Kashmir	Planning commenced		
5/08-10/09	Pakistani Kashmir	Training		
Attack 10/10/09				
~11:30am	GHQ, Rawalpindi	White van with 10 attackers approach and clear first checkpoint		
	GHQ	Attackers exit van, run toward and attack second checkpoint	Grenades, automatic weapons	
~12:45pm	GHQ	45-minute gun battle at second checkpoint 4 attackers killed	Grenades, automatic weapons	6 soldiers killed, 5 wounded
Afternoon	GHQ	4 attackers escape gun battle, enter complex, 34 hostages taken	Automatic weapons; suicide vests	
10/11/09 ~6:00am	GHQ	Pakistan commandos launch rescue operation		
Morning	GHQ	2 attackers attempt suicide bombing	Personal borne explosive device	
~10am	GHQ	Attack leader Aqeel attempts a suicide bombing to evade capture, Aqeel injured but captured	Explosives	5 commandos injured
~10am	GHQ	Pakistan commandos regain control, 2 attackers killed, 1 attacker captured	Firearms	3 hostages killed, 2 soldiers killed, 5 injured
10/12/09	Rawalpindi	Three commandos die of injuries suffered during the hostage rescue		3 soldiers killed

HARD TARGET. The Pakistan Pentagon has a dedicated, concentrated, well-armed, and prominent defense force with the sole mission of guarding the GHQ. (DOD photo by Master Sgt. Jerry Morrison, US Air Force/Released)

detonated his suicide vest during the rescue in the second room, ending the 22-hour siege.[19]

A summary of the GHQ attack is provided in Table 2.

Audacity Against Strength

The GHQ compound in Rawalpindi, near the Pakistan capital of Islamabad, is described as one of the most secure bases in Pakistan.[21] The Pakistan Pentagon has a dedicated, concentrated, well-armed, and prominent defense force with the sole mission of guarding the GHQ. By any definition, the GHQ presented its attackers with a hard target.

The TTP's success only highlighted the boldness of even attempting an attack against the principal Pakistani Army Headquarters. According to the *New York Times*, US military officials were "astonished that the militants could penetrate the high-security installation to the extent that they did."[22] By penetrating the compound, taking 34 hostages, killing 14 military and civilian officials, and holding siege for 22 hours, the TTP humiliated the Pakistani military and national leadership—all accomplished against a hard target fortified and protected by the Pakistani military.

The hard target presented by the GHQ required a well-armed, sufficiently manned team consolidating its attack along a single axis and insider information on the layout and security procedures. By concentrating a simple CAA against the GHQ's trained, dedicated, and visible security force, a team like the one assembled by the TTP could penetrate the perimeter of the target and continue wreaking havoc while raising the body count inside the compound. Simply attacking the hard target represents a victory; penetrating the perimeter and exacting casualties magnifies the impact.

"Just wait 'til you see the rest of the film": Implications for Target Defense

Although the Mumbai and GHQ CAAs differ in complexity, both share striking similarities beyond using combined arms. Both attacks hit high-profile targets: one a major city, the other a top military headquarters. Both involved cover and deception: The Mumbai attack began at night, and the GHQ attack used disguised assailants in a sham approach vehicle. Both utilized taking hostages and engagement in negotiations as delaying tactics, permitting the assailants an operational pause. Both used fedayeen, assailants intent on "killing until killed," armed with multiple weapons to prolong and accentuate the attack.[23] Both represent variations within the broad context of what may be called the Mumbai Model.

CAAs, complex and simple, are an increasingly popular option among extremist groups. For this option, symbols of US power and Western influence remain primary targets. Open-source reporting on the "Europe plot" strongly suggests that al Qaeda or its affiliates are planning a Mumbai-style attack in Europe.

These similarities bear noting by Western intelligence, security, and military agencies and services. CAAs, complex and simple, are an increasingly popular option among extremist groups. For this option, symbols of US power and Western influence remain primary targets. Open-source reporting on the "Europe plot" strongly suggests that al Qaeda or its affiliates are planning a Mumbai-style attack in Europe.[24]

The attractions of the Mumbai Model for al Qaeda, LT, TTP, and other extremist groups are the low-cost efficiency and the high potential payoff. As an operation, a Mumbai-type CAA is relatively easy to plan, is cheap to execute, and poses fewer difficulties in acquiring weapons and participants. Cheaper, smaller, and more frequent attacks fit the call to arms made most recently in al Qaeda's *Inspire* magazine.[25]

Additionally, the Mumbai Model offers terrorists a more surgical attack option with the ability to identify specific targets, such as the Nariman/Chabad-Lubavitch Jewish Center. With more precision, extremists can avoid the criticism weighed against them by Muslims for indiscriminately killing Muslims among the other attack victims.[26]

The Mumbai Model promises extremists almost irresistible benefits at relatively low costs, even if poorly executed. Soft targets generally mean high body counts, greater drama, and extensive media coverage, even if the operation is short or only partially successful from the extremist perspective.[27] The publicity and notoriety that accompanies media coverage provides extremist groups with a recruiting and fund-raising rush. Hard targets, by nature, present not only a more formidable challenge to extremists but also a different measure of success. The mere attempt at attacking what seems too hard represents success and can be spun as a success by media-savvy extremist propagandists.

Target Differentiation

Apart from the pervasive and expanding extremist threat to Western interests and the attraction of the Mumbai Model to extremists, lessons from Mumbai and Rawalpindi indicate a possible relationship between target type and attack variant that carries implications for target defense.

A soft target invites a complex CAA. Target defenses are either inadequate, slow to react, or nonexistent. Against a soft target like Mumbai, a complex CAA with smaller attack teams spread out along multiple vectors against several objectives promises a high probability of success, measured by body count. One analysis of the Mumbai attack has suggested that the use of separate teams was an effort to reduce operational risk; a loss of one or even two teams would not preclude mission success.[28] An alternative interpretation could be that Mumbai simply presented a soft target appropriate for a dispersed attack by smaller teams.

The target, soft or hard, will determine the type of attack. Additional research is required to develop the relationship between target type and attack method and to suggest any causal relationship. A model that explains this relationship could help determine the risk-appropriate and cost-efficient target defenses needed against the most likely form of attack.

Defending a soft target is problematic at best, but a lesson could be drawn from the observation that when confronted with serious armed opposition, the Mumbai CST attackers withdrew.[29] This indicates that strength matters to the point that it can deter an attack or at least alter an attack plan. For a soft target, a visible, well-armed roving patrol might present a defense that is not comprehensive but is sufficient for deterrence.

A hard target requires a simple CAA. Target defenses are readily available and manned, trained, and equipped to defeat an attack. Against a hard target like the GHQ, a simple CAA concentrating one larger attack team along a single axis is probably the only chance for success, as measured by the degree of breaching the objective and also by body count.

Already strongly defended, additional defensive considerations should include limiting access points to the hard target. For those access points remaining, multiple visible, defensive layers should complicate, if not thwart, even a concerted simple CAA similar to the GHQ attack. For hard-target defense, security forces should exceed or at least match terrorist weapon capability. Undermanned and underarmed defensive capabilities neither deter nor defeat potential or realized adversaries.

This article suggests that the harder the target, the less complex the CAA must be to ensure mission accomplishment. Softer targets permit more complex attacks. Target hardening may not prevent an attack but may result in a different type of attack. Few would dispute a Rand study conclusion that "since attacks against high-profile soft targets are relatively easy and cheap to mount, such institutions will remain targets of future attacks."[30] However, hard targets are not immune. The target, soft or hard, will determine the type of attack. Additional research is required to develop the relationship between target type and attack method and to suggest any causal relationship. A model that explains this relationship could help determine the risk-appropriate and cost-efficient target defenses needed against the most likely form of attack.

The views expressed in this article are those of the author and do not necessarily represent the Pentagon Force Protection Agency or the Department of Defense.

[1] Terrorism is more method than ideology. Therefore, this article distinguishes between the act of terrorism and the practice of extremism. The latter is defined in this paper as an ideological framework for supranational organizations or nonstate actors to pursue political objectives through violence, without regard to international law and accepted norms of political or religious behavior.

[2] This and subsequent section headers in quotes are transcribed from the HBO documentary "Terror in Mumbai" and are statements made by Sajid Mir aka "Wassi" the Mumbai attack planner, director, and principal remote handler.

[3] Los Angeles Police Department (LAPD)/Las Vegas Metropolitan Police Department (LVPD). "Terrorist Attack in Mumbai (26/11) and Implications for Major Cities and Urban Centers." Interdepartmental briefing, 2009.

[4] LAPD/LVPD.

[5] Rotella, Sebastian. "An intricate plot unleashed, the West confronts a new threat." *Washington Post*, 15 November 2010, Section A.

[6] Table 1 is derived from the following sources: Global Terrorism Database (s.v. "Mumbai attack"). National Consortium for the Study of Terrorism and Responses to Terrorism. College Park, MD: University of Maryland. Available at http://start.umd.edu/gtd (accessed 30 October 2010); LAPD/LVPD; "Mumbai Attack Analysis." New York Police Department Intelligence Division, 2008; Rabasa et al. "The Lessons of Mumbai." Santa Monica, CA: Rand Corporation, 2009; Rotella; "Terror in Mumbai." HBO Documentary Films (directed by Dan Reed). Quicksilver Media Ltd, 2009.

[7] Rabasa et al. "The Lessons of Mumbai." Santa Monica, CA: Rand Corporation, 2009. pp. 9–10.

[8] LAPD/LVPD.

[9] Global Terrorism Database; "Terror in Mumbai."

[10] Waraich, Omar. "Why Pakistan Must Widen Hunt for Militant Bases." *Time*, 13 October 2009. Available at www.time.com/time/world/article/0,8599,1929931,00.html (accessed 6 November 2010)

[11] Waraich, "Why Pakistan."

[12] Ali, Sadaqat, & Khurrum Shahzad. "Pakistan's army retakes HQ after siege." 11 October 2009. Available at www.samaa.tv/news (accessed 6 November 2010); Khan, Omer Farooq. "Taliban attack Pakistani army headquarters, 10 dead." *Times of India*, 10 October 2009. Available at http://articles.timesofindia.indiatimes.com/2009-10-10/pakistan/28088576_1_south-waziristan-army-headquarters-major-general-athar-abbas (accessed November 6, 2010); Waraich.

[13] Perlez, Jane. "Pakistani Police Had Warned Army About a Raid." *New York Times*, 12 October 2009. Available at http://www.nytimes.com/2009/10/11/world/asia/12pstan.html (accessed 6 November 2010)

[14] Perlez, "Pakistani Police."

[15] Perlez, "Pakistani Police."

[16] Perlez, Jane. "Pakistan Retakes Army Headquarters; Hostages Freed." *New York Times*, 11 October 2009. Available at http://www.nytimes.com/2009/10/110/world/asia/11pstan.html (accessed November 6, 2010); "Pakistan: terrorist attack kills six soldiers in Rawalpindi." *Telegraph*, 10 October 2009.

[17] Waraich, Omar. "Taliban Siege Shows Need for Pakistan Offensive." *Time*, 10 October 2009. Available at www.time.com/time/world/article/0,8599,01929592,00.html (accessed 6 November 2010)

[18] Perlez, "Pakistani Police"; Waraich, "Why Pakistan."

[19] "Hostages at Pakistani army HQ released." CNN.com, 11 October 2009. Available at http://edition.cnn.com/2009/WORLD/asiapcf/10/10/pakistan.shootings/index.html (accessed 6 November 2010); Perlez, "Pakistani Police."

[20] Table 2 is derived from the following sources: Birsel, Robert. "Q+A: Militant raid on Pakistan's army headquarters." Reuters, 12 October 2009. "10 Dead in Attack on Pakistani

Military HQ," CBS News, 10 October 2009. Available at http://www.cbsnews.com/stories/2009/10/10/world/main5375901.shtml (accessed 6 November 2010); "GHQ attackers demanded release of 100 militants." Dawn.com, 13 October 2009. Khan; Perlez, "Pakistan Retakes"; Perlez, "Pakistani Police"; Shah, Saeed. "Terrorist attack in Pakistan shows how vulnerable it is." McClatchy Newspapers, 11 October 2009. Available at http://www.mcclatchydc.com/2009/10/11/76954/terrorist-attack-in-pakistan-shows.html (accessed 6 November 2010); "Pakistan: Terrorist attack"; Waraich, "Taliban Siege"; Waraich, "Why Pakistan." The times and figures listed are approximate estimates based on available information; few sources agree on the exact numbers.

21 "Pakistan army raid frees hostages." BBC news, 11 October 2009. Available at http://news.bbc.co.uk/2/hi/8301175.stm (accessed 6 November 2010)

22 Perlez, "Pakistan Retakes."

23 Waraich, "Taliban Siege."

24 Simon, Steven, & Jonathan Stevenson. "Al-Qaeda takes it to the streets." *Washington Post*, 10 October 2010, Section B.

25 Miller, Greg. "Al-Qaeda group calls failed plot a 'bargain.'" *Washington Post*, 22 November 2010, Section A.

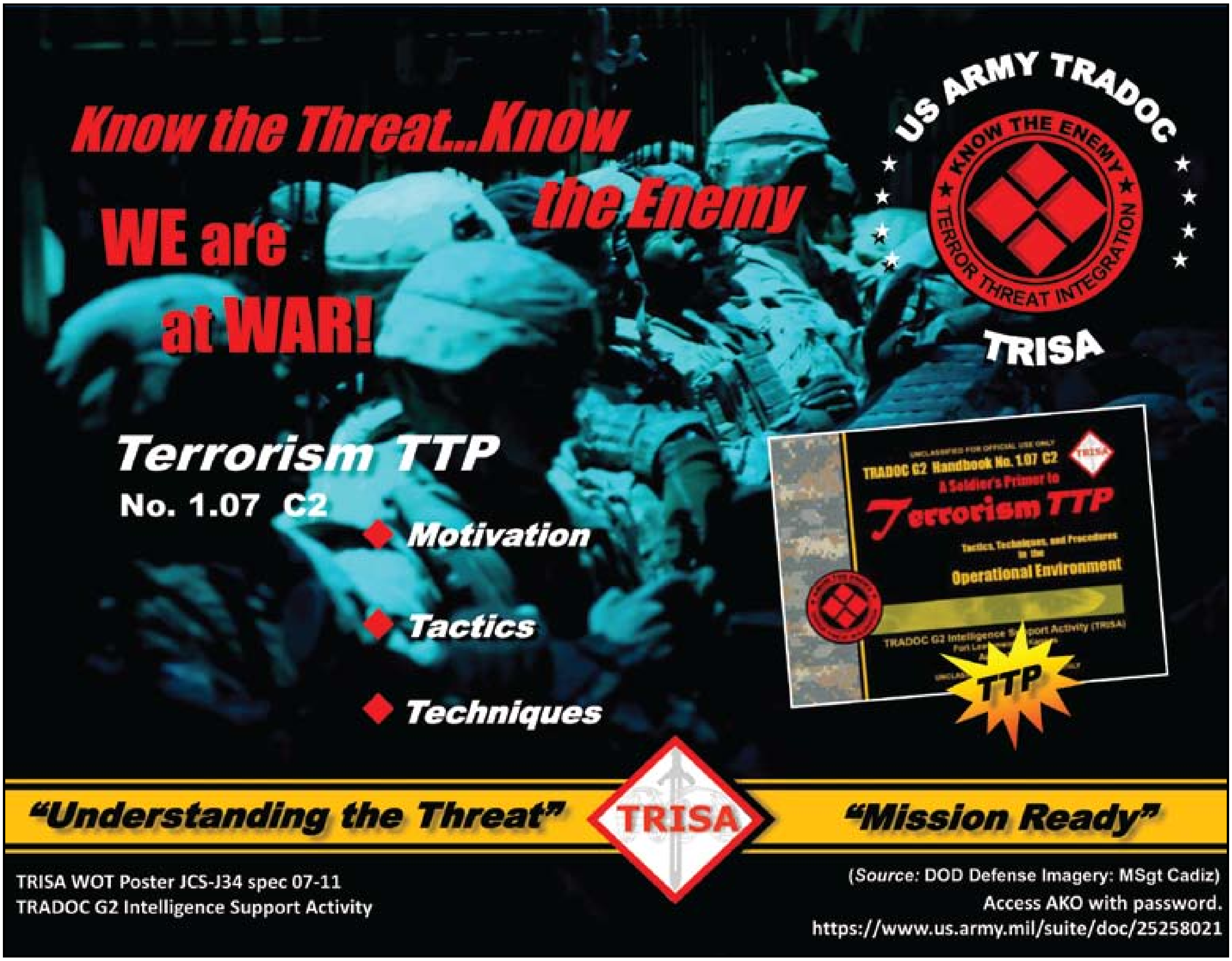
26 Simon & Stevenson.

27 Rabasa et al., p. 7.

28 Rabasa et al., p. 6.

29 Rabasa et al., p. 5.

30 Rabasa et al., p. 21.


Know the Threat...Know the Enemy
WE are at WAR!
US ARMY TRADOC
KNOW THE ENEMY
TERROR THREAT INTEGRATION
TRISA
Terrorism TTP
No. 1.07 C2
Motivation
Tactics
Techniques
UNCLASSIFIED FOR OFFICIAL USE ONLY
TRADOC G2 Handbook No. 1.07 C2
A Soldier's Primer to
Terrorism TTP
Tactics, Techniques, and Procedures in the
Operational Environment
TRADOC G2 Intelligence Support Activity (TRISA)
TTP
"Understanding the Threat"
TRISA
"Mission Ready"
TRISA WOT Poster JCS-J34 spec 07-11
TRADOC G2 Intelligence Support Activity

(*Source:* DOD Defense Imagery: MSgt Cadiz)

Access AKO with password.
https://www.us.army.mil/suite/doc/25258021

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®

THE SEVEN SIGNS OF TERRORISM

7

1 Surveillance

Someone recording or monitoring activities. This may include using cameras (either still or video), note taking, drawing diagrams, annotating on maps, or using binoculars or other vision-enhancing devices.

2 Elicitation

People or organizations attempting to gain information about military operations, capabilities, or people. Elicitation attempts may be made by mail, fax, telephone, or in person.

3 Tests of security

Any attempts to measure reaction times to security breaches or to penetrate physical security barriers or procedures in order to assess strengths and weaknesses.

4 Acquiring supplies

Purchasing or stealing explosives, weapons, ammunition. Also includes acquiring military uniforms, decals, flight manuals, passes or badges (or the equipment to manufacture such items), or any other controlled items.

5 Suspicious persons out of place

People who don't seem to belong in the workplace, neighborhood, or a business establishment. Includes suspicious border crossings and stowaways aboard ship or people jumping ship in port.

6 Dry run/trial run

Putting people into position and moving them around according to their plan without actually committing the terrorist act. This is especially true when planning a kidnapping, but it can also pertain to bombings. An element of this activity could also include mapping out routes and determining the timing of traffic lights and flow.

7 Deploying assets

People and supplies getting into position to commit the act. This is a person's last chance to alert authorities before the terrorist act occurs.

Source: Michigan Intelligence Operations Center

iSALUTE

SEE SOMETHING • SAY SOMETHING

What to Report:

- Unauthorized attempts to access classified or sensitive data
- Person advocating support for a terrorist organization
- Contacts that may suggest extremist group recruitment
- Suspicious behavior possibly associated with terrorist activity

How to Report:

- 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

U.S. ARMY ARMY STRONG®

US Marine Corps photo by Curtis Lambert/Released

"TEACH THEM PROPERLY"

Advanced training addresses the realities of the battlefield

By Bob Essmann

Preparation for successful response to sudden, unexpected violence requires more than practicing basic firearm skills in a static environment.

There is a short, powerful scene in the Civil War drama "Glory" in which Private Jupiter Sharts is found at the center of attention of the entire Massachusetts 54th Regiment during rifle practice. As Private Sharts successfully hits one glass bottle target after another, the surrounding crowd hoots and hollers its approval. But the mood rapidly changes when Colonel Robert Gould Shaw unexpectedly arrives to inspect the training evolution. Congratulating Sharts for his shooting skills, Shaw invites the nervous private to shoot again and then repeatedly pressures the frazzled soldier, who is obviously too slow in reloading his muzzle-loaded rifle. Colonel Shaw shouts increasingly louder and more urgent commands: "Reload … Discharge your weapon! Faster … faster!" When Private Sharts finally fires his shot, it wildly misses the target.

But the Colonel's lesson is not finished. "Do it again. Only this time, I want it done quickly!" he orders. Looming over the frantic private, who is struggling to hasten the reloading process, Shaw explains the level of advanced fighting skills necessary to survive the realities of the battlefield. Then, borrowing a Colt revolver from the responsible officer, Major Cabot Forbes, Shaw begins firing into the air from behind the shell-shocked private while continuing his verbal commands: "Faster!" Boom. "Reload … quickly!" Boom. "Faster!" Boom. "Do it!" Boom. "Do it!" Boom. "Do it!" Private Sharts is completely undone by the stress. Shaking and panicked, he drops the rifle and the ram rod. The regiment is silent. Turning to Major Forbes, the officer tasked with preparing the inexperienced regiment to fight and survive amid the horrors of the Civil War battles they will inevitably face, Colonel Shaw gives a stern, direct order: "Teach them properly, Major."

Colonel Shaw's wisdom offers lessons that are worth learning again today. Preparation for successful response to sudden, unexpected violence requires more than practicing basic firearm skills in a static environment. Marksmanship earns ribbons and medals, post orders provide correct response procedures, and drills ensure that the sentry can execute preplanned responses. History, however, has proven repeatedly that unless an armed sentry is exposed to realistic training environments that simulate stressors and allow the weapon handler to repeatedly rehearse judgment-based decisionmaking skills in threat recognition, hostile-intent determination, and use of force, response to actual hostile actions is likely to fail. The incoming boat will not be stopped, the inside attacker will not be confronted, and the terrorist at the gate will drive right through, not because the sentry is incompetent or unwilling but because he or she is unable. Like Private Sharts, the sentry will simply freeze, failing to use his weapon because he is unprepared and rendered mentally and physically incapable of a response.

Ultimately responsible for mission accomplishment and the protection of personnel and resources, the commander must ensure that those individuals who are entrusted with the protection of DOD assets, armed with loaded weapons, and posted between the aggressor and the target are not only well trained but are physically, mentally, emotionally, and morally able to perform their duties when confronted with an unexpected attack.

DOD AT Standard 27, found in DODI 2000.16, provides a list of topics that must be taught during Level III pre-command AT training. Toward the end of the list is a requirement for "Understanding Use of Force and Rules of Engagement—Terrorist Scenarios and Hostile Intent Decisionmaking," without further explanation or specifics. Nowhere else in the AT standards are "terrorist scenarios" or "hostile-intent decisionmaking" further explained, although, arguably, the tactical application of hostile-intent decisionmaking regarding the use of force is necessary well below the command level. So why is the training topic placed where it is? Consider this statement, found in Chairman of the Joint Chiefs of Staff Instruction 3121.01B, Enclosure L (U), Standing Rules for the Use of Force for US Forces: "Unit commanders at all levels must teach and train their personnel how and when to use both non-deadly and deadly force in self-defense."

The DOD AT Standards and Standing Rules for the Use of Force place the responsibility with the commanding officer to prepare armed sentries for the necessary and correct use of force. Ultimately responsible for mission accomplishment and the protection of personnel and resources, the commander must ensure that those individuals who are entrusted with the protection of DOD assets, armed with loaded weapons, and posted between the aggressor and the target are not only well trained but are physically, mentally, emotionally, and morally able to perform their duties when confronted with an unexpected attack. The question is how to "teach them properly." The answer most certainly involves "terrorist scenarios and hostile-intent decisionmaking," which indicates a need for readily available simulation devices and realistic scenarios.

Realistic decisionmaking training, which presents the armed sentry with conditions that simulate the stressors faced by weapons handlers responding to a sudden and unexpected attack, provides opportunities to rehearse instantaneous reactions and experience a taste of the effects of stress on the ability to perform. Thus the training provides a degree of "stress inoculation" for sentries. Sentries must be informed of the numerous factors that will inhibit their performance and decision–making in the heat of the attack: physiological changes, psychological influences, and the effects of false notions and impressions about guns, bullets, "bad guys," and the law. Sentries must experience, understand, and overcome these factors to effectively execute an appropriate use of force response when surprised by a sudden, violent confrontation. Because the sentry is not likely to confront an easily identifiable, designated "hostile" or "enemy combatant," the attacker will usually have the element of surprise. It is critical that armed sentries gain the ability to recognize a threat, determine the appropriate reaction, and then act decisively to halt the aggression while using the appropriate level of force. Accordingly, it is extremely important that our Service members are well educated in threat identification and determination of hostile intent.

Consider use of force decisionmaking training as an armed sentry's equivalent to ejection-seat training for pilots; emergency extraction drills for firefighters; or Survival, Evasion, Resistance, and Escape training for warfighters. The above-mentioned drills are essential training exercises that increase survival skills and readiness by exposing the individual in the simulated environment to unexpected events before they happen. No one would question the need for these training events. No one would consider strapping a pilot into a jet, sending a firefighter into a burning building, or putting a warrior into hostile territory without the training that would be necessary to survive when things go wrong. Yet, far too often, armed sentries are posted at entry control points with little more than basic weapons qualifications and sentry skills training, gear familiarization, and post orders, never having received the "emergency training" valued so highly among other warfare occupations. How will the sentry react when faced with the threat that his post was designed to oppose? No one knows. He has never faced the situation before.

Emergency training prepares armed sentries by acclimating them to a number of specific realities affecting their successful response to close-contact, sudden, violent, and life-threatening attacks[1]:

US Air Force Master Sgt. Stephen Fraley instructs a class during the Expeditionary Combat Skills Training at Charleston Air Force Base, SC. (US Air Force photo by Senior Airman Katie Gieratz/Released)

- **Protections of the Law.** Legal guidance, afforded by the US Constitution, addressed in related case law, and specifically provided by DOD and Service policy and directives, provides clear justification for the armed sentry making reasonable judgments concerning the use of force in the protection of self and others. Sentries armed with an understanding of their legal rights and with confidence in clear command guidance and support are mentally prepared to exercise appropriate use of force when required.

- **Tactical Dynamics of a Deadly Force Encounter.** Armed sentries must understand basic principles of psychology, physics, and physiology that will govern the events accompanying an attack. Tactical dynamics include—

  1. **Action versus reaction:** The attacker usually has the advantage because he acts first. Human mental and physical responses take time, demanding a sentry's astute observation of threat indicators; early hostile-intent determination; and immediate, effective responses to successfully counter the actions of an aggressor. Applying unnecessarily restrictive use of force rules and policies on the sentry adds time to the sentry's decisionmaking cycle and yields the advantage to the attacker.
  2. **Tache-Psyche effects:** The body's natural responses to the stresses imposed by a sudden and unexpected attack include chemical changes in the brain that produce an increased heart rate and blood pressure, vasoconstriction (drawing blood from the extremities to the central cortex to increase oxygenation of the brain and vital organs), increased blood sugar, dilation of the eyes, and increased perspiration. These physiological responses produce a number of other changes that affect the sentry's ability to function: loss of fine motor skills (including use of hands and fingers necessary to manipulate a weapon), cognitive processing deterioration, auditory exclusion (experiencing events as if watching a silent movie), time-space distortion (events seem to happen in slow motion), loss of peripheral vision or "tunnel vision," and loss of bowel and bladder control. Armed sentries must be taught to expect these effects so that they are prepared to respond adeptly to attacks while overcoming these negative, stress-induced consequences.
  3. **Wound ballistics:** Physics and physiology determine a bullet's effect on the human body when shot. Persistent misconceptions lead untrained weapons handlers to hold unrealistic expectations about what bullets do or how people react when hit by a bullet. Despite the lessons of Hollywood, small

> arms do not produce "knock-down power" and will not instantly disable or kill an attacker. The human body is very resilient and sometimes is capable of functioning for an extended time after receiving a bullet wound. An attacker is not likely to immediately stop aggressive actions and may continue to attack until either enough wounds are created to produce significant blood loss or vital brain-nerve function is disrupted. Overcoming false impressions, fears, and expectations concerning the effects of small-arms fire is necessary to prepare weapons handlers to effectively use their weapons.

Recognizing the difficult realities of decisionmaking under stress in close personal confrontation, Lt Col David G. Bolgiano, Staff Judge Advocate, Maryland Air National Guard, collaborated with a group of judge advocates and tactical weapons instructors to help pioneer the Judgment-based Engagement Training (JET) seminar, which is based on the training concepts of FBI Supervisory Special Agent John C. Hall and W. Hays Parks from DOD's Office of General Counsel. The program of instruction effectively trains military members, commanders, and their judge advocates concerning lawful and tactically sound applications and uses of deadly force, providing a detailed overview of the law and the tactical dynamics of deadly force encounters: action versus reaction, Tache-Psyche effect (the psychophysiological reactions of humans under high-stress tactical environments), and wound ballistics.

JET seminars include three necessary elements of training: (1) classroom instruction regarding the legal aspects and physical, psychological, and physiological factors involved in the use of force and self-defense; (2) diverse situational training exercises utilizing simulation devices including the engagement skills trainer, the firearms training system, or nonlethal training aids (e.g., Simunitions FX), through which students viscerally experience the phenomena and issues discussed in the classroom; and (3) weapons live-fire, through which students practice decisionmaking to engage targets on the range using realistic tactical skills and movement. By introducing stressors in a simulated environment, students are exposed to some of the more deadly aspects of fear- and stress-induced physiological and psychological effects. Throughout the dynamic and interactive training regimens, students are forced to rehearse near-instantaneous decisionmaking, building judgment skills that can only be gained by exposure to a variety of complex situations that require immediate detection, decision, and reaction.

Armed sentries are expected to respond decisively to defeat the unexpected actions of an attacker and are tasked to perform perfectly the first time the opportunity presents itself on the job. They need to be well-trained, with an understanding of the commander's guidance concerning the use of force and the protections and rights possessed under the law, with exposure to the psychophysiological responses and the Tache-Psyche effects that they will be required to overcome, and with extensive rehearsal opportunities under realistic simulated scenarios necessary to hone decisionmaking and hostile-intent-determination skills. This training will require an investment in well-prepared and well-presented classroom instruction, firearms training simulators loaded with dynamic scenarios that closely replicate the sentry's role and environment to provide realistic stressors, and live-fire weapons training that requires active decisionmaking skills. Our front line of defense deserves that investment—anything less is target practice, broken bottles, ribbons and medals, and a false sense of security.

Recommended additional reading:

- Bolgiano, David G. *Combat Self-Defense, Saving America's Warriors from Risk-Averse Commanders and Their Lawyers.* Little White Wolf Books, 2007.
- Grossman, Dave. *On Combat: The Psychology and Physiology of Deadly Conflict in War and Peace.* Warrior Science Group, 2007.
- Patrick, Urey W., & John C. Hall. *In Defense of Self and Others: Issues, Facts, and Fallacies—The Realities of Law Enforcement's Use of Deadly Force.* Carolina Academic Press, 2005.

Bob Essmann, Commander, US Navy (retired), is the Antiterrorism Leadership Team Lead at the Navy Center for Security Forces, where for the past six years he has been responsible for development and delivery of Antiterrorism Level III Pre-Command Training, Level II Antiterrorism Officer Training, and Navy Security Force Officer courses. He wrote, directed, and produced the training video "Judgment-Based Engagement and Tactics, and Individual ROE" based on Lt Col Bolgiano's JET seminar classroom instruction.

[1] See an excellent discussion of the military member's right of self-defense, the lawful use of force, and the tactical dynamics of a deadly force encounter in *Combat Self-Defense, Saving America's Warriors from Risk-Averse Commanders and Their Lawyers*, by David G. Bolgiano, Little White Wolf Books, 2007.

BEST PRACTICES FOR THE AT COMMUNITY

DOD photo by Staff Sgt. Brian Ferguson, US Air Force/Released

Recommendations from Joint Staff Integrated Vulnerability Assessment (JSIVA) teams

By DTRA Operations and Nuclear Support Assessments Division

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

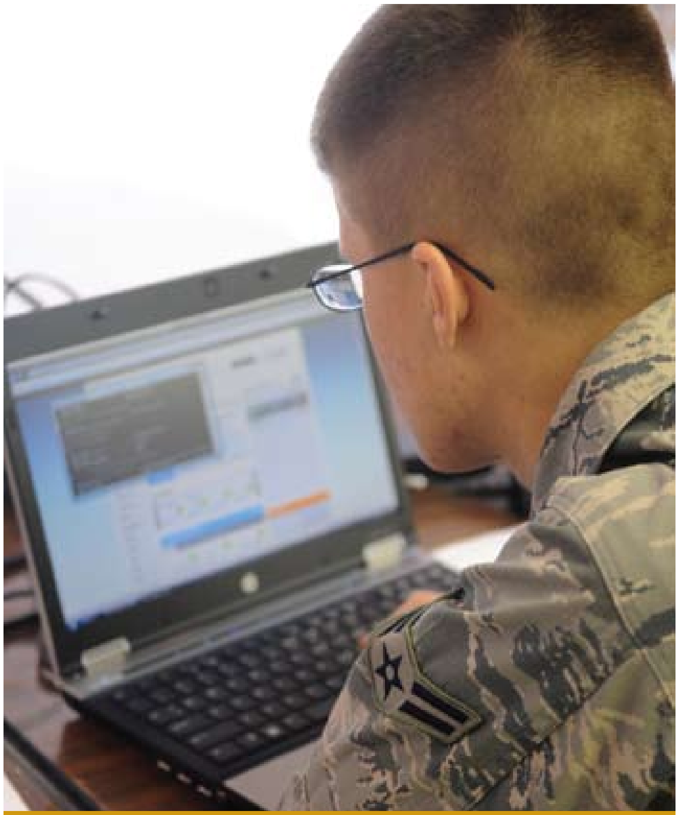
The Joint Staff Integrated Vulnerability Assessment (JSIVA) teams identify and nominate best practices that should be shared with the DOD AT Community.

Each practice described involves tactics, techniques, and procedures that were collected between 2006 and 2010. During a typical JSIVA visit, the teams often identify several other "positives," but not all apply uniformly across the DOD AT Community. These practices can be applied at most installations.

School-Specific Measures. The DOD Education Activity (DODEA) Far East District's school security and emergency standard operating procedures address several possible threats and courses of action to mitigate or reduce threat. The JSIVA teams recommend school-specific force protection condition (FPCON) measures to improve responsiveness during FPCON condition changes and to integrate DODEA's procedures.

Access Control Points with Limited Geographical Spacing. Access control points (ACP) can be designed to account for limited geographical spacing and to include features defined in Unified Facilities Criteria, Security Engineering: Entry Control Facilities/Access Control Points (UFC 4-022-01). The JSIVA teams recommend drop-arm barriers with sensors that activate the final-denial barrier if a vehicle makes contact with the drop arm. This response will eliminate the reaction time required by security personnel to activate the final-denial barriers, resulting in a dramatic reduction in land space needed for the ACP and increased probability of detection and response.

Public and Private Websites. JSIVA teams recommend installation-specific regulations that establish policy and guidance for information posted to websites, to include personal websites. For command websites, such a policy should include responsibilities, implementing guidelines, periodic reviews, and reporting procedures.



CYBER SECURITY. Regulations for both command and personal websites are critical to managing installation vulnerabilities. (US Air Force photo by Airman 1st Class Manisha Vasquez/ Released)

Additional Vulnerability Assessments. JSIVA teams recommend conducting operational security, information assurance, computer network defense, and wireless device detection vulnerability assessments as part of the annual requirements.

Barrier Plans. JSIVA teams recommend developing a barrier plan that incorporates existing permanent barriers and manual barriers to block off roadways. This plan decreases the time to execute the barrier plan and allows quick isolation of a specific area.

Countersurveillance Measures. JSIVA teams recommend a countersurveillance plan that is randomly conducted at ACPs independent of random AT measures (RAM). Countersurveillance teams should be equipped with optics, cameras, and fixed-point diagrams.

BARRIER PLANS. US Army Sgt. Ryan Sparks guides a vehicle entering Observation Post Savanna, in Wardak province, Afghanistan, 18 May 2011. (US Army photo by Spc. Mikel K. Peterson/Released)

JSIVA teams recommend deploying decoys to test the effectiveness of the program.

Information Control (INFOCON) Measures. JSIVA teams recommend implementing local INFOCON measures that provide options for response to cyber threats. These measures should be tested during local exercises.

Preplanned Responses. JSIVA teams recommend developing preplanned responses for threats that could occur at installation ACPs as well as incorporating these responses into security forces training. Responses to a detected explosive device or a suspicious activity at or near ACPs may be included.

Random Antiterrorism Measures. JSIVA teams recommend tasking threat working groups to develop RAMs based on threats, suspicious activity reporting, ongoing surveillance, and existing vulnerabilities. This will increase the effectiveness of the RAMs.

Vulnerability Mitigation Working Group. JSIVA teams recommend establishing a vulnerability mitigation working group chaired by the commander. Membership should involve organizations involved primarily in correcting physical deficiencies (e.g., support group commander, director of public works, director of logistics). This group should be empowered to develop mitigation plans and resource packages with the finance office.

THE PROS AND CONS OF SOCIAL MEDIA

AN ANTITERRORISM PERSPECTIVE

US Air Force photo by Master Sgt. Adrian Cadiz/Released

New technologies present new challenges and opportunities

LCDR Christopher F. Hill

We cannot stop the flood of information exchange, despite the risks—but we can use the flood to our advantage.

Social media has become an unavoidable environmental factor in our lives—a raging river of limitless information, ideas, and potential vulnerabilities. Commanders and Antiterrorism Officers (ATOs) need to become very smart about social media if they want to keep pace with the rest of the world. With just about every unit involved in official and unofficial social media networking and almost every young Service member "Tweeting," "Facebooking," or microblogging for their respective audiences of "friends," we simply cannot stop the flood of information exchange, despite the risks. But we can use the flood to our advantage.

From an AT perspective, we do not yet know the extent of our vulnerabilities from social media networking (the cons), and we are only beginning to grasp its capability in terms of expanding threat awareness and protection efforts (the pros). The sheer size of the social media domain is staggering. Facebook, for example, has more than 500 million users, 50 percent of whom use it every single day. As of 8 June 2011, the US Marines' page alone had more than 1.6 million followers. DOD is also well aware that 80 percent of major corporations use social media, despite inherent security concerns, because it increases advertising and improves customer satisfaction, loyalty, and trust, all of which can be advantageous for the military.[1] As one DOD official noted:

> "[DOD] is no different than any big company in America. What we can't do is let security concerns trump doing business. … Companies in the private sector that have policies like us don't dare shut down their Web sites. They have to sell their products and ideas—and this is how it's done … OPSEC [Operations Security] needs to catch up with this stuff."[2]

Although day-to-day social media issues fall largely under the OPSEC, Public Affairs, and Information Operations programs, the ATO still needs to be comfortable navigating the social media battlespace. To be sure, the enemy is actively engaged in promoting his efforts in this battlespace, and he is likely exploiting our efforts.

What Is Social Media?

The undisputed king of social media is called the "social networking site," examples of which include Facebook, Twitter, and MySpace. Each individual is essentially a media node, each with an average of 120 friends. These friends have their own friends, so all information shared goes to an audience with yet another audience.[3] Information goes "viral" when these friends share data in a continuous pyramidal sequence.

Other Internet communication tools through which information is freely exchanged at little or no cost to the user include:

- Blogs (e.g., Blogspot, Wordpress, Typepad)
- Podcasts (downloaded from sites such as iTunes)
- Text messaging (i.e., "texting")
- Wikis (e.g., Wikipedia, Wikileaks)
- Virtual worlds (e.g., Secondlife)
- Really Simple Syndication (RSS)
- Image or video sharing (e.g., YouTube, Flickr)
- Internet forums and message boards.[4]

With the constant use of hand-held devices (e.g., iPhone, Android) and the ability to share videos, photos, and text immediately, these Internet tools have become accessible to everyone, at all hours, at almost any location.

Disadvantages of Social Media

The old concern of many leaders from a productivity perspective was that people tended to waste too much time playing on the Internet (e.g., Tetris, Solitaire). This may still be true in some cases; however, one recent study showed that people who surf the Internet for fun at work for a reasonable amount of time (i.e., less than 20 percent of time) tend to be more productive than those who do not.[5]

Of greater concern to commanders and ATOs is social media's impact on critical assets and resources and its potential vulnerabilities. Social media can precipitate the spread of bad information, OPSEC failures, crimes against Service members, terrorist surveillance and exploitation, and a number of cyber security problems.

One of the biggest threats is the potential for the viral spread of bad, false, or misleading information. The "first-liar-wins" rule is a certainty in an age when information is disseminated rapidly and widely. Public affairs officers know that it can take days or weeks to clean up a false information campaign, even if the information began as an honest mistake. To prevent panic during a crisis, commanders need to ensure that they counter the first-liar-wins rule with rapid, relevant information. This requires expertise navigating popular social networking sites such as Facebook and Twitter. Similarly, for commanders seeking feedback in a social media realm, especially during a crisis, there is the potential for minority voices to appear to represent majority concerns, and that can lead to premature command decisions. Napoleon Bonaparte said it best: "Ten people who speak make more noise than ten thousand who are silent."

The ATO still needs to be comfortable navigating the social media battlespace. To be sure, the enemy is actively engaged in promoting his efforts in this battlespace, and he is likely exploiting our efforts.

OPSEC is another fundamental risk with social media usage. Social media sites encourage users to share information and inherently trust the information of others. Once information is uploaded to a site, it is not likely private, depending on the privacy settings of certain sites and third-party access, which tends to change frequently or is confusing to users.[6] Some users have been known to blatantly violate OPSEC. In March 2010, the Israeli Defense Force (IDF) had to cancel a raid after a soldier from an elite artillery unit posted the following information to his friends on Facebook: "On Wednesday, we are cleaning out [the name of the village]—today an arrest operation, tomorrow an arrest operation and then, please God, home by Thursday."[7]

Social media allows terrorists and criminals to conduct detailed surveillance and exploit targets without leaving their homes. The FBI uncovered a scam in 2009 involving the victimization of families of deployed military personnel through social networking sites. Criminals searched for private information on public websites so that they could pretend to be in the military and contact sympathetic grandparents of Service members—and then ask the grandparents for money.[8] In

INFORMATION REVOLUTION. Cell phone users can now break news to a worldwide audience well before traditional media outlets. (US Air Force photo by Tech. Sgt. Manuel J. Martinez/Released)

October 2010, Phoenix, Arizona, police officers issued a security alert when they discovered that a suspect was targeting officers on Facebook by gathering data from photographs and other personal information the officers had posted there.[9] As the IDF is aware, terrorists do the same intelligence gathering: "Enemy intelligence scans the Internet in search of pieces of information about the IDF. [sic] Information that could sabotage operations and endanger our forces."[10] From a cyber-technical perspective, social networking sites also increase the possibility of users accidentally downloading malicious content that could force the web browser to download malware, drain bandwidth, or cause a "denial of service" on the network.[11]

Even if Service members do not use social media, there is often enough information floating around the Internet to supplement pre-attack surveillance.[12] With the permission of a co-worker who does not use social media, I discovered his current command location, the names of his immediate family, and what he had done in previous commands—all in fewer than 30 minutes and with no knowledge of his background—by simply "Googling" his name and then seeing what his friends wrote about him. By aggregating information from multiple sites, one can gain access to everything from birthdates, e-mail addresses, clues to passwords and PINs, and even online banking records.

For the same reasons social media may be a benefit to the free world for information dissemination to wider audiences (e.g., revolutions in Tunisia and Egypt), it is also a helpful tool for terrorist propaganda. Terrorists use it for posting video footage of their successes and to make claims about allied atrocities and war crimes. And after hundreds of blog reposts of al Qaeda's new *Inspire* magazine, homegrown terrorists now have easy access to extremist rhetoric in English with corresponding tactics, techniques, and procedures for killing Americans.

Benefits of Social Media

> "For whether we embrace the fundamental communications changes underway today or not, our talented young workforce not only embraces them, they know nothing else. As leaders, then, it's not enough that we keep pace with these changes—we must lead the change."
>
> —Chief of Naval Operations ADM Gary Roughead[13]

Commanders and ATOs must "lead the change" as we embrace the power, pitfalls, and complexity of social media. For leaders, social media provides an opportunity for unprecedented transparency and feedback, recruitment, and improved morale. In the ATO community, social media's potential for providing real-time threat warning and guidance is invaluable.

The information lag that occurred in the wake of Hurricane Katrina in 2005 is a thing of the past. Just three years later in Mumbai, India, the victims of a combined-arms terrorist attack broke the news to a worldwide audience with mobile phones and by uploading text, videos, and photos on YouTube, Twitter, and Flickr well before traditional media outlets knew what was happening.[14]

This information revolution offers a superb opportunity for improving operational transparency

(OPSEC notwithstanding) to build trust with and provide feedback to the public, especially concerned military families and international partners. A recent example is DOD's response to the tsunami and nuclear crisis in Japan. As the 9.0 earthquake hit and subsequent tsunami warnings were posted, installation commanders went directly to their social networking sites to provide updates. On the Facebook page for "Commander, Naval Forces Japan," leaders were providing real-time "ground truth" on misleading news reports and answering the public's questions within roughly five minutes of a query. Even the Chief of Naval Operations signed up for the page; he remarked, "I was able to look at the Facebook threads and see what questions people had; where there remained areas of confusion and concern and what areas we needed to address."[15] Another example is provided in Figure 1.

Of particular interest to ATOs in the continental United States, the Department of Homeland Security is now using Facebook and Twitter to issue real-time alerts through its new National Terrorism Advisory System. Go to the following websites to sign up:

- Facebook: http://facebook.com/NTASAlerts
- Twitter: http://www.twitter.com/NTASAlerts

There is now no need to wait for alerts to come through traditional media channels.

DOD is embracing social media as a recruiting tool. Arguably, this approach is the best way to connect with 18- to 22-year-olds who are regularly surfing these sites. It also provides an opportunity to encourage these young men and women to ask questions and to provide them with answers in a no-pressure environment. As LTG Benjamin Freakley recently noted, "Since the late '80s, nine percent of the population is propensed toward military service," compared with about a third in the 1970s. Thus, he added, "[W]e have to reach out in forms like [social media] to get them to want to know more, to join us in social media and extend the dialog."[16]

For a broad snapshot of how DOD uses social media, go to DOD's website:

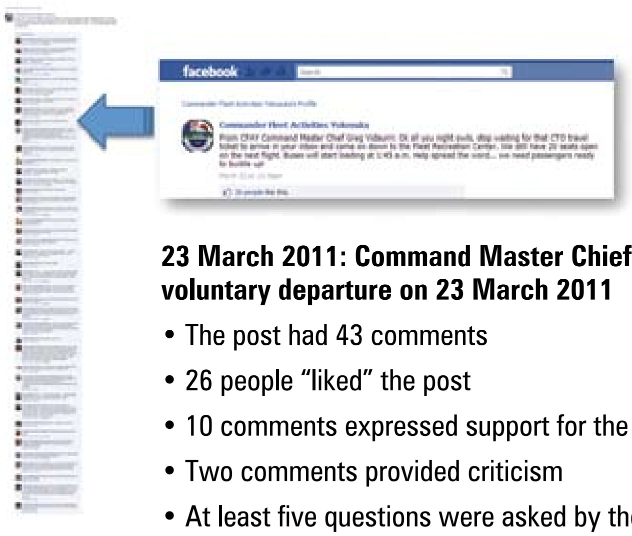
http://www.defense.gov/home/features/2009/0709_socialmedia/

Service-specific policies are also available online:

- Navy: http://www.navy.mil/navydata/internet/secnav5720-47b.pdf
- Army: http://ciog6.army.mil/PolicyLegislation/tabid/64/Default.aspx#webmaster_policies
- Air Force: http://www.af.mil/information/webpolicy/
- Marines: http://www.marines.mil/usmc/Pages/SocialMedia.aspx?pid=dodweb

Fig. 1

Example of Typical Facebook Post During Crisis in Japan



Commander Fleet Activities Yokosuka

From CFAY Command Master Chief Greg Vidaurri: OK all you night owls, stop waiting for that CTO travel ticket to arrive in your inbox and come on down to the Fleet Recreation Center. We still have 20 seats open on the next flight. Buses will start loading at 1:45 a.m. Help spread the word... we need passengers ready to buckle up!

23 March 2011: Command Master Chief at Yokosuka, Japan notes that there were seats available for voluntary departure on 23 March 2011

- The post had 43 comments
- 26 people "liked" the post
- 10 comments expressed support for the command
- Two comments provided criticism
- At least five questions were asked by the public—command responses took 1–19 minutes
- At least three members of the public also responded to public questions, providing additional information
- Of note, the command made 27 other posts that day on a variety of topics

Social Media Best Practices[17]

- Perform a risk assessment before posting information about you or your organization. Never post any sensitive information, and post information as if privacy or filtering settings do not exist within the site's functionality. Sensitive information (e.g., address, phone number) should be left off all social networking sites.
- Carefully consider what you publish on social networks. Before you post photos, videos, or text, ask yourself if it would embarrass you if your family or your employer saw them.
- Before accepting a friend or connection request, confirm with the requestor either verbally or face to face. This ensures that the involved accounts are neither compromised nor impersonated.
- Be selective about which third-party applications you add to your profile. These applications could contain malicious code attempting to exploit your account. In addition, think about whether you want the creators of third-party applications to be able to access your profile page and information about your activity on the social network.
- Report any abuses of a website's terms of use to the website's administrators. Any reputable website or social network will have a way for you to report abuses.
- Pay attention to the address of a website, located at the top of the screen. Malicious websites may look identical to a legitimate site, but the address may use a variation in spelling or a different domain (e.g., ".com" versus ".net").

Finally, social media and access to the Internet improves quality of life for Service men and women who enjoy keeping in touch with friends and family. Social networking is now the primary means for young Service members to communicate while on deployment.

For more information on DOD guidance and policy on the use of social media and other Internet-based capabilities (in an official and unofficial capacity) go to the DOD Social Media Hub (http://www.defense.gov/socialmedia/).

[1] Budzyna, Tom. "Social Media Is Shaping Markets, The Military And Life." Army.mil, 31 August 2010. Available at http://www.briansolis.com/2011/06/this-is-a-time-for-leaders-to-lead-not-react/

[2] Principal Deputy Assistant Secretary of Defense for Public Affairs Price Floyd in John J. Kruzel's article, "Pentagon Weighs Social Networking Benefits, Risks." American Forces Press Service, 4 August 2009. Available at http://www.defense.gov/news/newsarticle.aspx?id=55363

[3] "Social Networks. Primates on Facebook: Even online, the neocortex is the limit." *The Economist*, 26 February 2009. Available at http://www.economist.com/node/13176775

[4] Tinker, Tim L., Grant McLaughlin, & Michael Dumlao. "Risk Communication and Social Media: Tips and best practices for using new tools to communicate effectively." Disaster Resource Guide 2009/2010. Available at http://www.disaster-resource.com/newsletter/2009/subpages/v314/meettheexperts.pdf

[5] "Freedom to surf: workers more productive if allowed to use the Internet for leisure." *University of Melbourne News*, 2 April 2009. Available at http://uninews.unimelb.edu.au/news/5750/

[6] "Social Networking Sites." National Security Agency, Systems and Network Analysis Center Information Assurance Directorate. Available at http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf

[7] Katz, Yaakov. "Facebook Details Cancel IDF Raid." *Jerusalem Post*, 4 March 2010.

[8] "Social Networking Sites Victimizing Families of Deployed US Military Personnel." FBI press release, 24 June 2009. Available at http://www.fbi.gov/kansascity/press-releases/2009/kc062409.htm

[9] Levine, Mike. "Officials Warn Facebook and Twitter Increase Police Vulnerability." FoxNews.com, 10 May 2011.

[10] Katz, supra 7.

[11] This is called "cross-site scripting." More information is available on the National Security Agency's website (http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf).

[12] See JP 3-07.2, Antiterrorism, Chapter V on terrorist use of social networking media for casual questioning and probing.

[13] Chief of Naval Operations ADM Gary Roughead in remarks at the Institute for Public Relations Strategic Communications Summit, 6 June 2011.

[14] Tinker, supra 4.

[15] Chief of Naval Operations, supra 13.

[16] Elliot, Stuart. "Army Seeks Recruits in Social Media." *New York Times*, 24 May 2011. Available at http://www.nytimes.com/2011/05/25/business/media/25adco.html

[17] Includes best practices from the National Security Agency (http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf) and the Department of State (http://exchanges.state.gov/pro-admin/pdfs/safety_english.pdf).

DHS'S NATIONAL TERRORISM ADVISORY SYSTEM

New system provides timely, detailed information about potential threats

The National Terrorism Advisory System replaces the color-coded Homeland Security Advisory System.

> "The terrorist threat facing our country has evolved significantly over the past ten years, and in today's environment—more than ever—we know that the best security strategy is one that counts on the American public as a key partner in securing our country."
>
> —Secretary of Homeland Security Janet Napolitano

The National Terrorism Advisory System (NTAS) replaces the color-coded Homeland Security Advisory System. This new system will communicate information about terrorist threats more effectively by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. The following information comes from the US Department of Homeland Security's website (www.dhs.gov).

NTAS Alerts

After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other federal entities, whether an NTAS Alert should be issued. NTAS Alerts will be issued only when credible information is available.

These alerts will include a clear statement that there is an imminent threat or an elevated threat. Using available information, the alerts will provide a concise summary of the potential threat; information about actions being taken to ensure public safety; and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat.

The NTAS Alerts will be based on the nature of the threat: In some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, whereas other alerts will be issued more broadly to the American people through both official and unofficial media channels.

NTAS Alerts contain a "sunset provision" indicating a specific date when the alert expires; there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert:

- **Imminent Threat Alert** warns of a credible, specific, and impending terrorist threat against the United States.
- **Elevated Threat Alert** warns of a credible terrorist threat against the United States.
- **Sunset Provision** is an individual threat alert that is issued for a specific time period and that automatically expires. It may be extended if new information becomes available or the threat evolves.

The National Terrorism Advisory System (NTAS) replaces the color-coded Homeland Security Advisory System. This new system will communicate information about terrorist threats more effectively by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

NTAS: National Terrorism Advisory System
www.DHS.gov/alerts
Report suspicious activity to local law enforcement or call 9-1-1 in case of emergency.
if you SEE something SAY something™
NTAS
National Terrorism Advisory System
www.DHS.gov/alerts

SPREADING THE WORD. Advertisements for the NTAS encourage the public to be on the alert for suspicious behavior or objects and to alert authorities.

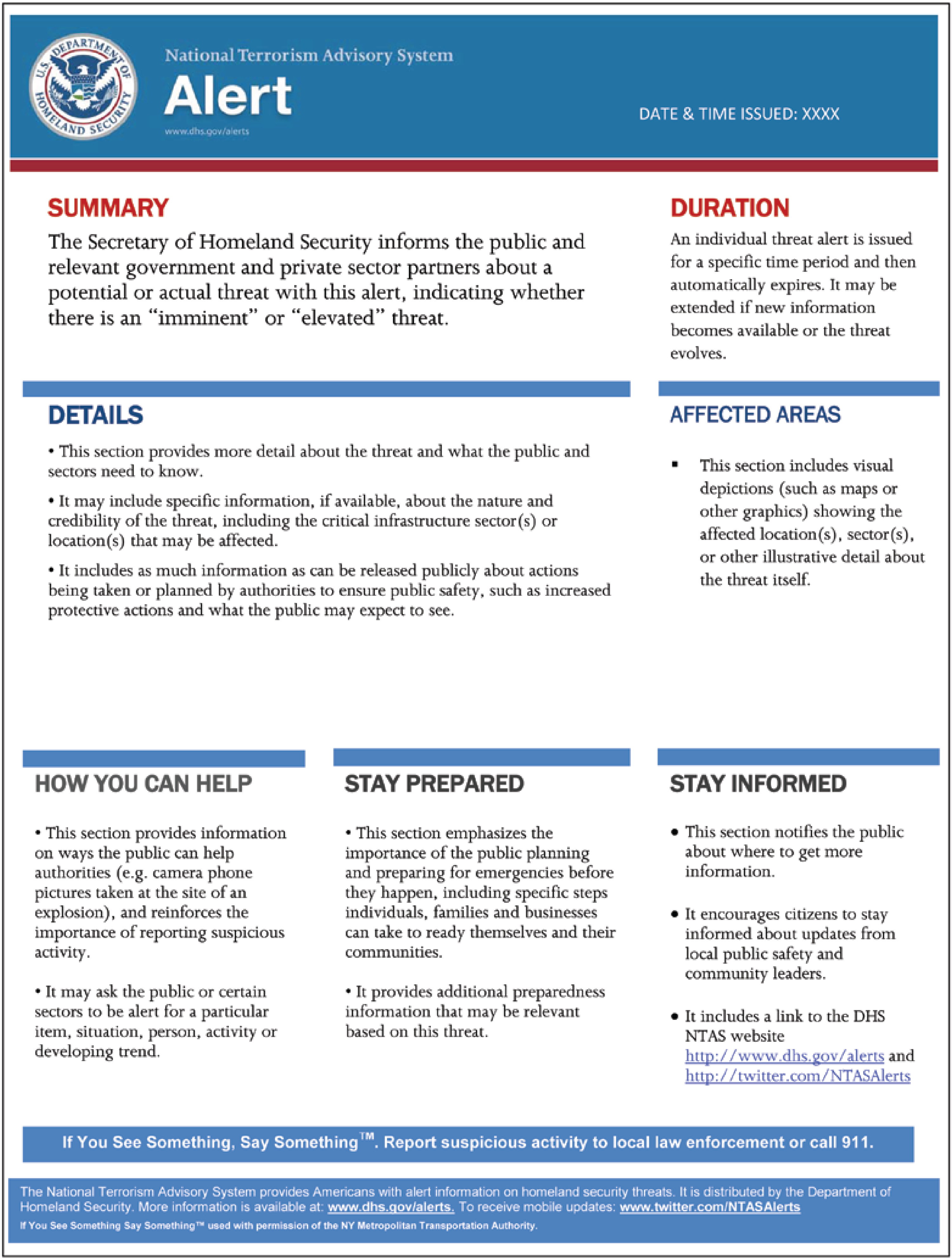
Alert Announcements

NTAS Alerts will be issued through state, local, and tribal partners; the news media; and directly to the public via the following channels:

- Via the official DHS NTAS website: http://www.dhs.gov/files/programs/ntas.shtm
- Via e-mail signup: go to the link above and select "NTAS Alerts via Email" under the heading **Action Center**
- Via social media:
  - Facebook: http://facebook.com/NTASAlerts
  - Twitter: http://www.twitter.com/NTASAlerts
  - Via data feeds, web widgets, and graphics: http://www.dhs.gov/alerts

The public can also expect to see alerts in places, both public and private, such as transit hubs, airports, and government buildings.

A summary of a typical NTAS bulletin is on the facing page.



National Terrorism Advisory System

Alert

www.dhs.gov/alerts

DATE & TIME ISSUED: XXXX

SUMMARY

The Secretary of Homeland Security informs the public and relevant government and private sector partners about a potential or actual threat with this alert, indicating whether there is an "imminent" or "elevated" threat.

DURATION

An individual threat alert is issued for a specific time period and then automatically expires. It may be extended if new information becomes available or the threat evolves.

DETAILS

- This section provides more detail about the threat and what the public and sectors need to know.
- It may include specific information, if available, about the nature and credibility of the threat, including the critical infrastructure sector(s) or location(s) that may be affected.
- It includes as much information as can be released publicly about actions being taken or planned by authorities to ensure public safety, such as increased protective actions and what the public may expect to see.

AFFECTED AREAS

- This section includes visual depictions (such as maps or other graphics) showing the affected location(s), sector(s), or other illustrative detail about the threat itself.

HOW YOU CAN HELP

- This section provides information on ways the public can help authorities (e.g. camera phone pictures taken at the site of an explosion), and reinforces the importance of reporting suspicious activity.

- It may ask the public or certain sectors to be alert for a particular item, situation, person, activity or developing trend.

STAY PREPARED

- This section emphasizes the importance of the public planning and preparing for emergencies before they happen, including specific steps individuals, families and businesses can take to ready themselves and their communities.

- It provides additional preparedness information that may be relevant based on this threat.

STAY INFORMED

- This section notifies the public about where to get more information.

- It encourages citizens to stay informed about updates from local public safety and community leaders.

- It includes a link to the DHS NTAS website http://www.dhs.gov/alerts and http://twitter.com/NTASAlerts

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at: **www.dhs.gov/alerts.** To receive mobile updates: **www.twitter.com/NTASAlerts**

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

UNDERSTANDING THE THREAT

US Marine Corps photo by Cpl. Patricia D. Lockhart/Released

The terrorist threat is continuously evolving and adapting

Office of the Provost Marshal General, Anititerrorism Branch, United States Army

We must leverage the entire Army community to ensure that our forces can prepare for, respond to, and recover from terrorist acts.

Understanding the nature of terrorism and the potential for terrorist threats to have a direct effect on DOD installations, stand-alone facilities, and units is critical to our defense. As such, the Army AT theme for the third quarter of FY 2011 (3QFY11), "Understanding the Threat," focuses on heightened awareness to understand terrorist ideologies, objectives, and tactics as well as Army resources and processes to enhance threat knowledge and information sharing. By enhancing the understanding of the continuously evolving and adapting terrorist threat, the Army, as a community, is better protected from terrorist attack or influence.

Terrorism is an enduring, persistent, and worldwide threat to Army forces. Extremist ideologies and separatist movements continue to have an anti-Western and anti-US orientation that threatens our nation. Moreover, the increased impact of homegrown extremism is disturbing as a growing number of unlikely militants become radicalized and plot attacks at home and abroad. The ease with which people can be influenced by extremist ideologies through online social media sites makes it hard to profile individuals who may be susceptible to radicalized thinking. This factor makes identification of insider threats particularly challenging.

Given the wide range of threats (national and international, internal and external), the entire force must sustain a strong defensive posture to prevent terrorist acts and protect the Army's critical assets (people, critical infrastructure, and sensitive information).

Army-wide focus during the 3QFY11 antiterrorism theme includes the integration of terrorist threat assessment and analysis, and indication and warnings into the operations and intelligence process to ensure that commanders and units at all levels apply specific knowledge and understanding of the threat to enhance their overall protection posture.

Efforts at Army Headquarters (HQDA) that support the 3QFY11 theme include the development and release of AT Information Requirements (IR) in support of the Army Chief of Staff's Priority Intelligence Requirements (PIR). The IR and PIR support the Army's ability to understand the terrorist threat within the process of planning, preparing, collecting, processing, and producing intelligence and related threat information. The department's annual threat assessment initiates a deliberate planning and assessment process in which Army Commanders, Army Service Component Commanders, Direct Reporting Unit Commanders, and the director of the Army National Guard incorporate terrorist threat information into an annual terrorism threat assessment. In turn, this process supports subordinate units, organizations, and installations in preparing their specific threat statements.

In addition, the Army's Antiterrorism Branch partnered with the Deputy Chief of Staff for Intelligence to market iSALUTE, the Counterintelligence Reporting Portal, to enhance community awareness of insider threats, espionage, extremism, and international terrorism.

In February 2011, the Army released the first AT doctrinal manual. The manual, FM 3-37.2, provides guidance on integrating AT into intelligence and operations processes as well as information on terrorist tactics and the terrorist planning cycle. As we continue to improve our AT capabilities, the Office of the Secretary of Defense for Policy recently decided to implement eGuardian as the DOD-wide suspicious activity reporting system, which will enhance reporting, analysis, and information sharing across the joint and interagency law enforcement and intelligence communities.

We must leverage the entire Army community to better understand the terrorist threat we face today and in the future to ensure that our forces and Army communities can prepare, respond, and recover from terrorist acts.

Understand the Threat

Guidance and Focus
Situational Understanding
OPERATIONS PROCESS
ASSESS
PREPARE
ASSESS
EXECUTE
ASSESS
PLAN
INTELLIGENCE PROCESS
PRODUCE
PROCESS
COLLECT
PREPARE
PLAN
Commander's Intent
Continuous Intel Input
ARMY STRONG

ANTITERRORISM WORKING GROUP

Process Integrator

CONFIRM	what you know
IDENTIFY	what you need to know
COLLECT	every Soldier a sensor
ASSESS	indicators of threat activity
DISSEMINATE	information & warnings

Strategic Event Assessment

By LCDR Christopher F. Hill

EVENT: The Arab Spring

Tunisia: In December 2010, thousands of citizens conducted a campaign of civil unrest that led to the overthrow of President Zine El Abidine Ben Ali a month later. From January 2011 to the present, one by one, dictatorships throughout the Middle East and North Africa have been threatened or toppled.

STRATEGIC SIGNIFICANCE:

The ongoing wave of revolutionary fervor in the Middle East and North Africa rivals the 1991 disintegration of the Soviet Union in breadth and intensity. What remains uncertain is the future success of combating-terrorism operations in that region, where the bulk of such operations take place.

Demonstrators in downtown Tunis on 14 January 2011. (VOA Photo/L. Bryant)

Two schools of thought dominate recent analysis of these revolutions and their effect on AT efforts. The first school of thought suggests that the changing political landscape is an ideological and strategic messaging victory for prodemocracy protestors (a notably diverse conglomeration of groups, depending on the country) and a significant blow to al Qaeda's strategic stance, which advocates violent jihad against Arab rulers. It also suggests that a plurality of citizens in the Middle East and North Africa believe that religious values, human rights, democracy, and accountability may be compatible with one another—again, contrary to al Qaeda's extremist philosophy and that of proxy extremist groups.

The second school of thought suggests that toppling dictators and taxing existing security paradigms gives extremist groups, in Anwar Al-Awlaki's words, "a chance to breathe." The expansion of al Qaeda in the Islamic Maghreb, especially in Libya, is of particular concern, despite the fact that Libya's rebel movement continues to deny the involvement of al Qaeda in its activities.[1] In Yemen, where security factions continue their infighting, the United States decided to pull back more than $1 billion in assistance, a good portion of which would have been earmarked for counterterrorism.[2] Certainly, the prospect for counterterrorism operations is uncertain without Yemeni leader Ali Abdullah Saleh in power.[3]

The bottom line is that it is too soon to tell what the future holds for AT efforts. We do not know what will happen to the robust state security apparatuses that existed in Egypt and Tunisia; they may be eliminated, reduced, or forced to operate under stricter controls. At a minimum, they will be distracted. In places where state security services have been challenged but not overthrown (e.g., Jordan or Bahrain), resources and time could be diverted to protecting the regime from political unrest rather than fighting terrorists. In places where terrorism is sponsored by the state (e.g., Syria), regime collapse might seem at first to be beneficial for combating terrorism; however, history shows that periods of great instability can lead to a failing-state scenario (e.g., Somalia) in which security vacuums allow crime and terrorism to fester.

In this period of great uncertainty, the AT Community needs to maintain a watchful eye.

QUOTES:

"Here is a vision for the future—for particularly the Arab Islamic world. It has nothing to do with al Qaeda's vision for the future. It's not some view of [pure] religion descending upon man and directing all actions. It's empowerment from people, through popular choice and plurality."

— Michael Hayden, former director of the Central Intelligence Agency, 23 February 2011, http://politics.blogs.foxnews.com/2011/02/23/middle-east-unrest-could-be-net-positive-us-counterterrorism-efforts-former-cia-chief-say#

"This is what your brothers in the al Qaeda Organization and other jihadi organizations have been working for: inspiring the people all over the world to rise up for the Islamic cause of eliminating the tyrants so that we have a clear shot at Israel."

— Abu Suhail, *Inspire* magazine, Spring 2011

"Whatever the outcome is, our mujahidin brothers in Tunisia, Egypt, Libya and the rest of the Muslim world will get a chance to breathe again after three decades of suffocation."

— Anwar Al-Awlaki, *Inspire* magazine, Spring 2011

"Whatever the outcome of these revolts they will not be to al Qaeda's satisfaction because almost no one in the streets of Cairo, Egypt, Benghazi, Libya, or San'a, Yemen, is clamoring for the imposition of a Taliban-style theocracy, al Qaeda's desired end state in the Middle East."

— Peter Bergen, "Al Qaeda Responds to CNN," CNN.com, 31 March 2011

[1] Lebovich, Andrew. "The LWOT: Middle East unrest tops counterterrorism agenda; Media wary of covering 9/11 Gitmo trial." Foreign Policy, 8 April 2011. Available at: http://www.foreignpolicy.com/articles/2011/04/08/the_lwot_middle_east_unrest_tops_counterterrorism_agenda_media_wary_of_covering_

[2] Johnson, Keith, Adam Entous, & Margaret Coker. "US Halted Record Aid Deal as Yemen Rose Up." *Wall Street Journal*, 8 April 2011. Available at: http://online.wsj.com/article/SB10001424052748704101604576249204208045910.html

[3] Finn, Peter, & Greg Miller. "Yemen's Future After Saleh Worries US Officials." *Washington Post*, 5 June 2011.

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.